UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SITEMAS COMPUTACIONALES E INFORMATICOS

SEMINARIO DE GRADUACION

"SEGURIDAD INFORMATICA"

Tema:

"IMPLANTACIÓN DE UNA HONEYNET PARA LA OPTIMIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS SERVIDORES DE LA UNIVERSIDAD TÉCNICA DE AMBATO".

Proyecto de Trabajo de Graduación. Modalidad: Seminario, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: Mauro Darío Jijón Ramos

TUTOR: Ing. Luis Solís

Ambato - Ecuador

Septiembre-2013

APROBACIÓN DEL TUTOR

En mi calidad de tutor el trabajo de investigación sobre el tema: "IMPLANTACIÓN DE UNA HONEYNET PARA LA OPTIMIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS SERVIDORES DE LA UNIVERSIDAD TÉCNICA DE AMBATO.", del señor Mauro Darío Jijón Ramos, estudiante de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales, de la Facultad de Ingeniería en Sistemas, Electrónica E Industrial, de la Universidad Técnica de Ambato, considero que el informe investigado reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Septiembre 2013

_____

Ing. Luis Solís

AUTORÍA

El presente trabajo de investigación titulado "IMPLANTACIÓN DE UNA HONEYNET PARA LA OPTIMIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS SERVIDORES DE LA UNIVERSIDAD TÉCNICA DE AMBATO". Es absolutamente original, autentico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Septiembre 2013

_____

Mauro Darío Jijón Ramos

C.I.:1804151775

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes revisó y aprobó el Informe Final del trabajo de graduación titulado "IMPLANTACIÓN DE UNA HONEYNET PARA LA OPTIMIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS SERVIDORES DE LA UNIVERSIDAD TÉCNICA DE AMBATO", presentado por el señor Mauro Darío Jijón Ramos de acuerdo al Art 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

_____

Ing. Mg. Edison Álvarez Mayorga

PRESIDENTE H. CONSEJO DIRECTIVO

_____ _____

Ing. David Guevara

DOCENTE CALIFICADOR

Ing. Clay Aldás

DOCENTE CALIFICADOR

ÍNDICE

APROBACIÓN DEL TUTOR ..... **II**
AUTORÍA ..... **III**
APROBACIÓN DE LA COMISIÓN CALIFICADORA ..... **IV**
ÍNDICE DE TABLAS ..... **VIII**
ÍNDICE DE GRÁFICOS ..... **X**
RESUMEN EJECUTIVO ..... **XV**
CAPÍTULO I **1**

EL PROBLEMA **1**

1.1 TEMA 1
1.2 PLANTEAMIENTO DEL PROBLEMA 1
1.2.1 CONTEXTUALIZACIÓN 1
1.2.2 ANÁLISIS CRÍTICO 3
1.2.3 PROGNOSIS 4
1.2.4 FORMULACIÓN DEL PROBLEMA 5
1.2.5 PREGUNTAS DIRECTRICES 5
1.2.6 DELIMITACIÓN DEL PROBLEMA 6
1.3 JUSTIFICACIÓN 6
1.4 OBJETIVOS 7
1.4.1 GENERAL 7
1.4.2 ESPECÍFICOS 7

CAPÍTULO II **8**

MARCO TEÓRICO **8**

2.1 ANTECEDENTES INVESTIGATIVOS: 8
2.2 FUNDAMENTACIÓN LEGAL 9
2.3 CATEGORÍAS FUNDAMENTALES 14
2.4.1. FUNDAMENTACIÓN TEÓRICA VARIABLE INDEPENDIENTE 16
2.4.2 LOS TIPOS DE CONTROLES DE SEGURIDAD 16
2.4.3 PLANIFICACIÓN DE LA SEGURIDAD: 18
2.4.4 CREACIÓN DE UN PLAN DE RESPUESTA A INCIDENTES 19
2.4.5 FASES PLAN DE RESPUESTA A INCIDENTES 20
2.4.6 ATAQUES A SERVIDORES 21
2.4.7 SEGURIDAD INFORMÁTICA 22

2.4.8 VPN 23
2.4.9 Firewall 24
2.4.9 ACL'S (Access Control List) 25
2.4.10 Informática 26
2.4.11 Sistema Operativo 26
2.4.12 Seguridad Informática 27
2.4.13 Hacking 28
2.4.14 Ataque Informático 30
2.4.15 Ataque distribuido de denegación de servicio 31
2.5 Hipótesis 32
2.6 Señalamiento de Variables 33

CAPÍTULO III 34

MARCO METODOLÓGICO 34

3.1 Enfoque 34
3.2 Modalidades básicas de la investigación 34
3.3 Tipos de Investigación 35
3.4 Población y Muestra 35
3.5 Recolección y análisis de la información 36
3.6 Procesamiento y análisis 38

CAPÍTULO IV 40

ANALISIS E INTERPRETACION DE LOS RESULTADOS 40

4.1 Análisis de la necesidad 40
4.2 Análisis de los resultados 41
4.3 Controles de Seguridad dentro de los ordenadores 57
4.3.1 Resumen de Vulnerabilidades 58
4.3.2 Patrones de ataque 59
4.3.3 Afectación a la seguridad informática 60

CAPÍTULO V 62

CONCLUSIONES Y RECOMENDACIONES 62

5.1 Conclusiones 62
5.2 Recomendaciones 63

CAPÍTULO VI 64

PROPUESTA 64

6.1 Tema 64
6.2 Datos informativos 64
6.3 Antecedentes 65
6.4 Justificación 65

6.5 OBJETIVOS 66
6.5.1 GENERAL 66
6.5.2 ESPECÍFICOS 66
6.6 FACTIBILIDAD 66
6.7 FUNDAMENTACIÓN CIENTÍFICO TÉCNICA 67
6.8 IMPLANTACIÓN HONEYNET 78
6.8.1 FASE DE PLANIFICACIÓN 78
6.8.1.1 UBICACIÓN HONEYNET 78
6.8.1.2 ANÁLISIS DE RECURSOS Y COMPONENTES 79
6.8.1.3 FASE DE DISEÑO 79
6.8.1.4 FASE DE IMPLEMENTACIÓN 81
6.8.1.5 DISEÑO HONEYNET 81
6.8.1.6 DETALLES TÉCNICOS 83
6.8.1.7 INSTALACIÓN DE VIRTUALBOX PARA WINDOWS 85
6.8.1.8 INSTALACIÓN SERVIDOR CENTOS 87
6.8.1.9 INSTALANDO SNORT 91
6.9 CONFIGURANDO SNORT 93
6.9.1 DESCARGANDO LAS ÚLTIMAS REGLAS DE SEGURIDAD PARA SNORT 93
6.9.2 BASE DE DATOS MYSQL 100
6.9.3 SNORT REPORT 102
6.9.4 INSTALACIÓN DE BARNYARD 103
6.10 INICIALIZANDO SNORT Y BARNYARD 106
6.10.1 INICIANDO SNORT 107
6.10.2 INICIANDO BARNYARD 107
6.10.3 PROBANDO EL FUNCIONAMIENTO DE SNORT 109
6.11 INICIANDO SNORT AUTOMÁTICAMENTE 111
6.12 INICIANDO BARNYARD AUTOMÁTICAMENTE 112
6.12.1 INSTALANDO BARNYARD COMO SERVICIO 114
6.13 IDS DE HOST OSSEC 115
6.13.1 INSTALANDO SERVIDOR OSSEC EN CENTOS 116
6.13.2 INSTALANDO INTERFAZ WEB DE OSSEC 121
6.14 INSTALACIÓN HONEYPOT WINDOWS 123
6.14.1 INSTALANDO AGENTE OSSEC EN WINDOWS XP 123
6.15 INSTALACIÓN HONEYPOT UBUNTU 129
6.15.1 INSTALANDO AGENTE OSSEC EN UBUNTU 129
6.16 FUNCIONAMIENTO HONEYNET 131
6.16.1 INICIANDO SERVICIOS EN SERVIDOR 131
6.16.2 INICIANDO SERVICIOS EN CLIENTES 132
6.16.2.1 PARA EL CLIENTE WINDOWS: 132
6.16.2.2 PARA EL CLIENTE UBUNTU: 132
6.17 ASEGURANDO DIRECTORIOS DE OSSEC Y DE SNORT 133
6.18 METODOLOGÍA DE LAS CAPTURAS EN LA HONEYNET 136

6.19 METODOLOGÍA DEL ANÁLISIS FORENSE DENTRO DE LA HONEYNET 136
6.20 CAPTURAS Y ANÁLISIS FORENSE EN HONEYNET 137
6.20.1 CAPTURAS DE DICIEMBRE 137
6.20.1.1 INTRUSIÓN 1 - PASSWORD GUESSING 137
6.20.1.2 ANÁLISIS FORENSE INTRUSIÓN 1 142
6.20.1.3 RESUMEN DEL ATAQUE 146
6.20.2 CAPTURAS DE ENERO 147
6.20.2.1 INTRUSIÓN 2 – ATAQUE DDOS 147
6.20.2.2 ANÁLISIS FORENSE INTRUSIÓN 2 148
6.20.2.3 RESUMEN DEL ATAQUE 151
6.20.3 CAPTURAS DE FEBRERO 152
6.20.3.1 INTRUSIÓN 3 - VIRUS POLIMÓRFICO 152
6.21 POLÍTICAS DE SEGURIDAD A SEGUIR PARA LA OPTIMIZACIÓN DE LA SEGURIDAD INFORMÁTICA. 160
6.21.1 INTRUSIÓN 1.- PASSWORD GUESSING 161
6.21.1.1 PARA WINDOWS 161
6.21.1.2 PARA LINUX 173
6.21.2 INTRUSIÓN 2.- ATAQUE DDOS 176
6.21.2.1 PARA WINDOWS 176
6.21.2.2 PARA LINUX 179
6.21.3 INTRUSIÓN 3.- VIRUS POLIMÓRFICO 182
6.21.3.1 PRECAUCIONES EN WINDOWS PARA EVITAR LA INFECCIÓN DE VIRUS . 182
6.21.3.2 MEDIDAS PREVENTIVAS PARA LINUX 185
6.22 IMPLANTACIÓN DE HONEYNET EN OFICINAS DEL DISIR 186
6.23 CONCLUSIONES Y RECOMENDACIONES 187
6.23.1 CONCLUSIONES 187
6.23.2 RECOMENDACIONES 189
6.24 GLOSARIO DE TÉRMINOS 189
6.25 BIBLIOGRAFÍA: 206
ANEXO 1 209
ANEXO 2 210
ANEXO 3 218
ANEXO 4 220
ANEXO 5 221
ANEXO 6 222
ANEXO 7 231

Índice de tablas

Tabla 4.1 Resultados campo mensaje de la ficha de observación..... 42

Tabla 4.2 Resultados campo resumen de la ficha de observación 43
Tabla 4.3 Resultados campo impacto de la ficha de observación..... 45
Tabla 4.4 Resultados campo información detallada de la ficha de observación... 47
Tabla 4.5 Resultados campo sistemas afectados de la ficha de observación 49
Tabla 4.6 Resultados campo escenarios de ataque de la ficha de observación..... 50
Tabla 4.7 Resultados campo falsos positivos de la ficha de observación..... 52
Tabla 4.8 Resultados campo falsos negativos de la ficha de observación 54
Tabla 4.9 Resultados campo acción correctiva de la ficha de observación 56
Tabla 4.10 Controles de Seguridad 58
Tabla 4.11 Resumen de Vulnerabilidades..... 59
Tabla 6.1 Detalles técnicos ordenador principal 83
Tabla 6.2 Detalles técnicos máquinas virtuales 84
Tabla 6.3 Parámetros de Snort 99
Tabla 6.4 Resumen del ataque del mes de diciembre 146
Tabla 6.5 Resumen del ataque del mes de enero 152
Tabla 6.6 Resumen del ataque del mes de febrero..... 160
Tabla 6.7 Valores recomendados para almacenar contraseñas 165
Tabla 6.8 Valores recomendados el historial de contraseñas..... 166
Tabla 6.9 Valores recomendados para requerimientos de complejidad de la contraseña..... 167
Tabla 6.10 Valores recomendados para la longitud mínima de la contraseña 167
Tabla 6.11 Valores recomendados para la vigencia máxima de la contraseña ... 168
Tabla 6.12 Valores recomendados para la vigencia mínima de la contraseña.... 169
Tabla 6.13 Valores recomendados para la duración del bloqueo de cuenta 171

Tabla 6.14 Valores recomendados para la restitución de la contraseña..... 172

Tabla 6.15 Valores recomendados para el umbral de bloqueos de la cuenta..... 172

Tabla 6.16 Detalles técnicos ordenador destino Honeynet 187

Índice de Gráficos

Gráfico 1.1 Árbol del Problema 3

Gráfico 2.1 Categorías Fundamentales 14

Gráfico 2.2. Categorización de la variable Dependiente..... 15

Gráfico 2.3. Categorización de la variable independiente 15

Gráfico 2.4. Tipos de controles de seguridad..... 18

GRÁFICO 2.5. RED VPN 23

Gráfico 2.6. Acceso a una VPN 24

Gráfico 4.1. Resultado campo mensaje de la ficha de observación 42

Gráfico 4.2. Resultado campo resumen de la ficha de observación..... 44

Gráfico 4.3. Resultado campo impacto de la ficha de observación 46

Gráfico 4.4. Resultado campo información detallada de la ficha de observación 47

Gráfico 4.5. Resultado campo sistemas afectados de la ficha de observación 49

Gráfico 4.6 Resultado campo escenarios de ataque de la ficha de observación ... 51

Gráfico 4.7 Resultado campo falsos positivos de la ficha de observación 53

Gráfico 4.9. Resultado campo acción correctiva de la ficha de observación..... 56

Gráfico 6.1 Tráfico de un servidor con ataque DDOS..... 77

Gráfico 6.2 Servidor Centos..... 82

Gráfico 6.3 Cliente Ubuntu 82

Gráfico 6.4 Cliente Windows..... 83

Gráfico 6.5 Sitio web de VirtualBox..... 85
Gráfico 6.6 Instalación de VirtualBox 85
Gráfico 6.7 Virtualbox agregando un nuevo dispositivo de red 86
Gráfico 6.8 Instalación de nuevo dispositivo de red..... 86
Gráfico 6.9 Interfaz de VirtualBox 87
Gráfico 6.10 Servidor PHP levantado..... 89
Gráfico 6.11 Sitio web de Snort..... 94
Gráfico 6.12 Creación de cuenta en sitio web de Snort 94
Gráfico 6.13 Inicio de sesión 95
Gráfico 6.14 Reglas de Snort 95
Gráfico 6.15 Descarga de ultimas reglas de Snort 96
Gráfico 6.16 Creación de la base de datos Snort 101
Gráfico 6.17 Sitio Web de Snort Report..... 102
Gráfico 6.18 Sitio Web de Barnyard..... 104
Gráfico 6.19 Archivo de configuración de Barnyard..... 105
Gráfico 6.20 Honeynet iniciando el software Ossec en Servidor (Izquierda) y Clientes (Derecha)..... 106
Gráfico 6.21 Iniciando servicio Snort en servidor Centos 107
Gráfico 6.22 Iniciando servicio Barnyard..... 108
Gráfico 6.23 Regla de prueba para Snort 109
Gráfico 6.24 Comprobando el funcionamiento de Snort Report 110
Gráfico 6.25 Comprobando el funcionamiento de Snort 112
Gráfico 6.26 Configurando Barnyard para inicio automático..... 113
Gráfico 6.27 Iniciando servicio Barnyard..... 115

Gráfico 6.28 Instalación de OSSEC 117
Gráfico 6.29 Instalación de OSSEC como servidor 117
Gráfico 6.30 Instalación de OSSEC como servidor 118
Gráfico 6.31 Opciones de instalación del servidor OSSEC 119
Gráfico 6.32 Instalación completa de OSSEC 120
Gráfico 6.33 Comandos para monitorear OSSEC 120
Gráfico 6.34 Instalación interfaz web de OSSEC 122
Gráfico 6.35 Interfaz web de OSSEC 123
Gráfico 6.36 Obtención de clave de autentificación desde el cliente Windows . 124
Gráfico 6.37 Agregando cliente Windows a OSSEC 125
Gráfico 6.38 Obteniendo llave de autenticación para cliente Windows XP 125
Gráfico 6.39 Ingreso de llave de autenticación para cliente Windows XP 126
Gráfico 6.40 Logs de OSSEC en Windows XP 127
Gráfico 6.41 Reinicio de servicio OSSEC 127
Gráfico 6.42 Logs OSSEC 128
Gráfico 6.43 Reiniciando OSSEC en el servidor 128
Gráfico 6.44 Clientes de OSSEC 129
Gráfico 6.45 Instalación de OSSEC en cliente Ubuntu 130
Gráfico 6.46 Instalación de OSSEC en cliente Ubuntu 130
Gráfico 6.47 Iniciando Snort & Barnyard en servidor 131
Gráfico 6.48 Iniciando OSSEC en cliente Windows XP 132
Gráfico 6.49 Iniciando OSSEC en cliente Ubuntu 132
Gráfico 6.51 Creación de usuarios para acceso a directorios de Ossec y Snort .. 134
Gráfico 6.52 Comprobando el acceso a directorio protegido de Ossec 135

Gráfico 6.53 Comprobando el acceso a directorio protegido de Snort 136
Gráfico 6.54 Alertas de OSSEC 138
Gráfico 6.55 Alertas de OSSEC 141
Gráfico 6.56 Logs de Ubuntu 145
Gráfico 6.57 Últimos usuarios logueados de cliente Ubuntu (Inicio de sesión satisfactoria) 145
Gráfico 6.58 Logs de Snort 147
Gráfico 6.59 Logs de OSSEC 148
Gráfico 6.60 Logs del servidor 149
Gráfico 6.61Logs del servidor 150
Gráfico 6.62 Logs de OSSEC (checksum cambiando) 153
Gráfico 6.63 Ventana “cmd” en cliente Windows XP 155
Gráfico 6.64 Propiedades archivo cmd 155
Gráfico 6.65 Propiedades archivo cmd infectado 156
Gráfico 6.66 Propiedades archivo cmd infectado 157
Gráfico 6.67 Análisis de archivo infectado en sitio virus total 158
Gráfico 6.68 Resultados positivos Análisis de archivo infectado 158
Gráfico 6.69 Información extra acerca de virus detectado 159
Gráfico 6.70 Herramientas Administrativas 162
Gráfico 6.71 Directiva de Seguridad local 162
Gráfico 6.73 Directivas de Contraseñas 163
Gráfico 6.74 Directivas de Bloqueo de Cuentas 170
Gráfico 6.75 Archivo shadow de cliente Ubuntu 173
Gráfico 6.76 Directivas de cuenta 174

Gráfico 6.78 IP tables..... 181

Gráfico 6.79 Máquinas virtuales de Honeynet listas para moverse a ordenador destino 186

RESUMEN EJECUTIVO

El tema del presente trabajo investigativo es Implantación de una Honeynet para la optimización de la seguridad de la información en los servidores de la Universidad Técnica de Ambato.

Los datos que circulan a través de los servidores y las redes de la Universidad Técnica de Ambato representan un papel muy importante para la institución ya que contiene información esencial tanto de docentes, alumnos como también información sensible como las calificaciones de alumnos o datos personales de docentes los cuales podrían estar expuestos a ser capturados, vistos, incluso cambiados por usuarios no deseados.

La Universidad Técnica de Ambato en la actualidad mantiene la mayor parte de la información de docentes y estudiantes en forma digital como por ejemplo en el UTAMATICO (http://estudiantes.uta.edu.ec/estudiantes/) en el que se almacenan las notas de todos los estudiantes, lo cual hace que todas las máquinas en especial los servidores sean víctimas potenciales de ataques con el objetivo de acceder y modificar todos estos datos privados, con este trabajo se pretende dar a conocer los principales puntos por los cuales se podría intentar acceder de forma ilícita a la información con el uso de una Honeynet (Red de sistemas destinada a ser comprometida por usuarios maliciosos).

A continuación se presenta el resumen por capítulos de toda la investigación realizada.

Capítulo I: denominado “EL PROBLEMA”, se identifica el problema a investigar, se plantea la justificación y los objetivos.

Capítulo II: denominado “MARCO TEÓRICO”, se presentan los antecedentes investigativos, la fundamentación legal, hipótesis y el señalamiento de las variables.

Capítulo III: denominado “METODOLOGÍA”, se determina la metodología de investigación a utilizar, el enfoque, la modalidad básica de la investigación, el tipo de investigación, la población y muestra.

Capítulo IV: denominado “ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS”, comprende el análisis e interpretación de resultados.

Capítulo V: denominado “CONCLUSIONES Y RECOMENDACIONES”, se presenta las conclusiones y recomendaciones en base los resultados obtenidos en la entrevista realizada al personal encargado del departamento de sistemas.

Capítulo VI: denominado “PROPUESTA”, se presenta el desarrollo de la propuesta ante el problema planteado.

Anexos: contiene la ficha de observación utilizada para este trabajo y el croquis de la Universidad Técnica de Ambato.

CAPÍTULO I

EL PROBLEMA

1.1 Tema

Implantación de una Honeynet para la optimización de la seguridad de la información en los servidores de la Universidad Técnica de Ambato.

1.2 Planteamiento del Problema

1.2.1 Contextualización

En la actualidad las organizaciones disponen de información importante en sus sitios web o alojados en sus servidores, así que deben tener una infraestructura de red lo suficientemente robusta para evitar posibles ataques en sus sistemas de información; hoy en día con la facilidad de acceso a Internet desde cualquier parte del mundo y muchos de los casos en forma anónima, los servidores pueden ser vulnerados y posteriormente atacados, tomando mucho tiempo en detectar el origen del ataque o en muchos de los casos ni siquiera notarlo; una cantidad de usuarios, administradores o proveedores de servicios de Internet carecen de conocimiento de debilidades o vulnerabilidades a las cuales está expuesta su información.

Para poseer una red de datos libre de intrusos deben tener en cuenta lo que deben proteger (para este caso los servidores de datos) y a quien dar acceso, para esto se definen políticas de seguridad; hay que tener en cuenta que las vulnerabilidades pueden darse tanto en el hardware como en el software.

En el Ecuador se han implementado Honeypots para proteger redes de datos como en el proyecto realizado por la Escuela Superior Politécnica Del Litoral en el año 2009 con el título "Diseño Preliminar De Una Honeynet Para Estudiar Patrones De Ataques En Las Redes De Datos De La Espol", o como el proyecto realizado en la Universidad Técnica Del Norte en el año 2013 de título "Honeynet virtual híbrida en el entorno de red de la Universidad Técnica del Norte de la ciudad de Ibarra" con lo cual hasta la actualidad se han logrado detectar varios tipos de ataques a sus servidores, manteniendo segura su información.

Muchas instituciones alojan información importante en sus servidores para la facilidad de acceso por parte de sus usuarios, pero al estar esta información en servidores que en muchos de los casos podrían están mal configurados en lo que tiene que ver con permisos de acceso y de usuarios, podría ocasionar que esta información no solo pueda ser accedida por personas no deseadas sino que también pueda ser modificada o borrada completamente causando graves imprevistos, todo esto se produce por falta de políticas de seguridad para la configuración de redes, computadores, clientes, servidores, facilitando así el acceso a intrusos.

La Universidad Técnica de Ambato en su condición de Universidad con categoría A, acoge mucha información en sus servidores con lo cual en el caso de que sea

parte de un ataque informático, toda la información, por ejemplo: registros de estudiantes, presupuestos y otros podrían ser accesibles para un intruso en esta red, asimismo estos registros pueden ser cambiados sin notarse, causando serios problemas.

La Universidad Técnica de Ambato, según la entrevista realizada a los administradores de red **(Ver Anexo 4)** en su red tiene sistemas de protección para evitar intrusos como Iptables. Vlans, Firewalls, el principal problema que se da con ellos es que al poder estar mal configurados dan la impresión de que la información está segura.

1.2.2 Análisis Crítico

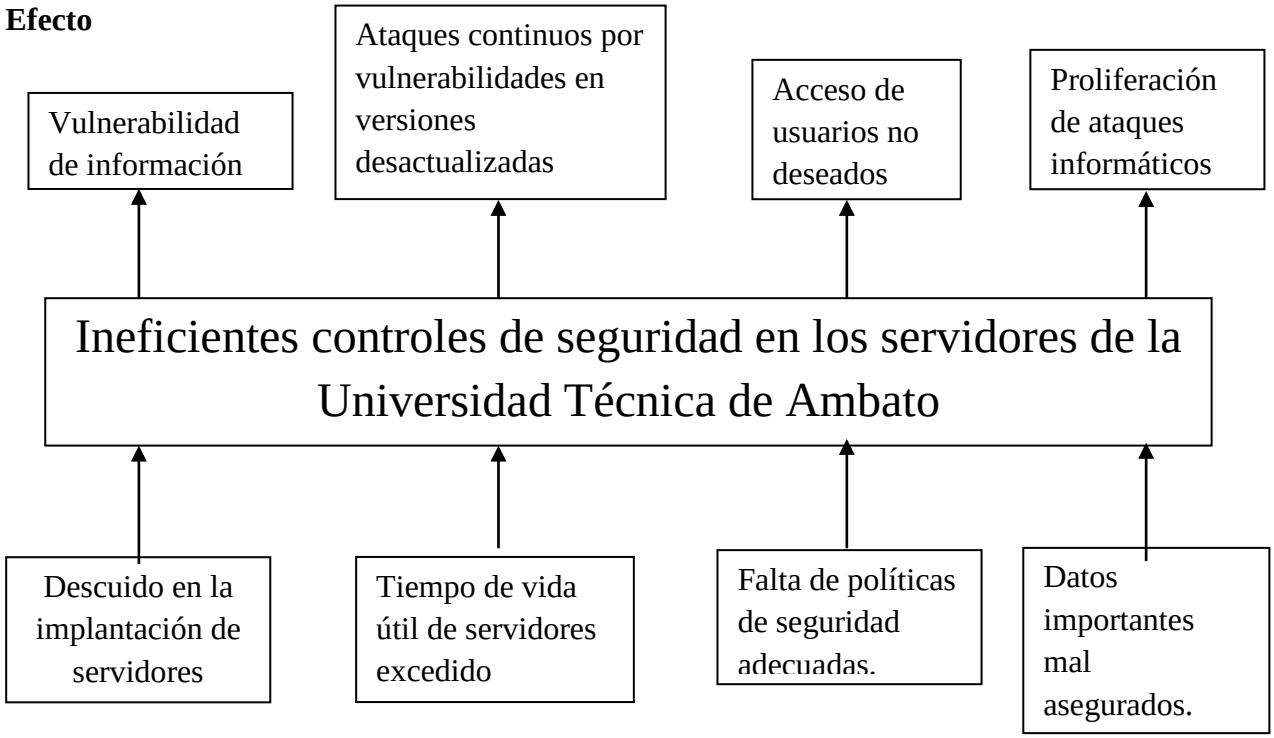


Gráfico 1.1 Árbol del Problema

Elaborado por: Mauro Jijón

Fuente: Investigación Directa/Entrevista

En la Universidad Técnica de Ambato al existir un descuido en la implantación de los servidores de datos, el dejar valores de configuración por defecto, servicios innecesarios para ese servidor ejecutándose o no quitar usuarios predefinidos (el usuario invitado por ejemplo), ocasiona que la información este vulnerable ya que cualquier persona puede intentar acceder con los usuarios y contraseñas por defecto sin necesariamente atacar al servidor de datos.

Los servidores que en la actualidad existen han excedido su tiempo de vida útil, según los resultados de la entrevista los servidores de la Universidad Técnica de Ambato**(Ver Anexo 4)** que están ubicados en las oficinas del DISIR tienen alrededor de 9 años, siendo el tiempo de vida útil de un servidor de 5 años; lo que hace que los atacantes busquen vulnerabilidades que no se hayan actualizado dentro de estos servidores por razones de compatibilidad, obteniendo acceso ilícito, y en muchos de los casos causando problemas irremediables.

No tener políticas de seguridad adecuadas se está permitiendo el acceso no autorizado a usuarios, sin ni siquiera notarlo, ocasionando que la información quede accesible a cualquier persona o grupo de personas.

La falta de seguridad en los datos y sobre todo al estar estos datos en un servidor que se encuentra accesible desde cualquier lugar de la red se está expuesto a un inminente ataque informático el cual puede causar desde la alteración de los archivos hasta un borrado completo de ellos.

1.2.3 Prognosis

De continuar la situación planteada y en caso de no tomarse medidas para optimizar la seguridad en los servidores de datos de la Universidad Técnica de

Ambato estos estarán completamente vulnerables a un ataque informático de gran proporción debido a que estos servidores no tienen las debidas seguridades que protejan la información tanto de docentes como de alumnos, siendo así un blanco deseado para ataques del cual tardaría mucho tiempo en encontrar su origen y corregirse.

La información que contienen los servidores de la Universidad Técnica de Ambato es de suma importancia y al perderse la Universidad quedaría completamente sin información acerca de docentes y estudiantes poniendo en riesgo su reputación.

1.2.4 Formulación del problema

¿Cómo influyen los controles de información en los ataques informáticos a los servidores de la Universidad Técnica de Ambato?

1.2.5 Preguntas Directrices

¿Qué tipo de controles se aplican actualmente para mantener la seguridad de la información de los servidores de la Universidad Técnica de Ambato?

¿Qué tipo de información es atacada en los servidores de la Universidad Técnica de Ambato?

¿A qué tipo de ataques informáticos están expuestos los servidores de la Universidad Técnica de Ambato?

¿Cómo una Honeynet ayuda a detectar vulnerabilidades en la Universidad Técnica de Ambato?

1.2.6 Delimitación del problema

Campo: Seguridad Informática

Área: Sistemas computacionales e Informáticos

Aspecto: Implantación de una Honeynet para la optimización de la seguridad de la información en los servidores de la Universidad Técnica de Ambato.

Tiempo: 6 meses

Lugar: Ambato, Dirección de Sistemas Informáticos y Redes de Comunicación (Universidad Técnica de Ambato)

1.3 Justificación

Los Honeypots y Honeynets presentan una mejor alternativa al problema planteado. Un Honeypot es un recurso más de la red destinado a ser atacado. Una Honeynet es un tipo de Honeypot de alta interacción, destinado a capturar información extensa sobre ataques, con sistemas, aplicaciones y servicios reales a ser comprometidos (los cuales no se encuentran realmente en funcionamiento).

La necesidad de desarrollar el presente proyecto es identificar, evitar y, en cierta medida, neutralizar los intentos de apropiarse de sistemas y redes de información. Siendo un proyecto de investigación aplicada, requiere crear toda la documentación que permitirá el buen entendimiento del desarrollo del mismo.

Con las herramientas utilizadas en este proyecto y que actualmente existen se puede realizar un desarrollo completo e integral, a costos medios. Por los motivos mencionados se hace imprescindible en la actualidad crear una herramienta que

permita reducir la atracción de los diferentes atacantes a los sistemas y redes de información.

Las cantidades de datos que se recolectan diariamente de la actividad hacia los Honeypots y Honeynets son relativamente bajas en comparación con otros sistemas de monitoreo. Sin embargo esta pequeña cantidad de datos es de gran valor, debido a que toda la actividad capturada puede ser un escaneo, una prueba o un ataque, reduciendo así los tiempos de detección y de análisis de la actividad maliciosa en la red; el uso de una tecnología llamada Honeypots permite conocer con detalle los ataques y vulnerabilidades de las redes.

1.4 Objetivos

1.4.1 General

Determinar los controles de seguridad de la información dentro de la Universidad Técnica de Ambato y su relación con los ataques informáticos.

1.4.2 Específicos

- Determinar vulnerabilidades de los actuales controles de seguridad de la información dentro de los ordenadores de la Universidad Técnica de Ambato.
- Analizar los patrones de ataques informáticos y su afectación a la seguridad informática dentro de la Universidad Técnica de Ambato.
- Plantear una propuesta que permita desarrollar una Honeynet que optimice la seguridad informática en la Universidad Técnica de Ambato.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos:

En el repositorio de la biblioteca de la Universidad Técnica de Ambato existe una tesis similar con el título: “Estudio, Administración e Implementación de Políticas de Seguridad en la Red Informática del Hospital Millennium de la ciudad de Ambato.”, que fue desarrollada por: Franklin Geovanny Flores Saltos en el año 2007, con las siguientes conclusiones:

- Con el mejoramiento de las técnicas de seguridad informática, los datos sensibles o importantes de la Institución están protegidos contra algún posible intento de robo de información.
- La implementación de políticas de seguridad informática, facilitan la administración de red, así como reducen errores de los usuarios por mal manejo en los computadores.
- Con la realización de copias de seguridad periódicas de datos importantes, se asegura la recuperación total o en su mayoría de la información respaldada, en caso de producirse daño o pérdida de un computador.

- La implementación de Kaspersky Anti-Virus 6.0 permitió fortalecer la seguridad de la información sensible en la Institución, protegiéndola principalmente de virus informáticos.
- La sencillez de manejo del software Anti-Virus en los clientes, es posible gracias a las facilidades de configuración y control que brinda el módulo de administración del mismo.
- Con un correcto control de acceso y asignación de permisos a los datos, se garantiza que la información es manipulada y utilizada por las personas responsables de ésta.
- Con la implementación del Servidor Corporativos de Actualizaciones Windows Server Update Service 3.0, el software de los computadores miembros de la red informática, se mantendrán correctamente actualizados mejorando su rendimiento, seguridad y productividad en la organización

2.2 Fundamentación legal

La presente investigación se basará en la ley publicada en el Registro Oficial N° 557 del 17 de Abril de 2002.

CONSTITUCIÓN DEL ESTADO

Sección tercera

Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.

3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.

4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.

5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Art. 19.- La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente.

Se prohíbe la emisión de publicidad que induzca a la violencia, la discriminación, el racismo, la toxicomanía, el sexismo, la intolerancia religiosa o política y toda aquella que atente contra los derechos.

Art. 20.- El Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación.

LEY ESPECIAL DE TELECOMUNICACIONES REFORMADA

Decreto No. 1790

TITULO VI: DEL RÉGIMEN DE INTERCONEXIÓN Y CONEXIÓN

CAPÍTULO II:

OBLIGATORIEDAD DE INTERCONEXIÓN Y CONEXIÓN

Art. 38.- Los concesionarios que tengan redes públicas están obligados a:

a) Suministrar las facilidades de conexión o interconexión entre redes de telecomunicaciones de manera eficiente, en concordancia con los principios de igualdad de acceso y trato no discriminatorio, para lo cual todo concesionario

deberá ofrecer las mismas condiciones técnicas, económicas, y de mercado a quien solicita la conexión o interconexión con la red operada.

b) Proporcionar acceso eficaz a la información técnica necesaria para permitir o facilitar la conexión o interconexión de dichas redes

c) Aplicar los precios de sus servicios de telecomunicaciones sin incluir el precio de los equipos terminales necesarios o útiles para recibirlos.

Así mismo, no impondrán como condición para la prestación de sus servicios, la compra, alquiler o uso de equipos terminales suministrados por ellos mismos o por un determinado proveedor.

Dichos equipos se proveerán en régimen de libre competencia.

Art. 39.- Toda conexión o interconexión entre redes de telecomunicaciones debe efectuarse de manera eficiente, en concordancia con los principios de igualdad de acceso y trato no discriminatorio, para lo cual todo concesionario deberá ofrecer las mismas condiciones técnicas, económicas y de mercado a quien solicite la conexión o interconexión con la red operada.

CAPÍTULO III:

CONTENIDO DE LOS ACUERDOS

Art. 40.- Los acuerdos de conexión e interconexión deberán contener, como mínimo:

a) Detalles de los servicios a ser prestados mediante la conexión o interconexión

b) Especificación de los puntos de conexión o interconexión y su ubicación geográfica

c) Diagrama de enlace entre las redes

d) Características técnicas de las señales transmitidas

e) Requisitos de capacidad

f) Índices de calidad de servicio

g) Responsabilidad con respecto a instalación, prueba y mantenimiento del enlace y de todo equipo a conectar con la red que pueda afectar la interconexión y la conexión

h) Cargos de conexión o interconexión

i) Formas y plazos de pago, incluyendo procedimiento de liquidación y facturación

j) Mecanismos para medir el tráfico en base al cual se calcularán los pagos

k) Procedimientos para intercambiar la información necesaria para el buen funcionamiento de la red y el mantenimiento de un nivel adecuado de conexión o interconexión

l) Términos y procedimientos para la provisión de llamadas de emergencia o con fines humanitarios, si es aplicable

m) Procedimientos para detectar y reparar averías, incluyendo el tiempo máximo a permitir para los distintos tipos de reparaciones

2.3 Categorías Fundamentales

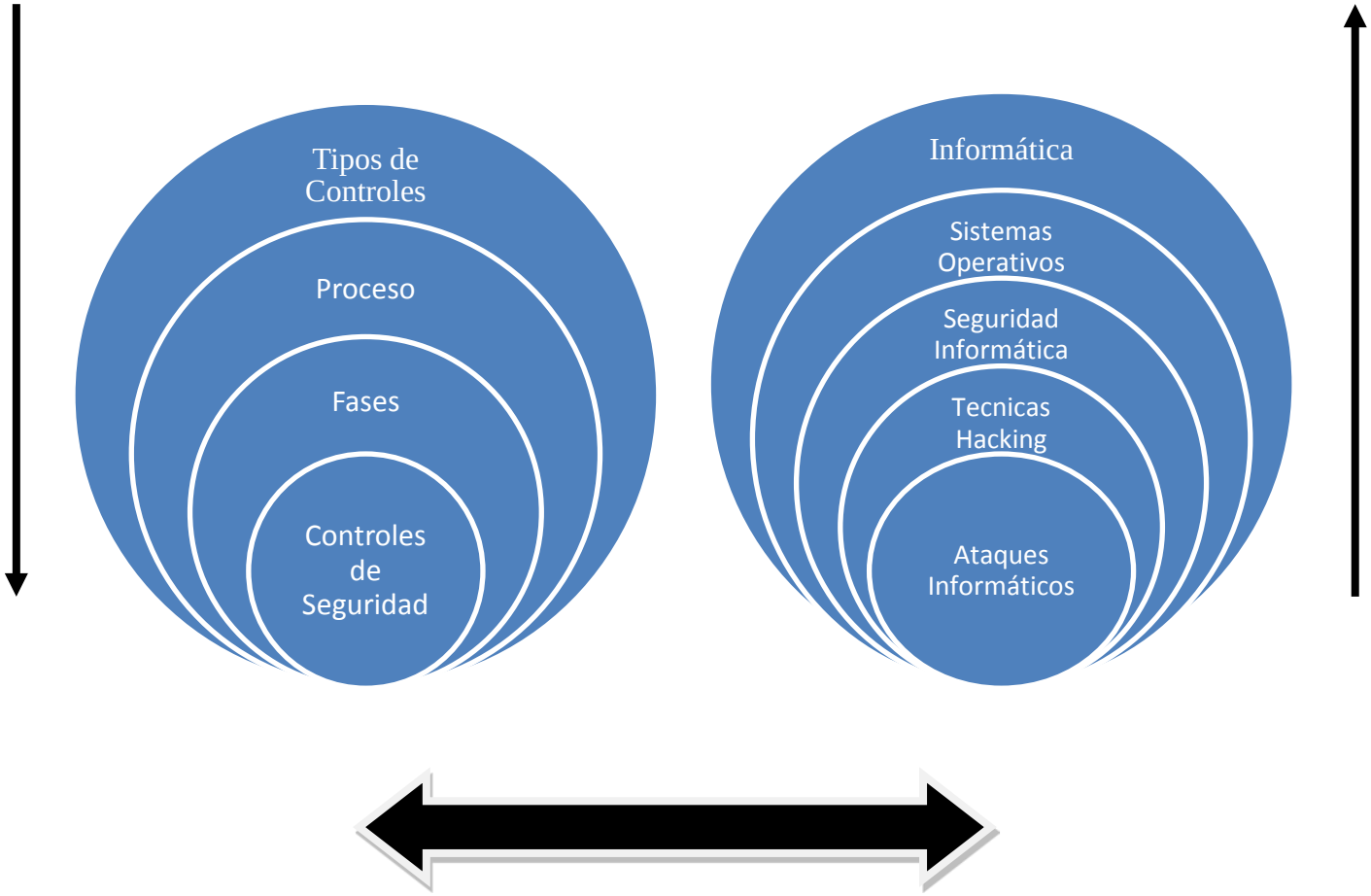


Gráfico 2.1 Categorías Fundamentales

Elaborado por: Mauro Jijón

Fuente: Investigación Directa

Constelación de Ideas

Variable Dependiente: Controles de Seguridad

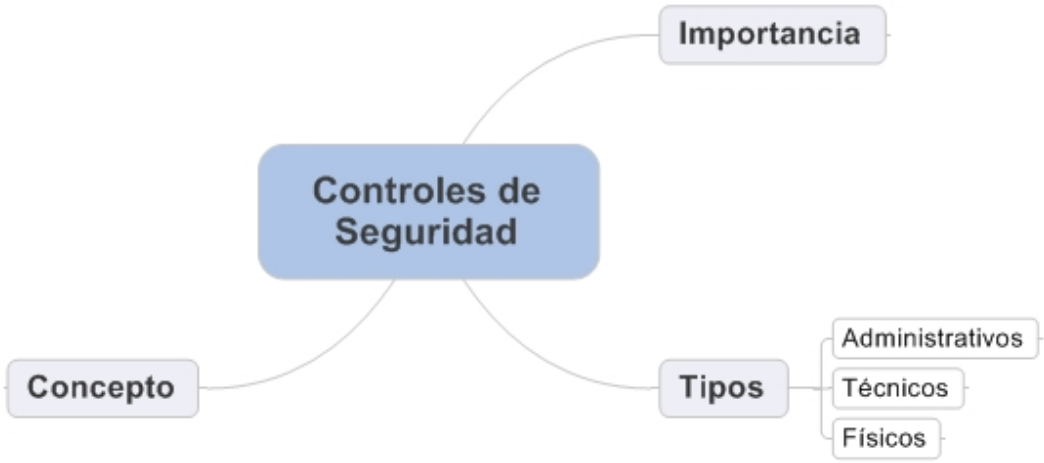


Gráfico 2.2. Categorización de la variable Dependiente

Elaborado por: Mauro Jijón

Fuente: Investigación Directa

Variable Independiente: Ataques Informáticos

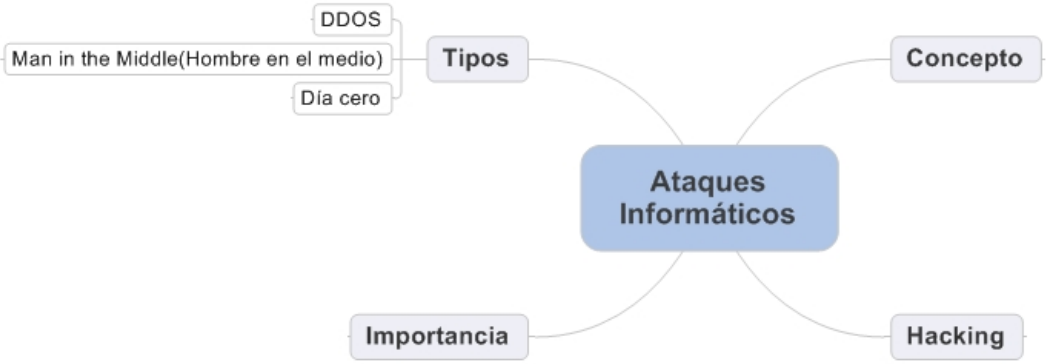


Gráfico 2.3. Categorización de la variable independiente

Elaborado por: Mauro Jijón

Fuente: Investigación Directa

2.4.1. Fundamentación teórica variable Independiente

2.4.2 Los tipos de controles de seguridad

Según VeidaDamara(Internet, 21/10/11; 22/10/11; 13:05), extraído desde http://www.slideshare.net/VeidaDamara/controles-de-seguridad argumenta que "Los controles son los mecanismos que se utilizan para poder controlar los accesos y privilegios a los recursos indicados. Es responsabilidad del dueño del activo sobre el que se le aplican los controles establecer los parámetros requeridos para disponibilidad, confidencialidad e integridad; el experto en seguridad informática será el responsable de diseñar, configurar y hacer cumplir los parámetros dictados. El profesional de la seguridad es quién realiza las sugerencias y decide qué tipo de controles (que pueden variar debido diversos factores como la naturaleza del negocio, el presupuesto asignado, el tipo de usuario, la criticidad del activo, etc.). La facultad de decidir cómo será el rol de la seguridad en la organización pertenece a la administración.

Los controles se dividen en tres tipos: administrativos, técnicos y físicos. Los controles administrativos son aquellos que están involucrados directamente con procedimientos, políticas, estándares, entrenamiento, procedimientos de monitoreo y control de cambios. Los controles técnicos están relacionados con el acceso lógico, accesos de control, contraseñas, administración de recursos, métodos de identificación o autorización, seguridad de dispositivos y configuraciones de red. Los controles físicos, como su nombre lo dicen, se encargan de controlar el acceso físico a los activos. Están relacionados directamente con candados, monitores ambientales, guardias, perros entrenados, etc.

Los controles administrativos deben incluir el desarrollo del programa de seguridad, indicar de forma explícita quién está autorizado y quién no a acceder a los activos, clasificación de los datos y refuerzo de la protección para cumplir la clasificación establecida, desarrollo de políticas, estándares (re edición de ellos cuando se detecte que no son suficientes), desarrollo de programa de respuesta a incidentes, desarrollo de programas de continuidad de negocio y recuperación de desastres. La primer pieza para construir los fundamentes de seguridad es tener una política de seguridad. Como en todo caso, la administración es la responsable de desarrollar las políticas y puede delegar la redacción y diseño de todos los procedimientos que salgan de ahí (procedimientos, estándares y guías).

Los controles técnicos implementan los mecanismos de acceso lógico; requieren que los usuarios realicen una identificación y autorización antes. También están relacionados con el cifrado de datos (ya sea en su almacenamiento o transmisión), elementos de telecomunicaciones como firewalls y detectores de intrusos, balanceo de carga y tolerancia a fallas.

Los controles físicos están relacionados con el impedimento físico de usuarios a activos. Estos pueden ser candados y alarmas en accesos exteriores a instalaciones, guardias de seguridad revisando personal sospechoso, equipos de cómputo con sensores para detectar presencia, acciones como remover unidades de disco para evitar el copiado de información, almacenamiento de respaldos en cuartos especiales (a prueba de casi todo) o fuera de las instalaciones por nombrar algunos.

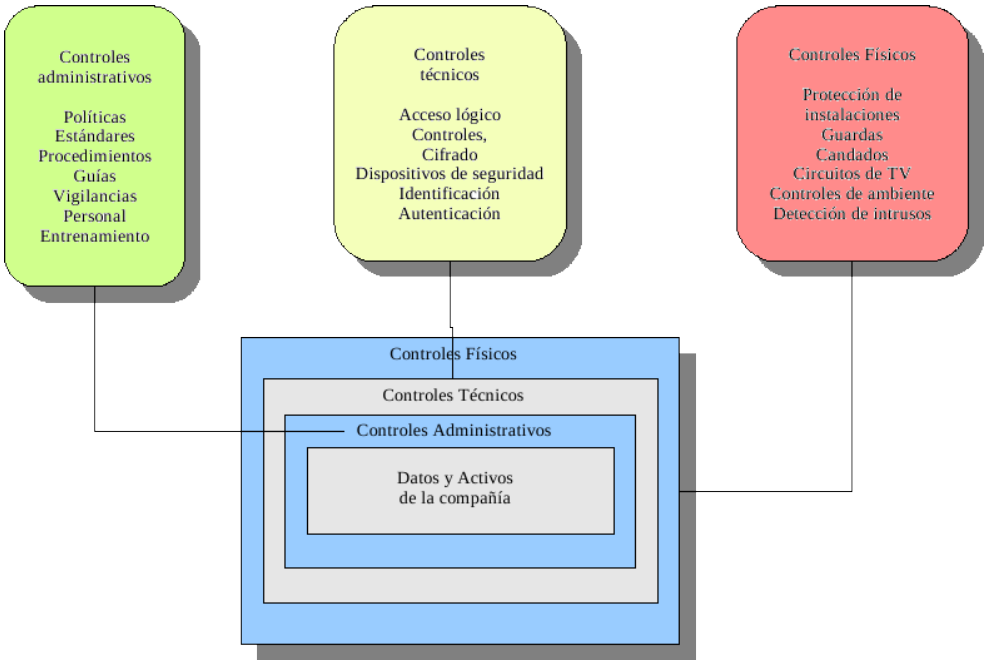


Gráfico 2.4. Tipos de controles de seguridad

Fuente: http://www.slideshare.net/

Los controles entre sí tienen una dependencia para poder existir. Aunque su existencia no es mutuamente exclusiva si su respaldo. Un control físico o técnico no puede tener el respaldo legal de existir sin su respectivo control administrativo (nos referimos a la política de seguridad). Si la política en cuestión no existiera la existencia del control está comprometida y sólo es cuestión de tiempo para que algún usuario con jerarquía la califique de ilegal para que sea removido. Así mismo, los controles técnicos requieren ser protegidos físicamente para evitar que un intruso los desactive. Todos los controles deben trabajar conjuntamente para poder ofrecer un óptimo nivel de protección al activo y entre ellos".

2.4.3 Planificación De La Seguridad:

Para César Escobar y Rafael Mendoza (Internet, 01/05/11; 29/04/11; 17:02), extraído desde blastersolaris.blogspot.com argumentan que: "Hoy en día la rápida

evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. El propósito del plan de seguridad del sistema es proporcionar una visión general de los requisitos de seguridad del sistema y se describen los controles en el lugar o los previstos para cumplir esos requisitos. El plan de seguridad del sistema también delinea las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema. Debe reflejar las aportaciones de distintos gestores con responsabilidades sobre el sistema, incluidos los propietarios de la información, el propietario de la red, y el alto funcionario de la agencia de información de seguridad (SAISO).

Los administradores de programas, los propietarios del sistema, y personal de seguridad en la organización debe entender el sistema de seguridad en el proceso de planificación. Los responsables de la ejecución y gestión de sistemas de información deben participar en el tratamiento de los controles de seguridad que deben aplicarse a sus sistemas".

2.4.4 Creación de un Plan de respuesta a incidentes

Para el sitio web.mit.edu (Internet, 20/10/11; 29/04/11; 17:10), extraído desde http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-response-plan.html argumenta que "Es importante formular un plan de respuestas a incidentes, soportarlo a lo largo de la organización y probarlo regularmente. Un buen plan de respuestas a incidentes puede no sólo minimizar los efectos de una violación sino también, reducir la publicidad negativa.

Desde la perspectiva del equipo de seguridad, no importa si ocurre una violación o abertura (pues tales eventos son una parte eventual de cuando se hacen negocios usando un método de poca confianza como lo es Internet), sino más bien cuando ocurre. No piense en un sistema como débil o vulnerable, es importante darse cuenta que dado el tiempo suficiente y los recursos necesarios, alguien romperá la seguridad hasta del sistema o red más seguro y protegido".

2.4.5 Fases plan de respuesta a incidentes

El sitio Seguridadinformaticaufps.wikispaces.com (Internet, 20/10/11; 29/04/11; 17:10), extraído desde:

https://seguridadinformaticaufps.wikispaces.com/Conceptos+Basicos+Seguridad+Informatica argumenta que "El aspecto positivo de entender la inevitabilidad de una violación a los sistemas es que permite al equipo de seguridad desarrollar un curso de acciones para minimizar los daños potenciales. Combinando un curso de acciones con la experiencia le permite al equipo responder a condiciones adversas de una manera formal y oportuna.

El plan de respuesta a incidentes puede ser dividido en cuatro fases:

- Acción inmediata para detener o minimizar el incidente
- Investigación del incidente
- Restauración de los recursos afectados
- Reporte del incidente a los canales apropiados

Una respuesta a incidentes debe ser decisiva y ejecutarse rápidamente. Debido a que hay muy poco espacio para errores, es crítico que se efectúen prácticas de

emergencias y se midan los tiempos de respuesta. De esta forma, es posible desarrollar una metodología que fomenta la velocidad y la precisión, minimizando el impacto de la indisponibilidad de los recursos y el daño potencial causado por el sistema en peligro.

Un plan de respuesta a incidentes tiene un número de requerimientos, incluyendo:

- Un equipo de expertos locales (un Equipo de respuesta a emergencias de computación)
- Una estrategia legal revisada y aprobada
- Soporte financiero de la compañía
- Soporte ejecutivo de la gerencia superior
- Un plan de acción factible y probado
- Recursos físicos, tal como almacenamiento redundante, sistemas en standby y servicios de respaldo”

2.4.6 Ataques a servidores

El sitio kioskea (Internet, 20/10/11; 23/10/11; 11:02), extraído desde http://es.kioskea.net/contents/16-ataques-al-servidor-web argumenta que “Los primeros ataques a la red aprovecharon las vulnerabilidades relacionadas con la implementación de conjuntos de protocolos TCP/IP. Al corregirlas gradualmente, los ataques se dirigieron a las capas de aplicaciones y a la Web en particular, ya que la mayoría de las empresas abrieron sus sistemas de firewall al tráfico en Internet.

El protocolo HTTP (o HTTPS) representa el estándar que posibilita la transferencia de páginas Web a través de un sistema de solicitud y respuesta.

Internet, que se utiliza principalmente para transferir páginas Web estáticas, se ha convertido rápidamente en una herramienta interactiva que permite proporcionar servicios en línea. El término "aplicación Web" se refiere a cualquier aplicación a cuya interfaz se pueda acceder en la Web desde un simple navegador. Hoy en día, el protocolo HTTP, la base para una determinada cantidad de tecnologías (SOAP, Javascript, XML-RPC, etc.), juega un indudable papel estratégico en la seguridad de sistemas de información.

Debido a que los servidores Web están cada vez más protegidos, los ataques están dirigiendo su atención al aprovechamiento de las fallas de las aplicaciones Web.

Como tal, la seguridad de los servicios de Internet debe tenerse en cuenta al momento del diseño y desarrollo".

2.4.7 Seguridad Informática

Para José Luis (Internet, 20/10/11; 23/10/11; 12:02), extraído desde http://blog.unach.mx/jose/2012/01/28/%C2%BFque-es-la-seguridadinformatica/ argumenta que: "La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas".

2.4.8 VPN

El sitio web de la Universidad de Valencia (Internet, 22/10/11; 23/10/11; 12:02), extraído desde http://www.uv.es/siuv/cas/zxarxa/vpn.htm objeta que "Una red privada virtual (Virtual Private Network) es una red privada que se extiende, mediante un proceso de encapsulación y en algún caso de encriptación, desde los paquetes de datos a diferentes puntos remotos, mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por un túnel definido en la red pública.

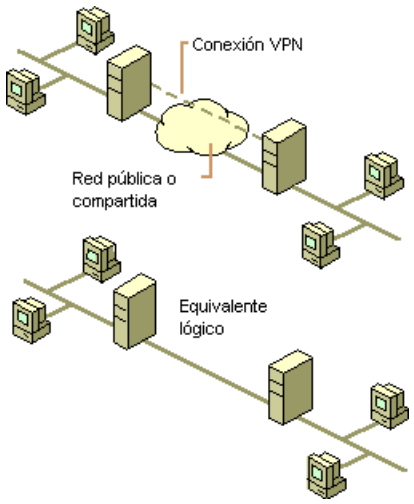


Gráfico 2.5. Red VPN

Fuente: http://www.uv.es/

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignando a su ordenador remoto las direcciones y privilegios de esta, aunque la conexión la haya realizado mediante un acceso público a Internet.

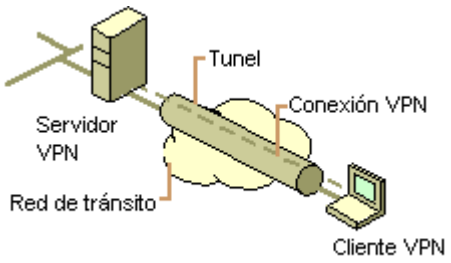


Gráfico 2.6. Acceso a una VPN

Fuente: http://www.uv.es/

En ocasiones, puede ser interesante que la comunicación que viaja por el túnel establecido en la red pública vaya encriptada para permitir una confidencialidad mayor".

2.4.9 Firewall

Para Miguel Ángel Álvarez (Internet,21/10/11; 25/10/11;11:02), extraído desde http://www.desarrolloweb.com/articulos/513.php "Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio

al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con software específico que lo único que hacen es monitorizar las comunicaciones entre redes".

2.4.9 ACL'S (Access Control List)

El diccionario informático glosarium (Internet, 21/10/11; 22/10/11; 15:22), extraído desde http://www.glosarium.com/term/28,14,xhtml argumenta que "Es una tabla que le dice a un sistema los derechos de acceso que cada usuario posee para un objeto determinado, como directorios, ficheros, puertos, etc. Técnicas para

limitar el acceso a los recursos según la información de autenticidad y las normas de acceso".

2.4.10 Informática

Según definicion.de (Internet, 20/10/11; 24/10/11; 15:20), extraído desde http://definicion.de/informatica/ nos dice que "la informática se refiere al procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales. Los sistemas informáticos deben contar con la capacidad de cumplir tres tareas básicas: entrada (captación de la información), procesamiento y salida (transmisión de los resultados). El conjunto de estas tres tareas se conoce como algoritmo.

La informática reúne a muchas de las técnicas que el hombre ha desarrollado con el objetivo de potenciar sus capacidades de pensamiento, memoria y comunicación. Su área de aplicación no tiene límites: la informática se utiliza en la gestión de negocios, en el almacenamiento de información, en el control de procesos, en las comunicaciones, en los transportes, en la medicina y en muchos otros sectores".

2.4.11 Sistema Operativo

Andrew Tanenbaum(1998, Pág. 03), Sistemas Operativos: Diseño e Implementación argumenta que "La mayoría de los usuarios de computadora han tenido algo de experiencia con un sistema operativo, pero no es fácil precisar con exactitud qué es un sistema operativo. Parte del problema consiste en que el sistema operativo realiza dos funciones que básicamente no están relacionadas

entre sí y, dependiendo de a quién le preguntemos, por lo general se nos habla principalmente de una función o de la otra, Veamos ahora las dos.

El sistema operativo como máquina extendida

Como ya dijimos, la arquitectura (conjunto de instrucciones, organización de memoria, E/S y estructura de buses) de la mayor parte de las computadoras en el nivel de lenguaje de máquina es primitiva y difícil de programar, sobre todo para entrada/salida.

Un sistema de información, no obstante las medidas de seguridad que se apliquen, no deja de tener siempre un margen de riesgo".

2.4.12 Seguridad Informática

La seguridad informática según AGUILERA, Purificación. ("sf", pág. 9). "es una disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable "

El sitio Infosec (Internet, 20/10/11; 24/10/11; 21:30), extraído desde http://infosec.aragon.unam.mx/a011.php argumenta que "A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación ha provocado el surgimiento de nuevos vectores de ataques y de nuevas modalidades delictivas que han transformado a Internet y las tecnologías informáticas en aspectos sumamente hostiles para cualquier tipo de organización, y persona, que tenga equipos conectados a la Word Wide Web.

A diferencia de lo que sucedía años atrás, donde personas con amplias habilidades en el campo informático disfrutaban investigando estos aspectos con el ánimo de

incorporar mayor conocimiento; en la actualidad se ha desvirtuado completamente dando origen a nuevos personajes que utilizan los medios informáticos y el conocimiento sobre su funcionamiento como herramientas para delinquir y obtener algún beneficio económico.

Cada día se descubren nuevos puntos débiles y, por lo general, son pocos los responsables de IT que comprenden en su justa medida la importancia que tiene la seguridad y cómo pueden abordar el grave problema que existe detrás de vulnerabilidades que permiten a un atacante, violar la seguridad de un entorno y cometer delitos en función de los datos robados.

Bajo esta escenografía donde los principales actores son las organizaciones de cualquier magnitud y rubro, los sistemas de información, el dinero y delincuentes informáticos; se torna realmente necesario y fundamental idear estrategias de seguridad que permitan establecer barreras defensivas orientadas a mitigar efectivamente ataques tanto externos como internos.

Pero para lograr mitigar de manera eficaz el impacto provocado por los ataques informáticos, es de capital importancia conocer de qué manera atacan y cuáles son los puntos débiles de un sistema, comúnmente explotados en los que se deben enfocar los esfuerzos de seguridad tendientes a la prevención de los mismos".

2.4.13 Hacking

El sitio Softlibre (Internet, 20/10/11; 24/10/11; 55:10), extraído desde http://www.softlibre.salta.org.ar/programacion/ comenta que "El Jargon File contiene un montón de definiciones del término "hacker", la mayoría basadas en la afición a lo técnico y en el placer de resolver problemas sobrepasando los

límites. Si deseas saber cómo convertirte en un hacker, bien, solo 2 puntos son realmente relevantes.

Existe una comunidad, una cultura compartida, de programadores expertos y magos de las redes, cuya historia se remonta décadas atrás a los tiempos de los primeros miniordenadores de tiempo compartido y los tempranos experimentos con ARPAnet. Los miembros de esta cultura crearon el término "hacker". Los hackers construyeron Internet. Los hackers hicieron de Unix el sistema operativo que es hoy día. Los hackers hacen andar Usenet. Los hackers hacen funcionar la WWW. Si eres parte de esta cultura, si has contribuido a ella y otras personas saben quién eres y te llaman hacker, entonces eres un hacker.

La mentalidad hacker no está confinada a esta cultura del software. Hay gente que aplica la actitud de hacker a otras cosas, como la electrónica o la música —de hecho, puedes encontrarla en los más altos niveles de cualquier ciencia o arte. Los hackers de software reconocen estos espíritus emparentados en otras partes y pueden llamarlos "hackers" también— y algunos sostienen que la naturaleza hacker es en realidad independiente del medio particular en el cual el hacker trabaja. Sin embargo, en el resto de este documento nos centraremos en las habilidades y actitudes de los hackers de software, y en las tradiciones de la cultura compartida que originó el término "hacker".

Existe otro grupo de personas que se llaman a sí mismos hackers, pero que no lo son. Son personas (generalmente varones adolescentes) que se divierten irrumpiendo ilegalmente en ordenadores y haciendo "phreaking" en el sistema telefónico. Los auténticos hackers tienen un nombre para esas personas:

"crackers", y no quieren saber nada de ellos. Los auténticos hackers opinan que la mayoría de los crackers son perezosos, irresponsables y no muy brillantes, y fundamentan su crítica en que ser capaz de romper la seguridad no le hace a uno un hacker, de la misma manera que ser capaz de arrancar un coche con un puente en la llave no le convierte en ingeniero de automotores. Desafortunadamente, muchos periodistas y escritores utilizan erróneamente la palabra "hacker" para describir a los crackers; esto causa enorme irritación a los auténticos hackers.

La diferencia básica es esta: los hackers construyen cosas; los crackers las destruyen".

2.4.14 Ataque Informático

El sitio Alegsa (Internet,20/10/11; 24/10/11;10:10), extraído desde http://www.alegsa.com.ar/Dic/ataque%20informatico.php lo define como "Intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red. Los ataques en grupo suelen ser hechos por bandas de piratas informáticos por diversión, para causar daño, buenas (relativamente buenas) intenciones, espionaje, obtención de ganancias, etc. Los blancos preferidos suelen ser los sistemas de grandes corporaciones o estados, pero ningún usuario de Internet u otras redes está exento.

Probablemente el primer ataque informático masivo de la historia se produjo un viernes 13 de 1989, cuando una revista informática regaló disquetes de promoción, pero estaban infectados con un virus; el virus afectó a cientos de empresas.

Actualmente los ataques suelen afectar principalmente a Internet, pero también

afectan otras redes como las de telefonía, redes Wi-Fi, redes de área local de empresas, etc”.

2.4.15 Ataque distribuido de denegación de servicio

El sitio web maestrosdelweb.com (Internet, 21/10/11; 22/10/11; 40:10), extraído de http://www.maestrosdelweb.com/editorial/ddos/ nos da una explicación fácil de entender de lo que es un Ataque distribuido de denegación de servicio:

“Imagínate que estás en un Bar junto a un amigo, bebiendo unas cervezas, aparte de ti y tu amigo hay dos personas más, un empleado público con su amante. La persona que atiende el Bar es un tipo fortachón llamado Hugo. De pronto tú y tu amigo quieren más cerveza, y llaman a Hugo, les sirven otra corrida, al mismo tiempo el empleado fiscal y su amante también piden otra corrida de cervezas heladas.

Todo sigue tranquilo, cada 15 minutos aproximadamente llega una persona más al Bar y Hugo le sirve una cerveza. ¡De pronto!, aumenta la frecuencia de clientes al Bar, ya no son los 4 iniciales, ahora son 15. Hugo comienza a transpirar por tanta demanda. A poco andar, la cantidad se duplica y en el Bar sólo se escucha: "Hugo…otra corrida", “Hugo…por acá por favor", "Más Hugo", "Hugo", "Hugo por favor","che flaco” (ese era argentino).

Hugo comienza a sentirse apremiado de tanta solicitud de cerveza pero atiende sin mayores problemas. El Bar tiene a esas alturas 55 personas. ¡De pronto!… llega todo un equipo de fútbol amateur a celebrar la obtención del campeonato y la

misma canción: "Hugo", "hey hugo, por acá", "hugo", "hey amigo", "hugooooo", "huguitoooo".

Ahora sí, Hugo comienza a dar signos de colapso. De pronto llega otro equipo más (el que perdió el campeonato) y luego los árbitros y luego todo el público que había en el estadio. Resultado: Hugo colapsado, ahora yace desmayado en una esquina del Bar, ya no puede atender a tanta gente. En eso, tú pides una cerveza pero el pobre Hugo no responde, a ti se te ha denegado el servicio a la cerveza.

Hugo→ El Servidor, las 55 personas del bar → los usuarios. Los árbitros, los equipos de fútbol y el público → falsos usuarios. Hubo alguien, mal intencionado por cierto, que envío a toda esa gente (falsos usuarios) al Bar de Hugo, sabiendo que no sería capaz, éste despreciable personaje es el atacante del Bar de Hugo, es decir, un Hacker o varios de ellos.

Este tipo de Hacker tiene bastante mala fama entre sus pares, ya que es la forma más simple de echar abajo un servidor. Ahora bien, los ataques de denegación pueden ser enviados desde un PC o por varios, pero también existe la posibilidad de que potentes servidores actúen de la misma forma, a esto se le llama un ataques distribuidos. Estos servidores se les llaman zombies, ya que actúan a la orden del Hacker, el cual con antelación intervino aquella máquina sin que el administrador se diera cuenta por supuesto".

2.5 Hipótesis

Los controles de seguridad incidirían en los ataques informáticos a la Universidad Técnica de Ambato

2.6 Señalamiento de Variables

Variable Independiente: Controles de Seguridad

Variable Dependiente: Ataques Informáticos

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Enfoque

La investigación que se realizará tiene un enfoque cualitativo ya que es contextualizado, pone énfasis en buscar menos la generalización ya que se tiene como único propósito solucionar problemas de una empresa, discute la validez del conocimiento utilizando varias técnicas como la observación.

Esta investigación es cuantitativa porque se basa en un positivismo lógico que busca las causas, la explicación de los hechos que originan al problema, y como estos afectan al desenvolvimiento de la institución.

Al definir los objetivos estos se orientaran a la obtención de resultados y además deberán estar orientados a la solución del problema de la institución en un contexto enmarcado en lo tangible, estable y sostenible.

3.2 Modalidades básicas de la investigación

La presente investigación tiene las siguientes modalidades:

Modalidad Bibliográfica o documentada.- Se ha considerado esta modalidad ya que se ha considerado información de libros técnicos, revistas, Internet, videos.

Modalidad Experimental.- Se ha considerado la relación de los controles de seguridad y su influencia y relación en los ataques informáticos para considerar sus causas y sus efectos.

Modalidad de Campo.- Se ha considerado esta modalidad ya que el investigador ira a recoger información primaria directamente de los involucrados a través de la encuesta.

3.3 Tipos de Investigación

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de la investigación con la Captura y Análisis de los ataques informáticos en los servidores de la Universidad Técnica de Ambato, mediante la implantación de una Honeynet. Como de la misma manera ayudo a plantear la hipótesis: Los ineficientes controles de seguridad permiten los continuos ataques informáticos en la Universidad Técnica de Ambato.

Se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar en tiempo y espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación correlacional ya que ha permitido medir la compatibilidad de los Honeynets con los ataques informáticos.

3.4 Población y Muestra

El universo de investigación es de 48 observaciones a realizarse en un periodo de 4 meses con 3 observaciones por semana de aproximadamente 4 horas dentro de los Laboratorios de la Facultad de Ingeniería en Sistemas los laboratorios #3, #5, #7 de la Universidad Técnica de Ambato; se utilizara la ficha de observación y las

siguientes herramientas para determinar los controles de seguridad con los cuales constan los ordenadores como por ejemplo un antivirus; también se utilizaran estas herramientas para determinar la presencia de malware.

Comodo HIPS and Firewall Leak Test Suite.- Es una herramienta que permite simular varios ataques típicos que se realizan, contiene cinco pruebas separadas que simulan una serie de ataques incluyendo rootkits, los ataques de inyección, etc, fuente: http://personalfirewall.comodo.com/cltinfo.html

HijackThis.- Es una pequeña herramienta gratuita que escanea rápidamente el sistema Windows para encontrar las modificaciones que puedan haber sido realizadas por algún Spyware, Browser Hijacker, Malware u otro programa malicioso, fuente http://portableapps.com/apps/security/hijackthis-portable

Se utilizaron versiones portables para evitar modificar los ordenadores a analizar.

3.5 Recolección y análisis de la información

Secundaria	**Primaria**
Se recolecta de estudios realizados anteriormente. Se encuentra registrada en documentos y material impreso: libros, revistas especializadas, informes técnicos, memorias de eventos científicos, tesis de grado,	Se recolecta directamente a través de la observación directa entre el sujeto investigador y el objeto de estudio, es decir, con la realidad. Para esto se utilizara la herramienta observación para recolectar

etc. Las fuentes de información son: La biblioteca de la Facultad de Ingeniería en Sistemas de la Universidad Técnica de Ambato, bibliotecas de otras universidades, repositorios de otras universidades en Internet, archivos, centros de documentación e Internet.	información tomada de los administradores del sistema de la Universidad Técnica de Ambato y actuar en base a los resultados obtenidos.

Técnicas de investigación

Bibliográficas	**De campo**
El análisis de documentos(lectura científica) Se procederá a recolectar información de distintas fuentes como por ejemplo de la biblioteca de la Universidad técnica de Ambato para obtener más información acerca del tema de investigación.	Observación

Recolección de la información

Preguntas	**Explicación**
1.- ¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis

2.- ¿A qué personas o sujetos?	A los administradores del sistema de la Universidad Técnica de Ambato.
3.- ¿Sobre qué aspectos?	Controles de Seguridad Ataques Informáticos
4.- ¿Quién?	Investigador
5.- ¿Cuando?	De acuerdo al cronograma establecido
6.- ¿Lugar de recolección de la información?	• Universidad Técnica de Ambato • Facultad de Ingeniería en Sistemas, Electrónica e Industrial. • DISIR (Dirección de Sistemas Informáticos y Redes de Comunicación).
7.- ¿Cuántas veces?	Una sola vez
8.- ¿Que técnica de recolección?	Observación
9.- ¿Con qué?	Guía de Observación
10.- ¿En qué situación?	Situación normal y cotidiana

3.6 Procesamiento y análisis

Revisión y codificación de la información

Categorización y tabulación de la información

- Tabulación manual
- Tabulación computarizada

Análisis de los datos.- La presentación de los datos se lo hará a través de los gráficos para analizarlos e interpretarlos.

Interpretación de los resultados.-

1. Describir los resultados
2. Estudiar cada uno de los resultados por separado.
3. Redactar una síntesis general de los resultados

CAPÍTULO IV

ANALISIS E INTERPRETACION DE LOS RESULTADOS

4.1 Análisis de la necesidad

La Universidad Técnica de Ambato a través de la Facultad de Ingeniería en Sistemas Electrónica e Industrial en vinculación con el DISIR (Dirección de Sistemas Informáticos y Redes de Comunicación), extraído de http://www.uta.edu.ec/v2.0/index.php?option=com_content&view=article&id=38&Itemid=99 que tiene como uno de sus objetivos: "Administrar los bienes y servicios de la **red de comunicaciones** y las aplicaciones informáticas **de la Universidad**" es decir la administración central de la red de comunicaciones de la Universidad Técnica de Ambato.

Es por eso que el DISIR en conjunto con el estudiante responsable analizaron la necesidad de ampliar los criterios de seguridad informática dentro los servidores de la Universidad Técnica de Ambato, empezando con la seguridad informática dentro de la Facultad de Ingeniería en Sistemas Electrónica e Industrial (facultad del estudiante investigador), así como dentro de toda la Universidad Técnica de Ambato la cual optimizará la seguridad de la información en general.

4.2 Análisis de los resultados

Para poder recolectar información se aplicó la ficha de observación en la cual constan de manera escrita las actitudes y características del problema tal y como se presenta, además se pudo obtener información primaria la cual ayudó para poder emitir las conclusiones y recomendaciones.

Se realizó una observación directa, estructurada, individual y de campo en los ordenadores de los laboratorios de la Facultad de Ingeniería en Sistemas de la Universidad Técnica de Ambato sin ningún orden en particular, utilizando la ficha de Observación.

En los anexos 2, 3 y 6 se pueden ver parte de los resultados recolectados con las herramientas especificadas en el punto 3.4.

Resultados ficha de observación aplicada a las ordenadores de la Facultad de Ingeniería en Sistemas.

El modelo de ficha de observación utilizada puede verse en el Anexo 1.

1.- Campo “Mensajes” ficha de observación:

Cuadro N.- 1

N.-	Ítems	Frecuencia	%
1	Fallas de configuración de equipos	15	37.5
2	Fallos del sistema operativo	10	25
3	Fallos de software	9	22.5

4	Fallos de Hardware	4	10
5	Otros	2	5
	Total	40	100

Tabla 4.1 Resultados campo mensaje de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

Cuadro N.- 2

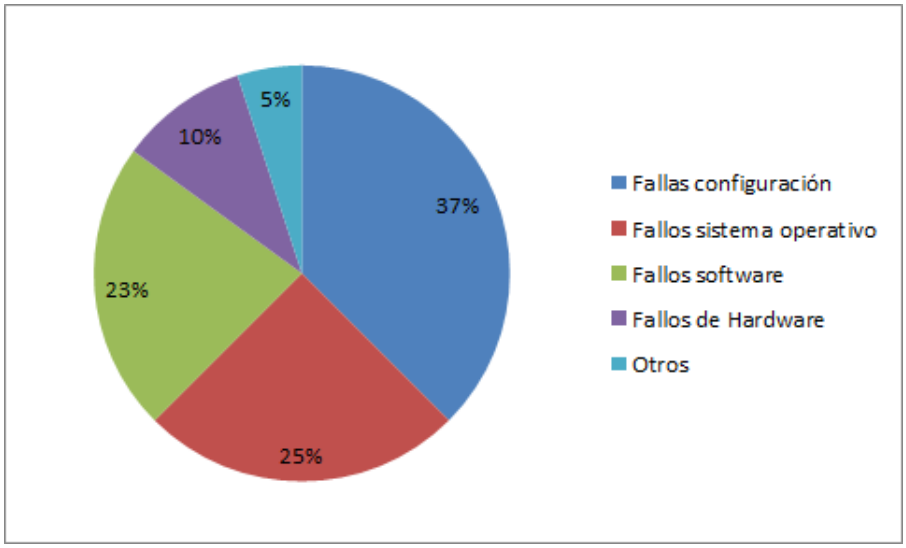


Gráfico 4.1. Resultado campo mensaje de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

De los resultados el 37.5% que representa a 15 observaciones indican que existen varias fallas en la configuración de equipos; el 25% que representa a 25 observaciones indican que existen fallas por parte del sistema operativo; el 22.5%

que representa a 9 observaciones indican que hay fallos de software en general por ejemplo programas informáticos; el 10% que corresponde a 4 observaciones indican que existen fallos de hardware y el 5% que corresponde a 2 observaciones indican que se tienen otros tipos de fallos, por ejemplo mal uso del computador.

Javier R. Cinacchi en su sitio web (http://www.estudiargratis.com.ar) nos dice que: "Un Virus informático. Los Virus informáticos pueden borrar o dañar archivos fundamentales del SO, esto va a ocasionar que este deje de funcionar. También puede crear conflictos, un programa malicioso como ser un Virus informático, al ejecutar en tiempo real su código".

2.- Campo "Resumen" ficha de observación

Cuadro N.- 3

N.-	**Ítems**	**Frecuencia**	**%**
1	Diferentes tipos de infección de virus.	20	50
2	Problemas de acceso a la red interna.	15	37.5
3	Fallos en puertos de la maquina	3	7.5
4	Otros	2	5
	Total	40	100

Tabla 4.2 Resultados campo resumen de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

Cuadro N.- 4

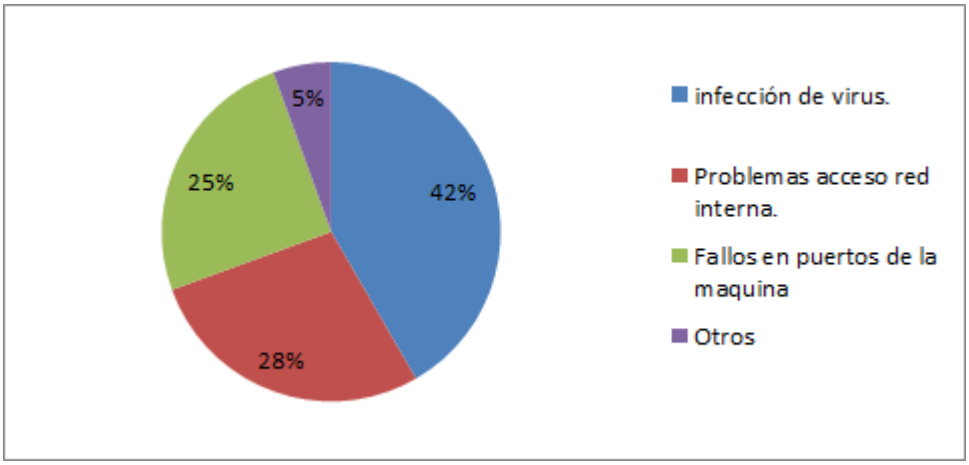


Gráfico 4.2. Resultado campo resumen de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

De los resultados el 50% que representa a 20 observaciones indican que existen infecciones de virus dentro de las maquinas; el 37.5% que representa a 15 observaciones indican que hay problemas de acceso a la red interna por ejemplo a compartir archivos; el 37.5% que representa a 15 observaciones indican que hay fallos generales en los puertos de las maquinas; y el 2% que corresponde a 5 observaciones indican que se tienen otros tipos de problemas, como por ejemplo el que no encienda la máquina.

Alan Rodríguez en su blog(http://www.rompecadenas.com.ar/articulos/2164.php) manifiesta que: “Cuando un equipo de cómputo es infectado por un virus o malware es muy poco probable que el usuario pueda darse cuenta de la infección

en el mismo momento en que esta sucede, y es aún más probable que se detecte dicha infección poco tiempo después, sobre todo por aparentes cambios significativos en el rendimiento y comportamiento del sistema operativo y aplicaciones instaladas en la computadora.”

3.- Campo “Impacto” ficha de observación

Cuadro N.- 5

N.-	**Ítems**	**Frecuencia**	**%**
1	Alto	27	67.5
2	Medio	8	20
3	Bajo	5	12.5
	Total	40	100

Tabla 4.3 Resultados campo impacto de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

Cuadro N.- 6

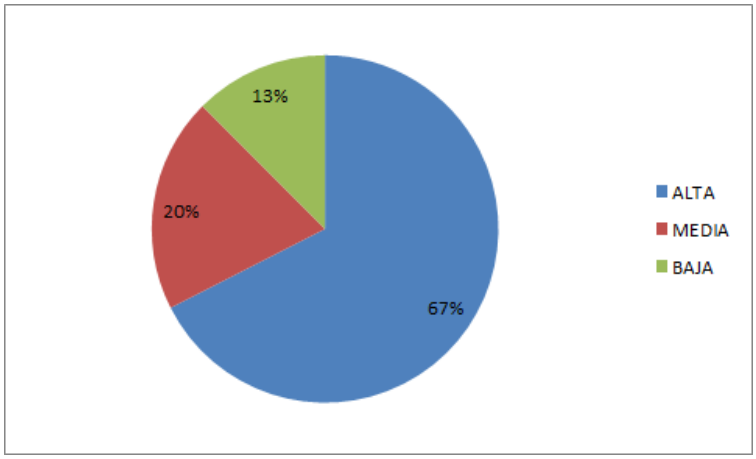


Gráfico 4.3. Resultado campo impacto de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

De los resultados el 67.5% que representa a 27 observaciones indican que existe un impacto alto dentro; el 20% que representa a 8 observaciones indican que existe un impacto medio; y el 12.5% que corresponde a 5 observaciones indican que existe un impacto bajo.

El sitio web misiglo advierte que (http://misiglo.com)

“Después de la aparición del primer virus informático, la seguridad de las computadoras nunca volvió a ser la misma. Su nombre fue adoptado por la semejanza con los virus que atacan a los organismos vivos.

Cuando se trata de las computadoras, los virus informáticos debilitan el sistema, logrando en algunos casos hacerlo inaccesible o imposible de usar.”

4.- Campo "Información detallada" ficha de observación

Cuadro N.- 7

N.-	Ítems	Frecuencia	%
1	El sistema operativo se bloquea continuamente	26	65
2	Se muestran errores del sistema con mucha frecuencia	9	22.5
3	Algunos programas instalados no funcionan adecuadamente o se cierran inesperadamente.	3	7.5
4	otros	2	5
	Total	40	100

Tabla 4.4 Resultados campo información detallada de la ficha de observación

Cuadro N.- 8

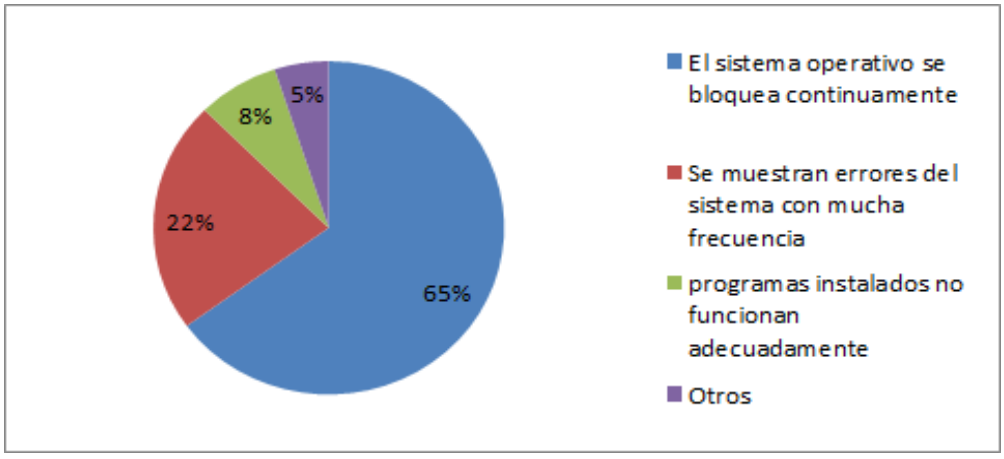


Gráfico 4.4. Resultado campo información detallada de la ficha de observación

De los resultados el 65% que representa a 26 observaciones indican que el sistema operativo se bloquea continuamente; el 22.5% que representa a 9 observaciones indican que se muestran errores del sistema con mucha frecuencia; el 7.5% que corresponde a 3 observaciones indican que algunos programas instalados no funcionan adecuadamente o se cierran inesperadamente; y el 5% que corresponde a 2 observaciones indican que existe otro tipo de problemas.

Alan Rodríguez en su blog (http://www.rompecadenas.com.ar/articulos/2164.php) nos manifiesta que:

“Millones de virus en todas sus variantes, malwares y demás aplicaciones de software malintencionado rondan en la Internet a diario poniendo en serio riesgo la seguridad de nuestros equipos de cómputo. Y el peligro no solo ronda en la red de redes, dado que actualmente la gran mayoría de los virus informáticos son capaces de propagarse no solo por la web, sino de igual forma de equipo a equipo a través de redes de computadoras y dispositivos de almacenamiento extraíble como diskettes, memorias USB, discos compactos y hasta DVD’s.”

5.- Campo “Escenarios de ataque” ficha de observación

Cuadro N.- 9

N.-	Ítems	Frecuencia	%
1	Windows	37	92.5
2	Linux	3	7.5
	Total	40	100

Tabla 4.5 Resultados campo sistemas afectados de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

Cuadro N.- 10

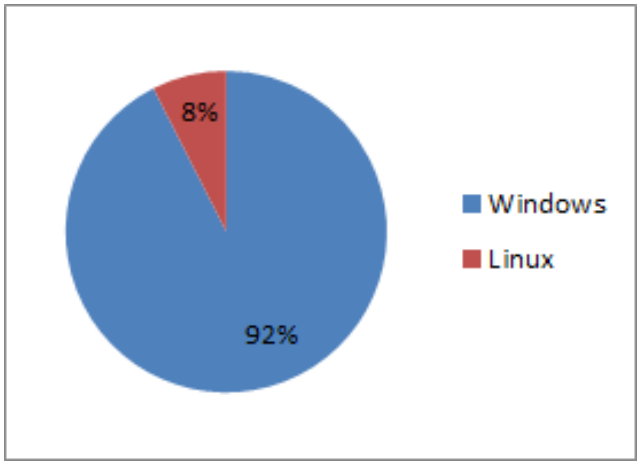


Gráfico 4.5. Resultado campo sistemas afectados de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

De los resultados el 92.5% que representa a 37 observaciones indican que el sistema afectado fue Windows; y el 7.5% que corresponde a 3 observaciones indican que el sistema afectado fue Linux.

Sebsauvage en su blog (http://es.kioskea.net/faq/1462-linux-es-invulnerable-a-los-virus) nos manifiesta que:

“Linux al igual que Windows y MacOS X tienen fallos de seguridad, los que pueden ser explotados por programas maliciosos. Por lo tanto Linux también es vulnerable a los virus, como Windows pero en una menor medida.

Sin embargo, existen muy poco virus bajo Linux (se contabilizan una treintena) comparados a los cientos de miles que existen bajo Windows. “

6.- Campo “Escenarios de ataque” ficha de observación

Cuadro N.- 11

N.-	**Ítems**	**Frecuencia**	**%**
1	Sistema operativo infectado	24	60
2	Archivos descargados de Internet	11	27.5
3	Hardware infectado	3	7.5
4	Infección por parte del usuario(programas espías)	2	5
	Total	40	100

Tabla 4.6 Resultados campo escenarios de ataque de la ficha de observación

Cuadro N.- 12

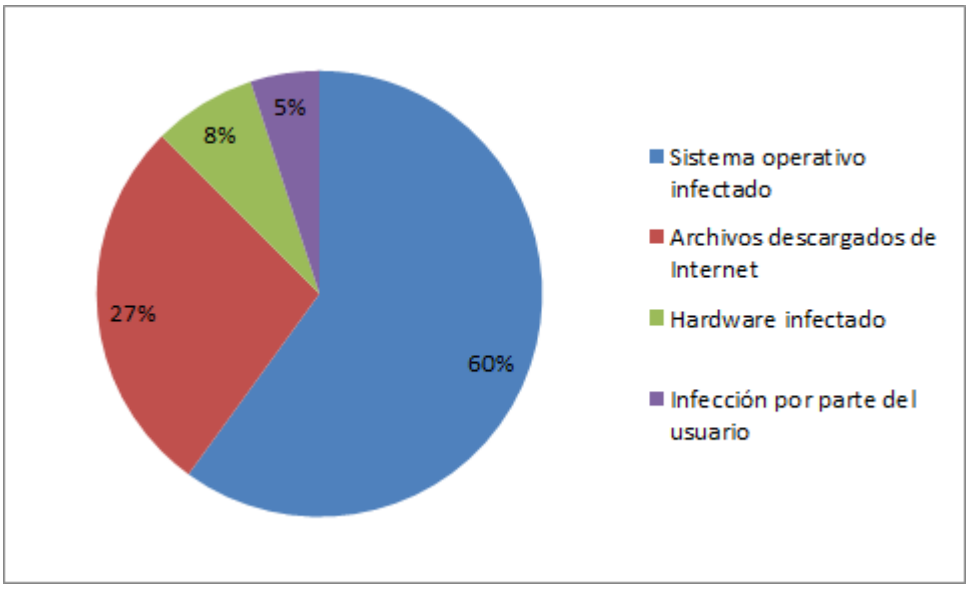


Gráfico 4.6 Resultado campo escenarios de ataque de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

De los resultados el 60% que representa a 24 observaciones indican que se producen ataques desde el sistema operativo infectado; el 27.5% que corresponde a 11 observaciones indican que se producen ataques desde archivos descargados de Internet; el 7.5% que corresponde a 3 observaciones indican que se producen ataques desde hardware infectado por ejemplo una unidad USB; y el 5% que corresponde a 2 observaciones indican que se producen ataques por parte del usuario es decir el mismo usuario produce la infección en el sistema sabiendo lo que está haciendo como por ejemplo la instalación de software espía.

El autor del blog (http://bloggadgets.es/programas-crackeados/) nos comenta que:

“La cultura de instalar programas “no originales” se volvió una costumbre, difícil de erradicar. Y lo anecdótico, es que la mayoría de estos usuarios, catalogan y hablan de seguridad y protección, cuando sus bases son programas cuyos códigos fuentes de los ejecutables, son alterados para dar larga vida a ese software.

Pero el problema más serio, además de estar utilizando software en forma ilegal, tiene que ver con que los creadores de gusanos y virus varios, saben de esta condición en los ordenadores, a la hora de atacar su débil protección. “

7.- Campo “Falsos positivos” ficha de observación

Se denomina falso positivo al hecho de que un antivirus detecte erróneamente un archivo limpio como portador de virus.

Cuadro N.- 13

N.-	**Ítems**	**Frecuencia**	**%**
1	SI	18	45
2	NO	22	55
	Total	40	100

Tabla 4.7 Resultados campo falsos positivos de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

Cuadro N.- 14

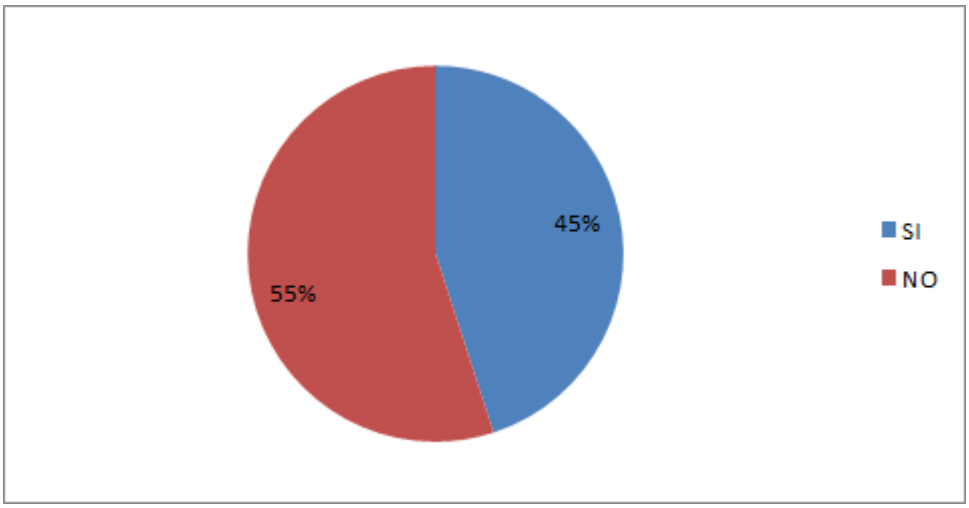


Gráfico 4.7 Resultado campo falsos positivos de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

De los resultados el 45% que representa a 18 observaciones indican que se produjeron falsos positivos; y el 55% que corresponde a 22 observaciones indican que no se produjeron falsos positivos.

Bernardo Quintero en su sitio web (http://unaaldia.hispasec.com/2008/06/falsos-negativos-y-falsos-positivos.html) nos comenta que:

“Las emulaciones, sandboxs, análisis del comportamiento, heurísticas más agresivas, firmas genéricas, etc. Todas estas tecnologías tienen en común la capacidad de identificación temprana y proactiva de especímenes desconocidos, sin necesidad de poseer una firma de detección específica. Por contra, también se prestan más a provocar falsos positivos, identificando como malware lo que en realidad no lo es. “

8.- Campo "Falsos negativos" ficha de observación

Cuadro N.- 15

N.-	Ítems	Frecuencia	%
1	SI	22	55
2	NO	18	45
	Total	40	100

Tabla 4.8 Resultados campo falsos negativos de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

Cuadro N.- 16

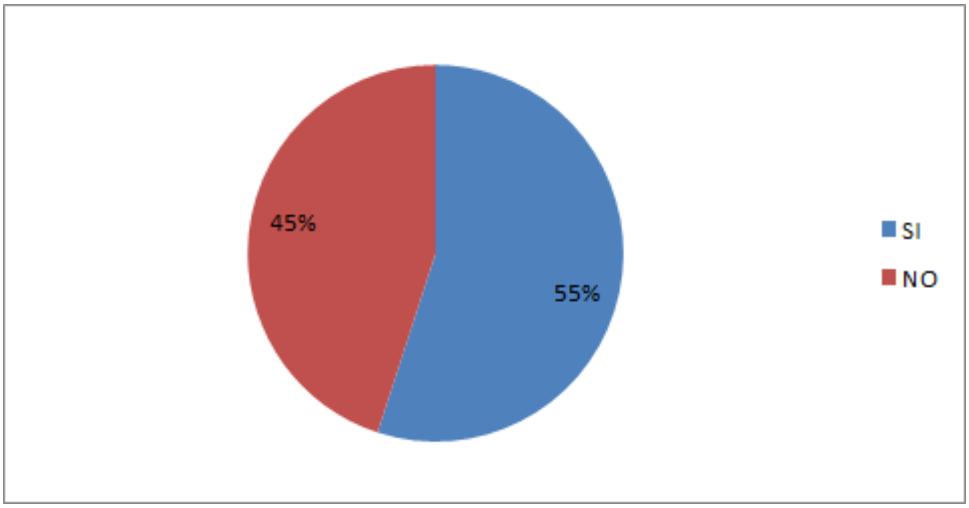


Gráfico 4.8 Resultado campo falsos negativos de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

De los resultados el 55% que representa a 22 observaciones indican que se produjeron falsos negativos; y el 45% que corresponde a 18 observaciones indican que no se produjeron falsos negativos.

Bernardo Quintero en su sitio web (http://unaaldia.hispasec.com/2008/06/falsos-negativos-y-falsos-positivos.html) nos comenta que:

"De un tiempo a esta parte tanto falsos negativos como positivos van en aumento entre los productos antivirus y, al margen de la efectividad de los antivirus, los desarrolladores de software lo están sufriendo.

Los tiempos en los que era manejable el problema del malware con la generación de firmas reactivas y concretas para cada espécimen ya pasaron. Si bien antes los antivirus tampoco eran perfectos, al menos con ese esquema podían proporcionar una protección suficientemente buena o aceptable (no había tantos falsos negativos). "

9.- Campo "Acción correctiva" ficha de observación

Cuadro N.- 17

N.-	**Ítems**	**Frecuencia**	**%**
1	Formateo de la máquina	23	57.5
2	Reinstalar software defectuoso	11	27.5
3	Actualizar antivirus	4	10

4	Reiniciar sistema operativo	2	5
	Total	40	100

Tabla 4.9 Resultados campo acción correctiva de la ficha de observación

Fuente: Ficha de Observación

Autor: Mauro Jijón

Cuadro N.- 18

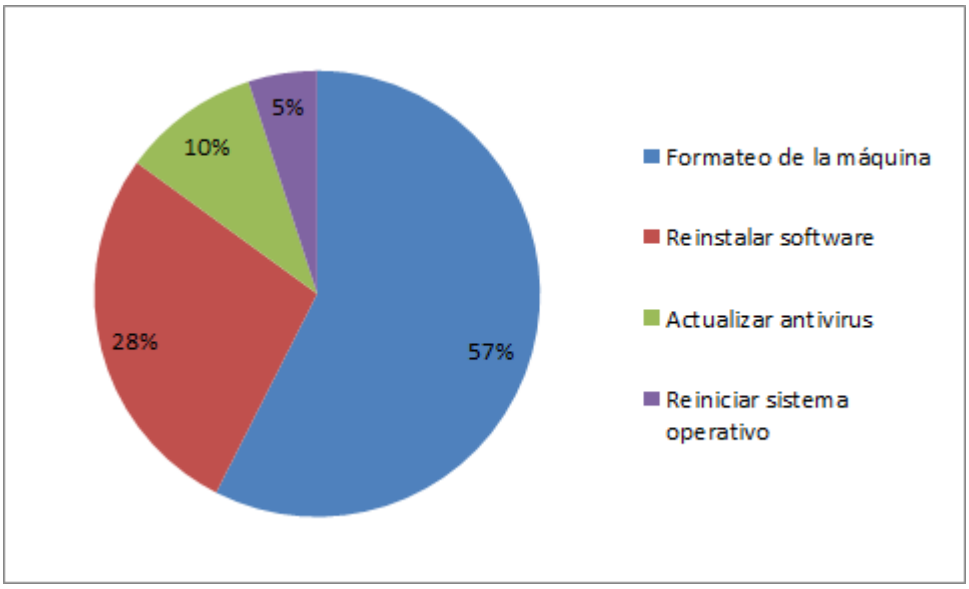


Gráfico 4.9. Resultado campo acción correctiva de la ficha de observación

De los resultados el 57.5% que representa a 23 observaciones indican que se debería formatear la maquina por los problemas encontrados; el 27.5% que corresponde a 11 observaciones indican que se debería reinstalar el software; el 10% que corresponde a 4 observaciones indican que se debería actualizar el antivirus; y el 5% que corresponde a 2 observaciones indican que se debería reiniciar la máquina para corregir el problema.

Amadeo Moreno en su sitio web (http://www.ordenadorlento.es/) nos comenta que: “Un virus o malware son conocidos por ralentizar el pc y pueden provocar que tu ordenador vaya muy lento. El más famoso es Adware. Este tipo de virus colecciona constantemente datos personales de tu sistema, para después mostrarte publicidad “adaptado” a tus intereses. En momentos específicos Adware puede usar más recursos ralentizando por un momento el ordenador. Se nota mucho esto, cuando quieres utilizar Internet. En el momento que quieres visitar una página web, se muestra de repente una publicidad no deseada. A parte de que resulta muy irritante, también causa un Internet lento. “

4.2.2 Campo “Interpretación de datos” ficha de observación

Al realizar la observación y al revisar los resultados se comprobó que la mayor parte de las maquinas dentro de la facultad de Ingeniería en Sistemas de la Universidad Técnica de Ambato se encontraban infectadas con diferentes tipos de virus adquiridos directa o indirectamente desde Internet.

En los siguientes puntos se detalla con más precisión qué tipo de malware se encontró

4.3 Controles de Seguridad dentro de los ordenadores

Tipo	
Hardware	**Firewall.-** Incluido en el propio sistema operativo **Antivirus.-** El más común que se encontró fue el antivuris Kaspersky y Avira(Esto se determinó mediante observación y con los logs de

	HijackThis resaltados con color verde; Ver Anexo 2). **IPTABLES.-** Mediante manejo de reglas internas, no se pudo acceder a más información debido a políticas de seguridad internas.

Tabla 4.10 Controles de Seguridad

Fuentes: Ficha de Observación, Herramientas de análisis, Encuesta

4.3.1 Resumen de Vulnerabilidades

Resumen de Vulnerabilidades	
Meses de Observación:	Septiembre - Diciembre
Listado de amenazas encontradas:	nwnmff_9.exe dfndrff_9.exe 54a75qwtnul.dll nnd.exe (Este tipo de amenazas se repite en la mayor parte de ordenadores analizados)
Detalles técnicos amenazas:	• Gusanos Informáticos • Dropper’s

	• Troyanos • Addware • Spyware

Tabla 4.11 Resumen de Vulnerabilidades

Fuentes: Ficha de Observación, Herramientas de análisis

4.3.2 Patrones de ataque

Vulnerabilidad	Patrón de ataque
Gusanos Informáticos	Copiarse a la mayor cantidad de equipos como sea posible. Intentan agotar los recursos del sistema como memoria o ancho de banda mientras intenta distribuirse e infectar más ordenadores.
Dropper's	Cuando se ejecuta libera un virus. Crea un virus e infecta el sistema del usuario al ejecutarse. Cuando es escaneado por un antivirus, generalmente no se detectará un virus, porque el código viral no ha sido

	creado todavía.
Troyanos	Crean puertas traseras o backdoors permitiendo el acceso a usuarios no deseados que pueden acceder a información confidencial o personal.
Addware	Muestran publicidad en los programas que estos vienen incluidos por medios de banners.
Spyware	Recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

4.3.3 Afectación a la seguridad informática

Al mirar los diferentes tipo de infección se considera que varios de los controles de seguridad establecidos fueron violados ya que no están cumpliendo con su acometido; varios de estos virus ocasionan que se tenga varios ordenadores "zombies" los cuales podrían estar formando parte de una Botnet consumiendo el ancho de banda de manera exagerada dejando sin acceso a usuarios legítimos; en otro de los casos estas ordenadores infectados podrían estar recopilando y enviando información no autorizada como pueden ser datos privados de la institución, una solución a corto plazo seria formatear la maquina infectada, pero

al no haber controles más estrictos por parte del administrador se volvería a la misma condición, es por eso que se procede con la ejecución del presente trabajo.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Dentro de la Universidad Técnica de Ambato tanto los servidores como los ordenadores clientes constan con protocolos de seguridad tales como Iptables, Firewalls, Vlans, Antivirus que evitan que usuarios no deseados intenten ingresar a datos confidenciales; así mismo estos controles de seguridad deben de ser constantemente actualizados periódicamente para evitar problemas de seguridad.

Se debe tener en cuenta no solo la seguridad dentro de los dispositivos principales como los servidores de datos o los routers que interconectan las distintas redes dentro de la Universidad Técnica de Ambato, ya que todos los dispositivos u ordenadores que estén sin los suficientes controles de seguridad, un antivirus actualizado por ejemplo, pueden llegar a infectar a varios equipos tanto de forma malintencionada como con el objetivo de ganar acceso a información confidencial.

Una vez reconocidos los patrones de ataques se identifica de una forma más fácil los “caminos” que puede tomar un usuario mal intencionado o malware para

lanzar su ataque pero todo estos ataques fueron realizados en ordenadores que estuvieron operativos, es decir fuera de un ambiente controlado.

5.2 Recomendaciones

Para disponer de un mayor control de seguridad en los servidores de datos estos deben de estar constantemente monitoreados y actualizados con sus últimas versiones ya que corrigen problemas que pueden ser aprovechados por atacantes.

También se deben de mantener al día con las actualizaciones de los servicios que estos ejecutan, por ejemplo: web, ftp, correo, con actualizaciones que se pueden encontrar en los sitios web del fabricante.

Además es necesario establecer protocolos de seguridad para los usuarios novatos al momento de manipular un computador para evitar la infección de virus.

Mediante la implantación de una Honeynet se pueden capturar y analizar en un ambiente controlado los ataques informáticos que sufren los ordenadores dentro de la Universidad Técnica de Ambato y con esto se optimizara la seguridad informática en estos.

CAPÍTULO VI

PROPUESTA

6.1 Tema

Implantación de una Honeynet para la optimización de la seguridad de la información en los servidores de la Universidad Técnica de Ambato.

6.2 Datos informativos

Institución ejecutora: Universidad Técnica de Ambato.

Beneficiario: Universidad Técnica de Ambato.

Cuidad: Ambato

Dirección: Avenida de Los Chasquis, Ambato

Investigador: Mauro Darío Jijón Ramos

Tiempo: El presente proyecto será ejecutado entre el mes de Septiembre de 2012 hasta Febrero de 2013

Tutor: Ing. Luis Solís

6.3 Antecedentes

Una vez realizada la investigación previa se encontró que los servidores de datos de la Universidad Técnica de Ambato, para ser más precisos dentro del DISIR, constan con protocolos de seguridad que evitan que usuarios no deseados o atacantes ingresen a información de suma importancia, como a un registro de notas por ejemplo, sin disponer de un ambiente controlado para evaluar posibles amenazas de seguridad como un Honeypot o una Honeynet; mediante la implantación de una Honeynet se capturaran y analizaran los ataques informáticos que sufren los servidores de la Universidad Técnica de Ambato y se optimizará la seguridad informática en estos.

6.4 Justificación

El presente proyecto se lo ha realizado pensando en la seguridad tanto de servidores como de redes de datos dentro de la Universidad Técnica de Ambato ya que al alojar varios tipos de sistemas informáticos en sus servidores, por ejemplo: el utamático, estos son blancos seguros para que cualquier persona con cierto grado de conocimientos intente ganar acceso ilícito hacia estos; existen diversos sistemas de seguridad para redes y servidores como es el caso de Fortigate pero se da el caso de que no se llega a saber si en realidad se está teniendo un nivel de protección “confiable” ya que la mayoría de estos sistemas son cerrados y poco sabemos sobre que procesos se están realizando internamente, existen Honeypots y Honeynets ya desarrolladas pero que no se adaptan a las necesidades reales, es por eso que se optó por realizar una Honeynet partiendo desde cero esto nos permite profundizar en el funcionamiento de las mismas y además aprender acerca de cómo se ven afectados los diferentes sistemas operativos ante un ataque y ya

que al tratar con una Honeynet partiendo desde cero se pondrán en práctica todos los conocimientos adquiridos durante la carrera.

6.5 Objetivos

6.5.1 General

Implantar una Honeynet para la optimización de la seguridad de la información en los servidores de la Universidad Técnica de Ambato.

6.5.2 Específicos

Analizar los patrones de ataques informáticos dentro de la Universidad Técnica de Ambato mediante la utilización una Honeynet.

Realizar un análisis forense a los ataques capturados dentro de la Honeynet para comprobar la veracidad de los mismos.

Plantear una propuesta que permita desarrollar políticas de seguridad con el uso de una Honeynet que optimice la seguridad informática de los servidores de la Universidad Técnica de Ambato.

6.6 Factibilidad

Según el tipo de propuesta se debe tener en cuenta ciertos aspectos de viabilidad:

Política: La Universidad Técnica de Ambato tiene como política asegurar la información por lo cual es viable aplicar controles de seguridad informática.

Socio Cultural: Si hay un buen manejo de la información se minimizarán las vulnerabilidades y se ayudará a tratar la información de los docentes y estudiantes en forma ética y confidencial.

Tecnológica: La implementación de una Honeynet mejorara las condiciones de seguridad en los servidores de la Universidad Técnica de Ambato.

Ambiental: En la realización del presente proyecto no se afectará al medio ambiente.

Económico-financiera: El proyecto en el ámbito económico es factible de realizarlo ya que todas las herramientas de software que se utilizaran son libres por lo cual no se pagaran los costos de licencia.

Legal: El proyecto de investigación es viable porque está cumpliendo todas las leyes y normas del libre acceso a datos.

6.7 Fundamentación Científico Técnica

Honeypot

Para el diccionario informático alegsa(Internet, 21/10/11; 22/10/11; 13:05), extraído desde http://www.alegsa.com.ar/Dic/honeypot.php "un honeypot es una trampa para detectar, desviar o contrarrestar de alguna manera, los intentos de uso no autorizado de los sistemas de información.

Generalmente un honeypot puede ser una computadora, datos o un sitio de red que parecen ser parte de una red pero que en realidad están aislados, protegidos y monitorizados, y que parecen contener información o recursos que serían valiosos para los posibles atacantes.

Un honeypot es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas".

Honeynet

El Ing. Miguel Angel Martín Soto (Internet, 02/05/11; 29/04/11; 18:54), extraído desde https://sites.google.com/site/scmarinsotomiguelangel/6-aplicaciones

Argumenta que "Los Honeynet son un tipo especial de Honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes. Se usan equipos reales con sistemas operativos reales y corriendo aplicaciones reales.

Este tipo de Honeypots se usan principalmente para la investigación de nuevas técnicas de ataque y para comprobar el modus-operandi de los intrusos.

El concepto de Honeynet empezó en 1999 con Lance Spitzner, fundador del Proyecto Honeynet publicó un artículo:

"A Honeynet is a network of high interaction Honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discreetly regulated."

Lance Spitzner"

Ordenadores Virtuales

Según el blog de la Universidad Tecnica Particular de Loja (Internet, 25/11/11; 24/10/11; 14:50), extraído desde:

http://blogs.utpl.edu.ec/sistemasoperativos/files/2010/01/maquinas-virtuales2.pdf

da a conocer que “Una máquina virtual es un sistema operativo que funciona de forma "simulada", es decir, es como tener un ordenador dentro de un ordenador, pero funcionando de forma "virtual", es decir, en realidad no se tiene un ordenador dentro de tu ordenador, ya que eso es imposible, pero lo que hacen los programas como lo mencionado antes es simular que se tiene otro ordenador funcionando dentro del nuestro.

En realidad los ordenadores virtuales son eso: simulaciones de otros ordenadores pero en modo "soft", es decir, el programa simula que tiene una BIOS, una memoria, unas conexiones de red, puertos, discos duros, etc., pero todo de forma "simulada".

Y lo bueno que tienen estos ordenadores virtuales es que se puede instalar cualquier sistema operativo en ellas, incluso sistemas operativos diferentes al sistema operativo real, por ejemplo, supongamos que tenemos un Windows XP, dentro de ese XP podemos tener desde un Linux hasta un Windows 2003 Server pasando por un Windows Vista.

Cuando se instala un sistema operativo en una máquina virtual es como instalar el sistema operativo desde cero, incluso se puede formatear un disco, crear particiones, etc., todo igual que si fuera un ordenador normal y corriente.

Lo bueno de tener o usar ordenadores virtuales es que en realidad no es necesario tener más discos duros ni más CD o DVD, ya que todo es "simulado", se puede crear discos duros virtuales que en realidad son también "simulados", ya que en realidad son ficheros que el programa crea y en el que instala todo lo necesario.

Además de los discos simulados (o virtuales), también se puede usar cosas que ya se tiene en el equipo, por ejemplo, un CD o un DVD, la impresora, otro disco duro "real", etc.

También se puede "simular" cosas que no se tiene, por ejemplo una disquetera o incluso un CD o DVD, esto es útil cuando se quiere probar cosas que ya casi nadie usa.

Y la ventaja de usar los CD o DVD simulados es que se puede trabajar con "imágenes" como si fueran discos compactos reales. Esas imágenes son las que los propios programas de grabación crean, y que suelen tener extensiones como .iso o .img.

Cuando se indica la memoria a usar, siempre se debe disponer de esa memoria, además por supuesto de la que el programa "simulador" requiera, por regla general el programa "virtualizador" indica de cuanta memoria máxima (y recomendable) se puede asignar".

Nat y Puente (Bridge)

Nat

El repositorio de la Universidad Politécnica Salesiana Ecuador(Internet, 12/10/11; 15/10/11; 20:47), extraído desde:

http://dspace.ups.edu.ec/bitstream/123456789/158/3/Capitulo%202.pdf

argumenta que "Las siglas Nat significan Network Address Translation, o sea, Traducción de Dirección de Red y no es más que un mecanismo utilizado por routers IP para intercambiar paquetes entre dos rede que se asignan direcciones

incompatibles es decir, convierte en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la "conversación" del protocolo".

Modelo puente (bridge)

Según guia-ubuntu (Internet,21/10/11; 21/10/11;12:40), extraído desde http://www.guia-ubuntu.com/index.php?title=Puente_de_red " Es un dispositivo de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Interconecta dos segmentos de red, o divide una red en segmentos haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete. Un bridge conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red. Funciona a través de una tabla de direcciones MAC detectadas en cada segmento a que está conectado. Cuando detecta u nodo de uno de los segmentos está intentado transmitir datos a un nodo del otro, el Bridge copia la trama para la otra subred".

Sniffer

Alma Arroyo Zavaleta(Internet,21/10/11; 21/10/11;13:16), extraído desde http://www.academia.edu/3688661/1 argumenta que "Un sniffer es un programa de captura de las tramas de red.

Es algo común que, el medio de transmisión (cable coaxial, UTP, fibra óptica etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el sniffer le dice a la computadora que deje de ignorar todo el

tráfico no destinado al equipo y le ponga atención, esto es conocido como poner en estado "promiscuo" a la NIC (Network Interface Card).

En la actualidad la seguridad en las redes es de vital importancia, ya que toda la información que se transmite a través de éstas muchas veces puede ser utilizada para fines de lucro o realizar delitos electrónicos.

Una vez que la NIC está en este estado se necesitarán los privilegios administrativos o de root, de ésta manera la computadora será capaz de ver todos los datos transmitidos. Es entonces cuando el programa comienza a hacer una lectura de toda la información entrante al PC por la tarjeta de red. Con esto el sniffer conseguirá observar el equipo de origen, el equipo de destino, número de puerto, etc. en resumen puede ver la información intercambiada entre dos computadoras.

El uso que se les den a éste tipo de aplicaciones es algo importante de señalar, ya que gracias a ellos podemos ayudar a que nuestra Red tenga más seguridad, hacer pruebas y así poder tener un muy buen resultado, el problema viene cuando otros usuarios lo utilizan con fines de delitos electrónicos, ya que con éste tipo de herramientas se puede obtener información confidencial.

Los principales usos que se le pueden dar son:

Captura de contraseñas enviadas sin cifrar y nombres de usuario de la red. Esta capacidad es utilizada en muchas ocasiones para atacar sistemas.

Análisis de fallos para descubrir problemas en la red, tales como: ¿por qué el ordenador A no puede establecer una comunicación con el ordenador B?

Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.

Para los desarrolladores, en aplicaciones cliente-servidor. Les permite analizar la información real que se transmite por la red".

Además el sitio mundocisco.com(Internet,14/11/11; 16/11/11;14:10), extraído desde http://www.mundocisco.com/2009/08/que-es-un-sniffer.html amplia este tema argumentando lo siguiente " Algunos sniffers trabajan sólo con paquetes de TCP/IP, pero hay otros más sofisticados que son capaces de trabajar con un número más amplio de protocolos e incluso en niveles más bajos tal como el de las tramas del Ethernet. Algunos los más utilizados tenemos los siguientes:

Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

Ettercap, es un interceptor/sniffer/registrador para LANs con switch.Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing.

Kismet, es un sniffer, un husmeador de paquetes, y un sistema de detección de intrusiones para redes inalámbricas 802.11. Kismet funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización raw, y puede rastrear tráfico 802.11b, 802.11a y 802.11g. El programa corre bajo Linux, FreeBSD, NetBSD, OpenBSD, y Mac OS X. El cliente puede también funcionar en Windows, aunque la única fuente entrante de paquetes compatible es otra sonda.

TCPDUMP, es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado.

Un sniffer puede ser de gran utilidad en la administración de una red, con fines de seguridad y funcionalidad, pero hay que tomar en cuenta de que es una herramienta que puede ser de doble filo, ya que algún usuario puede utilizarla con un fin no adecuado y pueda tomar ventaja de esto.

Es importante conocer el funcionamiento de estas aplicaciones para en un dado caso podamos utilizarlas en un determinada circunstancia".

Sistema de detección de intrusiones

La Universidad de Valencia (Internet,25/10/11; 25/10/11;14:11), extraído desde www.uv.es/~montanan/redes/trabajos/IDSs.doc argumenta que

"Los IDS se dividen en 2 grupos:

Sistema de detección de intrusiones de red (N-IDS)

Sistema de detección de intrusiones de red, se encarga de monitorear la seguridad dentro de la red.

Sistema de detección de intrusiones de host (H-IDS)

Sistema de detección de intrusiones de host, se encarga de monitorear la seguridad dentro del host".

Informática forense

Para el sitio Informática Forense (Internet,21/11/11; 21/11/11;13:41), extraído desde http://www.informaticaforense.com.ar/ "La Informática Forense se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

También puede servir para informar adecuadamente al cliente acerca de las posibilidades reales de la evidencia existente o supuesta.

La necesidad de este servicio se torna evidente desde el momento en que la enorme mayoría de la información generada está almacenada por medios electrónicos.

En informática forense hablamos ya no sólo de recuperación de información sino de descubrimiento de información dado que no hubo necesariamente una falla del dispositivo ni un error humano sino una actividad subrepticia para borrar, adulterar u ocultar información. Es por lo tanto esperable que el mismo hecho de esta adulteración pase desapercibido.

La informática forense apela a nuestra máxima aptitud dado que enfrentamos desde casos en que el dispositivo fue borrado, golpeado y dañado físicamente hasta ligeras alteraciones de información que pueden constituir un crimen".

Ataque DDOS

El sitio gitsinformatica.com (Internet,24/12/12; 26/12/12;15:11), extraído desde http://www.gitsinformatica.com/ciberataques.html argumenta que: "DDoS son las siglas de Distributed Denial of Service. La traducción es "ataque distribuido denegación de servicio", y traducido de nuevo significa que se ataca al servidor desde muchos ordenadores para que deje de funcionar.

Un ataque DoS puede ser perpetrado de varias formas. Aunque básicamente consisten en:

- Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
- Alteración de información de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.

Se puede modificar para que sea más efectivo. Por ejemplo, se pueden enviar los datos muy lentamente haciendo que el servidor consuma más recursos por cada conexión (Slow Read es un ejemplo de ataque de este tipo), o alterar los paquetes para que el servidor se quede esperando indefinidamente una respuesta de una IP falsa.

¿Cómo afecta un DDoS a una web?

Depende del ataque y del servidor. Los servidores se pueden proteger contra estos ataques con filtros que rechacen los paquetes mal formados o modificados con IPs falsas, de forma que al servidor sólo le llegan los paquetes legítimos. Por supuesto, las medidas no son infalibles y el servidor siempre puede acabar saturado si el ataque es suficientemente masivo y está bien preparado.

Tomemos el Gráfico como referencia. El tráfico durante el ataque (en verde) es tan grande que apenas se aprecia el tráfico normal del servidor.

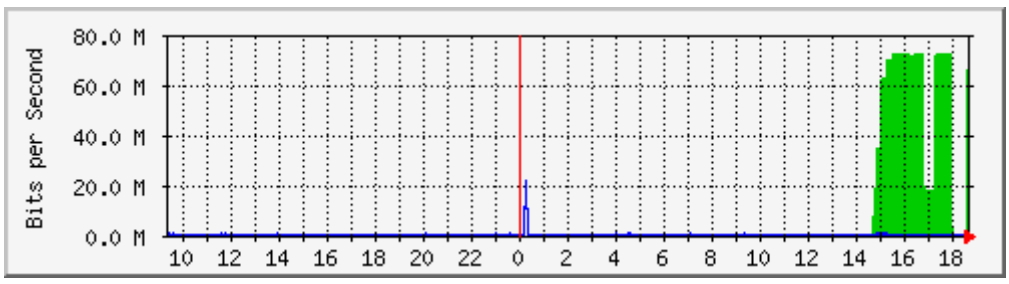


Gráfico 6.1 Tráfico de un servidor con ataque DDOS

Fuente: http://www.gitsinformatica.com/ciberataques.html

¿Y qué ocurre cuando el servidor se satura? Simplemente deja de estar disponible durante un tiempo hasta que el ataque para. Es muy difícil que se produzcan daños físicos en el servidor. Además, el DDoS por sí sólo no permite entrar en el

servidor: para ello es necesario aprovechar alguna vulnerabilidad, y eso no es nada fácil.

Dependiendo del tipo de web esto puede ser una catástrofe o no. Si la web genera dinero (venta online, publicidad), el propietario deja de ganar dinero mientras esa web está caída".

6.8 Implantación Honeynet

Para proceder con la Implantación de la Honeynet procederemos con las siguientes fases:

- Fase de Planificación
- Fase de Diseño
- Fase de Implementación

6.8.1 Fase de Planificación

6.8.1.1 Ubicación Honeynet

El presente proyecto de tesis se realizó como complemento al proyecto de investigación "EVALUACIÓN DE LAS SEGURIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA DIRECCIÓN DE SISTEMAS INFORMÁTICOS Y REDES DE TELECOMUNICACIÓN DE LA UNIVERSIDAD TÉCNICA DE AMBATO POR MEDIO DE PRUEBAS DE INTRUSIÓN" **(Ver Anexo 4)** Realizado por el Ing. Luis Solís, tutor del actual proyecto de tesis, que designo al estudiante investigador la implantación de la Honeynet dentro de las oficinas del UOCENIC ubicadas en la Facultad de

Ingeniería en Sistemas (Predios Huachi) para su posterior implantación en las oficinas del DISIR (Predios Ingahurco).

6.8.1.2 Análisis de recursos y componentes

En esta fase estableceremos las herramientas necesarias a utilizar para la implementación de la Honeynet, como ya se explicó en un apartado anterior las herramientas que utilizaremos son de software libre así que no es necesaria la adquisición de licencias.

Como se dispone de únicamente de una máquina para trabajar se utilizara software de virtualización para emular las maquinas necesarias para la implantación de la Honeynet, es decir la Honeynet será virtual facilitando la portabilidad y disminuyendo costos.

A continuación debemos seleccionar las herramientas que nos ayudaran en el monitoreo de las maquinas trampa de la Honeynet, para esto nos ayudaremos de los IDS(Sistema de detección de intrusiones) los cuales se encargan de monitorear el tráfico de la red, detectando y notificando de actividades sospechosas o anormales sin hacer notar al posible atacante.

6.8.1.3 Fase de Diseño

Una vez descritas las herramientas a utilizar y su funcionalidad seleccionaremos las que más se acoplen a nuestra necesidad, a continuación detallaremos los recursos que tenemos y los componentes a utilizar.

PC

En esta pc se instalara como servidor Centos que se encargara de recolectar la información enviada por los otros ordenadores las cuales son un Windows XP sin service pack para facilitar el ataque, y una maquina con ubuntu Las cuales servirán como ‘cebo’ para los ataques.

Software de virtualización

Utilizaremos el software de virtualización “Oracle VM VirtualBox” el cual es de licencia libre; nos permite emular varios sistemas operativos a la vez, consta de herramientas que nos facilitaran el proceso del manejo y mantenimiento de los ordenadores virtuales que formaran parte de la Honeynet.

IDS de red

Para el IDS de red se consideró como mejor alternativa a Snort, el cual también es de licencia libre que consta muchas características, como característica especial de este IDS de red podemos guardar los logs que se van generando directamente en una base de datos, lo cual nos facilitara el proceso de revisión de ellos ya que de manera predeterminada se almacenan en ficheros individuales; para esto utilizaremos una base de datos Mysql para guardar los logs en forma que sea fácil para el usuario leer los mismos; además para poder mostrar todos estos datos almacenados requerimos de la herramienta Snort Report proporcionada por el mismo Snort que requiere de un servidor web en php, se utilizara el servidor apache Este servidor se ubicara en la maquina centos .

IDS de host

Para el IDS de host se consideró utilizar el software ossec el cual es compatible con varios sistemas operativos (Windows, Linux y Mac) ajustándose perfectamente a este proyecto. Ya que en su sitio web nos provee del instalador adecuado para cada pc. En su sitio web http://www.ossec.net/ en la sección descargas encontraremos sus respectivos instaladores.

6.8.1.4 Fase de Implementación

En esta fase procederemos a detallar las herramientas que se van a utilizar para la implantación de la Honeynet, también se indicarán los pasos necesarios para la instalación de cada máquina virtual y los IDS a utilizar.

6.8.1.5 Diseño Honeynet

Para esta Honeynet se utiliza el software de virtualización “Oracle VM VirtualBox” dentro del PC físico y constara de 3 ordenadores virtuales:

Un servidor Centos, que se encarará de recopilar informes de los otros 2 pc’s clientes, con 2 IDS:

- IDS de red: Snort

- IDS host: Ossec

Gráfico 6.2 Servidor Centos

Autor: Mauro Jijón

Un ordenador cliente con el sistema operativo Ubuntu, que servirá como trampa para la Honeynet, con el cliente del IDS de host Ossec.

Gráfico 6.3 Cliente Ubuntu

Autor: Mauro Jijón

Un ordenador cliente con Windows XP (sin service pack), que servirá como trampa para la Honeynet, con el cliente del IDS de host Ossec.

Gráfico 6.4 Cliente Windows

Autor: Mauro Jijón

6.8.1.6 Detalles técnicos

Ordenador principal donde se van a instalar las máquinas virtuales.

Sistema Operativo	Windows 7
Capacidad disco duro	720 Gb
Memoria RAM	8Gb.
IP	192.168.30.8
Servidor proxy	192.168.124.13:8080 192.168.30.2:3333
Usuario*:	“Shadowafox”

Tabla 6.1 Detalles técnicos ordenador principal

Autor: Mauro Jijón

*Para asegurar el tráfico dentro de la Honeynet se utilizó el usuario que ya estuvo asignado a ese ordenador.

Máquinas Virtuales

Sistema Operativo	Centos reléase 5.8(Final)	Ubuntu 12.04 LTS	Windows XP Profesional Versión 2002
Capacidad disco duro	8 Gb	4 Gb	4 Gb
Memoria RAM	720Mb.	720Mb.	512Mb.
IP	192.168.30.30	192.168.30.31	192.168.30.29
Software instalado:	Instalación como servidor con los paquetes que vienen por defecto. Ossec(Servidor) SNORT	Instalación normal como cliente, paquetes por defecto. Ossec(Cliente)	Instalación normal, programas por defecto. Ossec(Cliente)

Tabla 6.2 Detalles técnicos máquinas virtuales

Autor: Mauro Jijón

6.8.1.7 Instalación de Virtualbox para Windows

El proceso de instalación es similar a cualquier programa para Windows, así que resumiremos el tutorial de instalación.

1.- Nos vamos a la sección de descargas de VirtualBox en la dirección http://www.virtualbox.org/wiki/Downloads y seleccionamos la opción de descarga para Windows.

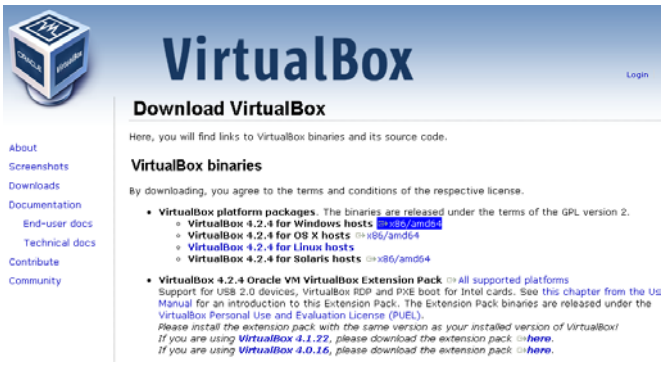


Gráfico 6.5 Sitio web de VirtualBox

Autor: Mauro Jijón

2.- Descargamos el archivo y procedemos con la instalación.

Gráfico 6.6 Instalación de VirtualBox

En una parte de la instalación se nos advertirá que las interfaces de red serán reiniciadas.

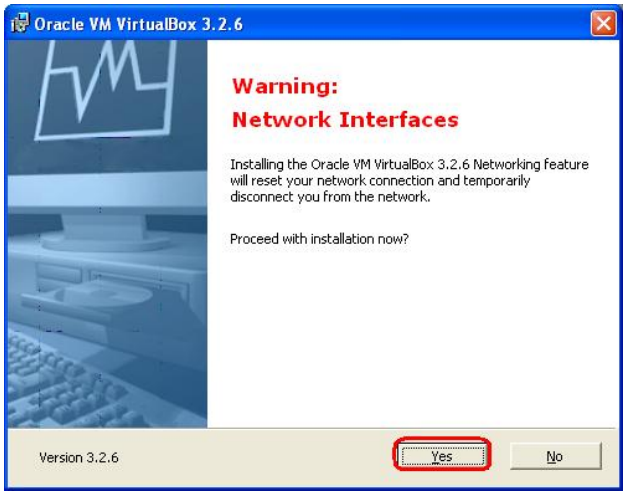


Gráfico 6.7 Virtualbox agregando un nuevo dispositivo de red

Autor: Mauro Jijón

3.- Después se procederá a instalar los controladores de red para los ordenadores virtuales, un mensaje similar al siguiente aparecerá.

Gráfico 6.8 Instalación de nuevo dispositivo de red

Seleccionamos continuar en los mensajes que aparezcan y culminamos con la instalación.

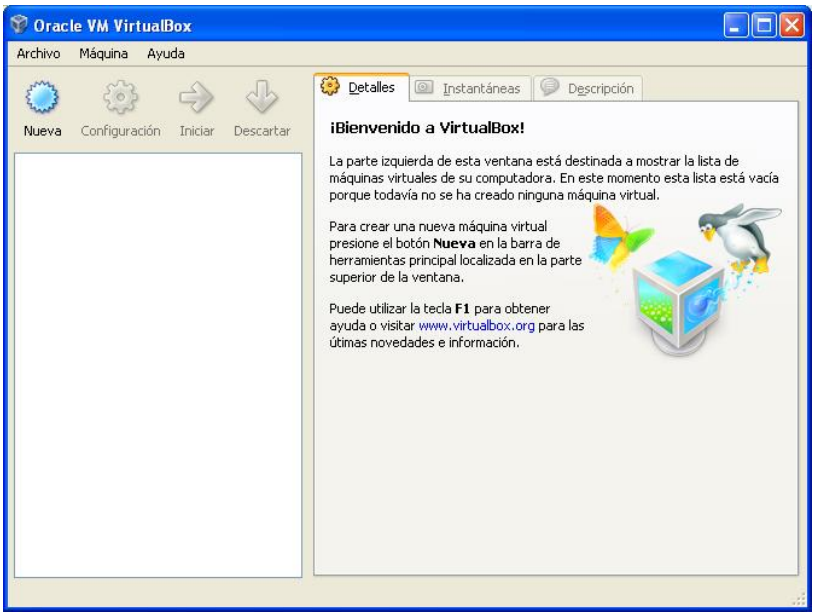


Gráfico 6.9 Interfaz de VirtualBox

Autor: Mauro Jijón

6.8.1.8 Instalación servidor Centos

Configurando Centos como servidor web

Como servidor Web usaremos Apache, para la base de datos Mysql y como lenguaje de programación PHP5.

Para la instalación utilizaremos el comando yum para bajar de los repositorios de Centos los paquetes e instalarlos automáticamente.

El primer paso es instalar Mysql mediante el siguiente comando:

```
yum install mysql mysql-server
```

Instalamos Apache con

```
yum install httpd
```

Ahora instalamos PHP y lo enlazamos a Apache:

```
yum install php
```

Agregamos la vinculación de mysql a php usando el siguiente comando

```
yum install php-mysql
```

Para probar que PHP funciona correctamente Generamos un archivo de prueba:

```
touch /var/www/html/info.php

echo '<?php phpinfo(); ?>' > /var/www/html/info.php
```

Ahora configuramos los servicios para que se inicien automáticamente:

```
chkconfig --levels 235 mysqld on

chkconfig --levels 235 httpd on
```

Iniciamos los servicios y comprobamos su funcionamiento:

```
service mysqld start

service httpd start
```

Accedemos a la dirección local y abrimos el archivo de prueba que creamos:

```
http://127.0.0.1/info.php
```

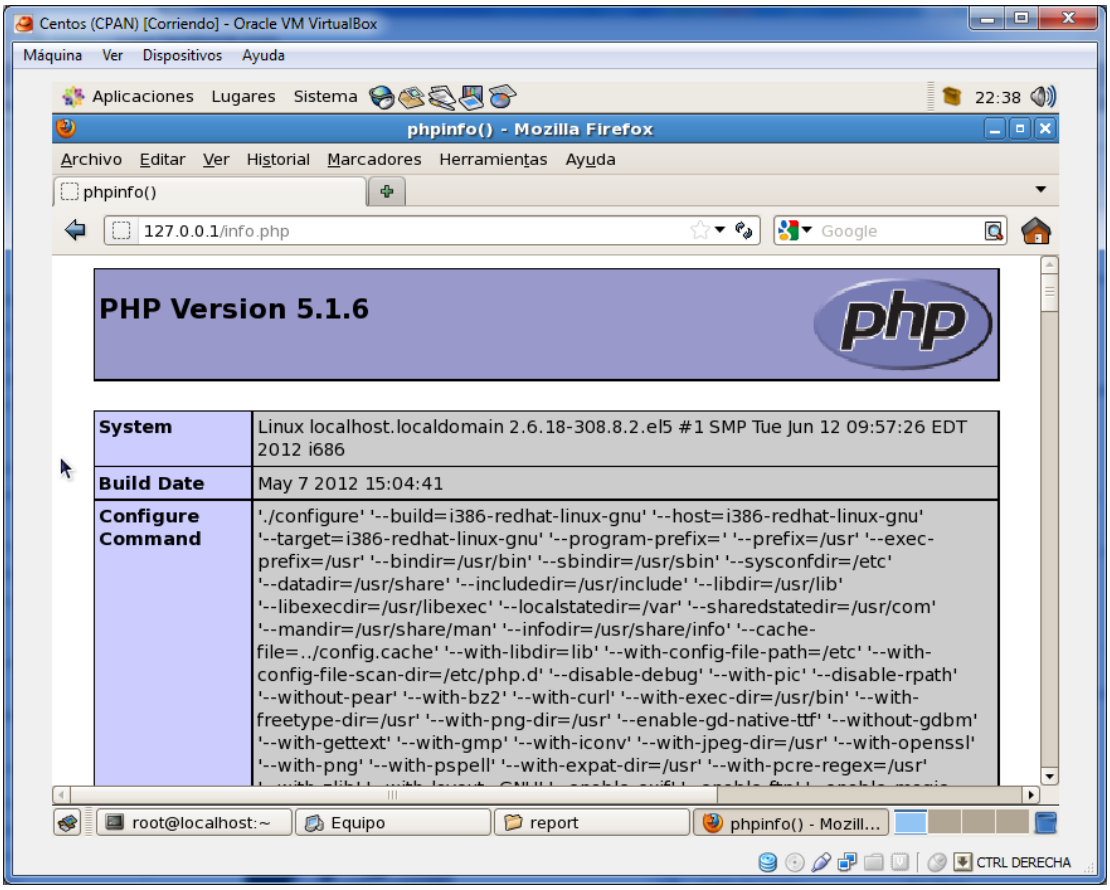


Gráfico 6.10 Servidor PHP levantado

Fuente: Honeynet

IDS de red Snort

El IDS de red únicamente será instalado en el servidor debido a que se encarga de monitorear toda la red y guardar la información en el mismo.

Instalación de Snort en servidor Centos

Para proceder con la instalación de Snort, primero nos descargaremos todos los paquetes necesarios para su correcto funcionamiento.

Descargando paquetes necesarios:

LIBNET

Descargar libnet-1.0.2a.tar.gz de:

http://www.filewatcher.com/m/libnet-1.0.2a.tar.gz.140191.0.0.html

LIBDNET

Descargar libdnet de:

http://code.google.com/p/libdnet/downloads/detail?name=libdnet-1.12.tgz&can=2&q=.

LIBPCAP

Descargar libpcap de http://tcpdump.org.

NBTSCAN

Descargar nbtscan de http://www.unixwiz.net/tools/nbtscan-source-1.0.35.tgz.

JPGRAPH

Descargar JpGraph de: http://hem.bredband.net/jpgraph/jpgraph-1.27.1.tar.gz

DAQ

Descargar de http://www.snort.org/snort-downloads

SNORT

Descargar la última versión de Snort desde: http://snort.org; también tenemos que descargarnos las ultimas reglas, para esto tenemos que registrarnos.

SNORT REPORT

Descargar Snort Report de http://www.symmetrixtech.com/ids/snortreport-1.3.1.tar.gz

6.8.1.9 Instalando Snort

A continuación procederemos con la instalación de los paquetes necesarios para el correcto funcionamiento de Snort

Instalación LIBNET

Descomprimimos el paquete libnet-1.0.2a.tar.gz y procedemos con su instalación con los siguientes comandos:

```
cd /usr/local
tar zxvf /home/usuario/Downloads/libnet-1.0.2a.tar.gz
cd Libnet-1.0.2a
./configure && make && make install
```

Instalación LIBDNET

```
cd /usr/local
tar zxvf /home/bubba/libdnet-1.12.tgz
cd libdnet-1.12
./configure && make && make install
```

Instalación LIBCAP

Por defecto CENTOS viene instalado con LIBCAP pero esta versión es desactualizada y causara problemas de compatibilidad con Snort.

```
cd /usr/local
tar zxvf /home/bubba/libpcap-1.0.0.tar.gz
cd libpcap-1.0.0
./configure && make && make install
```

Instalación NBTSCAN

Para la herramienta Snortreport requerimos los paquetes nbtscan y nmap. El paquete nmap ya viene instalado y trabaja correctamente con Snort, así que procederemos con la instalación del paquete nbtscan

```
cd /usr/local
mkdir nbtscan
cd nbtscan
tar zxvf /home/bubba/nbtscan-1-3-1.tar.gz
make
```

Instalación DAQ

```
cd /usr/local
tar zxvf /home/bubba/daq-0.6.1.tar.gz
cd daq-0.6.1
./configure && make && make install
```

Una vez instalado los paquetes necesarios procedemos con la instalación de SNORT, se sigue el mismo proceso que se realizó anteriormente:

```
cd /usr/local
tar zxvf /home/bubba/snort-2.9.1.tar.gz
```

```
cd snort-2.9.1
./configure && make && make install
```

6.9 Configurando Snort

Antes de iniciar Snort se tienen que configurar varios parámetros, como los directorios donde se encuentran instalados varios componentes, obteniendo las últimas reglas y creando usuarios.

6.9.1 Descargando las últimas reglas de seguridad para SNORT

Las reglas VRT (Sourcefire Vulnerability Research Team), son las reglas que desarrolla el equipo de soporte de Snort. Hay tres tipos de reglas VRT que podremos encontrar en el portal www.snort.org.

- Reglas para suscriptores. Es decir, de pago. Permanentemente actualizado.
- Reglas para usuarios registrados (basta con crearse una cuenta).
- Reglas disponibles para usuarios no registrados. Muy desactualizadas.

Por otra parte, hay un grupo de reglas de la comunidad. Son reglas que gente de todo el mundo va desarrollando y envía a Snort para que las publiquen.

Nos dirigimos hasta el sitio web de Snort http://www.snort.org pero antes nos registramos en el sitio.

Gráfico 6.11 Sitio web de Snort

Fuente: http://www.snort.org

Vamos a https://www.snort.org/signup y nos registramos como en cualquier sitio, tenemos que dar un correo real ya que se enviara una confirmación a dicho correo.

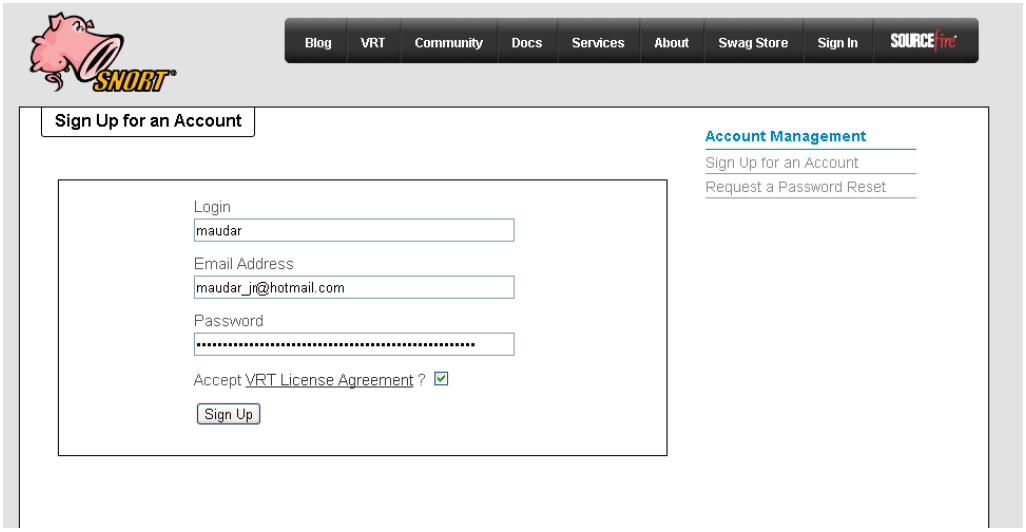


Gráfico 6.12 Creación de cuenta en sitio web de Snort

Fuente: http://www.snort.org

Iniciamos sesión una vez confirmada la cuenta:

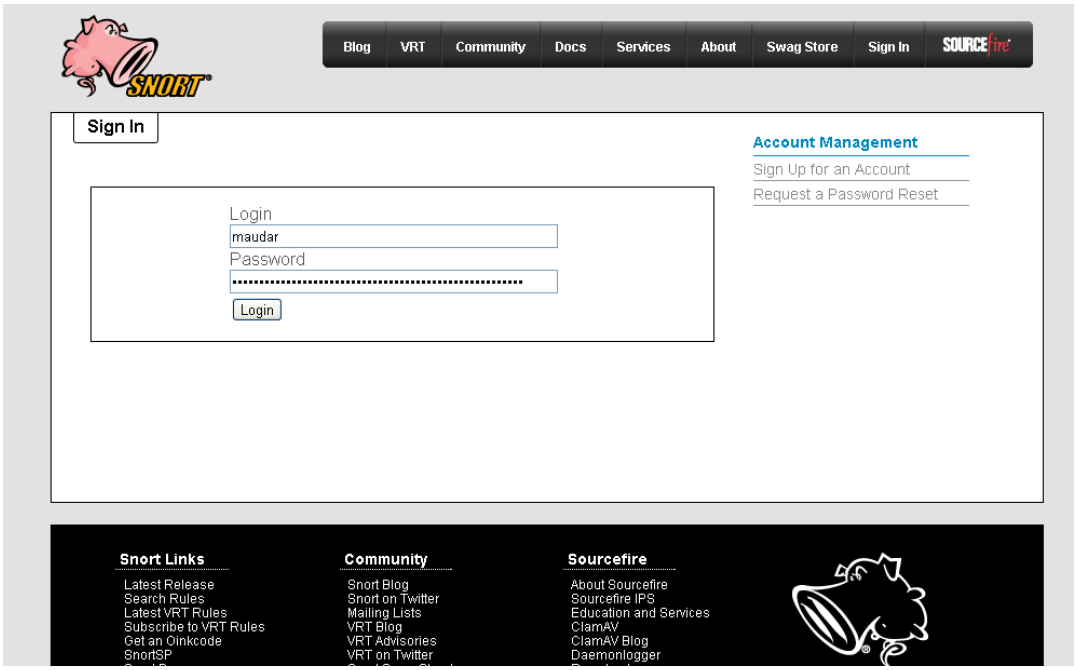


Gráfico 6.13 Inicio de sesión

Fuente: https://www.snort.org/login

Una vez iniciada sesión podemos descargar las últimas reglas:

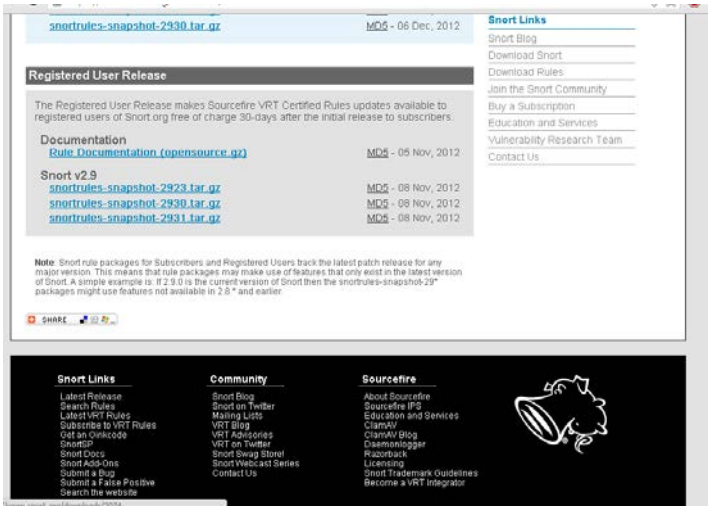


Gráfico 6.14 Reglas de Snort

En la parte inferior en la sección “Registered User Release” podemos descargarnos las últimas reglas, únicamente damos click y empezara la descarga.

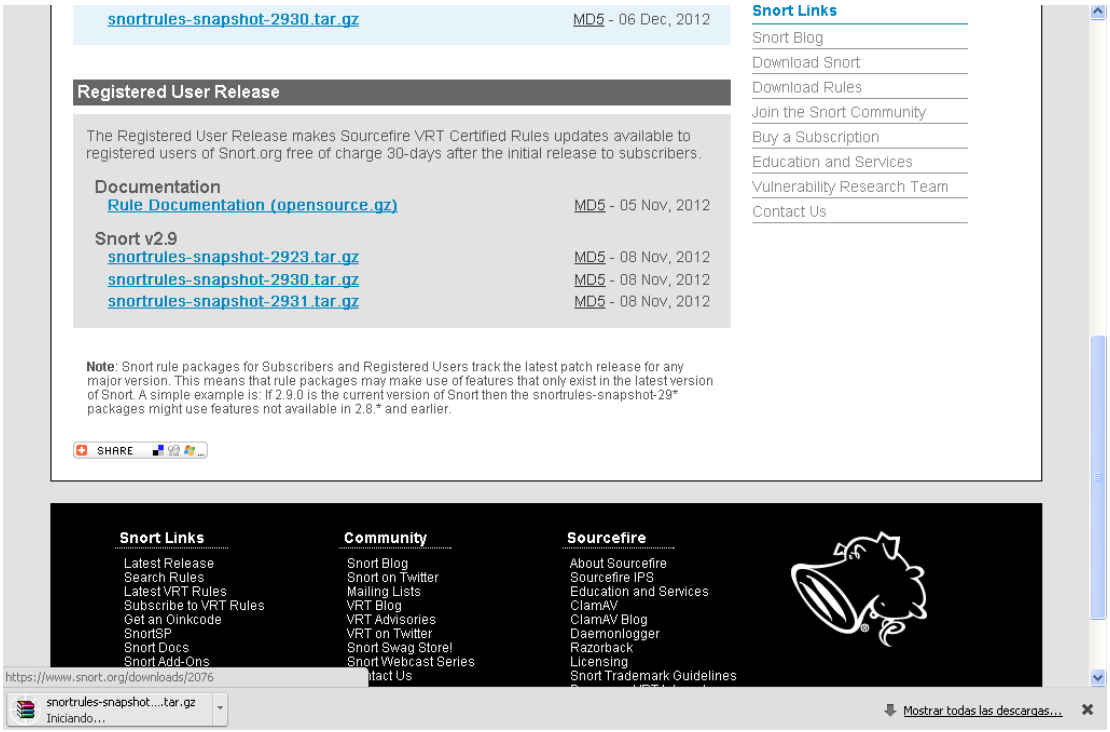


Gráfico 6.15 Descarga de ultimas reglas de Snort

Fuente: https://www.snort.org/snort-rules/?

Una vez descargado el archivo lo movemos al directorio de SNORT y lo descomprimimos, usamos los comandos:

```
mkdir /etc/snort

mkdir /var/log/snort

cd /etc/snort

tar zxvf /home/user/snortrules-snapshot.tar.gz -C /etc/snort

cp etc/* /etc/snort
```

Creación del usuario Snort

En esta parte crearemos el usuario Snort el cual se encargara del uso y la manipulación de archivos, esto por cuestiones de seguridad

```
groupadd snort
useradd -g snort snort
chown snort:snort /var/log/snort
```

Copiando reglas descargadas a Snort

```
touch /var/log/snort/alert
chown snort:snort /var/log/snort/alert
chmod 600 /var/log/snort/alert
mkdir /usr/local/lib/snort_dynamicrules
cp /etc/snort/so_rules/precompiled/Centos*/i386/2.9.1.0/*.so /usr/local/
lib/snort_dynamicrules
cat /etc/snort/so_rules/*.rules >> /etc/snort/rules/so-rules.rules
```

Editando el archivo snort.conf

En el archivo “snort.conf” definimos los parámetros de inicialización de Snort.

Snort tiene los siguientes modos de ejecución:

Sniffer mode. Lee todos los paquetes de la red y los muestra en consola.

Packet loger mode. Almacena los paquetes de la red en disco.

Network Intrussion Detection System (NIDS). Es la opción más completa y configurable. Permite analizar el tráfico de la red en busca de normas (rules) establecidas por el usuario, y permite realizar operaciones sobre los datos.

Inline Mode. Recibe los paquetes de iptables desde libpcap y, dependiendo de las normas de snort, iptables realiza una determinada acción.

Los modos de ejecución de Snort se activan dependiendo de los parámetros que le envía al programa. En la siguiente tabla se puede ver un resumen de los parámetros más importantes que puede utilizar en Snort.

Modos de ejecución en Snort

Activa los modos de ejecución			
-v	Sniffer	Muestra en pantalla la dirección IP y las cabeceras TCP/UDP/ICMP. Pone snort en modo sniffer	snort –v
-l	Packet loger	Sirve para especificar el directorio donde se almacenarán los ficheros de log generados por snort.	snort –l /etc/snort/log
-c	NIDS	Se utiliza para especificar	snort –dev –c

		el directorio del archivo de configuración snort.conf.	/etc/snort/snort.conf
Permite indicar el tipo de registro			
-b	Indica logging en modo binario. El formato binario es también conocido como TCPDump. El formato binario hace que la información de los paquetes vaya más rápido debido a que Snort no tiene que traducir al formato entendible por los humanos de forma inmediata.		snort -l /etc/snort /log –b Analiza el tráfico almacenando los log en el directorio /etc/snort/log en formato binario.
-L	Sirve para especificar un archivo de log binario.		snort -b -L {log-file} Loguea el paquete binario especificado en log-file.
-r	Procesa un archivo de log grabado en modo binario.		snort -dv -r packet.log Lee del fichero binario packet.log.

Tabla 6.3 Parámetros de Snort

Fuente: http://www.adminso.es/index.php/SNORT-Modos_de_ejecuci%C3%B3n

Se edita el archivo snort.conf, ubicado en /etc/snort/snort.conf

- Encontrar la variable RULE_PATH y cambiar a /etc/snort/rules
- Encontrar la variable PREPROC_RULE_PATH y cambiar a /etc/snort/preproc_rules
- Encontrar la variable SO_RULE_PATH y cambiar a /etc/snort/so_rules
- Encontrar el campo unified2, descomentar la línea y cambiar ‘merged.log’ a ‘snort.log’ también borrar la opción que dice nostamp. esta es una parte clave debido a que por lo general ocasiona problemas con el complemento Barnyard2 al intentar leer los logs. La línea a cambiar debe tener el siguiente aspecto:

```
output unified2: filename snort.log, limit 128
```

6.9.2 Base de datos MySQL

Con la base de datos MySQL nos ayudaremos para guardar en forma ordenada los logs que va generando SNORT y presentarnos en un formato más legible para el usuario complementándose con la herramienta SNORT REPORT.

En la terminal ejecutamos los siguientes comandos:

```
mysql
SET PASSWORD FOR root@localhost=PASSWORD(‘password’);
create database snort;
grant ALL PRIVILEGES on snort.* to snort@localhost with GRANT option;
SET PASSWORD FOR snort@localhost=PASSWORD(‘password’);
exit
```

```
cd /usr/local/snort-2.9.1/schemas

mysql -p < create_mysql snort
```

Revisamos que la base de datos se haya creado correctamente

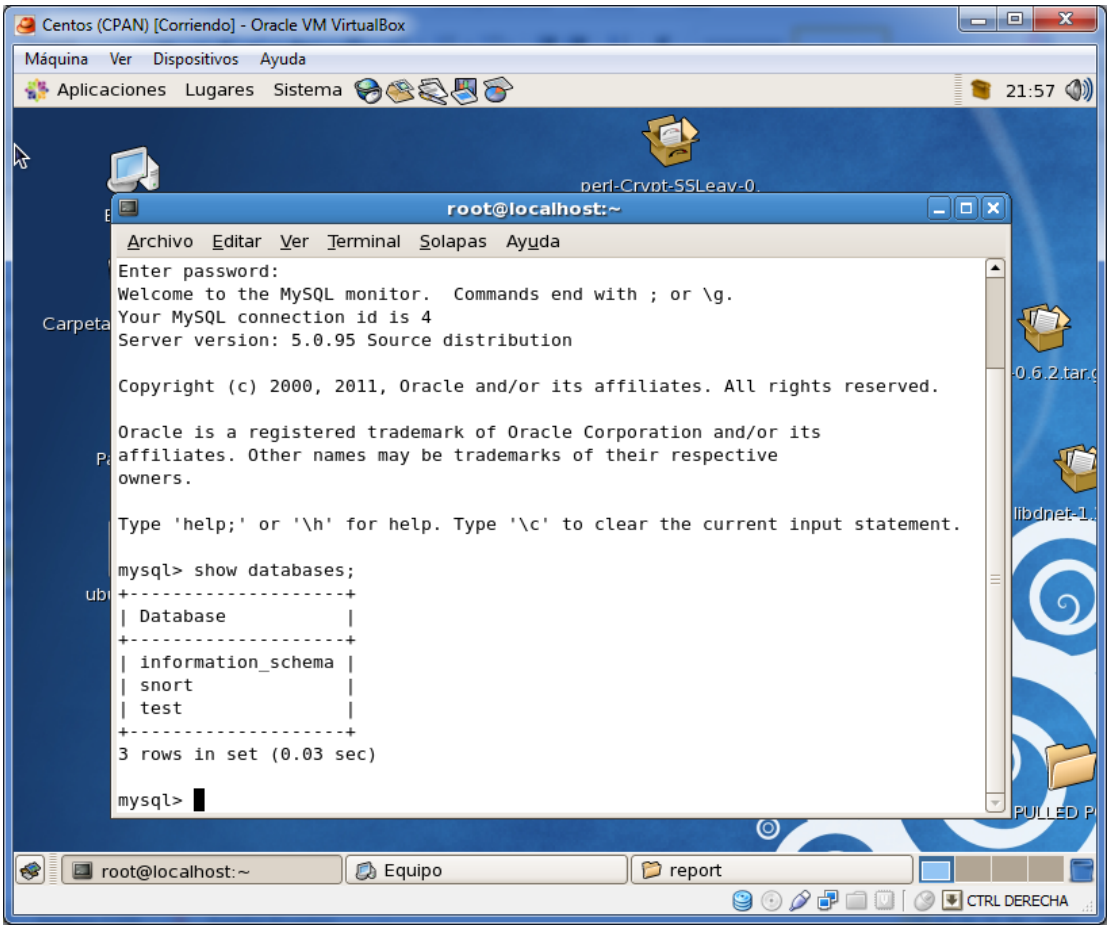


Gráfico 6.16 Creación de la base de datos Snort

Fuente: Honeynet

```
mysql -p

SHOW DATABASES;

use snort;

SHOW TABLES;
```

```
exit;
```

6.9.3 Snort Report

Esta herramienta se encargara de mostrar los datos almacenados en un formato web de fácil administración.

Descargamos desde el sitio web:

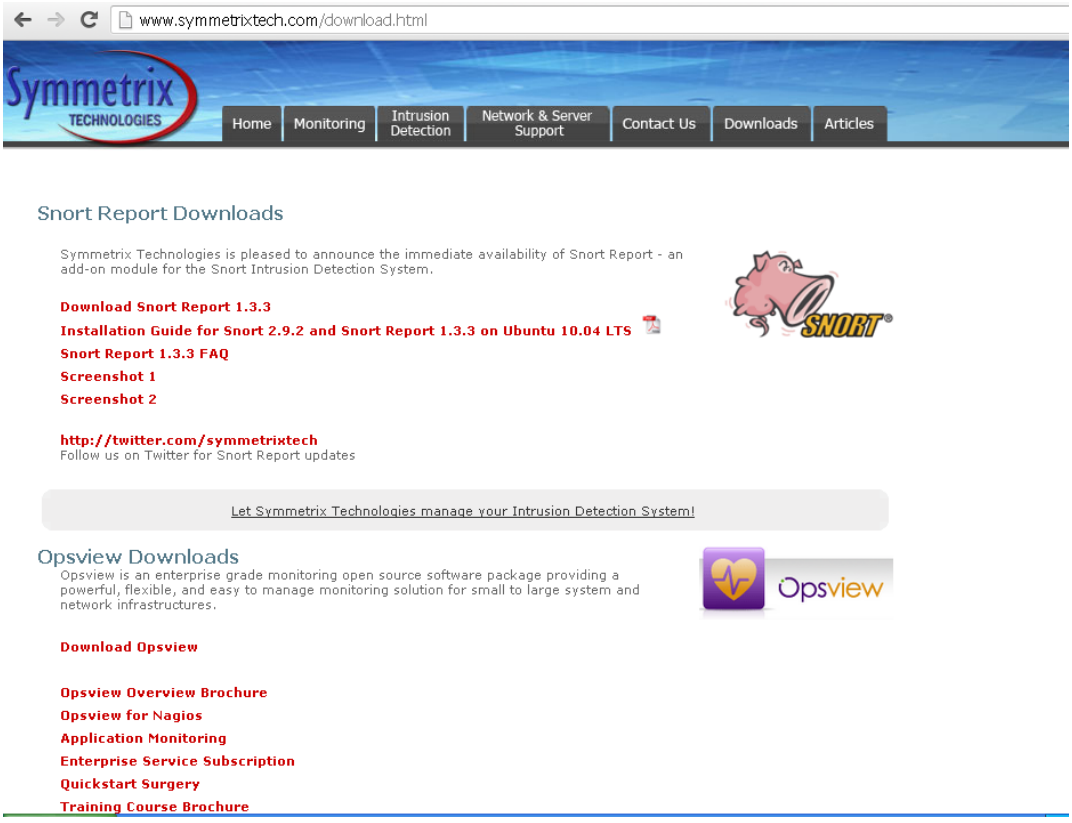


Gráfico 6.17 Sitio Web de Snort Report

Fuente: http://www.symmetrixtech.com/download.html

```
cd /var/www/html

tar zxvf /home/user/snortreport.tar.gz
```

```
cd snortreport

NANO srconf.php
```

- Encontrar el valor $pass y cambiar el valor YOURPASS a la contraseña asignada a la base de datos de SNORT.
- Encontrar el valor JPGRAPH_PATH y cambiar a ("JPGRAPH_PATH", "../jpgraph/src/");
- Encontrar el valor NMAP_PATH y cambiar a define("NMAP_PATH", "/usr/bin/nmap -v");
- y cambiar la línea NBTSCAN_PATH a: define("NBTSCAN_PATH", "/usr/local/nbtscan/nbtscan

6.9.4 Instalación de Barnyard

Barnyard ayuda en el procesamiento de datos de SNORT haciendo que este consuma menos recursos al procesar paquetes.

En entornos en los que un IDS Snort tiene que procesar una gran cantidad de tráfico es muy posible que su rendimiento se vea afectado y acabe descartando paquetes.

Esto es debido a que Snort no procesa el siguiente paquete hasta que no termina de escribir la alerta en la base de datos.

Para estos casos se puede configurar Snort (/etc/snort/snort.conf) para que escriba las alertas en un fichero local en lugar de hacerlo directamente en red:

```
output unified2: filename snort.log, limit=128
```

Con esta línea diremos a Snort que escriba las alertas en un fichero con nomenclatura base snort.log. (el. snort.log.1245910233); con un tamaño máximo de 128MB.

Se trata del formato unified2, un formato binario optimizado que permitirá a nuestro querido "cerdito" generar alertas más rápidamente.

Pero si tenemos las alertas en un fichero local, ¿cómo las escribimos entonces en la base de datos? Para esta tarea tenemos Barnyard2 (en español "corral"), un intérprete open source de los ficheros de salida en formato unified2.

Nos dirigimos al sitio y descargamos barnyard2

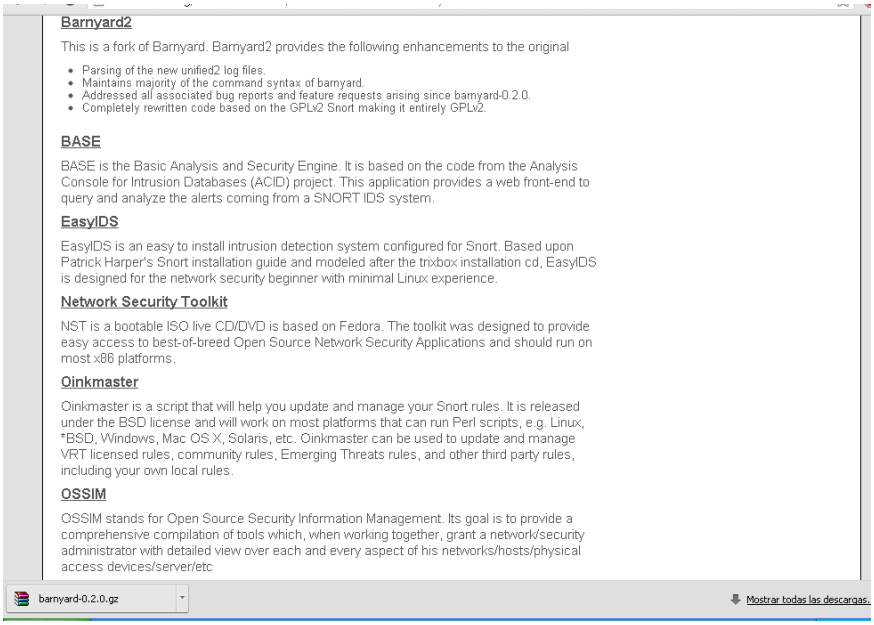


Gráfico 6.18 Sitio Web de Barnyard

Fuente: http://www.snort.org/snort-downloads/additional-downloads#barnyard2

```
tar zxvf /home/user/barnyard2-1.9.tar.gz

cd barnyard2-1.9
```

```
./configure --with-mysql &&make && make install

cp etc/barnyard2.conf /etc/snort
```

Configurando Barnyard

Editamos el archivo /etc/snort/barnyard2.conf

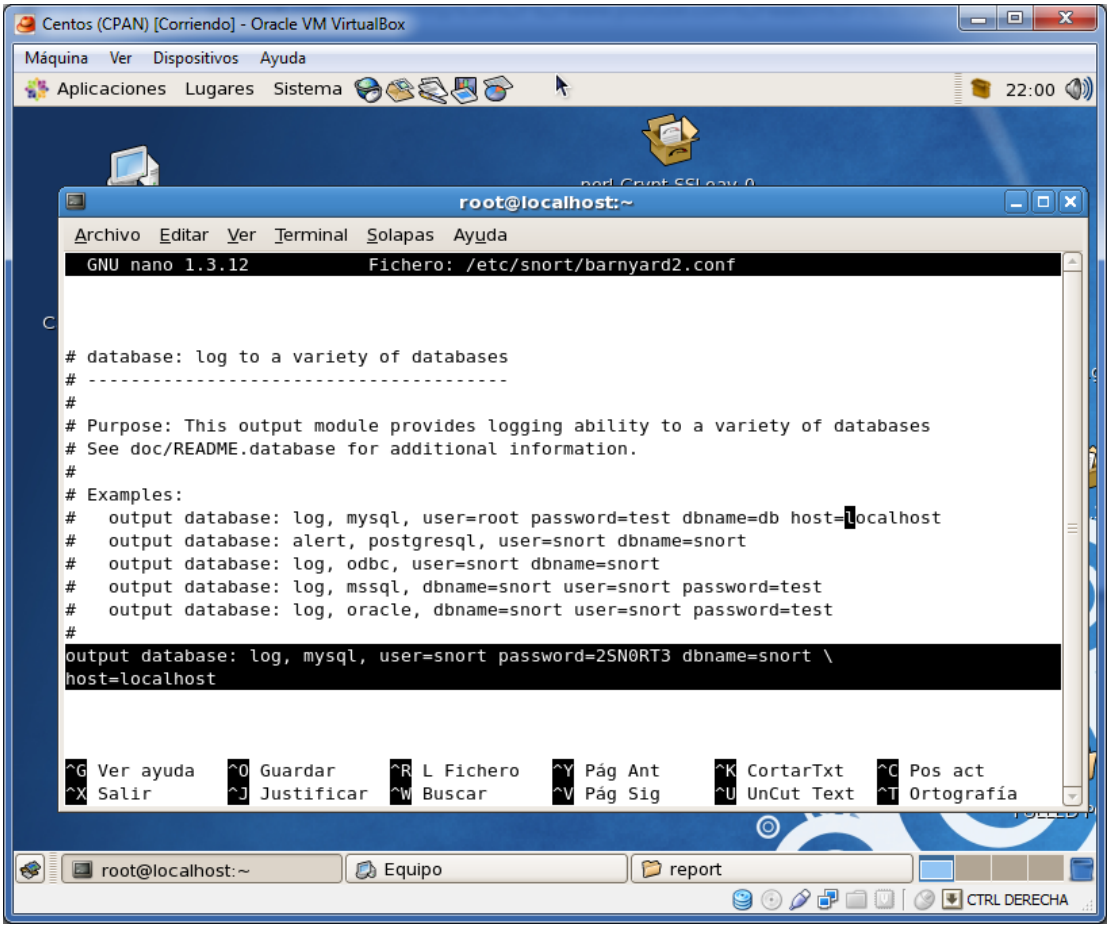


Gráfico 6.19 Archivo de configuración de Barnyard

Fuente: Honeynet

- Buscamos la línea “config hostname” y reemplazamos “thor” por “localhost”

- Buscamos la línea “config interface” y revisamos que el valor sea eth0 que es el dispositivo de red que estamos utilizando en este caso.
- Comentamos todos los “output methods” hasta llegar a “database” y editamos la línea mysql de la siguiente forma:

“output database: log, mysql, user=snort password=password dbname=snort host=localhost”

6.10 Inicializando Snort y Barnyard

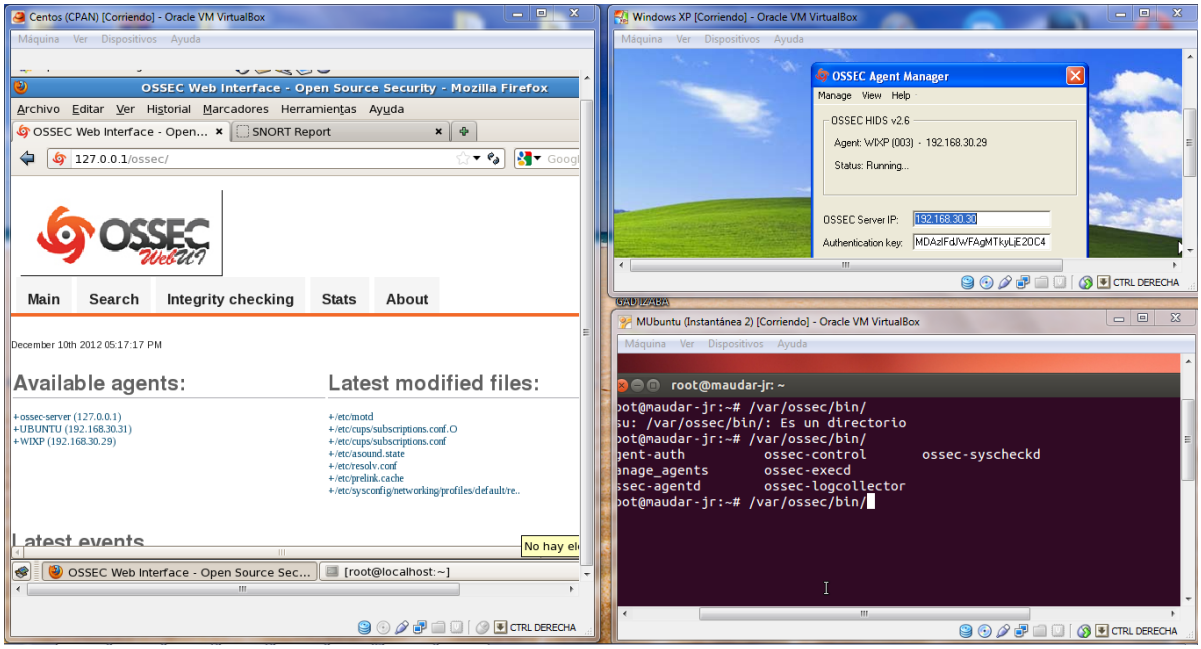


Gráfico 6.20 Honeynet iniciando el software Ossec en Servidor (Izquierda) y Clientes (Derecha)

Fuente: Honeynet

Iniciando el servicio Snort en servidor centos

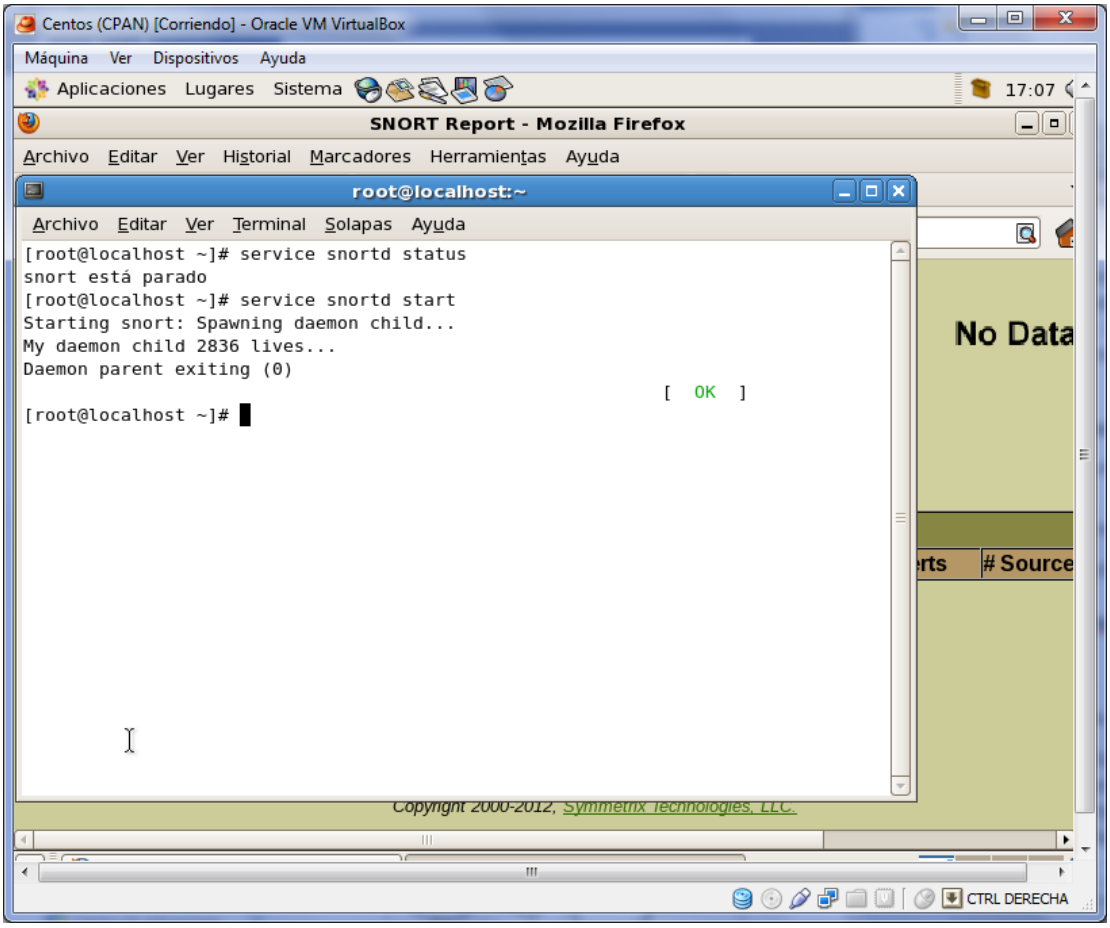


Gráfico 6.21 Iniciando servicio Snort en servidor Centos

Fuente: Honeynet

6.10.1 Iniciando Snort

Abrimos una nueva ventana de consola y escribimos:

```
snort -c /etc/snort/snort.conf -i eth0
```

6.10.2 Iniciando Barnyard

(Ver Gráfico 6.21 en página siguiente)

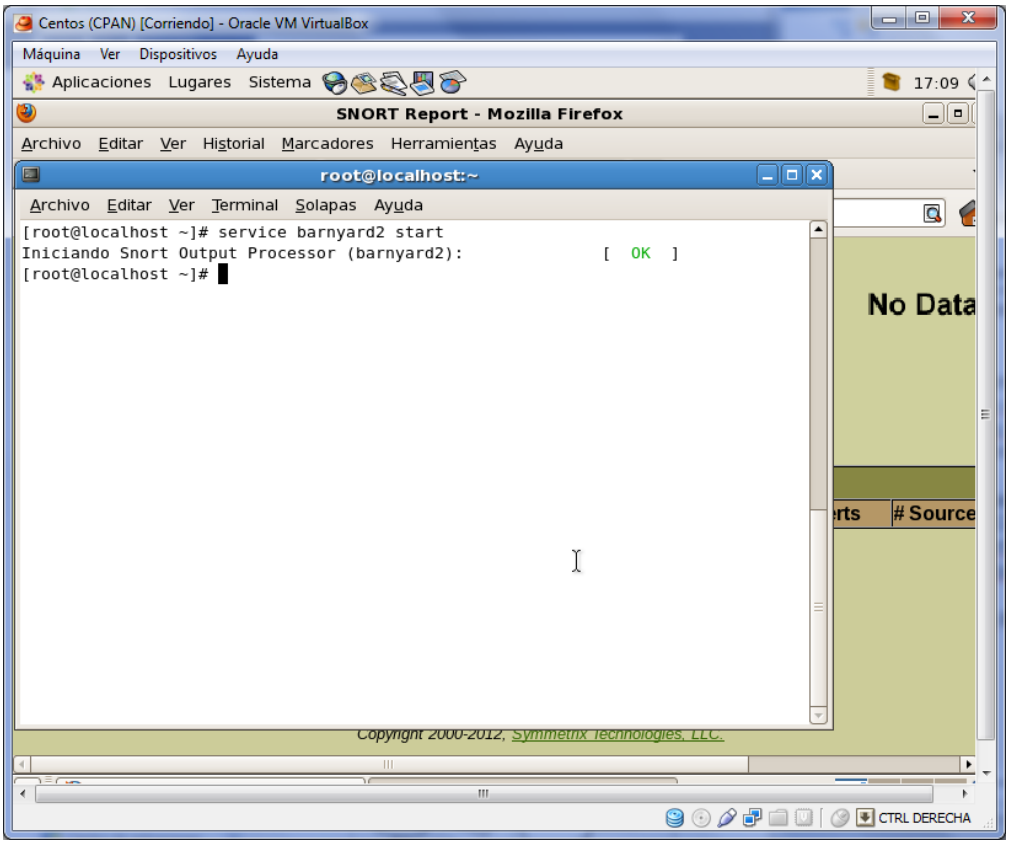


Gráfico 6.22 Iniciando servicio Barnyard

Fuente: Honeynet

Abrimos una segunda ventana de consola y escribimos:

```
cp /dev/null /var/log/snort/barnyard.waldo

mkdir /var/log/barnyard2

/usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.log -

w /var/log/snort/barnyard.waldo
```

*No cerrar las ventanas abiertas, hasta realizar el siguiente paso.

6.10.3 Probando el funcionamiento de Snort

Para comprobar el funcionamiento de Snort crearemos una regla simple en el archivo de reglas locales de Snort (local.rules). Las reglas locales son reglas que fueron escritas por el mismo administrador de SNORT se caracterizan por tener un Sid(SNORT ID) entre 1,000,000 y 1,999,999.

Creando una regla de prueba

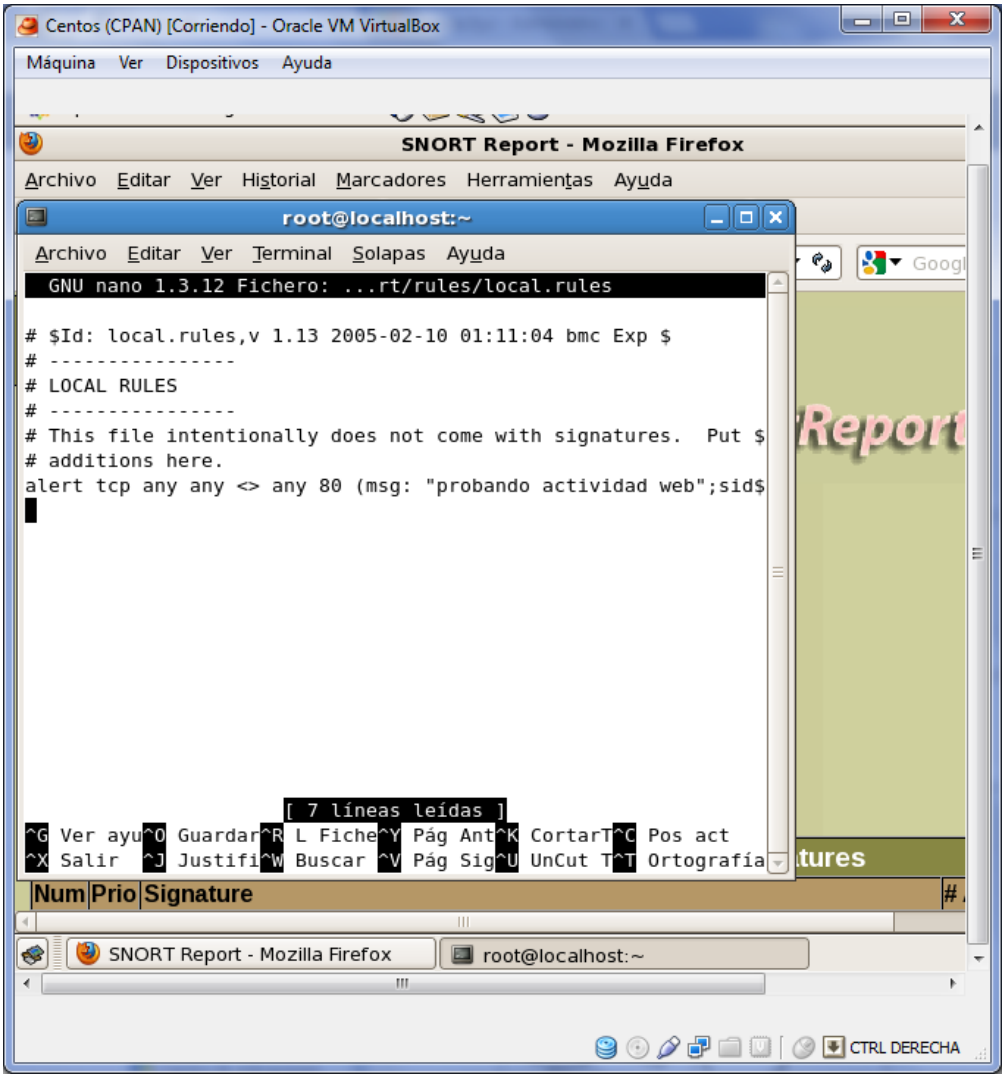


Gráfico 6.23 Regla de prueba para Snort

Fuente: Honeynet

Abrimos una tercera ventana de consola y modificamos el archivo "/etc/snort/rules/local.rules"

Y agregamos la nueva regla:

```
alert tcp any any <> any 80 (msg: "Probando actividad web"; sid:
1000001;)
```

Reiniciamos Snort, con los pasos dados anteriormente.

Comprobando funcionamiento de Snort Report

Abrimos el navegador y tecleamos: http://localhost/snortreport/alerts.php; revisamos en los últimos eventos, si vemos un evento con el SID 1000001 entonces Snort está funcionando, para evitar registros innecesarios, una vez hecha esta prueba eliminamos esta regla del archivo local.rules.

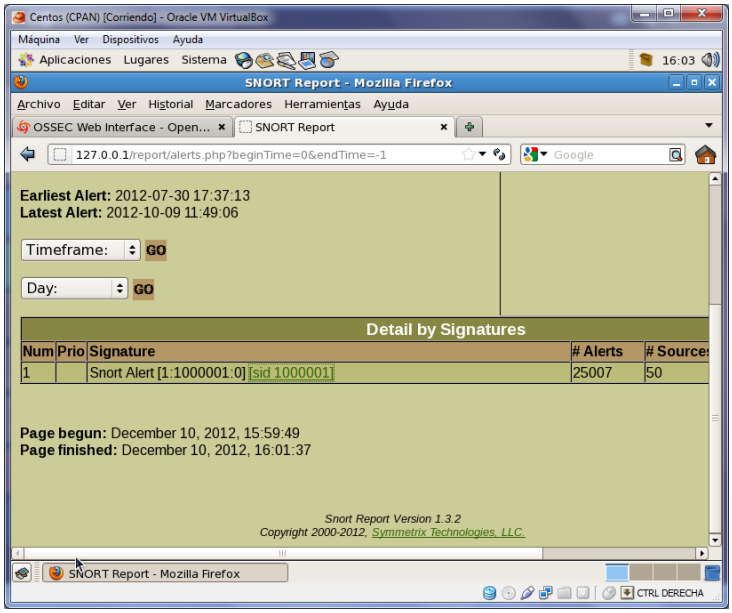


Gráfico 6.24 Comprobando el funcionamiento de Snort Report

Fuente: Honeynet

6.11 Iniciando Snort automáticamente

Para que la Honeynet este siempre lista para trabajar a pesar de un reinicio sea planificado o no, iniciaremos Snort al momento de encender la máquina, para esto seguimos los siguientes pasos:

```
ln -s /usr/local/bin/snort /usr/sbin/snort
cp /usr/local/snort-2.9.1/rpm/snortd /etc/init.d
cp /usr/local/snort-2.9.1/rpm/snort.sysconfig /etc/sysconfig/snort
cd /etc/rc3.d
ln -s ../init.d/snortd S99snortd
cd ../rc0.d
ln -s ../init.d/snortd K99snortd
cd /etc/rc5.d
ln -s ../init.d/snortd S99snortd
cd ../rc6.d
ln -s ../init.d/snortd K99snortd
chmod 755 /etc/init.d/snortd
```

Para comprobar el funcionamiento, abrimos una consola y escribimos:

```
service snortd start
```

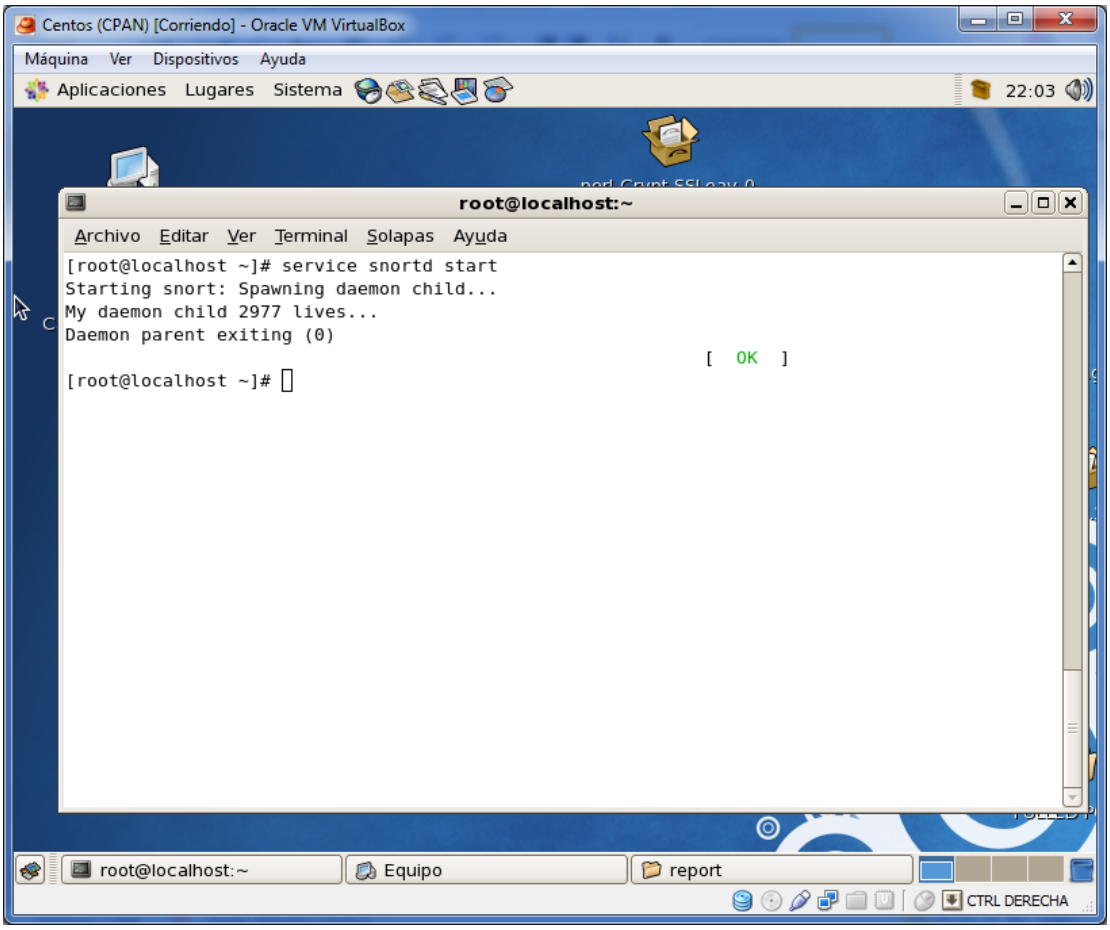


Gráfico 6.25 Comprobando el funcionamiento de Snort

Fuente: Honeynet

Si no da ningún problema el momento de iniciar entonces el servicio está instalado correctamente.

6.12 Iniciando Barnyard automáticamente

Como se explicó anteriormente Barnyard complementa a Snort haciendo que no consuma muchos recursos, por eso es necesario que se inicie junto con Snort. Para esto seguimos los siguientes pasos:

```
nano /etc/snort/barnyard2.conf
```

• descomentamos “config daemon”

• descomentamos y ponemos la ruta al archivo waldo:

```
/var/log/snort/barnyard2.waldo.
```

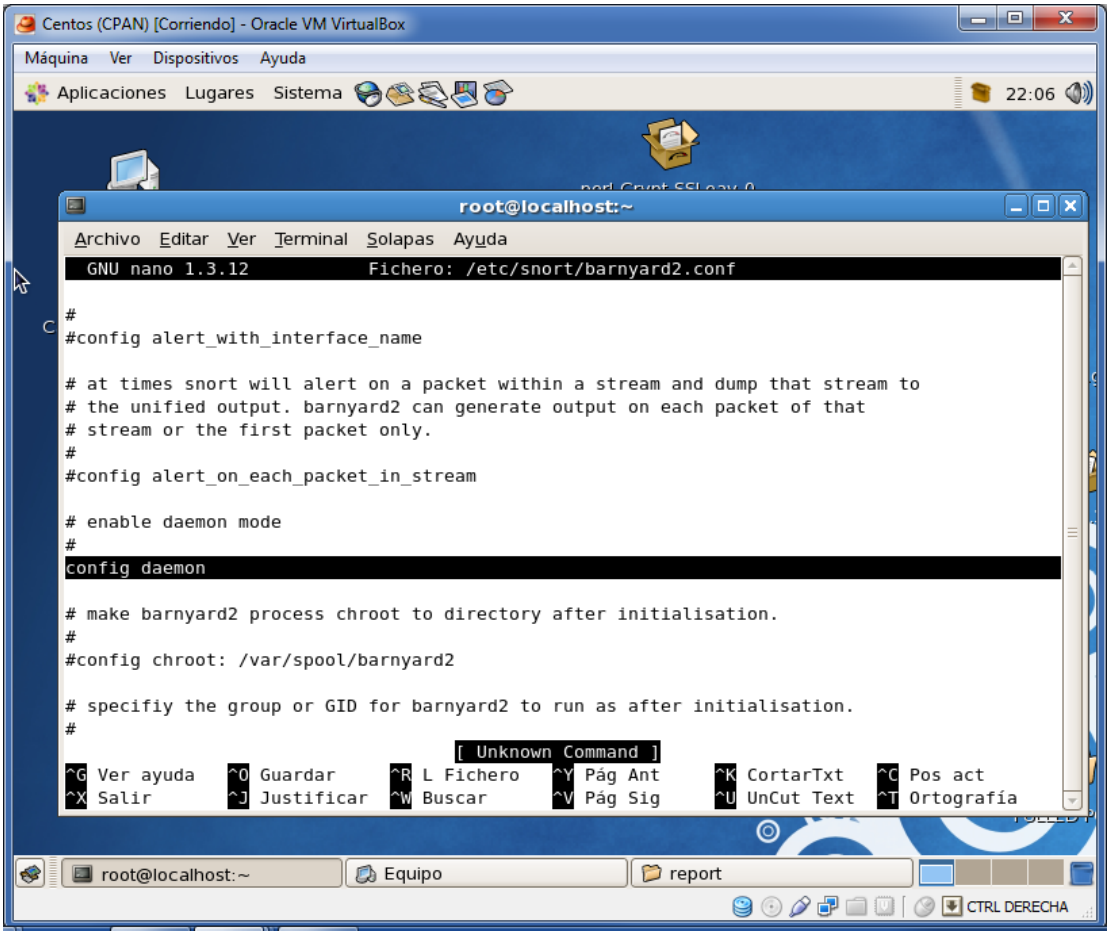


Gráfico 6.26 Configurando Barnyard para inicio automático

Fuente: Honeynet

Cambiamos LOG_FILE a snort.log y cambiamos la variable CONF a /etc/snort/barnyard2.conf.

Guardamos cambios y cerramos

6.12.1 Instalando Barnyard como servicio

```
ln -s /usr/local/bin/barnyard2 /usr/sbin/barnyard2

cp /usr/local/barnyard2-1.9/rpm/barnyard2 /etc/init.d
```

• modificamos el archivo /etc/init.d/barnyard2

•cambiamos la línea BARNYARD_OPTS a:

```
BARNYARD_OPTS="-D -c

$CONF -d $SNORTDIR -w $WALDO_FILE -f $LOG_FILE -X $PIDFILE

$EXTRA_ARGS".
```

Guardamos cambios y cerramos

```
cp /usr/local/barnyard2-1.9/rpm/barnyard2.config/etc/sysconfig/barnyard2

chmod 755 /usr/local/bin/barnyard2

cd /etc/rc3.d

ln -s ../init.d/barnyard2d S99barnyard2d

cd ../rc0.d

ln -s ../init.d/barnyard2d K99barnyard2d

cd /etc/rc5.d

ln -s ../init.d/barnyard2d S99barnyard2d

cd ../rc6.d

ln -s ../init.d/barnyard2d K99barnyard2d

chmod 755 /etc/init.d/barnyard2
```

Para comprobar el funcionamiento, abrimos una consola y escribimos:

```
service barnyard2 start
```

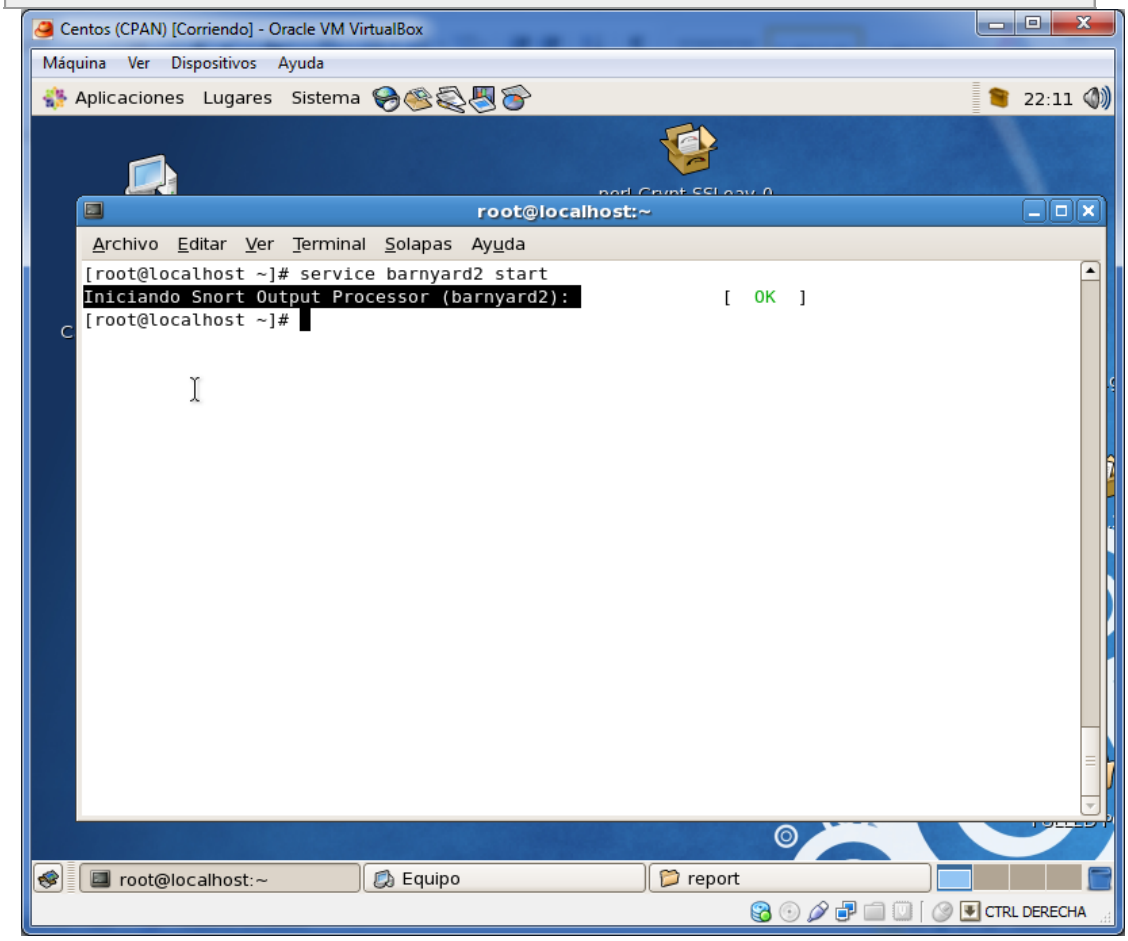


Gráfico 6.27 Iniciando servicio Barnyard

Fuente: Honeynet

6.13 IDS de host Ossec

Ossec es un proyecto open source de gestión de Logs, que monitoriza una máquina, y que detecta las anomalías que puedan producirse en ella. Para hacer esto utiliza herramientas para la detección de rootkits, para revisar la integridad de ficheros y ejecutables del sistema, y por último un potente sistema para analizar logs.

Está basado en un modelo de cliente-servidor, con lo cual tendremos un servidor centralizado que se encarga de recibir y actuar en base a la información que reciba de los agentes que, en definitiva, son las ordenadores que están siendo monitorizadas y atacadas. La forma de actuar del servidor es, por una parte, enviando notificaciones, y por otro lado, si así se configura, generando reglas firewall que se ejecutarán en los propios agentes.

Funciona en la mayoría de sistemas operativos, incluyendo Linux, OpenBSD, FreeBSD, MacOS, Solaris y Windows, ademas acaba de salir la nueva versión 2.5 de este proyecto, la cual incluye numerosos cambios que hacen de este proyecto una verdadera opción a elegir.

6.13.1 Instalando servidor Ossec en Centos

Tenemos que descargarnos los paquetes necesarios para la instalación que son gcc y gcc-c++.

En la página web de ossecwww.ossec.net se encuentran todos los paquetes necesarios para la instalación.

Una vez descargados procedemos con la instalación:

Ubicamos el archivo install.sh y lo ejecutamos con la orden ./install.sh

Seleccionamos el idioma español con "es".

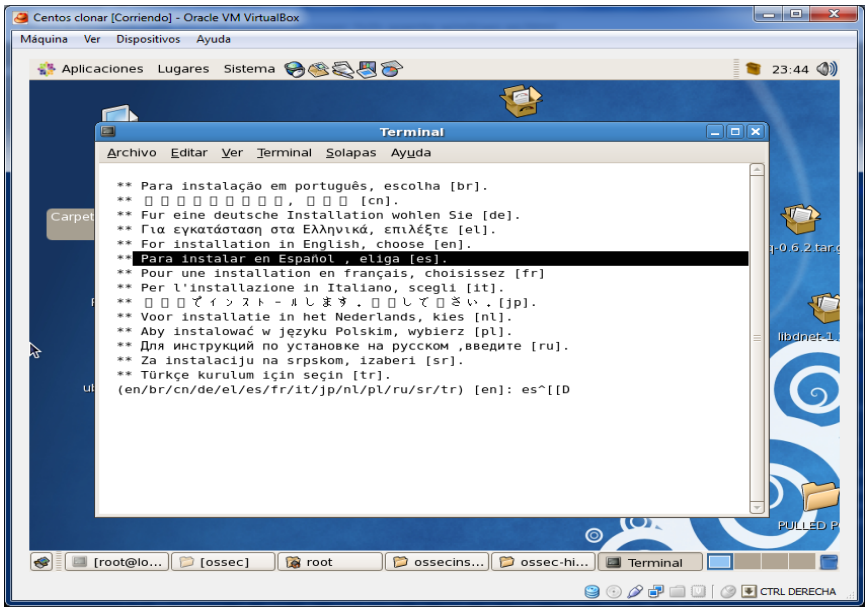


Gráfico 6.28 Instalación de OSSEC

Fuente: Honeynet

Nos dará una breve información del servidor, y pulsamos enter

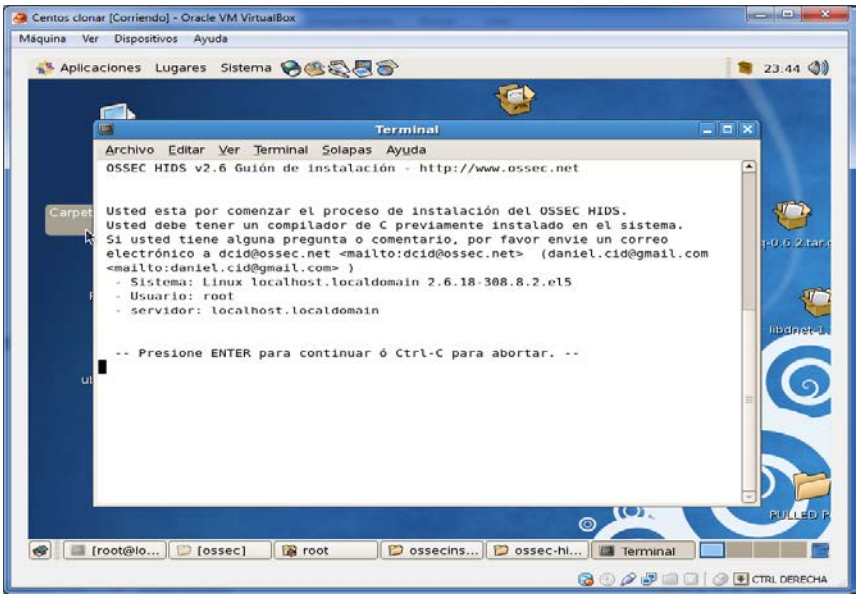


Gráfico 6.29 Instalación de OSSEC como servidor

Fuente: Honeynet

Nos preguntara el tipo de instalación, en este caso será servidor y nos pedirá la ruta en la que lo queremos instalar por defecto es /var/ossec/, también nos pedirá una dirección de correo donde enviarnos notificaciones de lo que pase en el servidor o en los agentes y le definiremos una, el inmediatamente ubicara el servidor SMTP y le daremos que lo use.

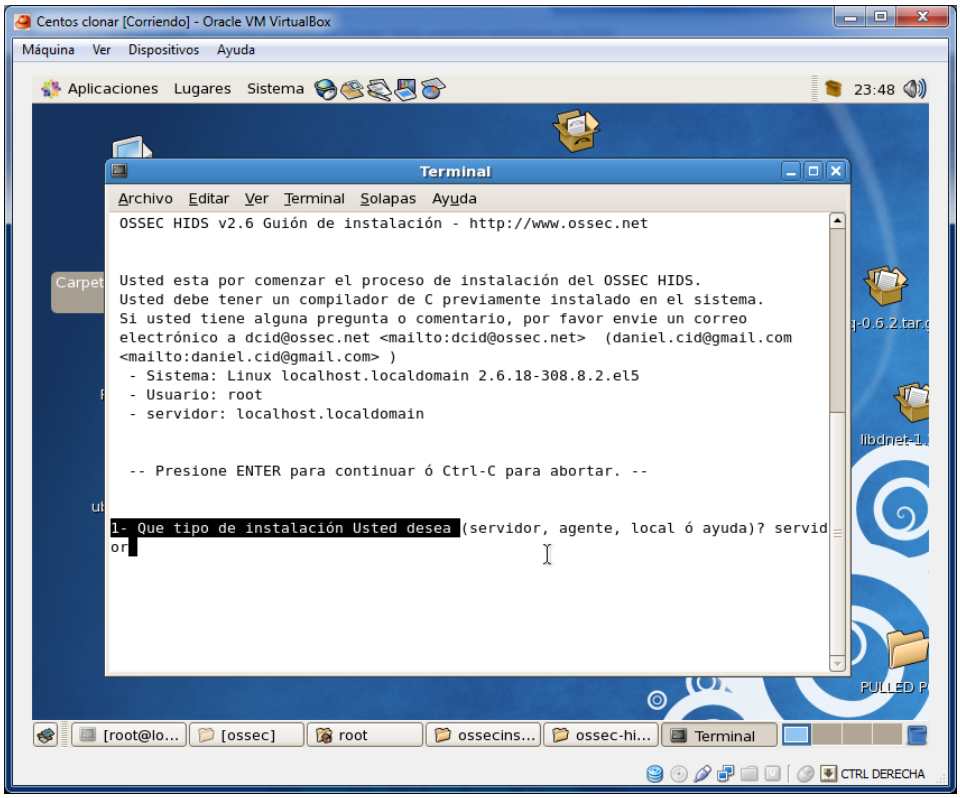


Gráfico 6.30 Instalación de OSSEC como servidor

Fuente: Honeynet

También preguntara si deseamos agregar el servidor de integridad del sistema, seleccionamos si, lo mismo para el sistema de detección de rootkit y la habilitación de respuesta activa.

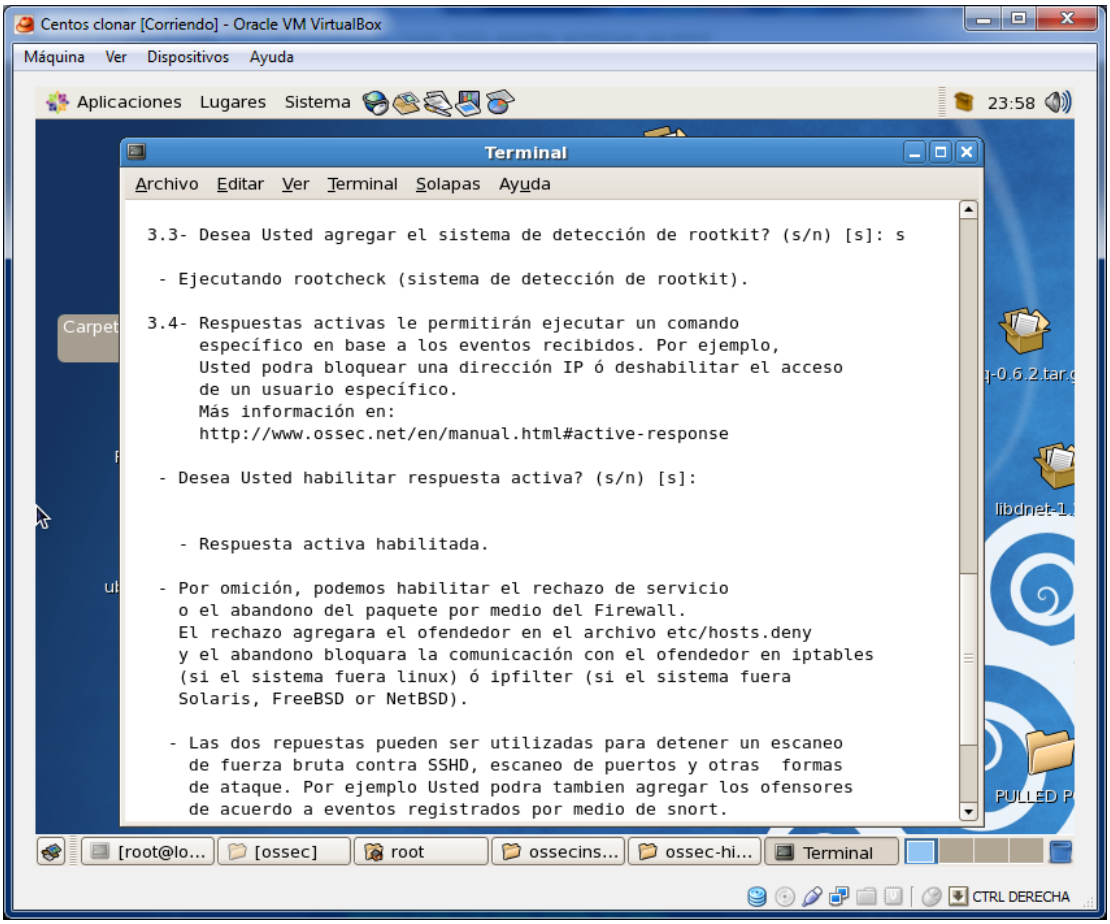


Gráfico 6.31 Opciones de instalación del servidor OSSEC

Fuente: Honeynet

Habilitamos la respuesta desechar en el Firewall, luego nos pedirá definir una lista blanca en la cual agregaremos ordenadores que sean de confianza, y tenemos que habilitar el syslog remoto.

Una vez establecidos estos parámetros comenzara la instalación:

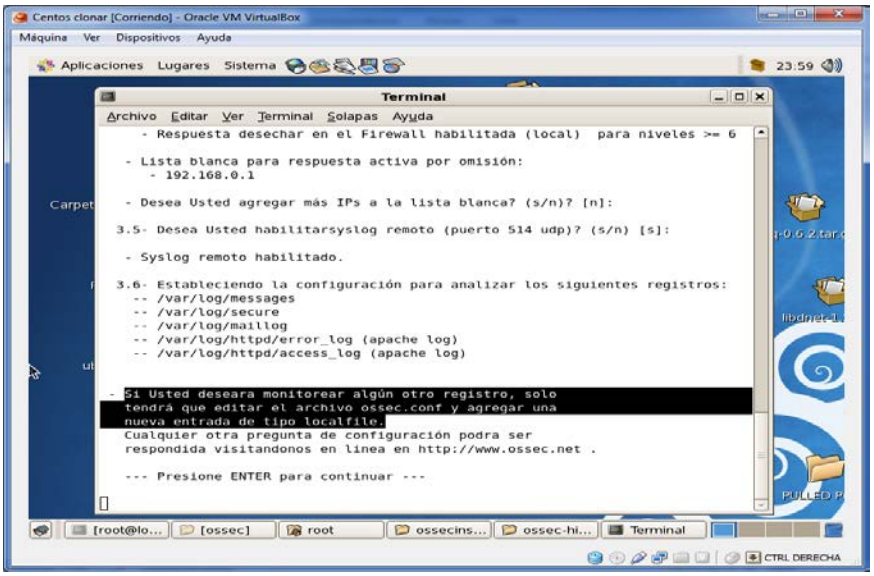


Gráfico 6.32 Instalación completa de OSSEC

Fuente: Honeynet

Al culminar la instalación nos dará los comandos necesarios para iniciar o detener el servicio.

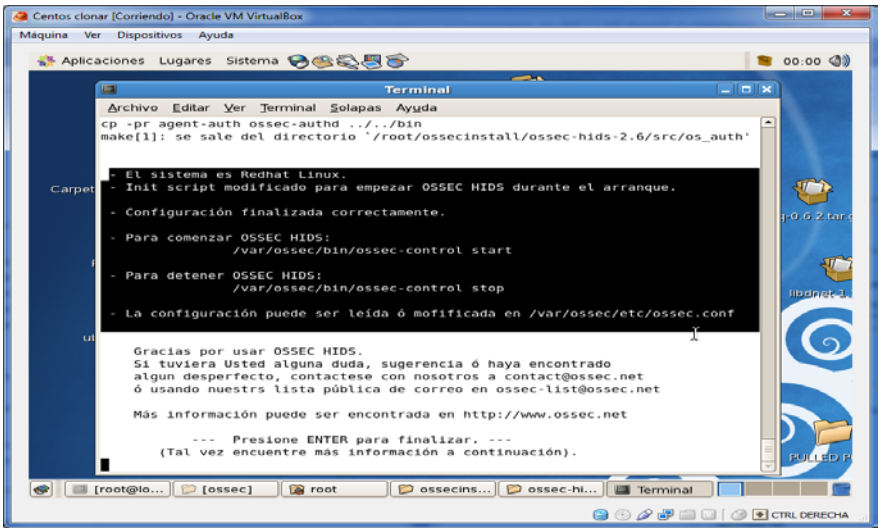


Gráfico 6.33 Comandos para monitorear OSSEC

Fuente: Honeynet

A continuación editaremos el archivo de configuración de OSSEC ubicado en /var/ossec/etc/ossec.conf

Y añadiremos las reglas, las reacciones y los comandos a ejecutar según el caso.

También habilitaremos el ingreso de conexiones remotas desde la subred 192.168.30.0/24 por el puerto 1514 UDP hasta nuestra dirección IP (192.168.30.30).

Además de esto le diremos que denegaremos en el archivo /etc/host.deny cualquier IP que realice intentos de intrusión al servidor o a los agentes.

Ya que designamos el puerto 1514 UDP para las comunicaciones con los clientes le daremos acceso a dicho puerto con iptables y reiniciamos el servicio.

6.13.2 Instalando interfaz web de OSSEC

Ahora instalaremos el entorno gráfico desde una interfaz WEB, para esto nos descargaremos dicha interfaz desde la página oficial de OSSEC.

Una vez que se haya descargado y descomprimido crearemos un DocumentRoot en el cual vamos a alojar la interfaz, este quedara en /var/www/html/ossec/, luego de crearlo moveremos todo el contenido de la carpeta que acabamos de descomprimir a la que acabamos de crear.

Ahora nos desplazáramos hasta el DocumentRoot y ejecutaremos el archivo setup.sh, el cual al final nos pedirá un usuario y una contraseña.

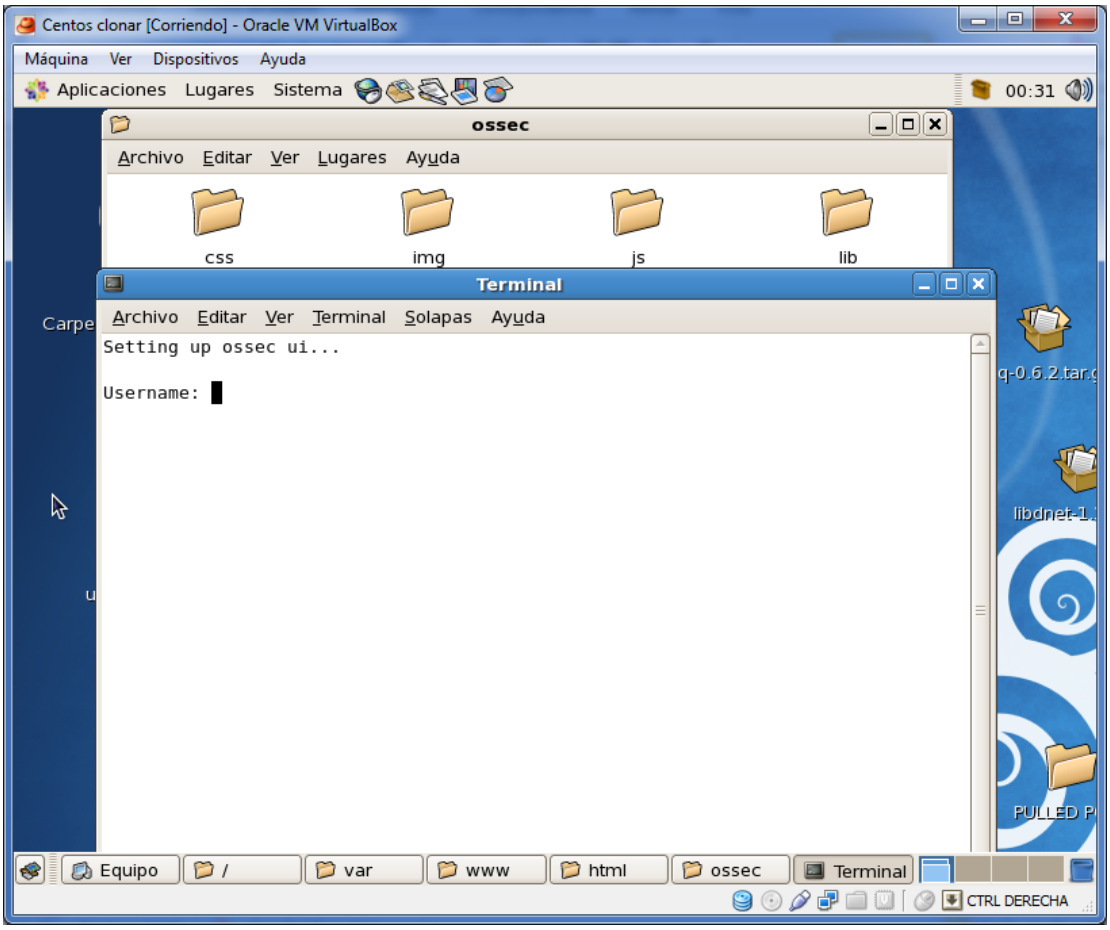


Gráfico 6.34 Instalación interfaz web de OSSEC

Fuente: Honeynet

Agregamos en /etc/group el usuario apache a ossec.

Y le daremos permisos y cambiaremos el grupo por apache a la carpeta temp dentro del DocumentRoot, finalmente reiniciaremos nuestro servidor apache.

Ahora nos desplazaremos hasta un navegador web e ingresaremos la URL de nuestro servidor, allí nos deberán aparecer los agentes disponibles, las últimas modificaciones y los últimos eventos tanto en el agente como en el servidor.

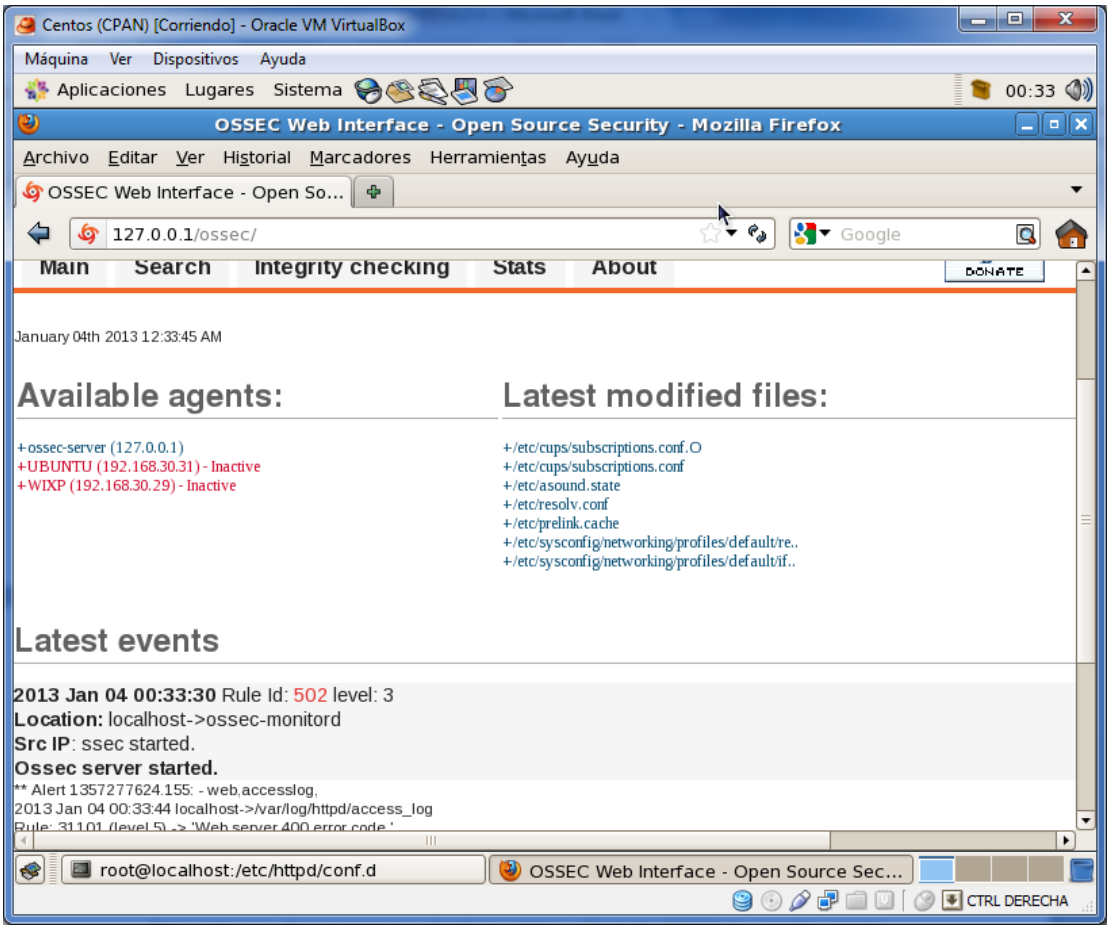


Gráfico 6.35 Interfaz web de OSSEC

Fuente: Honeynet

6.14 Instalación Honeypot Windows

6.14.1 Instalando agente OSSEC en Windows XP

Para esto nos descargaremos desde la página oficial de Ossec la versión agente para Windows y lo instalamos normalmente.

Una vez q finalice la instalación nos aparecerá una ventana en la cual ingresaremos la IP del servidor

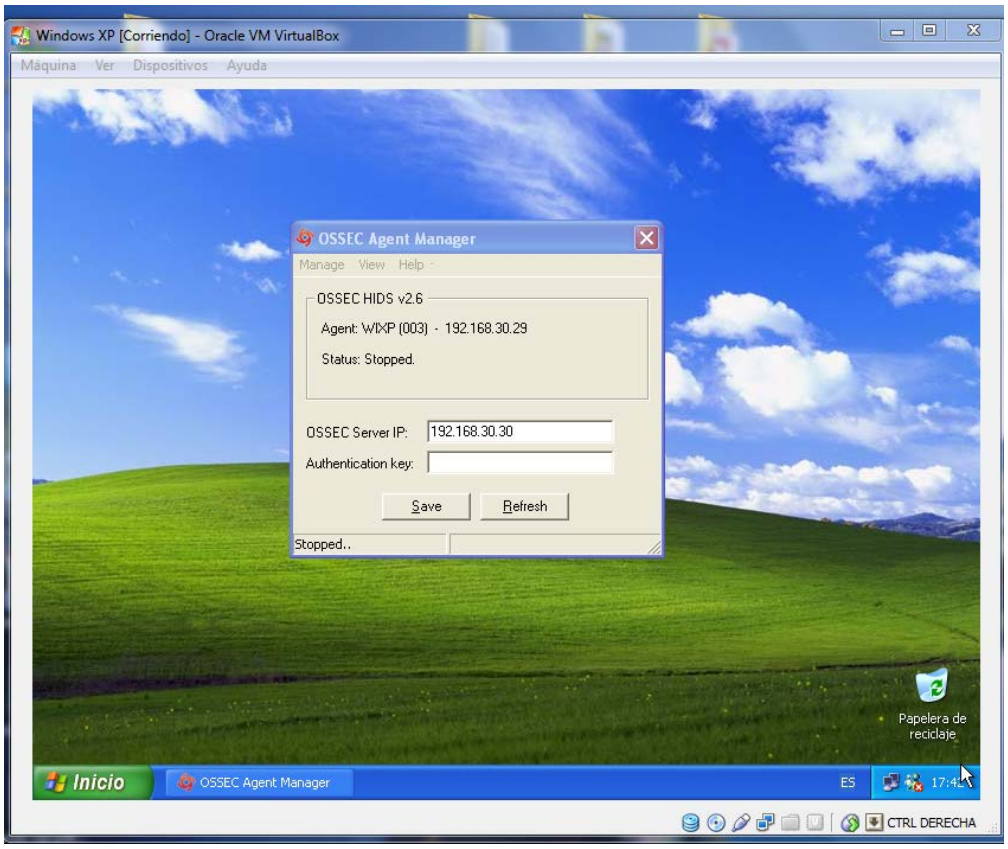


Gráfico 6.36 Obtención de clave de autentificación desde el cliente Windows

Fuente: Honeynet

La llave de autenticación que se obtiene del servidor de la siguiente manera:

Primero vamos al servidor OSSEC, allí ejecutamos desde consola el comando “manage_agents”, y nos aparecerá la opción Add an agent, la elegimos presionando "A", nos pedirá un nombre para el agente, luego una dirección IP la cual es la del agente que vamos a añadir y finalmente nos dirá que el ID del agente para este caso 001.

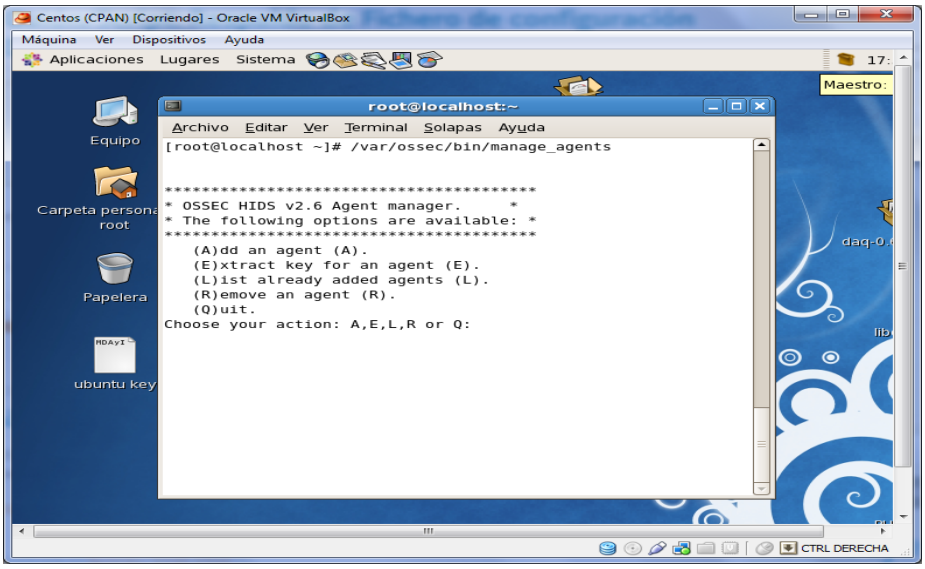


Gráfico 6.37 Agregando cliente Windows a OSSEC

Fuente: Honeynet

Una vez agregado, seleccionamos la opción “Extract key for an agent”, la elegiremos presionando "E"

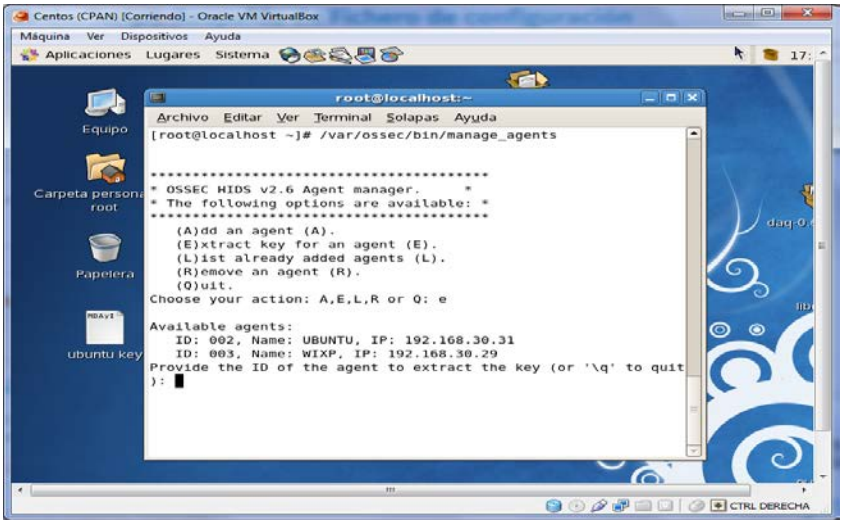


Gráfico 6.38 Obteniendo llave de autenticación para cliente Windows XP

Fuente: Honeynet

Nos dirá que hay un agente disponible le diremos el ID del agente el cual es 001 y él nos dará una llave, esta llave es la autenticación que debemos ingresar en el agente Windows para que se autentique contra el servidor OSSEC.

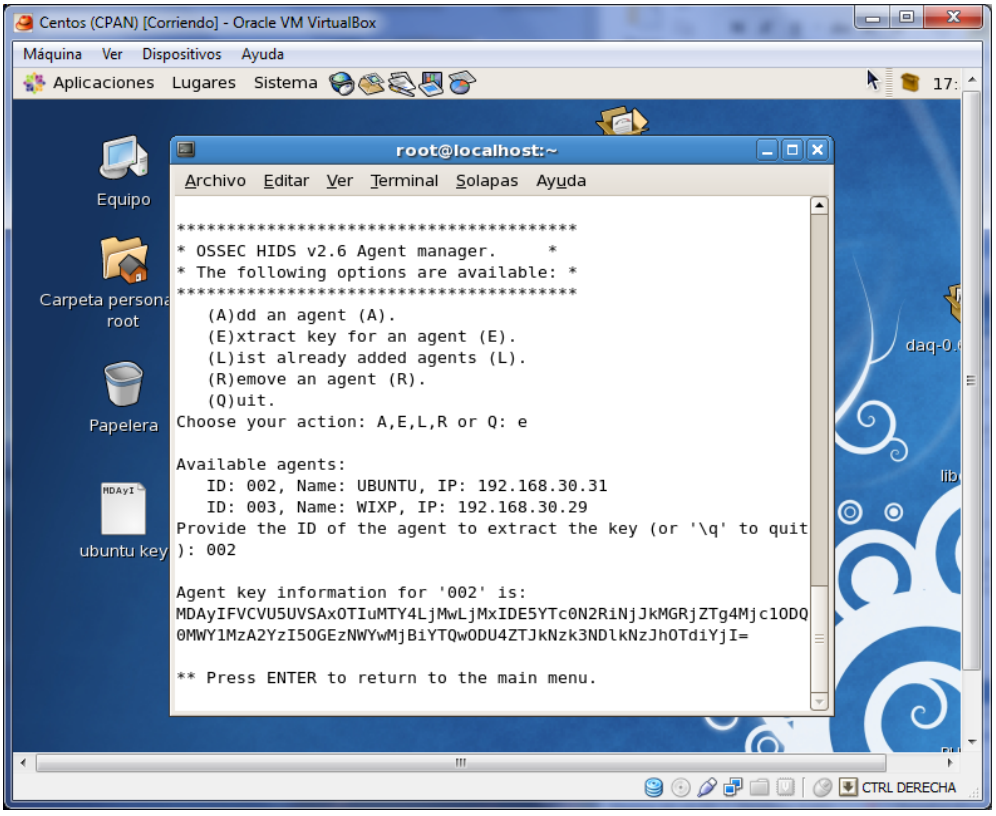


Gráfico 6.39 Ingreso de llave de autenticación para cliente Windows XP

Fuente: Honeynet

Una vez que obtuvimos la llave regresamos al agente Windows e ingresamos la llave y pulsamos aceptar para confirmar.

Luego vamos a la opción “View Logs” para que se genere por primera vez el archivo de logs del agente.

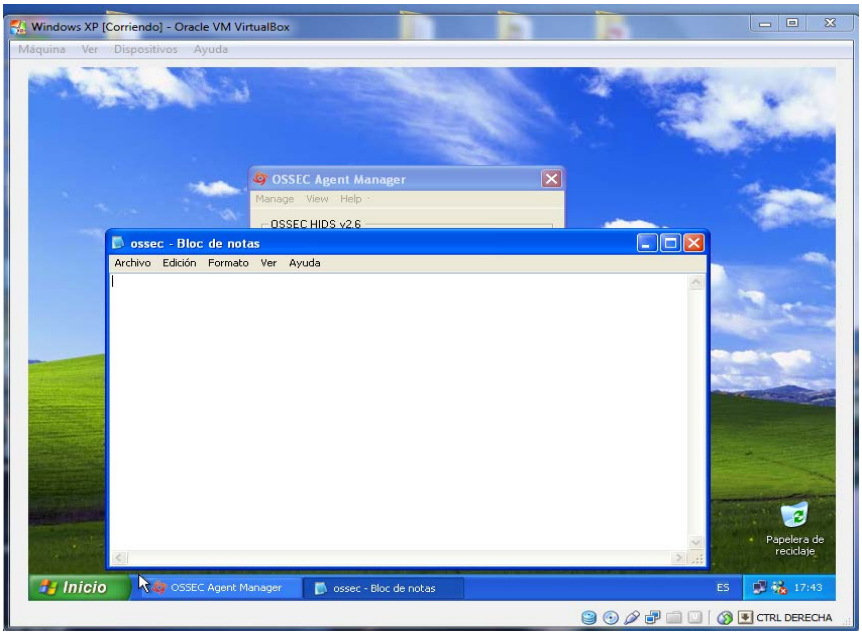


Gráfico 6.40 Logs de OSSEC en Windows XP

Fuente: Honeynet

Hecho esto reiniciamos el agente y volvemos a revisar el archivo de logs.

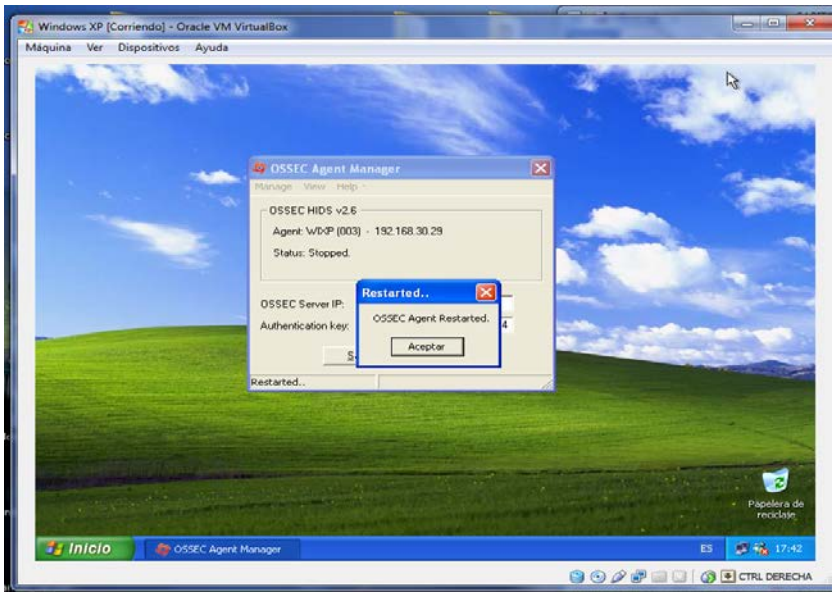


Gráfico 6.41 Reinicio de servicio OSSEC

Fuente: Honeynet

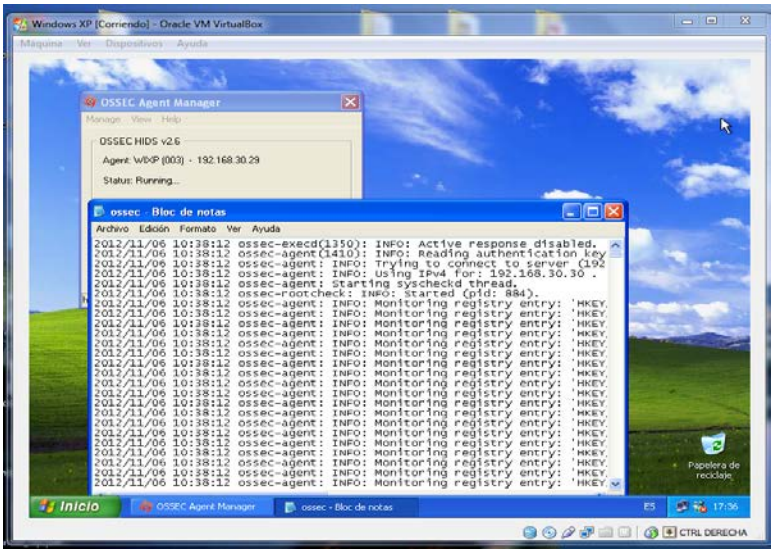


Gráfico 6.42 Logs OSSEC

Fuente: Honeynet

De vuelta en el servidor reiniciaremos el servicio ossec-remoted y ossec-control para que proceda a reconocer al nuevo agente agregado; con el comando /var/ossec/bin/ossec-remoted restart y /var/ossec/bin/ ossec-control restart

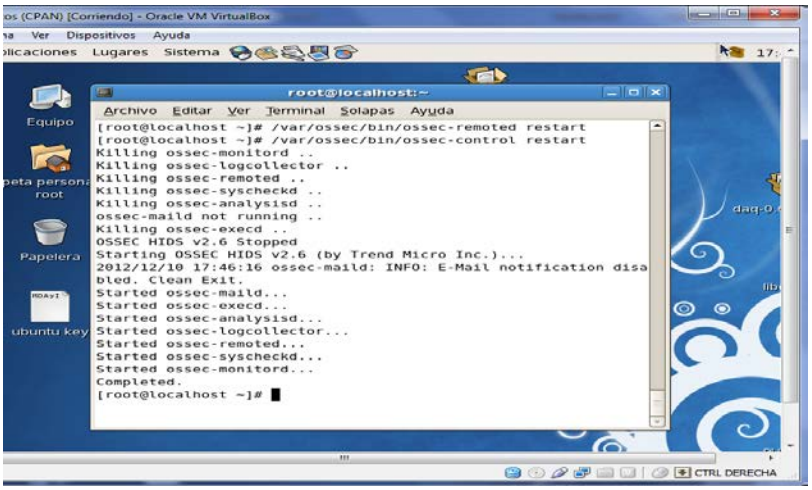


Gráfico 6.43 Reiniciando OSSEC en el servidor

Fuente: Honeynet

Con el comando /var/ossec/bin/agent_control -i#deID visualizaremos la información de los agentes, para este caso el 001 aparecerá Active que significa que está habilitado para enviar notificaciones al servidor.

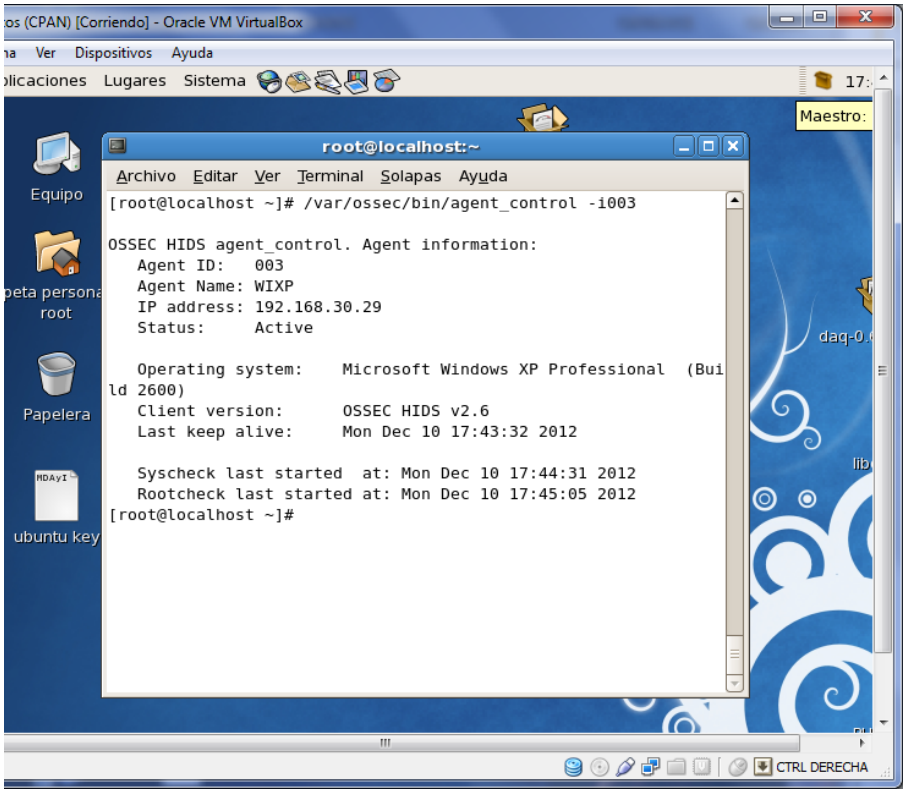


Gráfico 6.44 Clientes de OSSEC

Fuente: Honeynet

6.15 Instalación Honeypot Ubuntu

6.15.1 Instalando agente OSSEC en Ubuntu

Para esto descargaremos desde la página oficial de OSSEC la versión agente para Linux.

Descomprimimos el archivo empaquetado y nos cambiamos al directorio:

Ejecutamos el instalador mediante el comando:

```
./install.sh
```

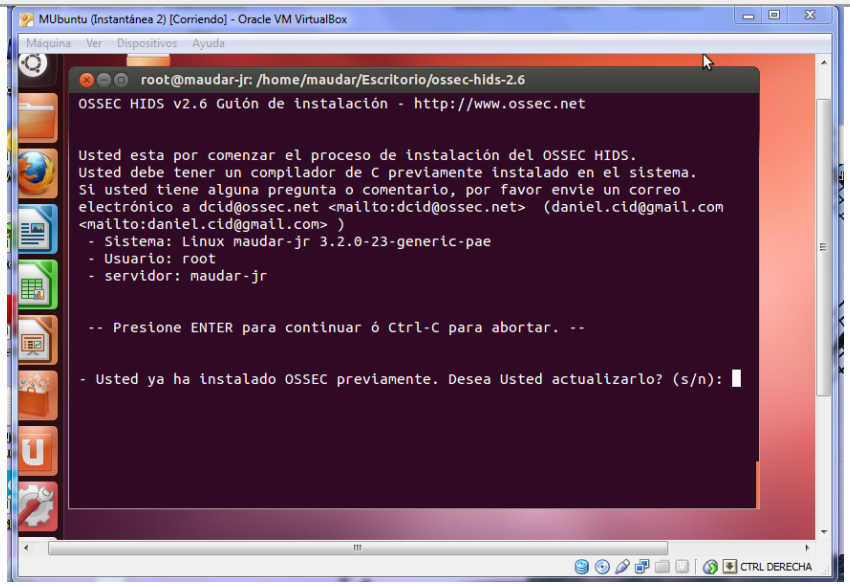


Gráfico 6.45 Instalación de OSSEC en cliente Ubuntu

Fuente: Honeynet

Y dejamos que se instale con los valores por defecto, presionando enter.

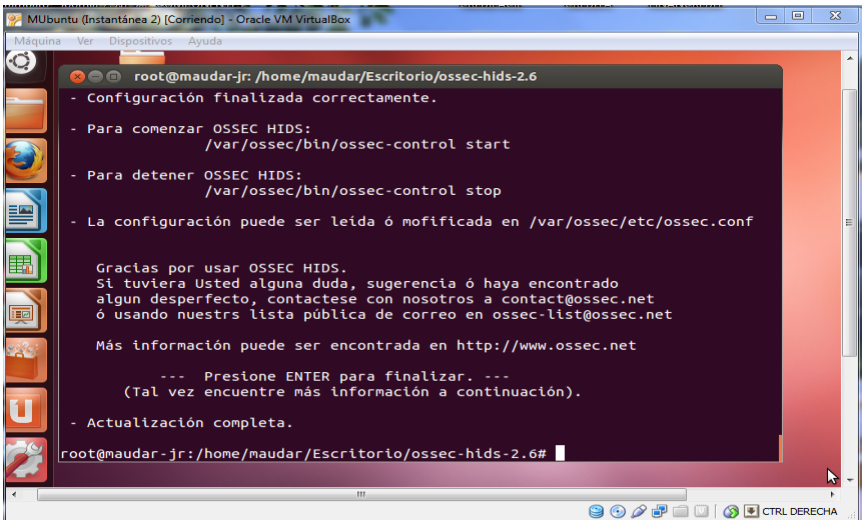


Gráfico 6.46 Instalación de OSSEC en cliente Ubuntu

Fuente: Honeynet

6.16 Funcionamiento Honeynet

6.16.1 Iniciando servicios en Servidor

A continuación vamos a iniciar los servicios necesarios para el funcionamiento de la Honeynet:

Como se explicó anteriormente iniciamos el IDS de host ossec que se encargara de recoger los logs de los clientes Windows y Ubuntu y el IDS de red SNORT que se encargara de monitorear el estado de la red en nuestra Honeynet.

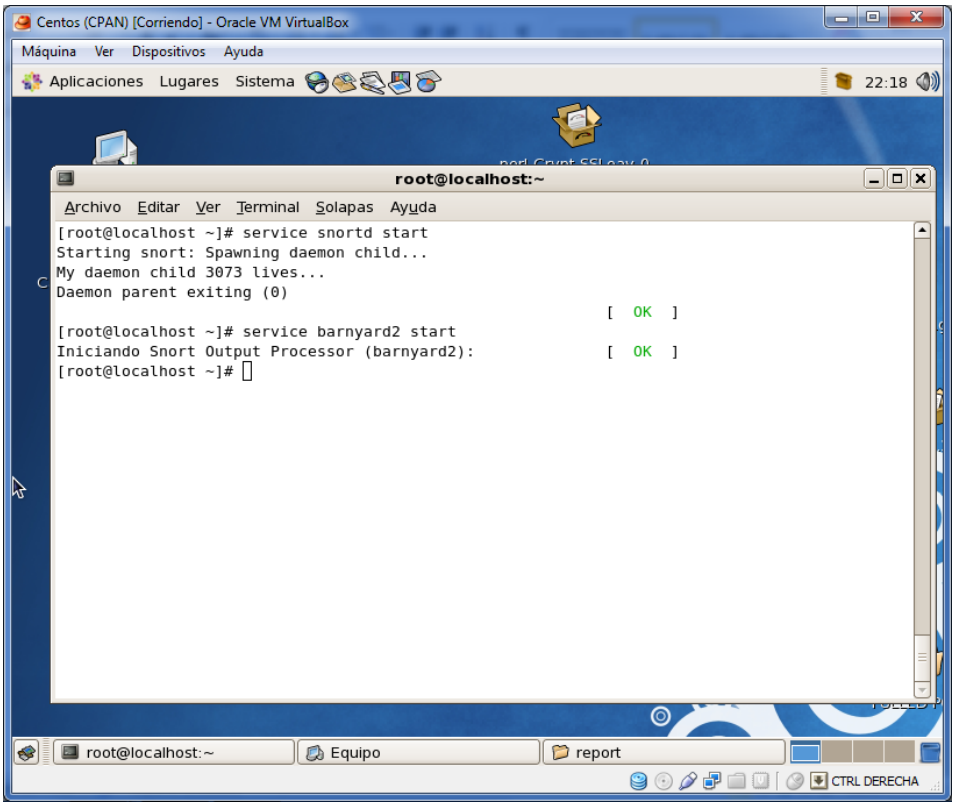


Gráfico 6.47 Iniciando Snort & Barnyard en servidor

Fuente: Honeynet

6.16.2 Iniciando servicios en clientes

Para el caso de los clientes únicamente debemos comprobar que el cliente del programa Ossec se encuentre iniciado y que se pueda comunicar con el servidor.

6.16.2.1 Para el cliente Windows:

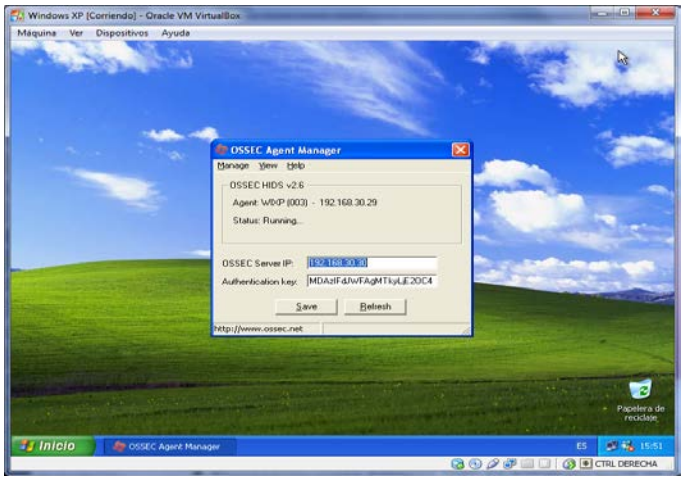


Gráfico 6.48 Iniciando OSSEC en cliente Windows XP

Fuente: Honeynet

6.16.2.2 Para el cliente Ubuntu:

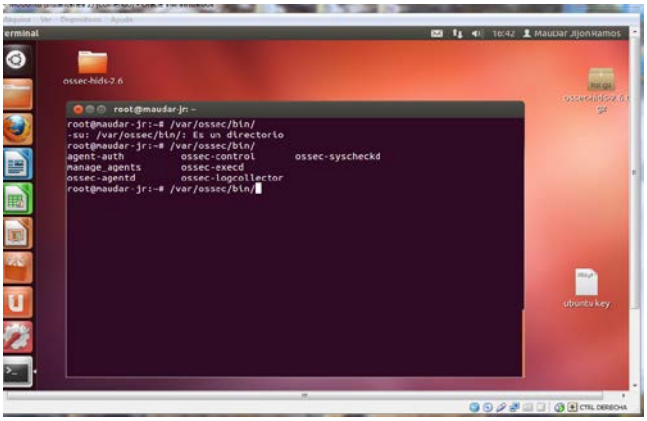


Gráfico 6.49 Iniciando OSSEC en cliente Ubuntu

Fuente: Honeynet

6.17 Asegurando directorios de Ossec y de Snort

Como medida de seguridad adicional aseguraremos los directorios donde se instalaron OSSEC y SNORT para evitar el acceso a usuarios no deseados

Creamos el directorio donde almacenaremos las contraseñas:

```
mkdir /var/www/passwords

/usr/bin/htpasswd -c /var/www/passwords/passwords snort
```

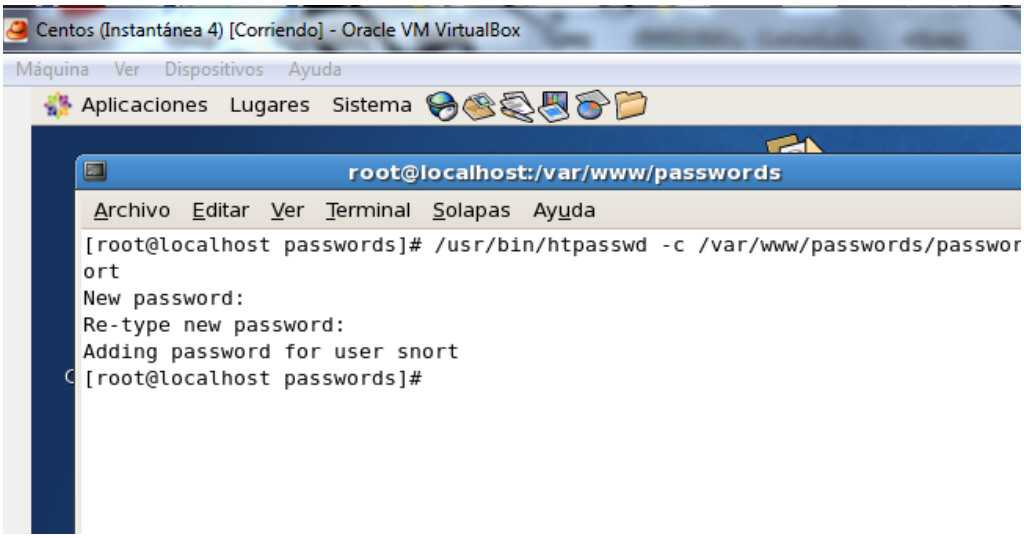


Gráfico 6.50 Asegurando directorios de Ossec y Snort

Fuente: Honeynet

Se creara una cuenta para el usuario snort,

El mismo paso se realizara para el usuario de ossec.

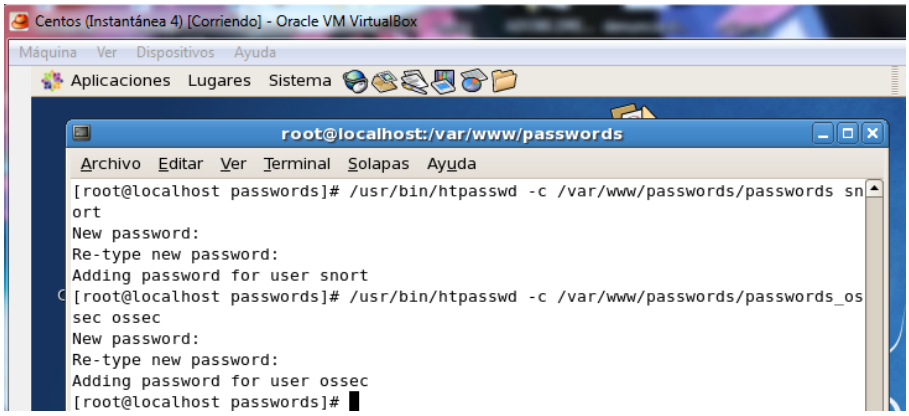


Gráfico 6.51 Creación de usuarios para acceso a directorios de Ossec y Snort

Fuente: Honeynet

Después tendremos que editar el archivo httpd.conf agregando las siguientes líneas:

```
nano /etc/httpd/conf/httpd.conf
```

De esta forma aseguramos el directorio snort

```
<Directory “/var/www/html/report”>
 AuthType Basic
 AuthName “SnortIDS”
 AuthUserFile /var/www/passwords/passwords
 Require user snort
</Directory>
```

Y el directorio ossec:

```
<Directory “/var/www/html/ossec”>

 AuthType Basic

 AuthName “SnortIDS”

 AuthUserFile /var/www/passwords/passwords_ossec

 Require user ossec

</Directory>
```

Reiniciamos el servicio y comprobamos su funcionamiento:

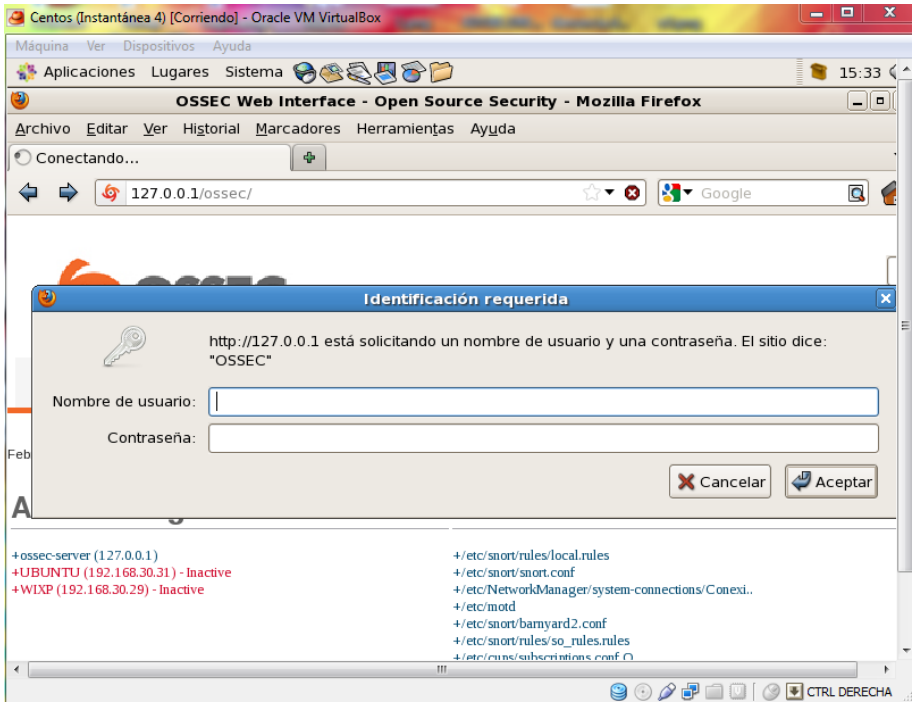


Gráfico 6.52 Comprobando el acceso a directorio protegido de Ossec

Fuente: Honeynet

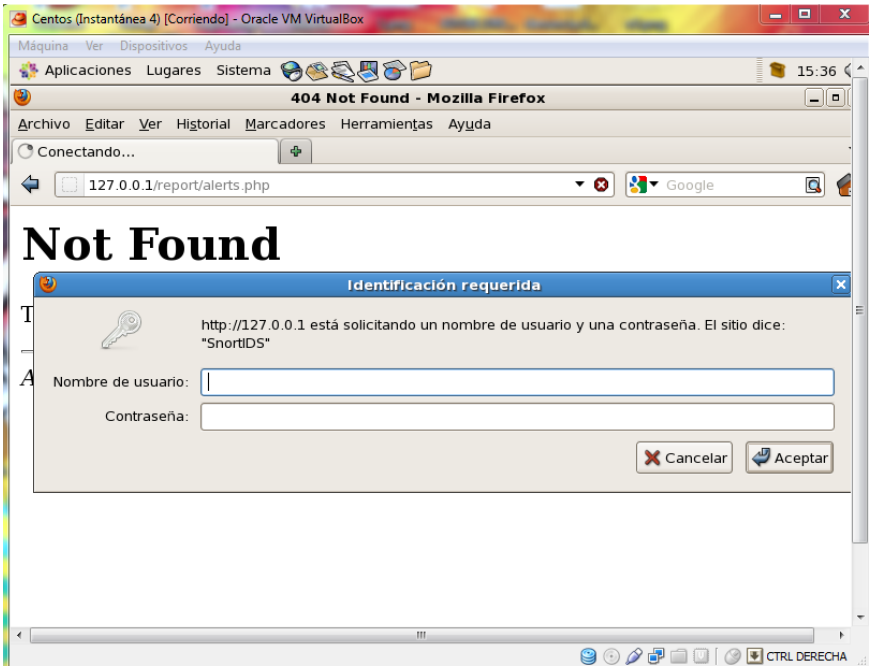


Gráfico 6.53 Comprobando el acceso a directorio protegido de Snort

Fuente: Honeynet

6.18 Metodología de las Capturas en la Honeynet

Para las capturas de datos se han tomado datos desde su posterior puesta en marcha, es decir los meses de Diciembre de 2012 hasta Febrero de 2013.

A estas ordenadores que forman parte de la Honeynet, se las utilizo exactamente igual que a otros ordenadores utilizadas dentro de la facultad de Ing. en sistemas, es decir se instaló el mismo software con el que se trabajaría normalmente, además se las utilizo para conectarse a Internet de manera aleatoria desde varios navegadores, todo esto para su posterior análisis.

6.19 Metodología del Análisis Forense dentro de la Honeynet

Una vez detectado y separado el malware, se procede a su estudio. Del mismo modo que con las capturas, para esto seguiremos un procedimiento en general:

Creamos una instantánea de la máquina virtual para poder volver a su estado inicial luego de ejecutar el virus que se va a analizar.

Una vez infectados procedemos a seguir utilizando la máquina virtual por un tiempo prudente en el cual daremos la oportunidad de actuar al virus y a que la máquina virtual recoja y envié al servidor toda la información necesaria para el análisis.

En el servidor se recolecta la información enviada por la o las ordenadores virtuales y se procede a comparar los resultados obtenidos con los que se obtuvieron del sitio web del primer paso.

6.20 Capturas y análisis forense en Honeynet

6.20.1 Capturas de Diciembre

Con la metodología de captura detallada en el punto 6.19 no se obtiene únicamente información del ataque en tiempo real, también se puede recrear el ataque tantas veces como se requiera gracias al uso de los “snapshots” con esto podemos estudiar el efecto que tiene cada virus dentro de cada sistema operativo.

6.20.1.1 Intrusión 1 - Password Guessing

Es el nombre que se utiliza al intento de obtener credenciales válidas tratando de adivinar contraseñas de un sistema remoto mediante fuerza bruta; esta intrusión se trata de un ataque típico que se realiza a un sistema, esta es una forma de ver cómo reacciona la Honeynet ante este tipo de ataques y la información que nos brinda, este ataque se facilita debido a que se puede ingresar contraseñas indefinidamente sin ningún tipo de bloqueo por parte del sistema operativo lo que en estaría ayudando al atacante a acceder a la maquina sin tantos problemas.

En la imagen se puede observar que por cada intento fallido de inicio de sesión OSSEC genera una alerta acompañada de la fecha y hora de esta.

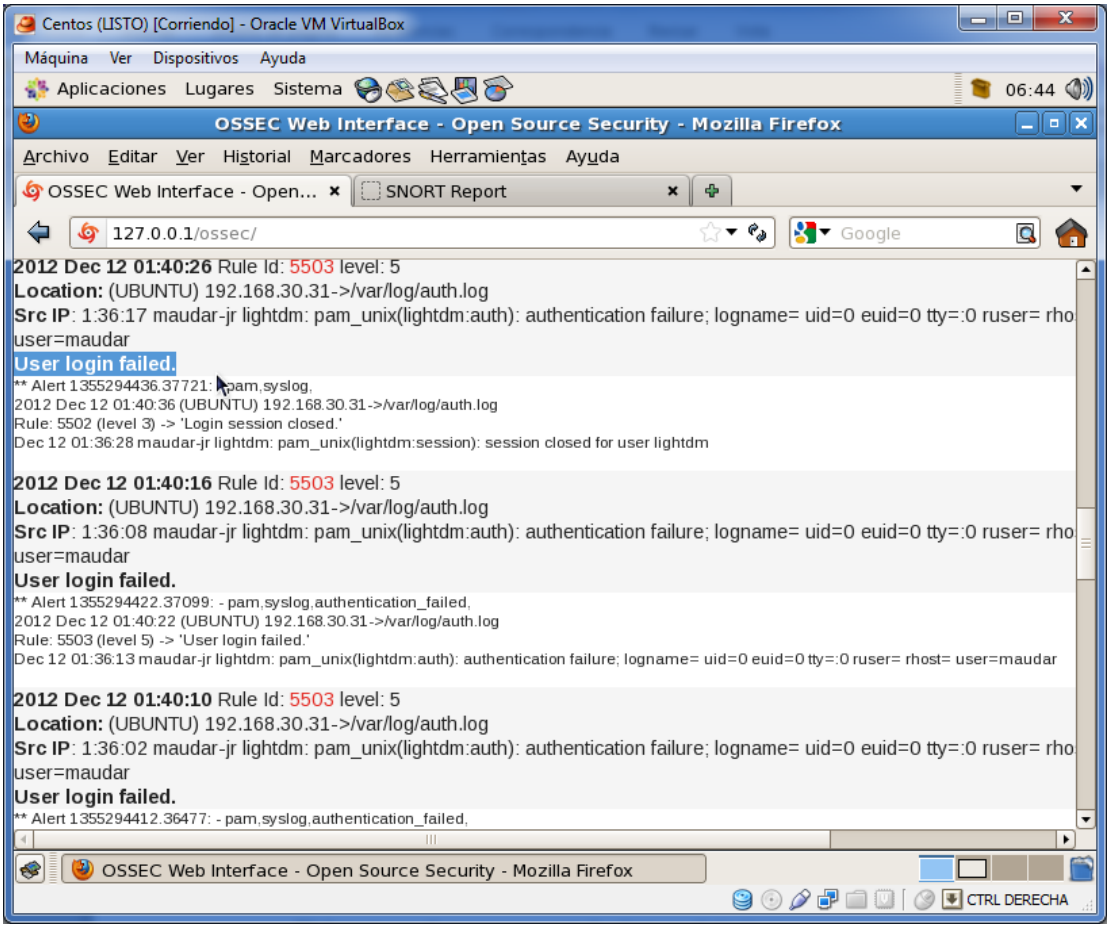


Gráfico 6.54 Alertas de OSSEC

Fuente: Honeynet

El formato en el que nos presenta la alerta es el siguiente:

2012 Dec 12 10:04:05

Rule Id: 5503

level: 5

Location: (UBUNTU)

192.168.30.31->/var/log/auth.log

Src IP: 3:00:12 maudar-jr lightdm: pam_unix(lightdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost= user=maudar User login failed.

** Alert 1355288647.7568: - pam,syslog,authentication_failed, 2012 Dec 12 00:04:07 (UBUNTU) 192.168.30.31->/var/log/auth.log Rule: 5503 (level 5) -> 'User login failed.' Dec 11 13:00:15 maudar-jr lightdm: pam_unix(lightdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost= user=maudar

- La fecha y la hora en la que se genera la alerta
- Un ID de la regla, para este caso: 5503
- El origen de la alerta, es decir desde que maquina se genero
- Un nivel de alerta que nos indica que tan grave fue la alerta

Niveles de Alerta en Ossec

Nivel 0: Ignorado, no se tomaron medidas. Se utiliza principalmente para evitar falsos positivos. Estas reglas se analizan antes de todos los demás y son eventos sin importancia para la seguridad.

Nivel 2: Sistema de notificación de baja prioridad. Sistema de notificación de mensajes de estado o que no tienen ninguna importancia para la seguridad.

Nivel 3: El éxito / eventos autorizados. Intentos exitosos de acceso, permitido en el firewall, etc

Nivel 4: Sistema de errores de baja prioridad. Los errores relacionados con malas configuraciones o dispositivos no utilizados / aplicaciones. No tienen importancia para la seguridad y generalmente son causados??por las Instalaciones por defecto o pruebas de software.

Nivel 5: El usuario los errores generados por contraseñas perdidas, las acciones denegado, etc. Estos mensajes no tienen de seguridad pertinentes.

Nivel 6: Ataques de baja relevancia. Indican un gusano o un virus que no ofrecen ninguna amenaza para el sistema, tales como un gusano de Windows atacar a un servidor Linux. También se incluyen con frecuencia provocado IDS eventos y sucesos comunes de error.

Nivel 9: Error de la fuente no válida. Incluyen los intentos de inicio de sesión como un usuario desconocido o de una fuente no valida. El mensaje podría tener importancia para la seguridad, especialmente si se repite. También se incluyen los errores en relación con el administrador o root.

Nivel 10: Múltiples errores generados por el usuario. Incluyen múltiples contraseñas incorrectas, varios intentos fallidos, etc Puede ser síntoma de un ataque, o podría ser simplemente que un usuario olvidó sus credenciales.

Nivel 12: Alta importancia del evento. Incluyen mensajes de error o de advertencia del sistema, kernel, etc. Podría indicar un ataque contra una aplicación específica.

Nivel 13: Error inusuales (importancia alta).Los patrones comunes de ataque como un intento de desbordamiento de búfer, uno más grande de mensaje syslog normal, o una cadena de URL más larga que la normal.

Nivel 14: Evento de alta seguridad de importancia. Por lo general el resultado de la correlación de las normas de ataque múltiple e indicativa de un ataque.

Nivel 15: Ataque de éxito. Muy pequeña posibilidad de falsos positivos. La atención inmediata es necesaria.

Se puede notar que el atacante intento varias veces acceder sin ningún acierto, lo cual como lo explicamos anteriormente genera más alertas.

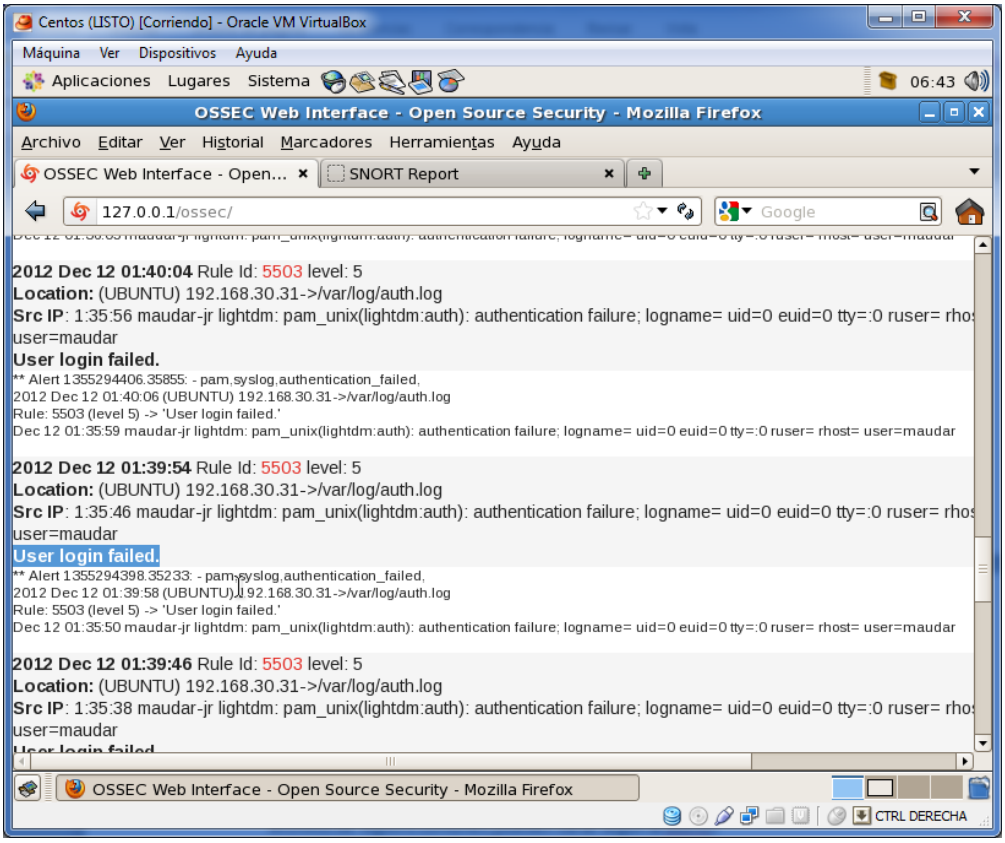


Gráfico 6.55 Alertas de OSSEC

Fuente: Honeynet

6.20.1.2 Análisis forense intrusión 1

Introducción

Ficheros log

En el directorio /var/log aparecerán todos los archivos de registro disponibles. Sus nombres son autoexplicativos.

Archivos de registro comunes (pueden variar según la distro):

/var/log/message: registro de mensajes generales del sistema

/var/log/auth.log: log de autenticación

/var/log/kern.log: registro del kernel

/var/log/cron.log: registro de crond

/var/log/maillog: registro del servidor de mails

/var/log/qmail/: registro de Qmail

/var/log/httpd/: registro de errores y accesos a Apache

/var/log/lighttpd: registro de errores y accesos a Lighttpd

/var/log/boot.log: registro de inicio del sistema

/var/log/mysqld.log: registro de la base de datos MySQL

/var/log/secure: log de autenticación

/var/log/utmp or /var/log/wtmp : registro de logins

Conclusión, en /var/log se almacenan todos los registros del sistema. No obstante, algunas aplicaciones como httpd incluyen ahí dentro un subdirectorio en el que almacenan sus propios archivos de registro.

El fichero /var/log/wtmp

En este fichero se almacenan las conexiones, mediante login, realizadas con éxito. Es un fichero con formato binario y para leerlo tendremos que utilizar el comando last.

Importante

Cada vez que se apaga el sistema se loguea una entrada con el usuario reboot. De esta forma podemos ver los reinicios de la máquina.

Si el fichero no se encuentra en el sistema no se loguea la actividad.

Este fichero es de acceso en modo lectura para todos los usuarios del sistema.

El comando last

Permite ver las conexiones realizadas con éxito a nuestra máquina, si se están logeando en /var/log/wtmp.

El fichero /var/log/btmp

Este fichero es análogo al fichero /var/log/wtmp sólo que registra los intentos fallidos de conexión.

El comando lastb

Tiene la misma funcionalidad que el comando last sólo que para los intentos fallidos de conexión.

El fichero /var/log/lastlog

El fichero almacena la última vez que los usuarios accedieron al sistema. Tiene formato binario con lo cual para consultarlo es necesario utilizar el comando lastlog.

El comando lastlog

Imprime por la salida estándar la última vez que un usuario se conectó al sistema.

Una vez conocido los logs donde se almacenan los accesos de los usuarios al sistema, comprobamos los resultados con los obtenidos del servidor Ossec.

Revisamos el archivo que contiene los log de autentificación (Gráfico 6.55):

```
cat /var/log/auth.log
```

Revisión de los logs

Con los comandos dados en la introducción se procederá a revisar los logs de acceso para corroborar la información dada por la herramienta Ossec.

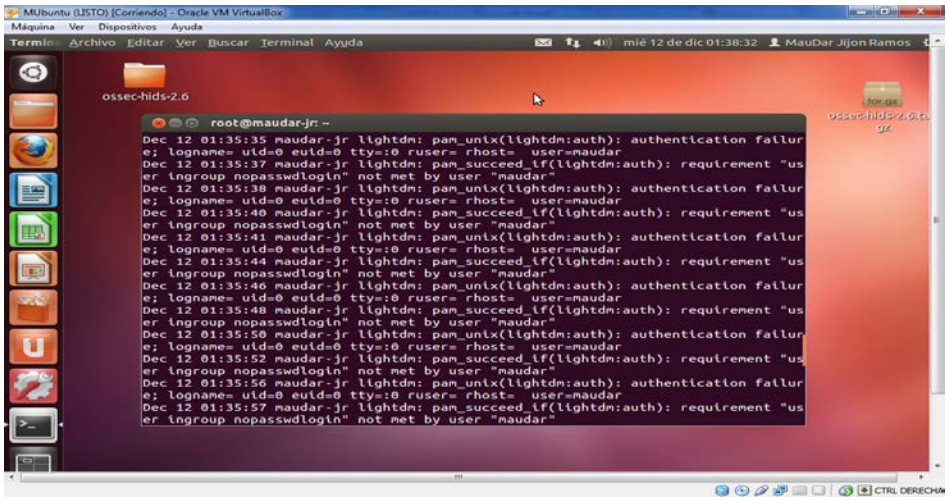


Gráfico 6.56 Logs de Ubuntu

Fuente: Honeynet

Como se puede observar en las imágenes los logs concuerdan con la información que se obtuvo en el servidor Ossec, se encuentran varios intentos de inicio de sesión fallidos.

Y en el siguiente gráfico se encuentran todos los inicios de sesión satisfactorios.

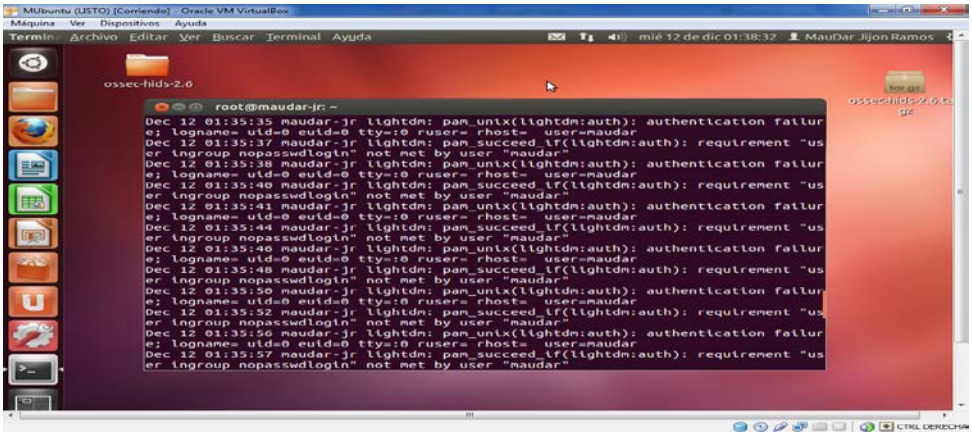


Gráfico 6.57 Últimos usuarios logueados de cliente Ubuntu (Inicio de sesión satisfactoria)

Fuente: Honeynet

6.20.1.3 Resumen del ataque

Resumen del ataque	
Nombre:	Password Guessing
Fecha del Ataque:	12 de diciembre de 2012
S.O. Afectado:	Honeypot Ubuntu
Descripción del ataque:	En este tipo de ataque se intenta adivinar la contraseña de un equipo mediante la fuerza bruta, es una intrusión típica a un sistema, este ataque se facilita debido a que se puede ingresar contraseñas indefinidamente sin ningún tipo de bloqueo por parte del sistema operativo lo que en estaría ayudando al atacante a acceder a la maquina sin tantos problemas.
Estado del Ataque:	No satisfactorio.

Tabla 6.4 Resumen del ataque del mes de diciembre

Fuente: Honeynet

6.20.2 Capturas de Enero

Al revisar los logs de Snort y de Ossec del mes de Enero se notó un gran incremento en la cantidad de alertas recibidas, es por eso que se concluyó que se trata del siguiente ataque:

6.20.2.1 Intrusión 2 – Ataque DDOS

Al revisar los logs de Ossec y Snort nos encontramos con la anomalía:

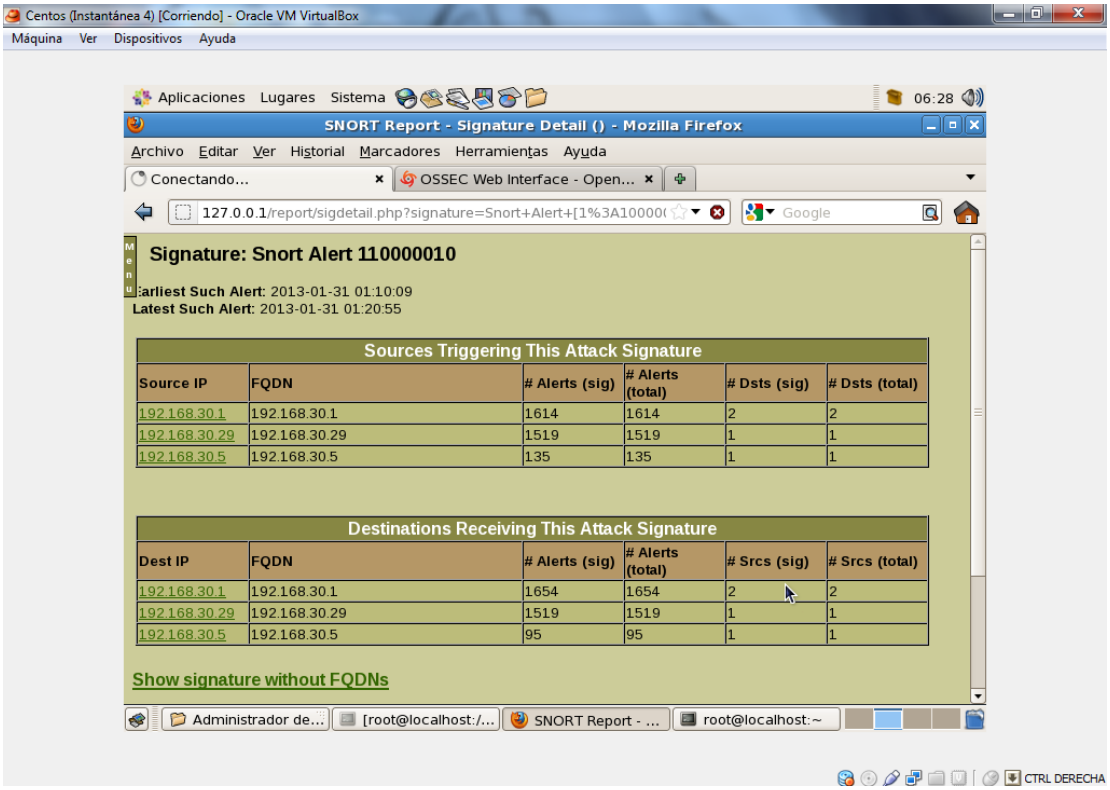


Gráfico 6.58 Logs de Snort

Fuente: Honeynet

Se puede observar que en poco tiempo se generaron **1614** alertas, desde un equipo que se encuentra dentro de la misma Honeynet que probablemente se encuentre infectado, para estar completamente seguros revisamos los log de Ossec

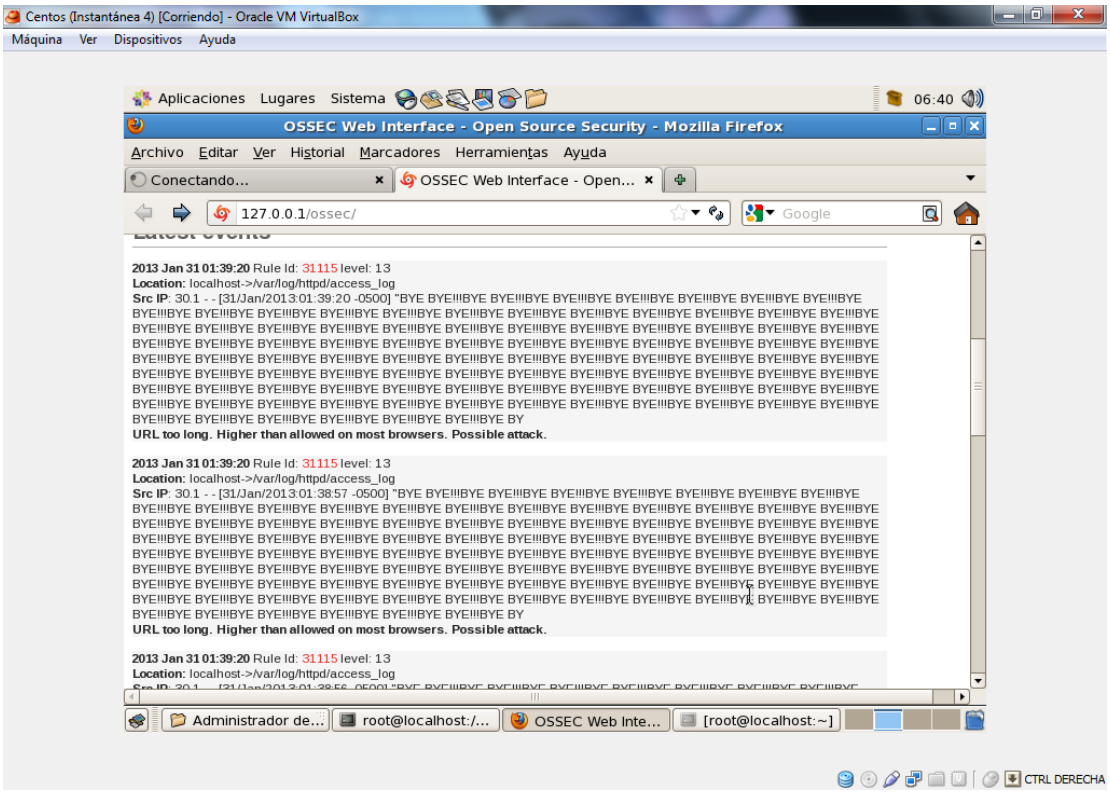


Gráfico 6.59 Logs de OSSEC

Fuente: Honeynet

El mensaje mostrado es: “url too long. Highter tan allowed on most browsers. Posible attack”, este ataque fue dirigido hacia el servidor Centos que forma parte de la Honeynet, en la figura se puede observar que se accedió hacia la url anexando el texto “BYE”, todo esto se corroborara en el análisis forense.

6.20.2.2 Análisis forense intrusión 2

Una vez revisados y comprobado el ataque que se recibió se procede a revisar los logs del servidor en búsqueda más precisa del ataque, obteniendo los siguientes resultados:

Para visualizar de mejor manera se optó por utilizar el editor de texto gedit porque al intentar utilizar el comando cat los resultados no se mostraban en un formato legible.

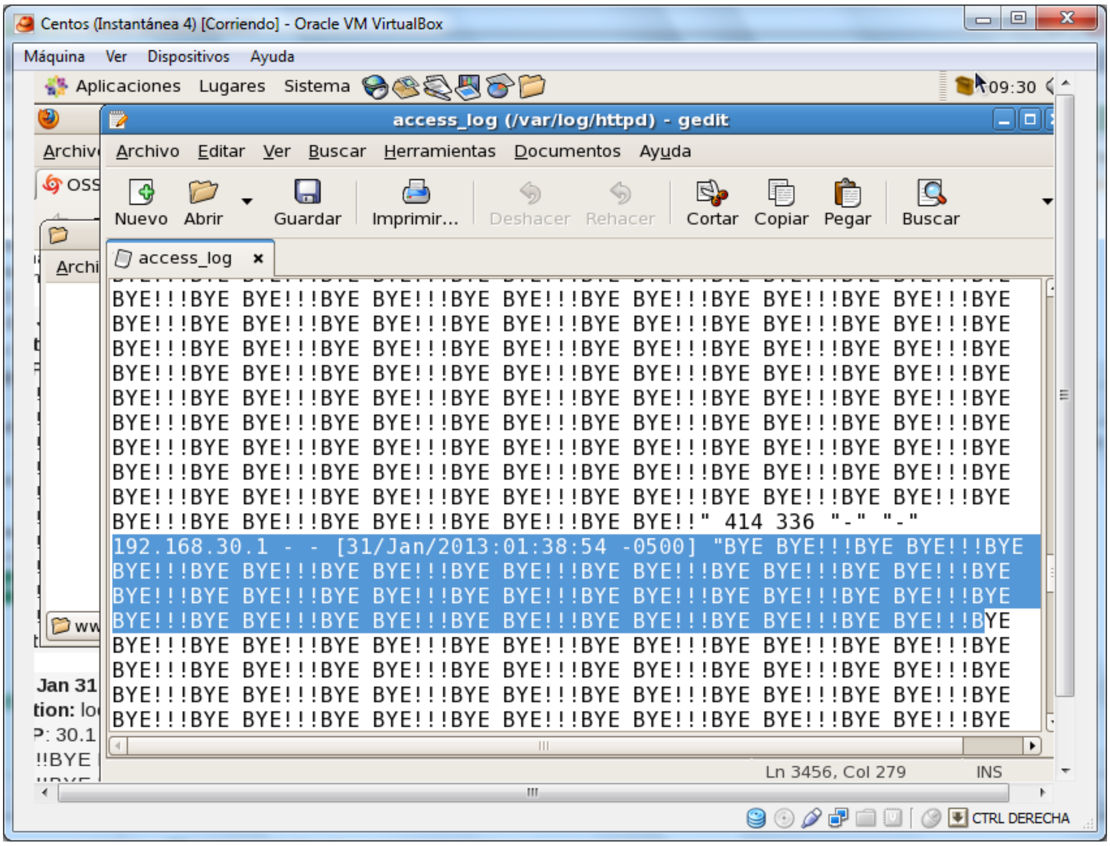


Gráfico 6.60 Logs del servidor

Fuente: Honeynet

Se puede observar que se realiza varias peticiones al servidor con la url " BYE BYE!!! " lo cual representa un ataque DDOS de tipo HTTP FLOOD.

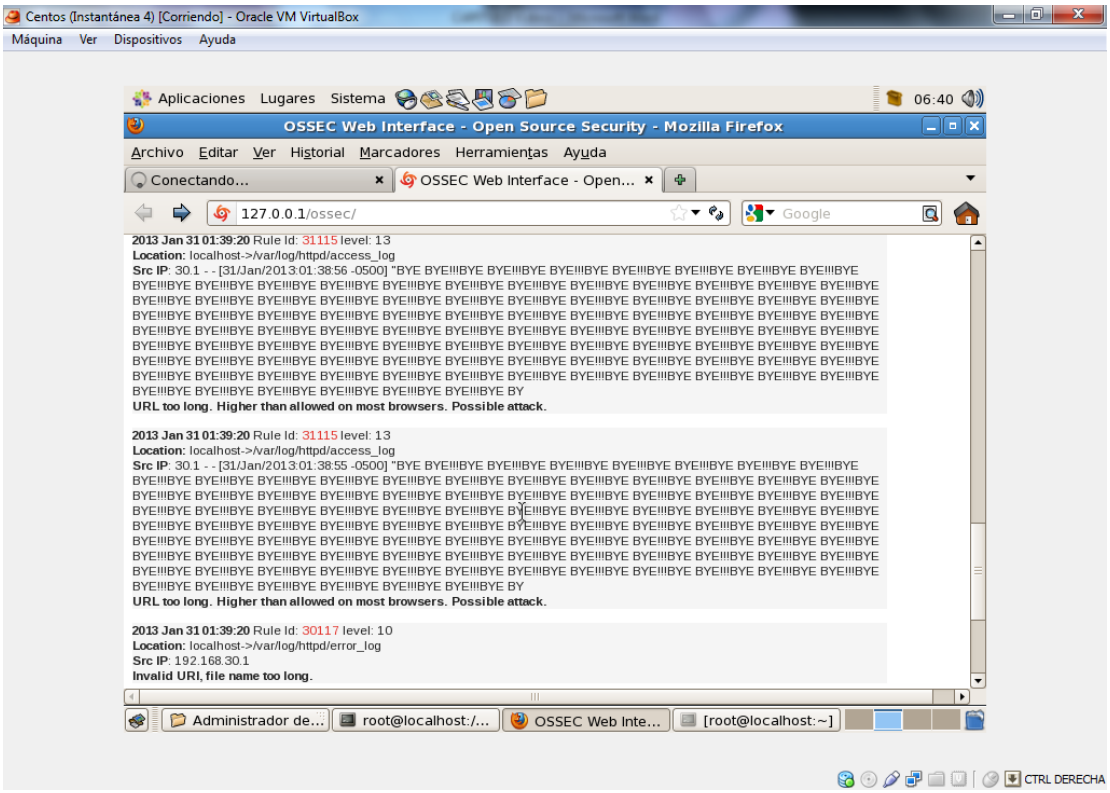


Gráfico 6.61Logs del servidor

Fuente: Honeynet

Explicación de un ataque Http Flood o inundación http

Una inundación HTTP es un método de ataque utilizado para atacar servidores web y aplicaciones. Consiste en enviar conjuntos aparentemente legítimos de sesiones HTTP GET o POST a un servidor web de destino. Estas solicitudes están específicamente diseñadas para consumir una cantidad significativa de recursos del servidor, y por lo tanto pueden dar lugar a una condición de denegación de servicio (sin que necesariamente se requiera una alta tasa de tráfico de red). Estas solicitudes se envían a menudo en masa por medio de una red de bots, incrementando la potencia global del ataque.

Longitudes máximas según el tipo de navegador Web son:

- Internet Explorer: 2 083 caracteres.
- Firefox: 65 536 caracteres.
- Safari: 80 000 caracteres.
- Opera: 190 000 caracteres.

Acorde al servidor web:

- Apache: 4 000 caracteres.
- Microsoft Internet Information Server (IIS): 16 384 caracteres.
- Perl HTTP::Servidor Daemon: 8 000 caracteres.

Urls con más de 2000 caracteres no funcionaran en los navegadores más populares. Sin embargo, el método POST no está limitado por el tamaño de la dirección URL al enviar pares de nombre y valor. Estos pares se transfieren en el encabezado y no en la dirección URL.

6.20.2.3 Resumen del ataque

Resumen del ataque	
Nombre:	Http Flood
Fecha del Ataque:	31 de enero de 2013
S.O. Afectado:	Servidor Centos
Descripción del ataque:	Consiste en enviar conjuntos

	aparentemente legítimos de sesiones HTTP GET o POST a un servidor web de destino. Estas solicitudes están específicamente diseñadas para consumir una cantidad significativa de recursos del servidor, y por lo tanto pueden dar lugar a una condición de denegación de servicio.
Estado del Ataque:	Satisfactorio, para proceder al análisis forense se tuvo que detener los servicios http del servidor.

Tabla 6.5 Resumen del ataque del mes de enero

Fuente**:** Honeynet

6.20.3 Capturas de Febrero

Revisando las capturas de febrero nos encontramos con varias alertas, según un diagnóstico rápido de los logs se trata de un ataque de virus polimórfico al ver que ha cambiado la checksum (suma de verificación) de varios archivos.

6.20.3.1 Intrusión 3 - Virus Polimórfico

Se denomina un virus polimórfico al que produce copias distintas, pero operacionales de sí mismo, esta estrategia ha sido usada con la particularidad de que los antivirus no sean capaces de detectar todas las variaciones del virus.

Una de las técnicas para hacer virus polimórficos es seleccionar entre distintos métodos de cifrado con distintas rutinas de descifrado solo una de estas rutinas esta en claro en cualquier forma del virus.

Detección

Hay algunos antivirus que pueden detectar virus polimórficos observando eventos característicos que los mismos deben realizar para sobrevivir y expandirse. Cualquier virus, sin importar sus características debe hacer ciertas cosas para sobrevivir. Por ejemplo, debe infectar otros archivos y residir en memoria.

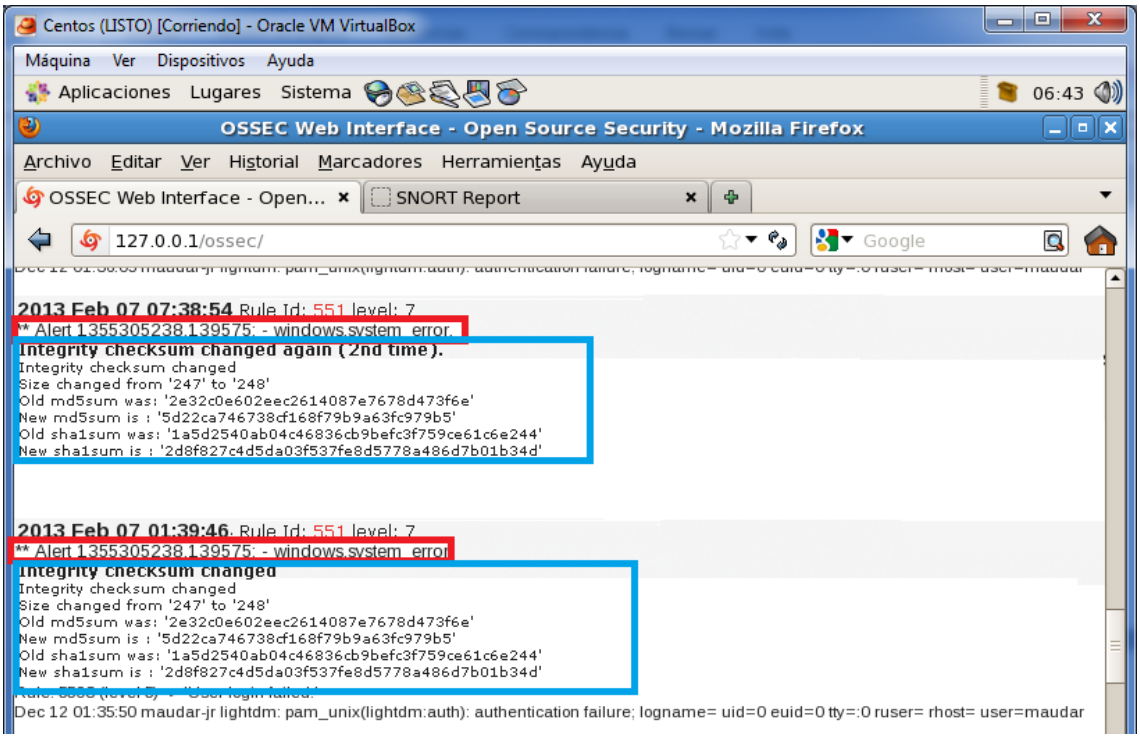


Gráfico 6.62 Logs de OSSEC (checksum cambiando)

Fuente: Honeynet

Como se observa en el Gráfico el ataque fue realizado hacia el Honeypot que tiene instalado el sistema operativo Windows XP

Suma de verificación

Una suma de verificación, también llamada suma de chequeo o checksum, es una función hash que tienen como propósito principal detectar cambios accidentales en una secuencia de datos para proteger la integridad de datos, verificando que no haya discrepancias. La idea es que se transmita el dato junto con su valor hash, de esta forma el receptor puede calcular el valor hash de la secuencia recibida y la puede comparar con el valor hash recibido. Si hay una discrepancia se pueden rechazar los datos o pedir una retransmisión.

Esto es empleado para comunicaciones (Internet, comunicación de dispositivos, etc.) y almacenamiento de datos (archivos comprimidos, discos portátiles, etc.).

6.20.3.2 Análisis Forense Intrusión 3

Para el análisis forense nos centraremos únicamente en un archivo ya que el método de ataque es similar para todos los archivos infectados.

Utilizaremos el archivo “cmd.exe” que es el que abre la ventana de comandos de Windows para pasar a ver el proceso de infección por el que ha pasado y como ha afectado esto en su tamaño.

El archivo cmd.exe lo podemos encontrar en la carpeta

C:\\WINDOWS\system32

Peso normal del archivo cmd.exe: 381KB

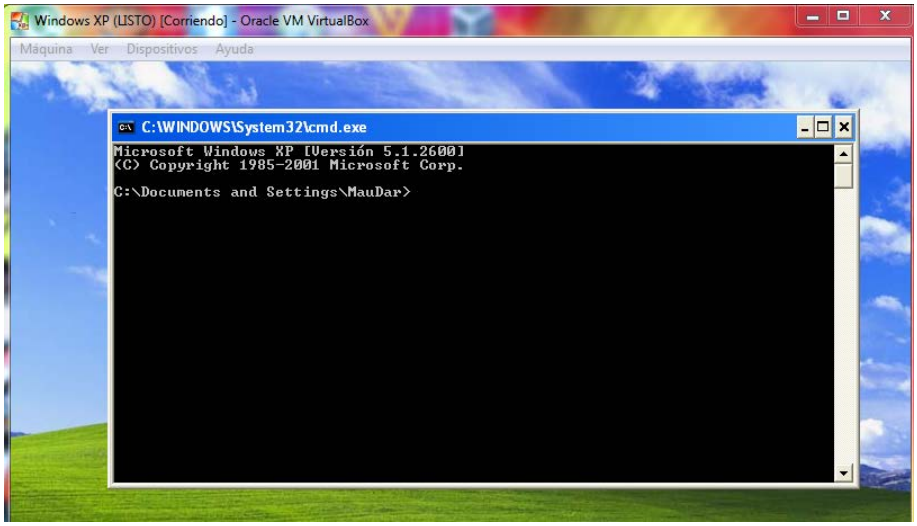


Gráfico 6.63 Ventana "cmd" en cliente Windows XP

Fuente: Honeynet

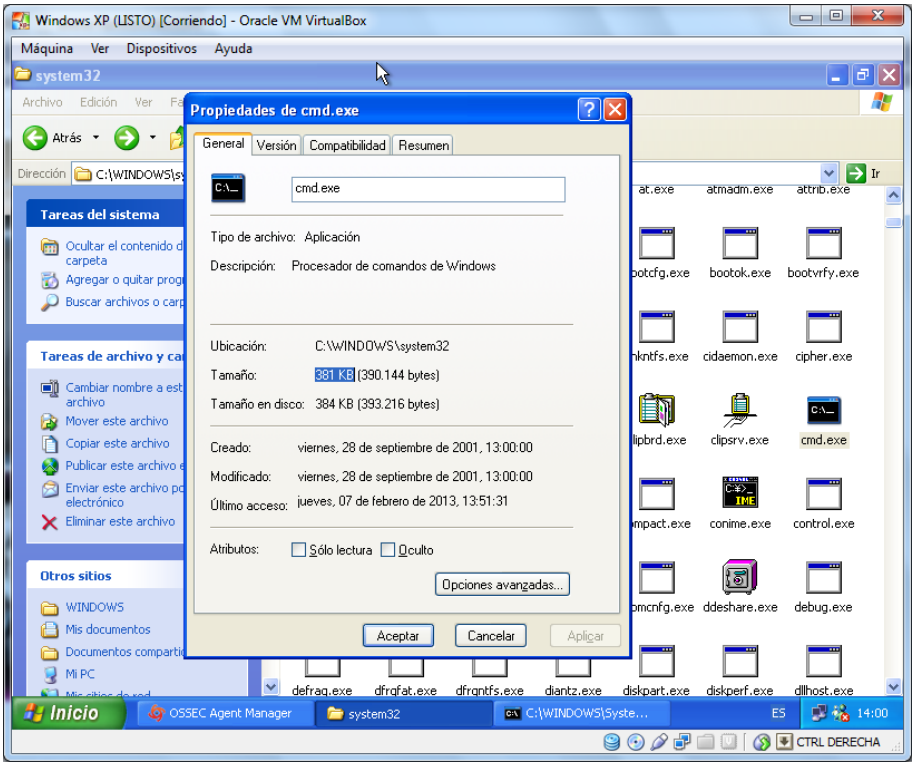


Gráfico 6.64 Propiedades archivo cmd

Fuente: Honeynet

Después de varias horas se volvió a observar las propiedades del archivo “cmd.exe” dando a notar un cambio en su tamaño:

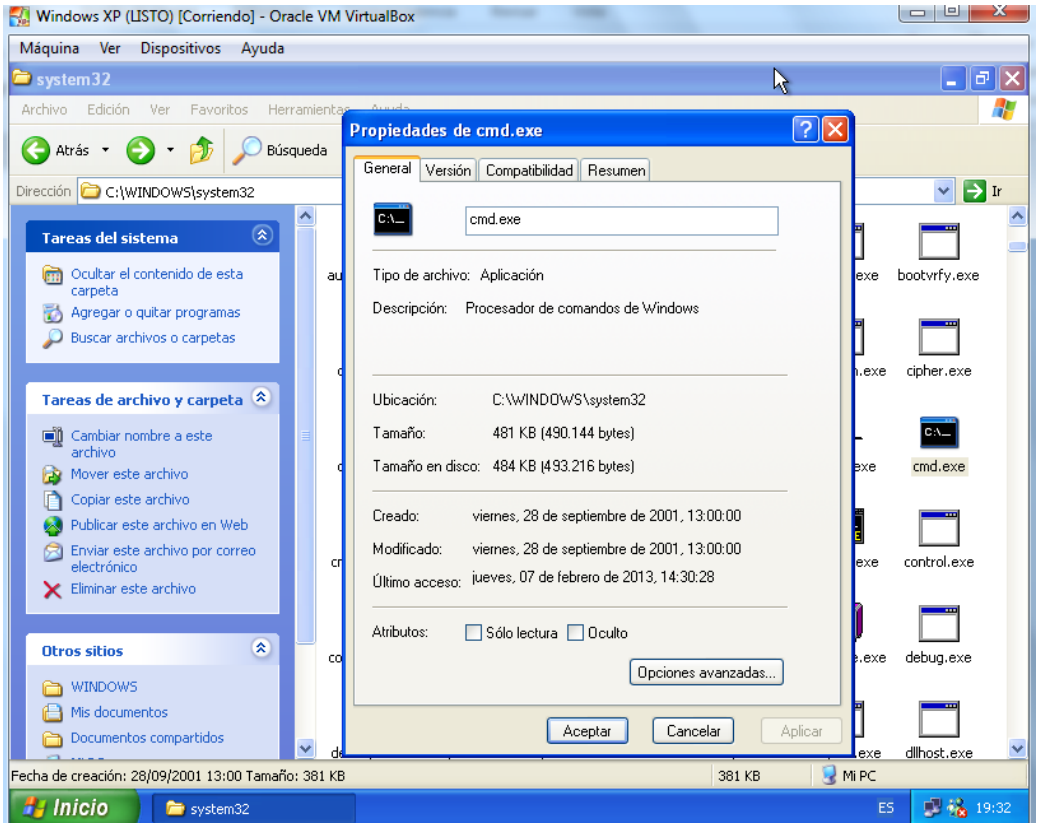


Gráfico 6.65 Propiedades archivo cmd infectado

Fuente: Honeynet

Ahora el archivo pesaba 481KB, 100KB mas pesado que en la anterior revisión.

Al realizar una tercera revisión al archivo días después se notó que había incrementado su peso aún más:

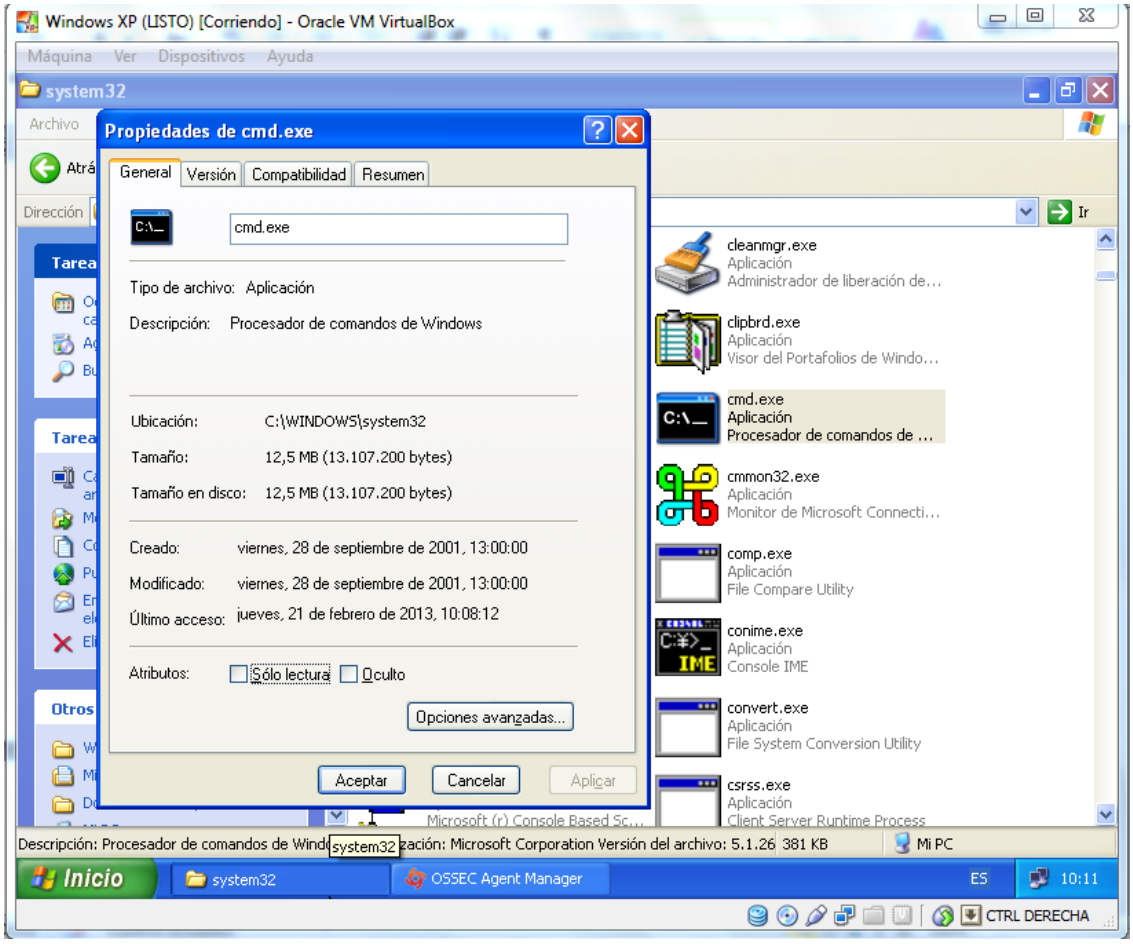


Gráfico 6.66 Propiedades archivo cmd infectado

Fuente: Honeynet

Ahora su peso es de 12,5 MB en comparación con los 381 KB que pesa el archivo normalmente. Con esto se pudo comprobar como un virus polimórfico afecta a los archivos modificando su peso e inyectando otra versión del mismo virus para seguirse replicando hasta colapsar la maquina ocupando todo el espacio en el disco duro.

Para obtener más información acerca de este virus se procedió a analizarlo en la página: https://www.virustotal.com/es/

Gráfico 6.67 Análisis de archivo infectado en sitio virus total

Fuente: https://www.virustotal.com/es/

Podemos ver que el resultado de la infección es positivo, se trata del virus"W32.Junkcomp", a continuación se buscará más información del mismo.

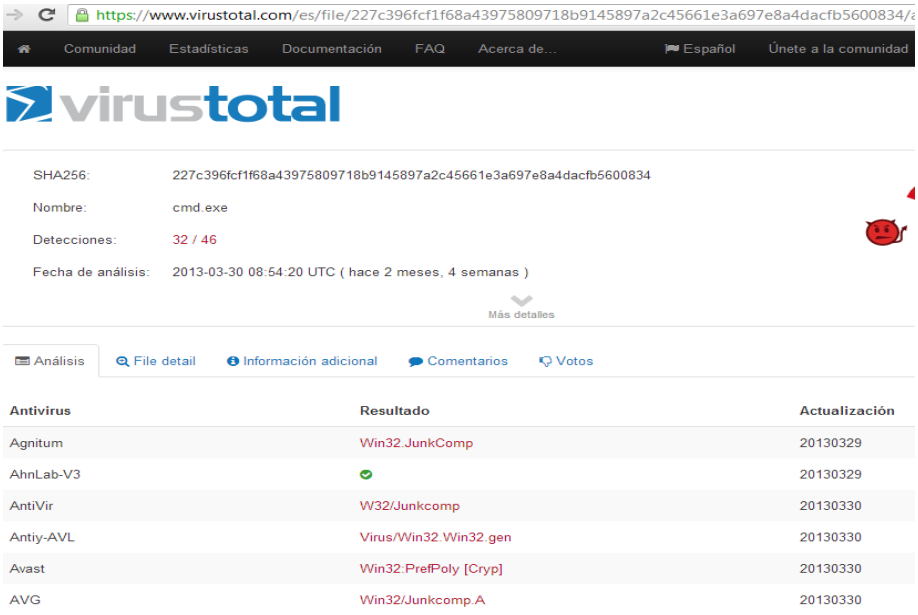


Gráfico 6.68 Resultados positivos Análisis de archivo infectado

Fuente: https://www.virustotal.com/es/

En el sitio web de Symantec encontramos más información acerca de este virus, lo que concuerda con los informes de la Honeynet y el análisis forense, es decir de que se trata de un virus polimórfico.

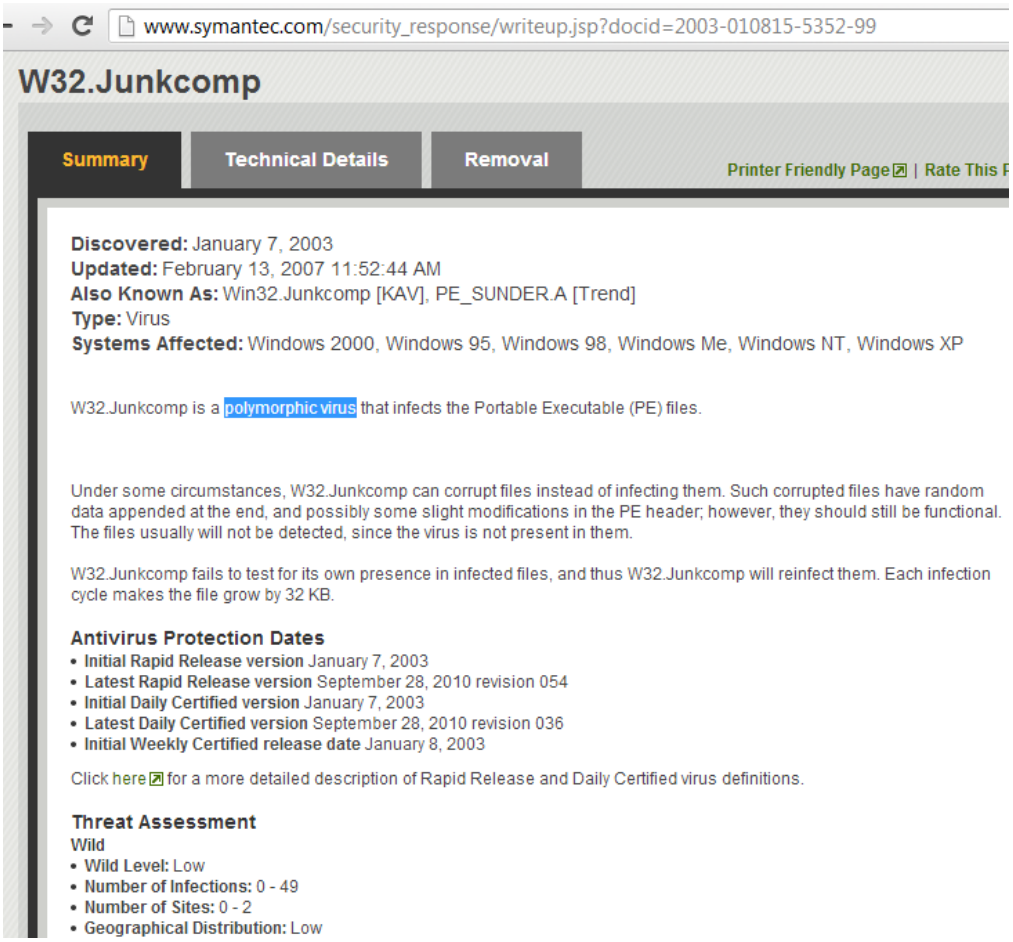


Gráfico 6.69 Información extra acerca de virus detectado

Fuente: http://www.symantec.com

6.20.3.3 Resumen del ataque

Resumen del ataque	
Nombre:	Virus Polimórfico(W32.Junkcomp)

Fecha del Ataque:	7 de febrero de 2013
S.O. Afectado:	Honeypot Windows
Descripción del ataque:	Los virus polimórficos tratan de evadir la detección cambiando su patrón de byte con cada infección, así que no existe una secuencia de bytes constante que un programa antivirus pueda buscar. Pero si se puede rastrear un cambio en la checksum de cada archivo.
Estado del Ataque:	Satisfactorio, varios archivos de la carpeta System32 resultaron infectados, creciendo de tamaño hasta hacer colapsar el S.O.

Tabla 6.6 Resumen del ataque del mes de febrero

Fuente: Honeynet

6.21 Políticas de seguridad a seguir para la optimización de la seguridad informática.

Una vez realizada la captura de datos con el uso de la Honeynet y al evidenciar los patrones de ataques que se obtuvieron, se plantean las siguientes políticas de seguridad, según el tipo de intrusión que se tuvo y el sistema operativo afectado.

6.21.1 Intrusión 1.- Password guessing

6.21.1.1 Para Windows

Directivas de cuentas

Las directivas de cuentas nos permiten configurar el comportamiento que van a tener estas ante una serie de sucesos. La importancia de una correcta configuración de estas directivas radica en que desde ellas vamos a poder controlar de una forma más eficiente la forma de acceder a nuestro ordenador.
Ante todo, estamos ante unas configuraciones Administrativas. Esto quiere decir dos cosas. En primer lugar, que solo los administradores de equipos pueden acceder a ellas, y en segundo lugar, que cuando toquemos algún parámetro dentro de este apartado debemos estar muy seguros de lo que estamos haciendo. No se trata de una parte de configuración con la que se puedan hacer experimentos, ya que podemos dejar inaccesible a nuestro sistema operativo.
Dicho esto, vamos a ver en primer lugar como accedemos a la ventana de Directivas de seguridad de cuentas.

Para eso accedemos al Panel de control y seleccionamos la opción “Herramientas Administrativas”

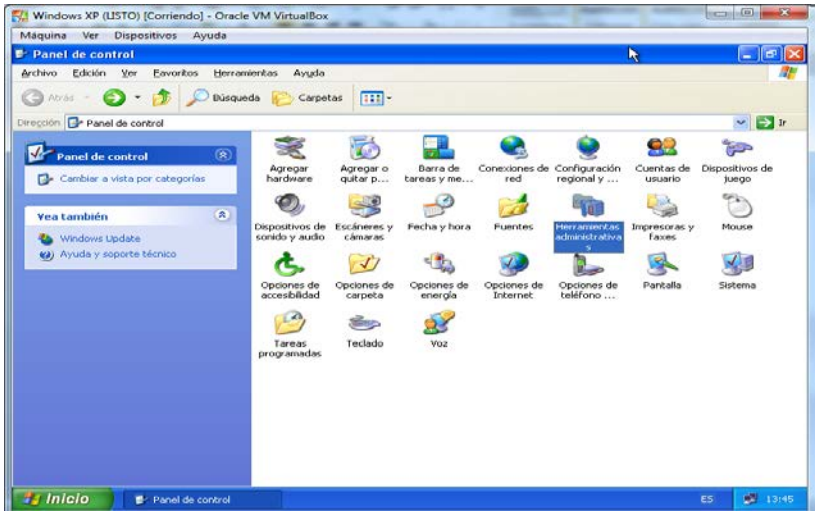


Gráfico 6.70 Herramientas Administrativas

Fuente: Honeynet

Una vez dentro seleccionamos la opción “Directiva de seguridad local”.

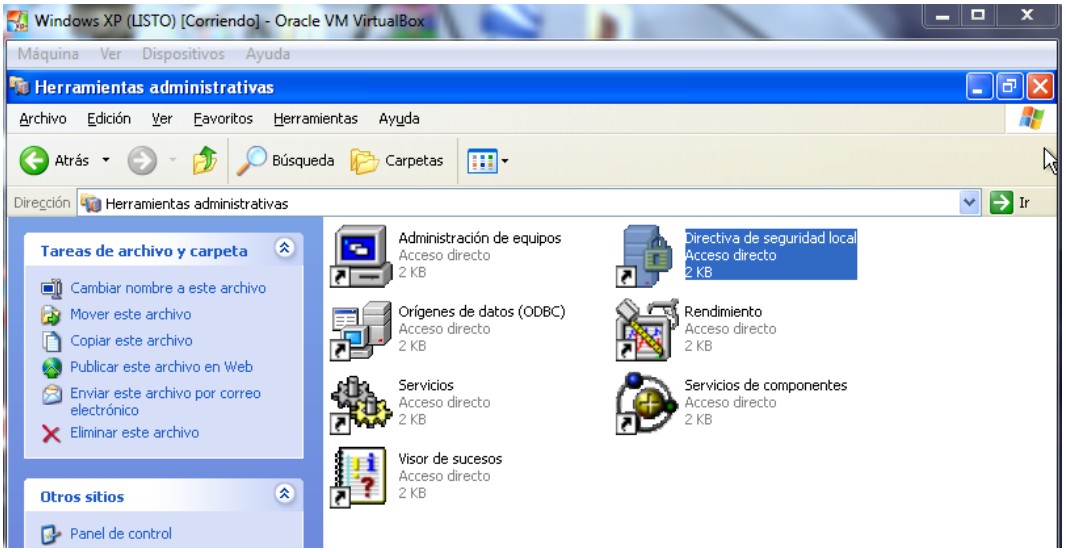


Gráfico 6.71 Directiva de Seguridad local

Fuente: Honeynet

Dentro del apartado “Directivas de cuenta” podemos configurar todo lo relacionado con el inicio de sesión y bloqueo de cuentas que es lo que vamos a realizar.

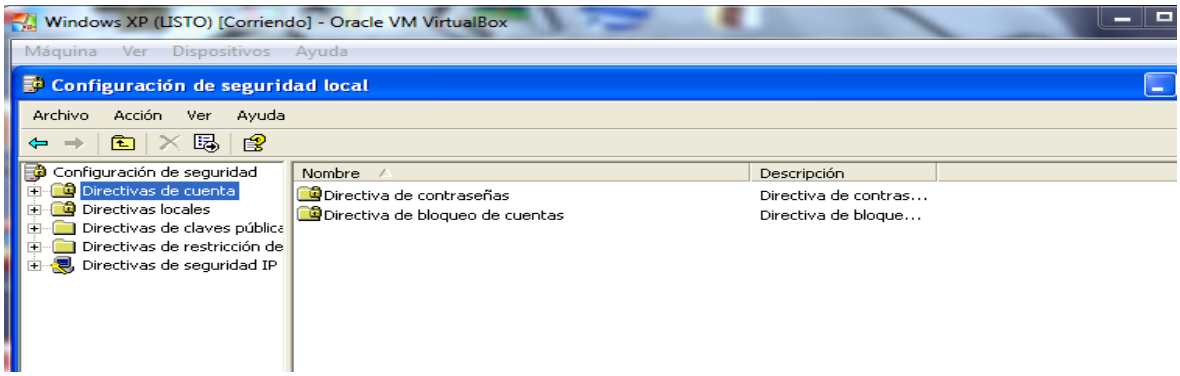


Gráfico 6.72 Directivas de cuenta

Fuente: Honeynet

En la opción Directiva de contraseñas nos muestra varias opciones:

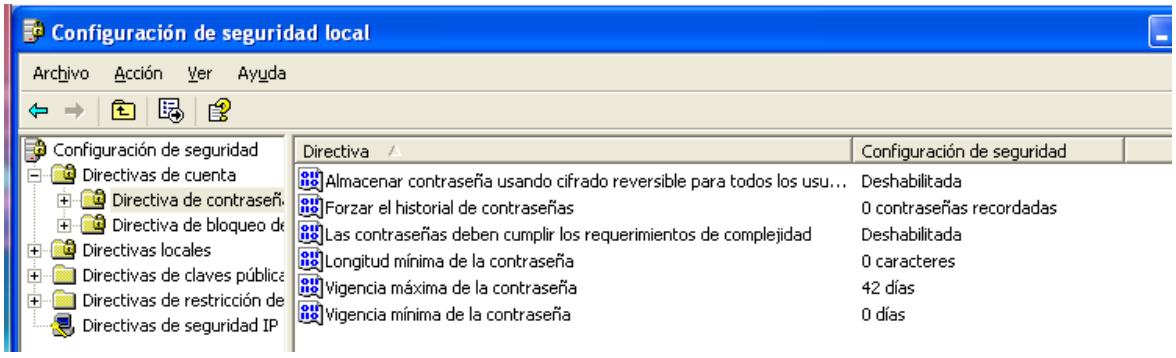


Gráfico 6.73 Directivas de Contraseñas

Fuente: Honeynet

Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio.- Su mismo nombre indica para qué se utiliza. Las opciones

son Habilitado o Deshabilitado.

Forzar el historial de contraseñas.- Establece el número de contraseñas a recordar.

Las contraseñas deben cumplir los requerimientos de complejidad.- Obliga a que las contraseñas cumplan unos requisitos de complejidad.

Longitud mínima de la contraseña. - Obliga a que las contraseñas tengan un mínimo de caracteres, estableciendo este mínimo.

Vigencia máxima de la contraseña. - Establece el número de días máximo que una contraseña va a estar activa.

Vigencia mínima de la contraseña.- Establece el número de días mínimos que una contraseña va a estar activa.

Según el caso se configuraran estas directivas para que cada usuario cree una contraseña segura para su inicio de sesión y se evite crear contraseñas débiles las cuales podrían comprometer la seguridad del sistemas operativo.

Según la página de Microsoft:

http://www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx
sugiere que se establezcan los siguientes valores:

Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio

Predeterminada del controlador de dominio	Cliente de empresa	Nivel de seguridad alto
Deshabilitado	Deshabilitado	Deshabilitado

Tabla 6.7 Valores recomendados para almacenar contraseñas

Fuente: www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

La configuración Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio determina si el sistema operativo almacena contraseñas con el cifrado reversible. Admite las aplicaciones que utilizan protocolos que requieren que se conozca la contraseña del usuario para la autenticación. El almacenamiento de contraseñas con el cifrado reversible es prácticamente la misma operación que almacenar versiones en texto no cifrado de las contraseñas. Por esta razón, esta directiva nunca se debe habilitar a menos que los requisitos de la aplicación tengan más peso que la necesidad de proteger la información de contraseña. El valor predeterminado de esta configuración es Deshabilitado.

Asegúrese de que el valor de Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio es Deshabilitado. Esta directiva se deshabilita en el GPO predeterminado de dominios de Windows Server 2003 y en la directiva de seguridad local para las estaciones de trabajo y servidores.

Debido a la gran vulnerabilidad que produce la activación de esta directiva, Microsoft recomienda utilizar el valor predeterminado Deshabilitado en los dos entornos definidos en esta guía.

Forzar el historial de contraseñas

Predeterminada del controlador de dominio	Cliente de empresa	Nivel de seguridad alto
24 contraseñas	24 contraseñas	24 contraseñas

Tabla 6.8 Valores recomendados el historial de contraseñas

Fuente: www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

La configuración Forzar el historial de contraseñas determina el número de nuevas contraseñas únicas que se deben asociar con una cuenta de usuario antes de que se pueda reutilizar una contraseña anterior. El valor debe estar entre 0 y 24 contraseñas. El valor predeterminado de Windows XP es de 0 contraseñas, pero el de un dominio es de 24. Para mantener la efectividad del historial de contraseñas, utilice la configuración Vigencia mínima de la contraseña, y evite de esta forma que los usuarios puedan cambiar reiteradamente sus contraseñas y burlar la configuración Forzar el historial de contraseñas.

Establezca la configuración Forzar el historial de contraseñas como 24 contraseñas para los dos entornos de seguridad definidos en esta guía. El valor de configuración máximo mejora la seguridad de las contraseñas al garantizar que los usuarios no pueden reutilizar las contraseñas fácilmente, ni por accidente ni intencionadamente. También contribuye a que las contraseñas robadas por un atacante se invaliden antes de que se puedan emplear para burlar la seguridad de

una cuenta de usuario. No existen problemas conocidos relacionados con la configuración de este parámetro en su valor máximo.

Las contraseñas deben cumplir los requerimientos de complejidad

Predeterminada del controlador de dominio	**Cliente de empresa**	**Nivel de seguridad alto**
Habilitado	Habilitado	Habilitado

Tabla 6.9 Valores recomendados para requerimientos de complejidad de la contraseña.

Fuente: www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

Las contraseñas deben cumplir los requerimientos de complejidad comprueba todas las nuevas contraseñas para asegurarse de que se cumplen los requisitos básicos de las contraseñas seguras.

Longitud mínima de la contraseña

(Ver Tabla 6.10 en la siguiente página)

Predeterminada del controlador de dominio	**Cliente de empresa**	**Nivel de seguridad alto**
7 caracteres	8 caracteres	12 caracteres

Tabla 6.10 Valores recomendados para la longitud mínima de la contraseña

Fuente: www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

La configuración Longitud mínima de la contraseña requiere que las contraseñas incluyan un número específico de caracteres. Las contraseñas largas, de 8 o más caracteres, son generalmente más seguras que las cortas. Con esta configuración, los usuarios no pueden usar contraseñas en blanco, sino que además, deben crear contraseñas con un número determinado de caracteres. El valor predeterminado es de 0 caracteres.

Vigencia máxima de la contraseña

Predeterminada del controlador de dominio	**Cliente de empresa**	**Nivel de seguridad alto**
42 días	42 días	42 días

Tabla 6.11 Valores recomendados para la vigencia máxima de la contraseña

Fuente: www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

Los valores de esta configuración van de 1 a 999 días. También puede definir el valor como 0 para especificar que las contraseñas nunca caduquen. Esta configuración define el período en el que un atacante que ha llegado a conocer una contraseña puede utilizarla para tener acceso a un equipo de la red antes de que la contraseña caduque. El valor predeterminado de esta configuración es de 42 días.

Establezca la configuración Vigencia máxima de la contraseña en un valor de 42 días para los dos entornos de seguridad definidos en esta guía. La mayoría de las contraseñas se pueden llegar a averiguar, por tanto, cuanto mayor sea la

frecuencia con la que éstas se cambien, menores serán las posibilidades de que el atacante pueda utilizarlas.

Vigencia mínima de la contraseña

Predeterminada del controlador de dominio	**Cliente de empresa**	**Nivel de seguridad alto**
1 día	2 días	2 días

Tabla 6.12 Valores recomendados para la vigencia mínima de la contraseña

Fuente: www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

La configuración Vigencia mínima de la contraseña determina el número de días que se debe utilizar una contraseña antes de que el usuario la cambie. Los valores van de 1 a 999 días, o bien, se puede permitir que la contraseña cambie inmediatamente estableciendo el valor en 0. El valor predeterminado es de 0 días.

El valor de la configuración Vigencia mínima de la contraseña debe ser inferior al especificado para Vigencia máxima de la contraseña, a menos que el valor de esta última opción se configure como 0, lo que hace que la contraseña nunca caduque. Si el valor de Vigencia máxima de la contraseña se configura como 0, el valor de Vigencia mínima de la contraseña se puede configurar en cualquier valor entre 0 y 999.

En el apartado Directiva de bloqueo de cuentas, tenemos las siguientes opciones:

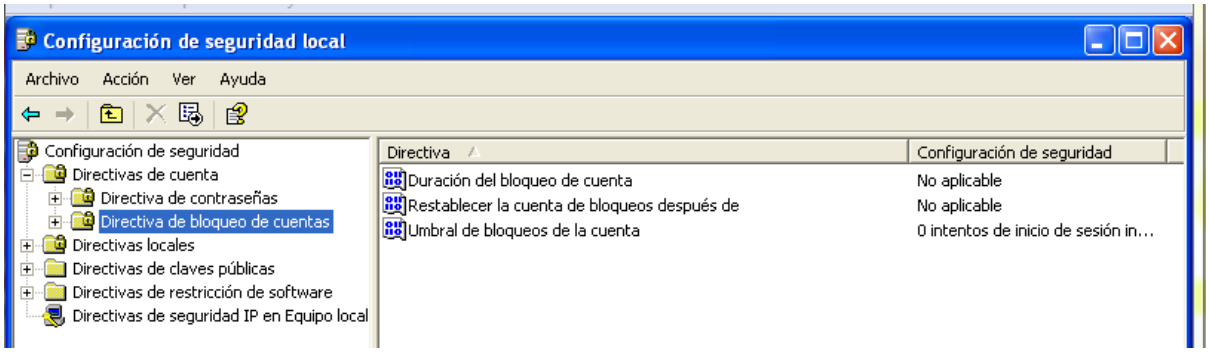


Gráfico 6.74 Directivas de Bloqueo de Cuentas

Fuente: honeynet

Duración del bloqueo de cuentas.- Establece, en minutos, el tiempo que una cuenta debe permanecer bloqueada.

Restablecer la cuenta de bloqueos después de.- Establece, en minutos, el tiempo que ha de pasar para restablecer la cuenta de bloqueos.

Umbral de bloqueos de la cuenta. -Establece el número de intentos fallidos para bloquear el acceso a una cuenta.

Según la página de Microsoft:

http://www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

sugiere que se establezcan los siguientes valores:

Duración del bloqueo de cuenta

(Ver tabla 6.13 en la siguiente página)

Predeterminada del controlador de dominio	Cliente de empresa	Nivel de seguridad alto
No está definido	30 minutos	30 minutos

Tabla 6.13 Valores recomendados para la duración del bloqueo de cuenta

Fuente: www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

La configuración Duración del bloqueo de cuenta determina el tiempo que debe pasar antes de que una cuenta se bloquee y de que un usuario pueda volver a intentar iniciar sesión. Funciona especificando el número de minutos que permanece no disponible una cuenta bloqueada. Si el valor de Duración del bloqueo de cuenta se configura en 0, las cuentas permanecen bloqueadas hasta que el administrador las desbloquea. El valor predeterminado de Windows XP para esta configuración es No está definido.

Para reducir el número de llamadas al servicio de asistencia y al mismo tiempo favorecer una infraestructura segura, configure el valor de Duración del bloqueo de cuenta en 30 minutos para los dos entornos definidos en esta guía.

Restablecer la cuenta de bloqueos después de

(Ver tabla 6.14 en la siguiente página)

Predeterminada del controlador de dominio	Cliente de empresa	Nivel de seguridad alto
No está definido	30 minutos	30 minutos

Tabla 6.14 Valores recomendados para la restitución de la contraseña.

Fuente: www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

La configuración Restablecer la cuenta de bloqueos después de determina la cantidad de tiempo antes de que Umbral de bloqueos de la cuenta se restablezca a 0. El valor predeterminado de esta configuración es No está definido. Si se define Umbral de bloqueos de la cuenta, este tiempo de restablecimiento debe ser inferior o igual al valor de Duración del bloqueo de cuenta.

Configure Restablecer la cuenta de bloqueos después de en 30 minutos para los dos entornos definidos en esta guía.

Umbral de bloqueos de la cuenta

Predeterminada del controlador de dominio	Cliente de empresa	Nivel de seguridad alto
0 intentos de inicio de sesión incorrectos	50 intentos de inicio de sesión incorrectos	50 intentos de inicio de sesión incorrectos

Tabla 6.15 Valores recomendados para el umbral de bloqueos de la cuenta

Fuente: www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx

La configuración Umbral de bloqueos de la cuenta determina el número de intentos que puede realizar el usuario para iniciar sesión en una cuenta antes de que ésta se bloquee.

Los usuarios autorizados pueden bloquear sus propias cuentas al no recordar su contraseña, al escribirla incorrectamente o al cambiarla en un equipo mientras han iniciado sesión en otro.

Configure el valor de Umbral de bloqueos de la cuenta en 50 intentos de inicio de sesión incorrectos para los dos entornos definidos en esta guía.

6.21.1.2 Para Linux

Forzar la creación de contraseñas robustas

Es una buena idea para los administradores de sistemas verificar que las contraseñas usadas dentro de la organización sean robustas

Normalmente, las distribuciones actuales utilizan contraseñas MD5 por defecto:

Permiten más de 8 caracteres (contraseñas DES limitadas a 8 caracteres)

En el fichero /etc/shadow empiezan por 1

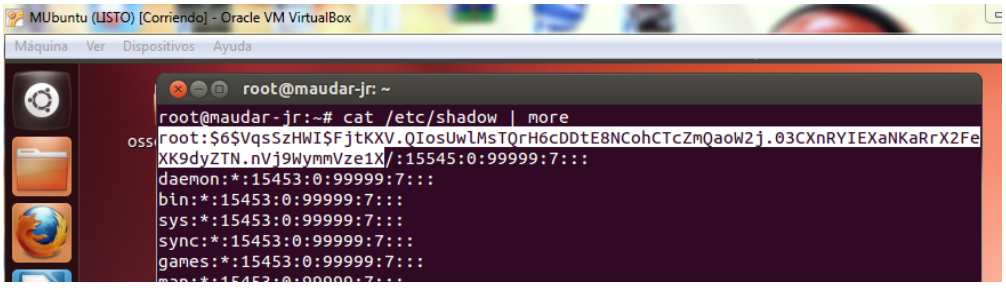


Gráfico 6.75 Archivo shadow de cliente Ubuntu

Fuente: Honeynet

Podemos forzar un tamaño mínimo mediante PAM(Pluggable Authentication Modules), poniendo en el fichero

/etc/pam.d/common-password

password required pam_unix.so md5 nullok obscure min=6 max=16

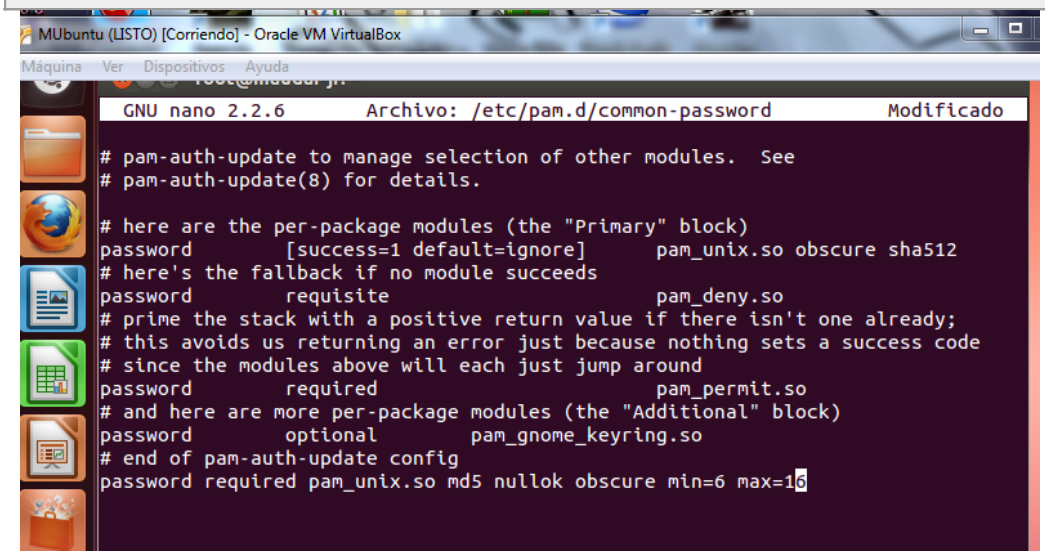


Gráfico 6.76 Directivas de cuenta

Fuente: Honeynet

También podemos usar PAM para verificar si la contraseña es fácil de descifrar o si es demasiado corta, a través del módulo PAM pam_cracklib.so

Para que este módulo funcione, debemos instalar el paquete libpam-cracklib

Alternativamente, es posible añadir más verificaciones para la integridad de la contraseña, tales como pam_passwdqc (paquete libpam-passwdqc)

Ejemplo de uso de librería libpam-cracklib:

Instalación de la librería:

```
# apt-get install libpam-cracklib
```

Y la activaremos en el fichero common-password:

```
# vi /etc/pam.d/common-password
password requisite pam_cracklib.so retry=3 minlen=8 difok=3
```

Esta línea la tendremos que colocar arriba del todo del bloque primario (“Primary” block)

Además esta librería nos permite realizar varias restricciones, por ejemplo

```
password requisite pam_cracklib.so try_first_pass retry=3 minlen=8 lcredit=1 ucredit=1 dcredit=1 ocredit=0
```

Dónde:

minlen: especifica el número mínimo de caracteres.

lcredit: especifica el número mínimo de letras minúsculas.

ucredit: especifica el número mínimo de letras mayúsculas.

dcredit: especifica el número mínimo de caracteres numéricos ocredit especifica el número de caracteres de otro tipo, como por ejemplo símbolos.

Este ejemplo requerirá 1 minúscula y 1 mayúscula, además de un número.

Otra cosa que se puede hacer para mejorar la seguridad es obligar a los usuarios a cambiar su password cada tiempo, esto se hace en el fichero login.defs:

```
/etc/login.defs
PASS_MAX_DAYS 60
```

```
PASS_MIN_DAYS 7
PASS_WARN_AGE 10
```

Nos hará cambiar la contraseña pasados 2 meses, avisándonos cada vez que hagamos login los 10 días previos a la caducidad.

6.21.2 Intrusión 2.- Ataque DDOS

6.21.2.1 Para Windows

Podemos evitar un ataque DDOS utilizando el editor de registros creando un registro con ciertas características:

Para eso vamos a => INICIO=>EJECUTAR, y escribimos "regedit"

Ahora vamos a =>

```
HKey_Local_Machine/ System/ CurrentControlSet/ Services/ Tcpip/ Parameters
```

(Para Equipos basados en la arquitectura NT, como Windows 2000 o XP)

Colocamos los siguientes valores DWORD:

```
EnableICMPRedirect = 0
SynAttackProtect = 2
TCPMaxConnectResponseRetransmissions = 2
TCPMaxHalfOpen = 500
TCPMaxHalfOpenRetired = 400
TCPMaxPortsExhausted = 5
TCPMaxDataRetransmissions = 3
EnableDeadGWDetect = 0
```

```
EnablePMTUDiscovery = 0

NoNameReleaseOnDemand = 1

PerformRouterDiscovery = 0
```

Explicación de los parámetros usados:

EnableICMPRedirect = 0(Se deshabilitan las redirecciones ICMP, impidiendo que un ataque se redirija a un tercero).

SynAttackProtect = 2 (Establece el límite SYN, para que no se cree una situación en la que la conexión TCP se bloquee en un estado semi abierto. La configuración predeterminada es 0. Un valor de 2 controla la caducidad de las conexiones abiertas y medio abiertas).

TCPMaxConnectResponseRetransmissions = 2 (Determina las veces que TCP transmite un mensaje SYN/ACK que no es respondido. TCP retransmite confirmaciones hasta alcanzar el número de este valor).

TCPMaxHalfOpen = 500 (Número de conexiones que el servidor puede mantener en estado semi abierto antes de que TCP/IP inicie la protección contra ataques SYN).

TCPMaxHalfOpenRetired = 400 (Número de conexiones que el servidor puede mantener en estado semi abierto, incluso después de retransmitir una conexión. Si se sobrepasa esta entrada, TCP/IP inicia la protección contra ataques SYN).

TCPMaxPortsExhausted = 5 (Número de solicitudes de conexión que el sistema rechazará antes de que TCP/IP inicie la protección contra ataques SYN).

TCPMaxDataRetransmissions = 3 (Número de veces que TCP retransmite un segmento de datos desconocido en una conexión existente).

EnableDeadGWDetect = 0 (Determina si el ordenador tiene que detectar puertas de enlace inactivas. Un valor de 1 implica que el sistema solicite a TCP que cambie a una puerta de enlace de reserva en caso de conexiones con problemas. Las puertas de enlace de reserva están definidas en <st1>ersonName productid="la Configuración TCP" wt="on">la Configuración TCP</st1>ersonName>/IP, en Red, del Panel de control).

EnablePMTUDiscovery = 0 (Determina si está habilitado el descubrimiento MTU de ruta de acceso, donde TCP descubre el paquete de mayor tamaño en la ruta a un host remoto).

DisableIPSourceRouting = 2 (Determina si un Equipo permite que los clientes conectados establezcan la ruta que los paquetes deben seguir hasta su destino. Un valor de 2 impide el enrutamiento de origen de los paquetes IP).

NoNameReleaseOnDemand = 1 (Determina si el Equipo libera su nombre NetBIOS a otro Equipo que lo solicite o si un paquete malintencionado quiere apropiarse del nombre NetBIOS).

PerformRouterDiscovery = 0 (Determina si el Equipo realiza un descubrimiento del router de esta tarjeta. El descubrimiento solicita la información del router y

agrega la información a una tabla de ruta -ARP-. El valor de 0 incluso impide el envenenamiento ARP).

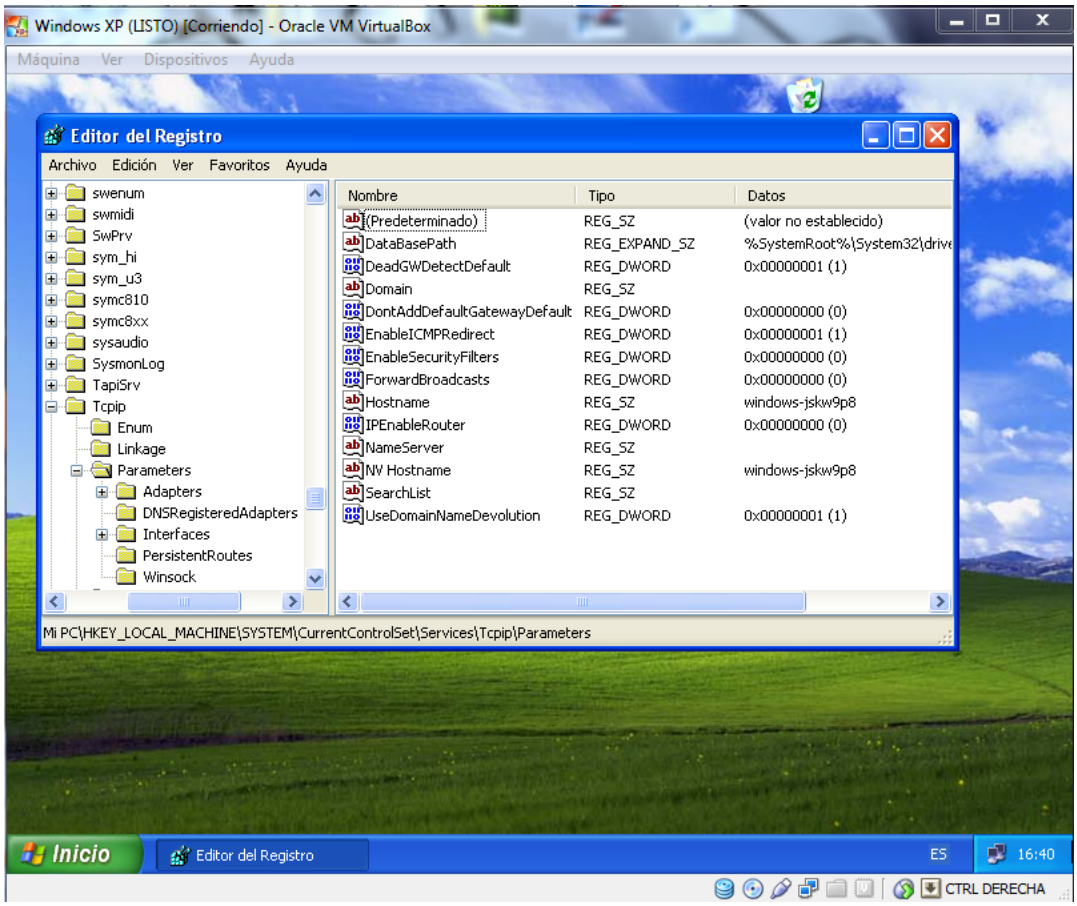


Gráfico 6.77 Directivas de red

Fuente: Honeynet

6.21.2.2 Para Linux

Iptables

Iptables es el nombre de la herramienta a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de NAT. Iptables es la herramienta estándar de todas las distribuciones modernas de GNU/Linux.

Reglas específicas.

Las opciones más comunes son:

-A añade una cadena, la opción -i define una interfaz de tráfico entrante -o define una interfaz para trafico saliente

-j establece una regla de destino del tráfico, que puede ser ACCEPT, DROP o REJECT. La -m define que se aplica la regla si hay una coincidencia específica

--state define una lista separada por comas de distinto tipos de estados de las conexiones (INVALID, ESTABLISHED, NEW, RELATED).

--to-source define que IP reportar al tráfico externo

-s define tráfico de origen

-d define tráfico de destino

--source-port define el puerto desde el que se origina la conexión

--destination-port define el puerto hacia el que se dirige la conexión

-t tabla a utilizar, pueden ser nat, filter, mangle o raw.

La primera sintaxis permite al cortafuegos denegar los paquetes con cierta longitud;

```
iptables -A INPUT -p tcp -d IP -m length –length 40:48 -j DROP
```

Con la segunda sintaxis crearemos una cadena de nombre DDOS para evitar ataques de tipo SYN-flood;

```
iptables-N DDoS
iptables -A DDoS -m limit –limit 1/s –limit-burst 10 -j RETURN
iptables -A DDoS -j LOG –log-prefix “[Recibiendo ataque DDOS]“
iptables -A DDoS -j DROP
```

Se guardan los cambios ingresados al cortafuegos;

```
service iptables save
```

Se verifican las nuevas reglas;

```
iptables -nL
```

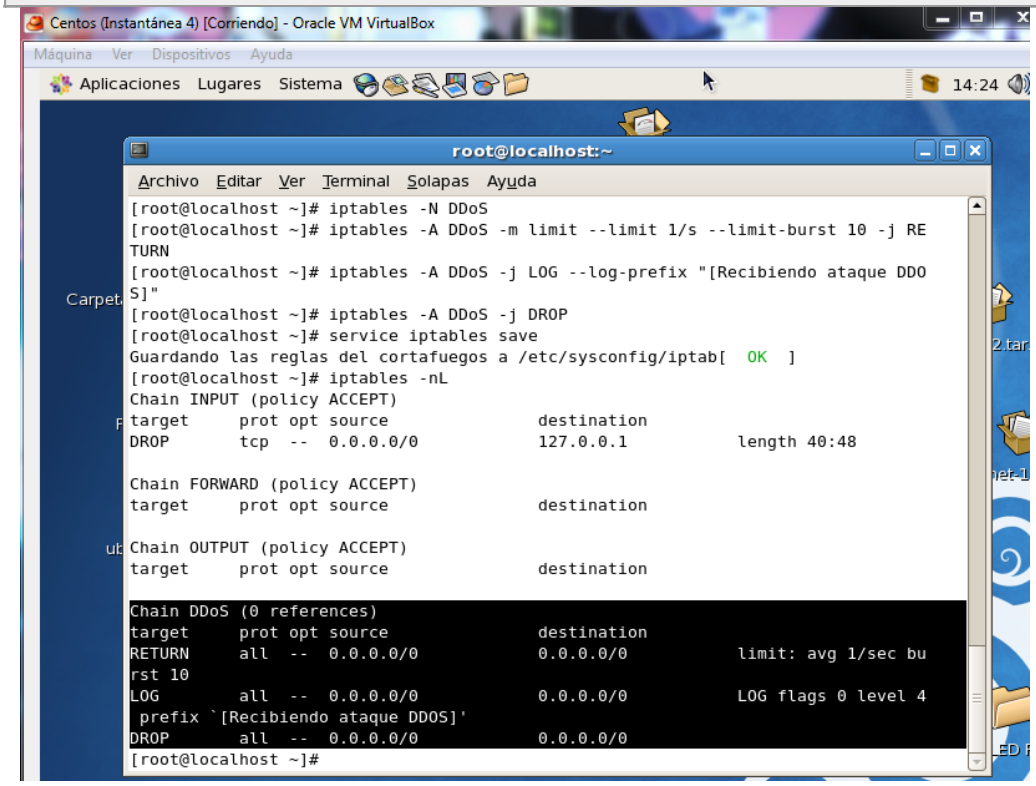


Gráfico 6.78 IP tables

Fuente: Honeynet

6.21.3 Intrusión 3.- Virus polimórfico

Este tipo de infección se la puede llegar a obtener mediante el mal manejo del computador es decir el no ser precavido al momento de tratar con información de fuentes externas, una memoria USB por ejemplo, por lo cual a continuación se darán consejos generales para un correcto manejo de información externa.

6.21.3.1 Precauciones en Windows para evitar la infección de virus

Desactivar la reproducción automática de medios

No es necesario en Windows 7, ya que de forma predeterminada está deshabilitada.

La reproducción automática de medios es una noble y útil posibilidad para el usuario de comenzar a reproducir automáticamente medios que se inserten en la PC de acuerdo con su contenido. Esta característica es aprovechada habilidosamente por el malware para penetrar en el equipo sin tu consentimiento al insertar una memoria flash, un CD, una tarjeta de memoria o cualquier tipo de dispositivo.

Activar la opción de mostrar los archivos ocultos

Es necesario para estar consciente del contenido de los archivos en el interior de los dispositivos insertados en el equipo.

Después de instalar Windows no se muestra ningún archivo oculto. Hay dos opciones disponibles en la herramienta: Opciones de carpeta.

• Mostrar archivos, carpetas y unidades ocultas.

• Mostrar archivos del sistema operativo.

La primera opción debe dejarse habilitada permanentemente, la otra activarla temporalmente, solo cuando sea necesario examinar el contenido de los dispositivos insertados completamente, después desactivarla para evitar daños accidentales a los archivos del sistema.

Activar la opción de mostrar las extensiones de archivos

De forma predeterminada las extensiones de archivos en Windows no se muestran.

¿Para qué es necesaria esta opción?

Simplemente para conocer con seguridad los tipos de archivos, algunos son inofensivos, otros son sumamente peligrosos.

Por ejemplo:

• Los archivos que terminan en EXE son ejecutables, es decir al dar dos clics en ellos estamos dando la autorización para desencadenar una tras otra todas las instrucciones que portan en su interior, estas pueden ser desde mostrar un simple mensaje, hasta modificar por completo nuestro sistema.

• Los archivos que terminan en TXT son completamente inofensivos, son simples archivos de texto plano, es decir sin formato, incapaces de contener nada dañino.

Una forma sutil de ocultar la verdadera función de un archivo es enmascarando su nombre.

Por ejemplo: CUENTO.TXT.EXE

Revisar manualmente el contenido de los dispositivos USB

Revisar todos los archivos que contenga en su interior cualquier memoria flash u otro dispositivo USB conectado al equipo, no dejar toda la tarea al software antivirus.

• Desconfiar de cualquier archivo reciente.

• Desconfiar especialmente de cualquier archivo de extensión .EXE

• Desconfiar de cualquier archivo que se vea semi-transparente, indica que es un archivo oculto.

Precauciones y medidas de seguridad al navegar en Internet

Al navegar en Internet hay que tener presente que los navegadores web cuentan con el sistema de seguridad necesario para impedir que automáticamente entre contenido dañino al equipo, pero al usuario dar clic en un botón en una página, marcar una casilla o introducir datos en un formulario está dando la orden de saltar estas restricciones.

Evitar dar clic o marcar cualquier casilla en sitios que no sean de confianza, puede bastar para dar la autorización necesaria para que penetre malware en el equipo.

Evitar descargar contenido gratis en sitios que no sean de confianza. El método de distribuir el Spyware y los Troyanos es incluirlos en el interior de pequeñas aplicaciones útiles y populares, al ofrecerlas gratis poseen un atractivo extremo.

Evitar las redirecciones en Internet, que pueden llevarte a sitios totalmente diferentes de lo que indican los vínculos.

Actualizar regularmente los navegadores o usa las versiones más recientes, las actualizaciones siempre incluyen parches de seguridad.

6.21.3.2 Medidas preventivas para Linux

El usuario root no debe ser usado como un usuario más; ni si quiera se debería poder iniciar sesión como root jamás (debería dejarse bloqueada con un asterisco en el campo contraseña de /etc/shadow)

El comando sudo es muy cómodo, pero también es un tremendo agujero de seguridad si no se configura adecuadamente. Los tres puntos de los que nos advierte esta herramienta cuando no la tenemos configurada deberían tomarse más en serio. En resumidas cuentas, nunca configurar para que sudo no pida contraseña.

Los repositorios de software (sean los del apt, yum, o los que correspondan), siempre de fuentes de confianza y firmados.

Ciertos directorios deberían poder leerse (o escribirse) sólo por root. Nunca dejar los permisos de directorios del sistema sólo porque nos sea más cómodo de administrar desde el usuario corriente.

Continuando con el tema de los permisos, el permiso de ejecución (modo +x de los archivos) sólo debería estar activo para directorios y ejecutables que vengan con el sistema o hayamos compilado nosotros mismos. Tener particiones de Windows con este permiso de ejecución activado por defecto no es buena idea, debemos montar siempre con noexec.

6.22 Implantación de Honeynet en oficinas del DISIR

Como se acordó en el punto 6.8.1.1 (Ubicación Honeynet) una vez terminado con la implementación de la Honeynet y comprobado su correcto funcionamiento se procedió a la implantación en las oficinas del DISIR, para esto se procedio a la copia de todos los archivos del ordenador original para luego simplemente copiarlos al ordenador de destino en el que previamete se instaló el software Oracle VM VirtualBox, esta es una ventaja de esta Honeynet que tiene la capacidad de ser plug and play, el ordenador en que se instalo tiene similares características que el original(Ver tabla x.x.x).

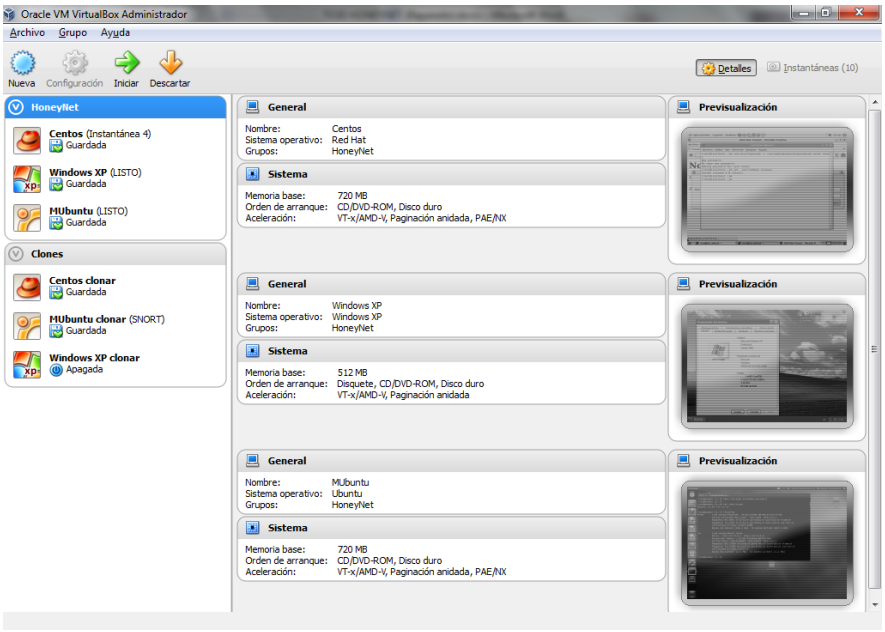


Gráfico 6.79 Máquinas virtuales de Honeynet listas para moverse a ordenador destino

Fuente: Honeynet

Ordenador destino donde se implanto Honeynet.

Sistema Operativo	Windows 7
Capacidad disco duro	500 Gb
(Continua en la siguiente página)	
Memoria RAM	8Gb.
IP	192.168.100.3
Usuario:	Administrador

Tabla 6.16 Detalles técnicos ordenador destino Honeynet

Autor: Mauro Jijón

6.23 Conclusiones y Recomendaciones

6.23.1 Conclusiones

- Algunas herramientas no son capaces de detectar ataques por si solas sino que requieren de una combinación adecuada para mejorar su funcionamiento y detectar con más facilidad y de forma más precisa los ataques de los que se está siendo parte; la implementación que se realizó es solo una de varias combinaciones que se pueden realizar para magnificar el proceso de detección de intrusos.

- Métodos de intrusión en la máquina, modos de ocultación, objetivos del ataque y demás aspectos de las intrusiones son mostrados en este documento por medio de la recolección y examen de datos realizados por

la Honeynet; mediante este proceso de análisis se llega a conocer los procesos que hay detrás de sus ataques, lo cual evitaría gran cantidad de sus secuelas, ya que, si se conoce el comportamiento, se puede proceder de forma más óptima a su contención.

- A pesar que se disponga de mucha información acerca de las amenazas en Internet, la documentación actual en cuanto a las Honeypots y Honeynet no se encuentra en gran cuantía. Con este estudio se demuestra la necesidad de profundizar en un área de suma utilidad para el combate de los ataques por parte de hackers y demás intrusos en la red, donde un alto porcentaje de los datos personales y de empresa se encuentran gravemente expuestos en Internet.
- Los Honeypots y Honeynets son muy buenas y factibles soluciónes para la detección y el análisis de tipos de ataques informáticos debido a que no son sistemas en producción y toda actividad dirigida hacia ellos es controlada. De esta manera, las cantidades de datos que se recolectan diariamente de la actividad hacia los Honeypots y Honeynets son relativamente bajas en comparación con otros sistemas de monitoreo. Sin embargo esta pequeña cantidad de datos es de gran valor, debido a que toda la actividad capturada puede ser analizada posteriormente en un ambiente controlado; el uso de las Honeynets permite conocer con detalle los ataques y vulnerabilidades de servidores y redes de datos.

6.23.2 Recomendaciones

- Ante todo tener en cuenta que ningún sistema es completamente seguro, el único sistema seguro es aquel que está apagado y desconectado de Internet.
- Realizar copias de seguridad constantemente, pero no únicamente de archivos sino imágenes completas del Sistema Operativo con esto al existir algún tipo de falla o error en los discos duros se evitaran muchos contratiempos.
- En muchos casos las vulnerabilidades tienen que ver con el hecho que los administradores están enfocados en solo en un sistema operativo, Windows por ejemplo y no saben cómo manejar sistemas Linux. Así que una constante capacitación en diferentes tipos de sistemas operativos y servidores ayudaría mucho a los administradores.
- El aplicar actualizaciones al sistema operativo, cerrar ciertos puertos habitualmente no usados puede detener buena parte de los ataques mostrados.
- Nunca confiar en aplicaciones o software pirateado ya que la mayoría de este software contiene virus ocultos que pueden estar enviando datos de manera oculta hacia un atacante remoto o utilizando nuestra maquina como un “zombie” para realizar ataques DDOS como el que se mostró en la realización de este tema.

6.24 Glosario de términos

Adware: Programa o aplicación que un usuario puede utilizar a condición de que acepte la publicidad que viene incorporada. También es un tipo de spyware que se

instala en el equipo, recolecta información del usuario y muestra publicidad durante la navegación o el uso del ordenador, relacionada con diferentes productos, muchas veces puede ser de protección antivirus. Son dos aceptaciones distintas pero ambas relacionadas con los “ads” o publicidad, tras la descarga de una aplicación salvo que la primera es voluntaria y la segunda es engañosa.

Agujero de seguridad: Es una vulnerabilidad, es un error en una aplicación o sistema operativo por el cual se compromete de alguna manera la seguridad del equipo donde se está ejecutando dicho programa vulnerable. Si un usuario malicioso se aprovecha de un agujero de seguridad, se dice que explota esa vulnerabilidad para causar daños en un equipo o también para obtener su control, dependiendo de la vulnerabilidad.

Análisis Heuristico: Sistema de análisis que tienen algunos antivirus basados en la suposición de comportamientos en vez de contrastar fragmentos de código con patrones previamente conocidos como nocivos. El análisis heurístico aplicado a antivirus busca nuevas especies de virus que se comporten de forma no pre estudiada en especies anteriormente encontradas, permitiendo así-, detectar nuevos virus antes de que se expandan y distribuyan por las redes.

Esta mecánica es útil para prevenir infecciones desconocidas, sin embargo, debe usarse con cuidado ya que aumenta las falsas alarmas de los antivirus o los falsos positivos detectados. Como usuario, al encontrar un aviso de un archivo infectado con un tipo de virus desconocido o nuevo, debemos reportarlo a la empresa del antivirus para que lo analicen adecuadamente y si realmente es un virus, desarrollen la forma de limpiarlo.

Antirastreo: El antirastreo es una característica de algunos programas maliciosos como los virus y también un conjunto de técnicas utilizadas por los programadores de virus, spammers y gente que se dedica a difundir malware, emplean para evitar ser detectados e investigados. El término en inglés es anti-debug.

Anti-Spyware: Es un programa desarrollado para el ámbito de la seguridad informática, el cual protege a los usuarios de programas maliciosos, tales como el software espía, spywares, la publicidad no deseada en nuestro navegador, adwares, pérdida de control sobre nuestro equipo, hijackers, entre otros malwares, que voluntaria o involuntariamente se instalan en la computadora, detectándolos y eliminándolos de la misma para evitar que nos causen problemas.

Antivirus: Los antivirus son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos que componen un conjunto denominado en inglés, malware. Es la protección básica de un equipo informático.

Un antivirus compara el código de cada archivo con una base de datos de los códigos llamada firma digital, de los virus ya conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado, para esto el software antivirus suele tener actualizaciones automáticas que se descargan directamente. Aparte del sistema de búsqueda habitual existe el análisis heurístico que analiza comportamientos típicos de virus o la verificación contra virus en redes de computadores.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados

y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así- como los scripts y programas que pueden ejecutarse en un navegador web (ActiveX, Java, JavaScript).

Backdoor: Se trata de una técnica de acceso para que un usuario pueda ingresar sin autorización a otros sistemas por medio de la instalación de un sistema de acceso considerado como un virus, permite revisar datos, borrar archivos, infectar con otro tipo de virus, todo esto sin aviso previo que permita saber lo que sucede en el ordenador o dentro de una red de equipos.

Backup: Se trata de una copia de seguridad que contiene en un archivo los datos que se encuentran en nuestro disco duro o en un almacenamiento externo a nuestro equipo, se suele descargar en un archivo comprimido con el fin de conservarlo y protegerlo en caso de posible daño o destrucción de la fuente original.

Bot: Tipo de virus troyano con el que el atacante se hace con el control de nuestro ordenador, habitualmente para atacar a otros ordenadores, como enviar correo electrónico no solicitado de forma masiva desde una red de botnets, grupos de ordenadores zombi que envían el SPAM.

Los bots son propagados a través de Internet empleando un gusano como transporte, envíos masivos de ellos a través de correo electrónico o aprovechando vulnerabilidades en navegadores. También se llama de forma confusa bot a todo robot que rastrea por Internet, algo erróneo ya que incluye a los robots que no son dañinos como los de los buscadores.

Browser Hijackers: Son los programas que procuran cambiar la página de inicio y búsqueda entre otros ajustes del navegador web, se dice que secuestran el navegador. Estos pueden ser instalados en el sistema sin nuestro consentimiento al visitar ciertos sitios web mediante controles ActiveX o bien ser incluidos por un virus troyano.

Bug: Un error de software, una falla de programación introducida en el proceso de creación de programas de software.

Certificado digital: es un documento digital mediante un sistema seguro de claves administrado por una tercera parte de confianza, la autoridad de certificación, que permite a las partes tener confianza en las transacciones en Internet, garantizando la identidad de su poseedor en Internet. Permite realizar un conjunto de acciones de forma segura y con validez legal, da acceso y permite transacciones.

Código malicioso: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos son algunos ejemplos de código malintencionado, también se le llama en conjunto mediante la palabra en inglés, malware.

Contraseña: Una contraseña, password en inglés, es una forma de autenticación que utiliza una información secreta para controlar el acceso hacia alguna zona de acceso restringido mediante clave. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se les permite el acceso.

Cortafuegos: Se trata de un mecanismo de protección, el cual puede ser construido mediante software, hardware o ambos. Su función es proteger un

equipo o conjunto de ellos mediante el análisis de paquetes de datos entrantes y salientes, pueden actuar a nivel de puertos de comunicaciones, permitiéndole al usuario autorizar o no la utilización de éstos por parte de aplicaciones o servicios, controlar el tránsito de información a través de Internet, desde y hacia el equipo.

Cracker: Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo. El término deriva de la expresión “criminal hacker”, y fue creado alrededor de 1985 por contraposición al termino hacker, en defensa de estos últimos por el uso incorrecto del término.

También se denomina cracker a quien diseña o programa cracks informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo. Esta acepción está más cercana al concepto de hacker en cuanto al interés por entender el funcionamiento del programa o hardware, y la adecuación a sus necesidades particulares, generalmente desarrolladas mediante ingenierí-a inversa.

No puede considerarse que la actividad de esta clase de cracker sea ilegal si ha obtenido el software o hardware legítimamente, aunque la distribución de los cracks pudiera serlo ya que muchos sirven para utilizar software de pago de manera gratuita modificando algunos archivos para su utilización sin pagar.

Criptografía: conjunto de procedimientos para cifrar los mensajes, de forma que si son interceptados no se pueda saber su contenido. Disciplina que estudia los

principios, métodos y medios de transformar los datos con objeto de ocultar la información contenida en los mismos, detectar su modificación no autorizada y prevenir su uso no permitido.

Cuarentena: Función de protección característica de los antivirus que nos permite dejar sin efecto a archivos que puedan estar infectados, hasta que nuestros sistemas de seguridad tengan una nueva actualización para poder desinfectarlos o hasta que el administrador decida qué hacer con ellos, si desinfectarlos o borrarlos directamente.

DDoS: siglas de Distributed Denial-of-Service, es un ataque de Negación de servicio, no es un virus pero es un método que utilizan los hackers para evitar o negar el acceso del usuario legítimo a un equipo. Los ataques DDoS se ejecutan típicamente usando herramientas DDoS que envía-n muchos paquetes con peticiones a un servidor de Internet (generalmente servidor Web, FTP o de correo), lo cual agota los recursos del servidor, haciendo el sistema inutilizable, que da colapsado durante unos momentos. Cualquier sistema que está conectado a Internet y equipado con servicios de red TCP está expuesto a un ataque.

Defacement: El defacement es una manera de hacking malicioso en el cual un portal Web está siendo dañado. El hacker borra todo el contenido del sitio web en cuestión e ingresa datos que no son apropiados, de carácter social o de política. Muchos crackers lo que hacen es borrar todo y dejar en la portada un mensaje sobre su “hazaña”, con una bandera de su país o un símbolo de su grupo de criminales.

Demo: versión demostrativa de un tipo de software. Es una versión restringida, que muestra una parte de todas las posibilidades que ofrece la aplicación.

Dirección IP: El Protocolo de Internet (IP, de sus siglas en inglés Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

La dirección IP está conformada por un número de 32 bits la cual identifica cada emisor y receptor de paquetes de información a través de Internet. Cada paquete enviado dentro del protocolo TCP/IP incluye la dirección IP de origen y de destino para poder distribuir los datos de manera correcta y si fuese necesario confirmar al emisor la recepción de los datos. Ésta consta de dos partes, una que identifica a cada red dentro de Internet y un identificador para cada dispositivo, el cual puede ser un router, un servidor o una estación de trabajo.

Dropper: Es un programa que ha sido alterado para instalar el virus cuando sea ejecutado. El código del virus intenta camuflarse para que no sea detectado por el antivirus.

Exploit: (del inglés to exploit, explotar o aprovechar) es un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa, se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

Falso Positivo: Se le llama así cuando un programa Anti-Virus, Anti-Spyware o un sistema antispam como Akismet, por ejemplo, detecta un archivo legitimo

como infectado o un spam que no lo es en realidad. Los creadores de Malwares cada día utilizan procesos muy sofisticados para que las aplicaciones puedan fallar. Esto ocurre raras veces ya que se pueden reportar los falsos positivos para perfeccionar aún más la protección anti malware.

Freeware: Tipo de licencia de distribución un software que permite utilizar dicho software sin coste alguno.

FTP: siglas de File Transfer Protocol, aplicación que permite descargar o cargar archivos en un servidor conectado a Internet.

Gusanos: Los gusanos tienen ciertas similitudes con los virus informáticos, pero también diferencias fundamentales. Un gusano se parece a un virus en que su principal función es reproducirse, pero por el contrario de cómo lo hacen los virus, en lugar de copiarse dentro de otros archivos, un gusano crea nuevas copias de si mismo para replicarse.

Hoaxes: La palabra hoax viene del inglés, es un verbo que significa embaucar; en cambio, si se utiliza como sustantivo, se traduce como engaño, bulo o broma de mal gusto. En Internet, se habla de hoax cuando se difunde masivamente una noticia que en realidad es falsa, es un vulgar bulo.

Ingeniería Social: Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma, pulsar en enlaces, introducir contraseñas, visitar páginas de cebo, convencido de que está haciendo lo correcto cuando realmente está siendo engañado. La ingeniería social estudia la condición humana y explota las emociones, el orgullo, la codicia, el oportunismo, el miedo, entre otras

sensaciones que experimentamos.

Intranet: Red privada de una empresa de tipo Internet. Su aspecto es similar al de las páginas de Internet pero con un acceso a miembros, generalmente empleados y otra para clientes. También existen las intranets en entornos educativos, para estudiantes.

Intrusiones: Cuando un pirata informático, accede sin autorización al equipo de un usuario de forma que el usuario no se dé cuenta, y ya con el control de esa máquina, puede realizar cualquier tipo de actividades. También se pueden dar intrusiones a redes locales, por ejemplo, la de una empresa, y así obtener información sensible y confidencial.

IP spoofing: Es una técnica que permite que un bandido tome la identidad de un host "confiable" (cambiando su dirección IP por la dirección de éste) y obtenga de este modo accesos no autorizados a otros sistemas.

ISP: Proveedor de Servicios de Internet (ISP o Internet Service Provider). Empresa dedicada a conectar a Internet a usuarios o a las distintas redes que tengan. También ofrecen mantenimiento necesario para un correcto funcionamiento.

Joker: Programas que tienen como objetivo hacer creer a los usuarios que sus equipos han sido afectados por un virus. Para conseguirlo muestran falsos mensajes que advierten de la inminente realización de acciones destructivas en el ordenador, modificando la configuración de la pantalla.

Junk Mail: Es un típico correo basura, SPAM. Publicidad masiva y no solicitada, a través del correo electrónico. Se la considera una práctica comercial poco ética.

Keygen: Se denominan así, a los programas creados por Crackers, los cuales son capaces de generar las claves de registro de un programa shareware. Estos generadores de registro, normalmente muestran el número de serie a introducir en la aplicación que se quiere registrar.

Keylogger: (Capturadores de Teclado) Aplicaciones encargadas de almacenar en un archivo todo lo que el usuario ingrese por el teclado. Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados.

Lammer: Individuos sin conocimientos avanzados de computación que presumen de ser expertos en temas informáticos, hackers e incluso piratas informáticos.

Macro / Virus de macro: Una macro es una secuencia de operaciones o instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) realice de forma automática y secuencial. Estas son 'microprogramas' que pueden ser infectados por los virus. Los documentos de texto, las bases de datos o las hojas de cálculo, no son programas y por ello no deberían ser infectados por ningún virus. No obstante, en cada uno de los ficheros creados con este tipo de aplicaciones se pueden definir macros y éstas sí son susceptibles de ser infectadas. Los virus de macro son aquellos que infectan exclusivamente documentos, hojas de cálculo o bases de datos que tienen macros definidas. El virus se propaga de un documento a otro y la infección tiene lugar cuando se abre el documento.

Malware: es la abreviatura de Malicious software (software malicioso), término que engloba a todo tipo de programa o código de computadora cuya función es

dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Gusano, Spywa re, Adware, Rootkits, Hijackers, Keyloggers, FakeAVs, Rogues.

MAPI: siglas de Messaging Application Program Interface, es un sistema empleado para que los programas puedan enviar y recibir correo electrónico mediante un sistema de mensajería concreto. MAPI es una interfaz de programa de Microsoft Windows que brinda la posibilidad de enviar correos electrónicos a través de una aplicación Windows. Esta librería de enlace dinámico (dll), programada en el lenguaje C, permite además adjuntar los archivos con los que estamos trabajando a los mensajes.

P2P: siglas de peer 2 peer, es un modelo de comunicaciones en el cual cada parte tiene las mismas capacidades y cualquiera de ellas puede iniciar la comunicación. Otro modelo totalmente opuesto es el cliente/servidor en donde el servidor se encuentra a la espera de una comunicación por parte del cliente. Este modelo se basa en que ambos nodos actúen como servidores y clientes a la vez. Actualmente, este tipo de comunicaciones es utilizado por aplicaciones de intercambio de archivos en donde los usuarios pueden comunicarse uno con el otro o mediante un servidor intermedio o red, como por ejemplo en el Emule. El peligro de las redes P2P reside en las descargas de contenidos que pueden ser ilegales o contenidos adultos incluidos en archivos con nombres que pueden atraer la atención de menores.

Parche: También conocidos como actualizaciones, en inglés patches o updates, son soluciones a problemas o agujeros de seguridad en aplicaciones o sistemas

operativos. En el ambiente Windows son normalmente programas ejecutables que reemplazan los componentes fallados por otros sin problemas; en otras plataformas también son conocidos como PTFs (Program Temporary Fixes).

Existen conglomerados de parches, más estables, que incluyen varias actualizaciones a diversas fallas, que suelen ser llamados Service Packs, y son liberados cada cierto tiempo por las empresas responsables de las aplicaciones y sistemas operativos más utilizados.

Dentro de los gestores de contenido CMS y el software libre, las actualizaciones de seguridad sin importantes descargas para ponerse rápidamente al día y proteger el núcleo del sitio web, ya sea la plataforma utilizada un sistema como WordPress, Joomla o Drupal entre otros.

Pharming: Se denomina pharming a la explotación de vulnerabilidades en servidores DNS que puede permitir que un atacante modifique los registros de dominio de una página para redireccionarla hacia otra. Esta técnica se conoce en algunos casos como DNS spoofing. Por ejemplo, un atacante puede modificar un servidor DNS para que cuando el usuario intente acceder un dominio conocido, en lugar de acceder al verdadero sitio, se acceda a otro falso que el atacante desee. Esta técnica es utilizada para robo de información de acceso a sitios seguros, números de tarjetas de crédito, etc.

Phishing: Se utiliza el término “phishing” para referirse a todo tipo de prácticas utilizadas para obtener información confidencial (como números de cuentas, de tarjetas de crédito, contraseñas, etc.). La gran parte de estos ataques son llevados a cabo a través de un e-mail falso (scam), enviado por el atacante, que notifica al

usuario la necesidad de que confirme cierta información sobre su cuenta. Estos mensajes pueden parecer muy reales ya que muchas veces incluyen logos de la entidad bancaria y una gráfica muy profesional. Debido a ciertas vulnerabilidades en los principales navegadores, los atacantes puede redireccionar al usuario a un servidor falso sin que este note la diferencia, salvo por el link o enlace que suele mostrar que realmente no estamos siendo dirigidos al sitio web que conocemos si no a una página web de cebo donde apenas funciona un formulario pero donde la estética es muy similar a la web auténtica.

Proxy: Software que permite a varios ordenadores acceder a Internet a través de una única conexión física y puede permitir acceder a páginas Web, FTP, correo electrónico, etc., y también, servidor de comunicaciones, responsable de canalizar el tráfico entre una red privada e Internet, que contiene un cortafuegos.

Robo de Identidad: El robo de identidad online consiste en realizar acciones utilizando los datos de otra persona. Como lo más normal es que esas acciones sean ilegales: compras online con tarjetas robadas, apertura de cuentas bancarias, este tipo de ataques suelen tener graves consecuencias para los usuarios que han sido víctima de ellos. Como norma general, se define que ha habido un robo de identidad cuando una persona utiliza la información personal de otra, como nombre, dirección, número de Seguro Social, para realizar actividades ilegales como abrir cuentas de crédito, sacar dinero del banco o hacer compras.

Rootkit: Los rootkits se iniciaron bajo los sistemas operativos Unix, basándose en un conjunto de herramientas específicamente modificadas para ocultar la actividad de quien las utilizara. Por esto, se define a rootkit como un conjunto de

herramientas especiales que permiten esconder procesos activos, archivos en uso, modificaciones al sistema, etc., de manera que las utilidades de seguridad tradicionales no puedan detectarlas una vez en el sistema. Cuando se habla de técnicas rootkit en un código malicioso, básicamente nos referimos al hecho de que el malware en cuestión es capaz de aprovechar funciones propias o de herramientas externas para esconder parte o todo su funcionamiento.

Shareware: Tipo de licencia de un software que permite compartir (to share), distribuir un software gratuitamente para ser probado, pero que posee ciertas limitaciones en su funcionalidad o disponibilidad.

Sniffing: Se trata de dispositivos que permiten al atacante "escuchar" las diversas comunicaciones que se establecen entre ordenadores a través de una red (fí-sica o inalámbrica) sin necesidad de acceder física ni virtualmente a su ordenador.

Spam: Es llamado Spam al correo basura, el cual llega a nuestras casillas de correo sin que nosotros lo hayamos solicitado. Generalmente estos mensajes contienen anuncios publicitarios sobre productos, sitios webs, o cualquier otra actividad comercial que puedan imaginarse. Con estos envíos masivos el "anunciante" logra llegar a una gran cantidad de usuarios que de otra manera no se enterarí-an de su producto o servicio, abaratando muchísimo el coste del envío de la publicidad.

Los Spammers, personas dedicadas al envío de correo basura, van generando bases de datos de direcciones de correo electrónico las cuales son obtenidas de diferentes formas, ya sea manualmente, mediante bots o comprando ilegalmente bases de datos con información de usuarios.

Spyware: Software espía, programa o aplicación que sin el conocimiento del usuario recolecta información de su equipo o de lo que hace al utilizar Internet. Normalmente utilizado con fines de publicidad o marketing. Son programas que invaden la privacidad de los usuarios y también la seguridad de sus computadoras. Actualmente, este tipo de software es incluido junto a aplicaciones gratuitas de gran difusión, como las utilizadas herramientas de intercambio de archivos.

Troyanos: (Caballos de Troya) Programas que, enmascarados de alguna forma como un juego o similar, buscan hacer creer al usuario que son inofensivos, para realizar acciones maliciosas en su equipo. Estos troyanos no son virus ni gusanos dado que no tienen capacidad para replicarse por sí mismos, pero en muchos casos, los virus y gusanos liberan troyanos en los sistemas que infectan para que cumplan funciones específicas, como, por ejemplo, capturar todo lo que el usuario ingresa por teclado (keylogger). La principal utilización de los troyanos es para obtener acceso remoto a un sistema infectado a través de una puerta trasera. Este tipo de troyano es conocido como Backdoor.

Virus: Son sencillamente programas creados para infectar sistemas y otros programas creándoles modificaciones y daños que hacen que estos funcionen incorrectamente. Suelen ser programaciones sencillas que buscan explotar un fallo o vulnerabilidad concreta en un sistema.

WEP: (Wired Equivalent Privacy) Protocolo para la transmisión de datos segura. El cifrado puede ser ajustado a 128 bits, 64 bits o deshabilitado. La configuración de 128 bits da el mayor nivel de seguridad. Este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

Zombie: Un ordenador generalmente infectado con un troyano de acceso remoto, capaz de recibir órdenes externas, y de actuar, generalmente en actividades maliciosas, sin el conocimiento de sus dueños.

6.25 Bibliografía:

Libros

- ANDREW s. Tanenbaum, Redes de Computadoras 4ta edición, pearson educación, México, 2003
- AGUILERA, Purificación. Seguridad Informática. Editorial Editex, Madrid- España.

Tesis

- Franklin Flores, "Estudio, Administración e Implementación de Políticas de Seguridad en la Red Informática del Hospital Millennium de la ciudad de Ambato." Facultad de ingeniería en sistemas electrónica e Industrial

Leyes

- **Ley de comercio electrónico, firmas electrónicas y mensajes de datos,** ley publicada en el Registro Oficial N° 557 del 17 de Abril del 2002.

Internet

- Instituto Tecnológico de Massachusetts, creación de un Plan de respuesta a incidentes, extraído el 29 de Abril de 2011 desde http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-response-plan.html
- Security by default, ataques de contraseñas, extraído el 11 de Octubre de 2012 desde http://www.securitybydefault.com/2010/03/ataques-de-contrasenas-password.html
- Snort, instalación de Snort, extraído el12 de Octubre de 2012 desde http://www.snort.org/assets/159/Snort_2.9.1_CentOS_5.pdf

- Ubuntudriver, comandos para Ubuntu, extraído el 14 de Octubre de 2012 desde http://ubuntudriver.blogspot.com/2012/01/como-usar-la-orden-locate.html
- Hackhispano, foro de seguridad informática, extraído el 14 de Octubre de 2012 desde http://foro.hackhispano.com/foro/f17/syn-flood-que-es-y-como-mitigarlo-36604.html
- Proyecto-Malware, tipos de virus, extraído el 16 de Octubre de 2012 desde http://proyecto-malware.webnode.es/investigacion-del-fenomeno/tipos-de-virus-/virus-polimorficos/
- Microsoft, configuración de la infraestructura de dominios de Active Directory, extraído el 20 de Octubre de 2012 desde http://www.microsoft.com/spain/technet/recursos/articulos/secmod61.mspx
- Seguridadjabali, firewall de Windows, extraído el 25 de Octubre de 2012 desde http://www.seguridadjabali.com/2012/10/firewall-de-windows-desde-shell.html
- Spam Spam, Glosario de términos, con definiciones acerca de palabras relacionadas con la seguridad informática estraido el 26 de Octubre de 2012 desde http://www.spamspam.info

ANEXOS

ANEXO 1

Modelo de ficha de Observación

Mensaje	
Resumen	
Impacto	
Información Detallada	
Sistemas Afectados	
Escenarios de Ataque	
Facilidad de Ataque	
Falsos Positivos	
Falsos Negativos	
Acción Correctiva	

ANEXO 2

Logs de HijackThis resumidos, se resaltan las posibles amenazas encontradas

Log obtenido el 01/10/2011:

Fuente: Laboratorio #3 Facultad de Ingeniería en Sistemas.

Logfile of Trend Micro HijackThis v2.0.4

Scan saved at 10:15:00, on 01/10/2011

Platform: Windows 7 SP1 (WinNT 6.00.3505)

MSIE: Internet Explorer v9.00 (9.00.8112.16421)

Boot mode: Normal

C:\WINDOWS\System32\smss.exe

C:\WINDOWS\system32\winlogon.exe

C:\ARCHIV~1\MYWEBS~1\bar\1.bin\mwsoemon.exe

C:\windows\system32\ycewca.exe

C:\ARCHIV~1\Yahoo!\MESSEN~1\ymsgr_tray.exe

C:\Archivos de programa\Kaspersky Lab\Kaspersky Anti-Virus 7.0\avp.exe

C:\WINDOWS\System32\svchost.exe

C:\WINDOWS\system32\nvsvc32.exe

C:\WINDOWS\System32\svchost.exe

C:\WINDOWS\system32\svchost.exe

C:\WINDOWS\system32\wuauclt.exe

C:\WINDOWS\system32\wscntfy.exe

G:\HijackThisPortable\HijackThisPortable.exe

G:\HijackThisPortable\App\HijackThis\HijackThis.exe

F2 - REG:system.ini: Shell=Explorer.exe C:\WINDOWS\WndowsXP.exe

O2 - BHO: MyWebSearch Search Assistant BHO - {00A6FAF1-072E-44cf-8957-5838F569A31D} - C:\Archivos de programa\MyWebSearch\SrchAstt\1.bin\MWSSRCAS.DLL

O2 - BHO: Yahoo! Toolbar Helper - {02478D38-C3F9-4EFB-9B51-7695ECA05670} - C:\Archivos de programa\Yahoo!\Companion\Installs\cpn\yt.dll

O2 - BHO: AcroIEHlprObj Class - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} - C:\Archivos de programa\Adobe\Acrobat 7.0\ActiveX\AcroIEHelper.dll

O2 - BHO: mwsBar BHO - {07B18EA1-A523-4961-B6BB-170DE4475CCA} - C:\Archivos de programa\MyWebSearch\bar\1.bin\MWSBAR.DLL (file missing)

O4 - HKLM\..\Run: [sijbolji] c:\windows\system32\sijbolji.exe sijbolji

O4 - HKLM\..\Run: [Windows Lsass Services] C:\WINDOWS\system\lsass.exe

O4 - HKLM\..\Run: [GrooveMonitor] "C:\Archivos de programa\Microsoft Office\Office12\GrooveMonitor.exe"

O4 - HKLM\..\Run: [AVP] "C:\Archivos de programa\Kaspersky Lab\Kaspersky Anti-Virus 7.0\avp.exe"

O4 - HKCU\..\Run: [ycqca] "c:\windows\system32\ycewca.exe" ycewca

Log obtenido el 28/10/2011

Fuente: Laboratorio 5 Facultad de Ingeniería en Sistemas.

Logfile of Trend Micro HijackThis v2.0.4

Scan saved at 18:30:34, on 28/10/2011

Platform: Windows 7 (WinNT 6.00.3504)

MSIE: Internet Explorer v9.00 (9.00.8112.16421)

Boot mode: Normal

C:\WINNT\System32\smss.exe

C:\WINNT\system32\winlogon.exe

C:\Archivos de programa\Cisco Systems\VPN Client\cvpnd.exe

C:\WINNT\System32\svchost.exe

C:\Archivos de programa\Archivos comunes\supportsoft\bin\sprtlisten.exe

C:\Archivos de programa\Spyware Terminator\sp_rsser.exe

C:\WINNT\system32\svchost.exe

C:\Documents and Settings\Administrador\wkki.exe

C:\WINNT\Explorer.EXE

C:\Archivos de programa\Java\jre1.5.0_06\bin\jusched.exe

C:\Archivos de programa\Spyware Terminator\SpywareTerminatorShield.exe

C:\Archivos de programa\Microsoft ActiveSync\Wcescomm.exe

C:\Archivos de programa\PC Connectivity Solution\Transports\NclUSBSrv.exe

C:\Archivos de programa\PC Connectivity Solution\Transports\NclRSSrv.exe

F:\HijackThisPortable\HijackThisPortable.exe

F:\HijackThisPortable\App\HijackThis\HijackThis.exe

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =
http://www.google.com

R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings,ProxyServer = http=proxy_server:8080

O2 - BHO: SSVHelper Class - {761497BB-D6F0-462C-B6EB-
D4DAF1D92D43} - C:\Archivos de programa\Java\jre1.5.0_06\bin\ssv.dll

O4 - HKLM\..\Run: [Synchronization Manager] mobsync.exe /logon

O4 - HKLM\..\Run: [nnd] C:\WINNT\system32\nnd.exe \u

O4 - HKLM\..\Run: [SpywareTerminator] "C:\Archivos de programa\Spyware Terminator\SpywareTerminatorShield.exe"

O4 - HKUS\.DEFAULT\..\RunOnce: [^SetupICWDesktop] C:\Archivos de programa\Internet Explorer\Connection Wizard\icwconn1.exe /desktop (User 'Default user')

O4 - Global Startup: Magic Keyboard.lnk = C:\Archivos de programa\Magic Keyboard\MagicKey.exe

O4 - Global Startup: VPN Client.lnk = C:\Archivos de programa\Cisco Systems\VPN Client\vpngui.exe

O8 - Extra context menu item: Crawler Search - tbr:iemenu

O9 - Extra button: PokerStars - {3AD14F0C-ED16-4e43-B6D8-661B03F6A1EF} - C:\Archivos de programa\PokerStars\PokerStarsUpdate.exe

O10 - Unknown file in Winsock LSP: c:\winnt\system32\54a5qwtnul.dll

O10 - Unknown file in Winsock LSP: c:\winnt\system32\54a75qwtnul.dll

O16 - DPF: {6414512B-B978-451D-A0D8-FCFDF33E833C} (WUWebControl Class) - http://update.microsoft.com/windowsupda ... 2450574734

O16 - DPF: {67DABFBF-D0AB-41FA-9C46-CC0F21721616} (DivXBrowserPlugin Object) - http://go.divx.com/plugin/DivXBrowserPlugin.cab

O16 - DPF: {6E32070A-766D-4EE6-879C-DC1FA91D2FC3} (MUWebControl Class) - http://www.update.microsoft.com/microso ... 0070913015

O23 - Service: Cisco Systems, Inc. VPN Service (CVPND) - Cisco Systems, Inc. - C:\Archivos de programa\Cisco Systems\VPN Client\cvpnd.exe

O23 - Service: iSeries Access for Windows Remote Command (Cwbrxd) - IBM Corporation - C:\WINNT\cwbrxd.exe

O23 - Service: SupportSoft Listener Service (sprtlisten) - SupportSoft, Inc. - C:\Archivos de programa\Archivos comunes\supportsoft\bin\sprtlisten.exe

Log obtenido el 11/11/2011

Fuente: Laboratorio 7 Facultad de Ingeniería en Sistemas.

Logfile of Trend Micro HijackThis v2.0.4

Scan guardado en 8:35:45 PM, en 11/11/2011

Plataforma: Windows XP SP3 (WinNT 5.01.2600)

MSIE: Internet Explorer v8.00 (8.00.6001.18702)

Procesos en ejecución:

C: \ Archivos de programa \ ewido anti-spyware 4,0 \ GUARD.EXE

C: \ Archivos de programa \ Trend Micro \ PC-cillin 2002 \ Tmntsrv. exe

C: \ WINDOWS \ wdfmgr.exe

C: \ Archivos de programa \ Messenger \ msmsgs.exe

C: \ PROGRA ~ 1 \ FREEIN ~ 1 \ Clearpch.exe

C: \ Archivos de programa \ Adobe \ Adobe Acrobat 6,0 \ Distillr \ acrotray.exe

C: \ PROGRA ~ 1 \ MOZILL ~ 1 \ FIREFOX.EXE

H:\HijackThisPortable\HijackThisPortable.exe

H:\HijackThisPortable\App\HijackThis\HijackThis.exe

O4 - HKLM \ .. \ Run: [TrackPointSrv] tp4mon.exe

O4 - HKLM \ .. \ Run: [RemoteControl] "C: \ Archivos de programa \ CyberLink \ PowerDVD \ PDVDServ.exe"

O4 - HKLM \ .. \ Run: [teclado] C: \ \ kybrdff_9.exe

O4 - HKLM \ .. \ Run: [defensor] C: \ \ dfndrff_9.exe

O4 - HKLM \ .. \ Run: [sswbd210] rundll32.exe w0023f79.dll, n 002bd20e0000000a0023f79

O4 - HKLM \ .. \ Run: [SurfSideKick 3] C: \ Archivos de programa \ SurfSideKick 3 \ Ssk.exe

O4 - HKLM \ .. \ Run: [newname] C: \ \ nwnmff_9. exe

O4 - HKLM \ .. \ Run: [! Ewido] "C: \ Archivos de programa \ ewido anti-spyware 4,0 \ ewido.exe" / minimizado

O4 - HKLM \ .. \ Run: [pccguide.exe] "C: \ Archivos de programa \ Trend Micro \ PC-cillin 2002 \ pccguide.exe"

O4 - HKLM \ .. \ Run: [PCCClient.exe] "C: \ Archivos de programa \ Trend Micro \ PC-cillin 2002 \ PCCClient.exe"

O23 - Servicio: Atheros Configuration Service (ACS) - Desconocido propietario - C: \ WINDOWS \ System32 \ acs. exe

O23 - Servicio: Adobe LM Service - Adobe Systems - C: \ Program Files \ Common Files \ Adobe Systems Shared \ Service \ Adobelmsvc.exe

O23 - Servicio: csrsr - Desconocido propietario - C: \ WINDOWS \ csrss. exe (archivos que faltan)

O23 - Service: ewido anti-spyware 4,0 guardia - Anti-Malware Desarrollo como - C: \ Archivos de programa \ ewido anti-spyware 4,0 \ GUARD.EXE

O23 - Servicio: Microsoft Windows Spool Service (Servicio de Windows Spool) - Desconocido propietario - C: \ WINDOWS \ wdfmgr.exe

ANEXO 3

Logs de COMODO Laboratorios: 3 y 5 Facultad de Ingeniería en Sistemas.

COMODO LEAKTESTS V.1.1.0.3	
Date	20:19:14 - 14/10/2011
OS	Windows XP SP3 build 2600
1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Vulnerable
3. RootkitInstallation: DriverSupersede	Vulnerable
4. RootkitInstallation: ChangeDrvPath	Vulnerable
5. Invasion: Runner	Protected
6. Invasion: RawDisk	Vulnerable
7. Invasion: PhysicalMemory	Vulnerable
9. Invasion: DebugControl	Vulnerable
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Vulnerable
13. Injection: Services	Vulnerable
14. Injection: ProcessInject	Vulnerable
15. Injection: KnownDlls	Vulnerable
16. Injection: DupHandles	Vulnerable
17. Injection: CreateRemoteThread	Vulnerable
18. Injection: APC dll injection	Vulnerable
19. Injection: AdvancedProcessTermination	Vulnerable
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Protected
22. Impersonation: OLE automation	Vulnerable
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Vulnerable
25. Impersonation: Coat	Protected
26. Impersonation: BITS	Vulnerable
27. Hijacking: WinlogonNotify	Vulnerable
28. Hijacking: Userinit	Vulnerable
29. Hijacking: UIHost	Vulnerable
30. Hijacking: SupersedeServiceDll	Vulnerable
31. Hijacking: StartupPrograms	Vulnerable
32. Hijacking: ChangeDebuggerPath	Vulnerable
33. Hijacking: AppinitDlls	Vulnerable
34. Hijacking: ActiveDesktop	Vulnerable
Score	60/340

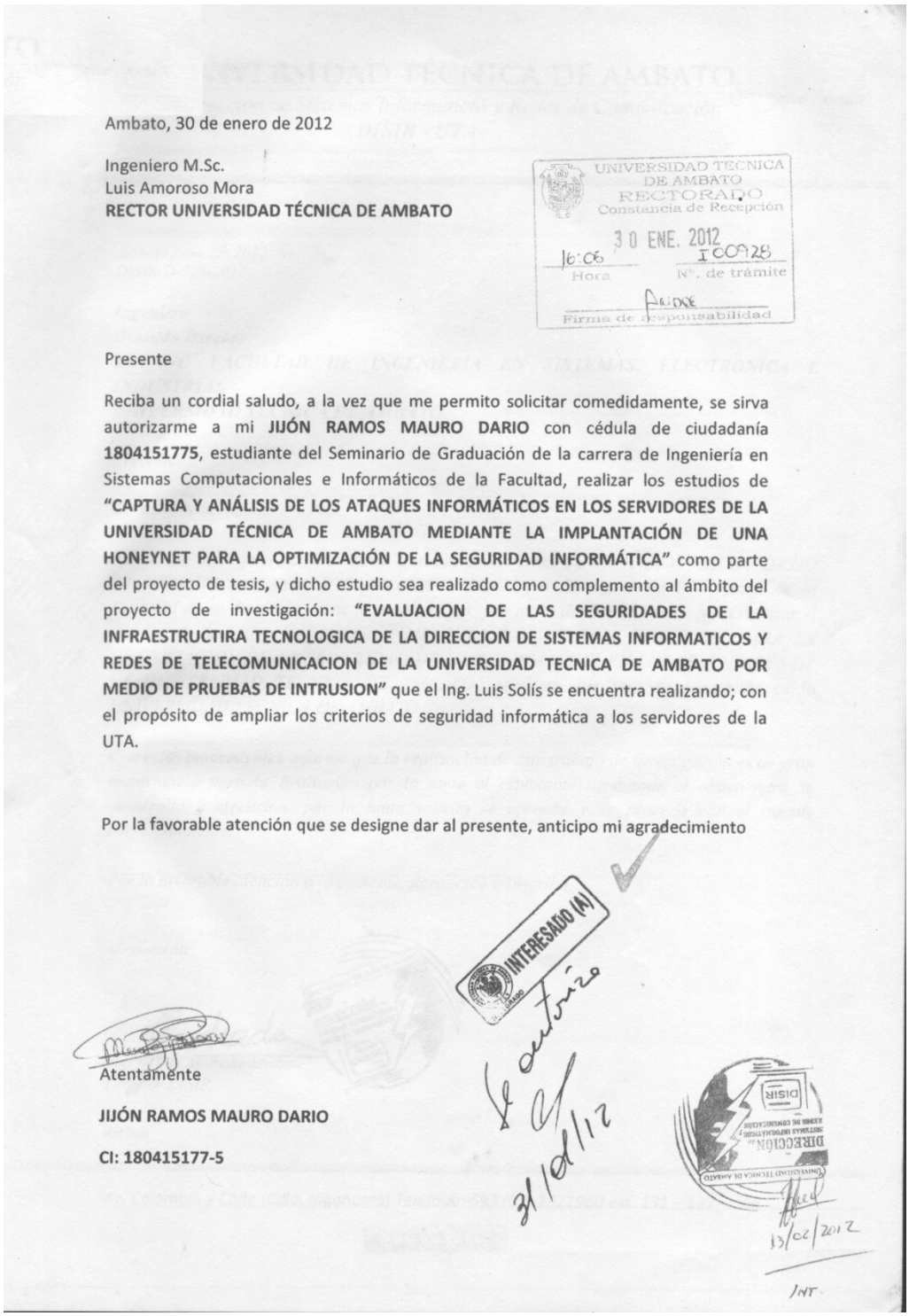
COMODO LEAKTESTS V.1.1.0.3	
Date	10:18:59 - 26/11/2011
OS	Windows Vista SP1 build 7601

1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Protected
3. RootkitInstallation: DriverSupersede	Protected
4. RootkitInstallation: ChangeDrvPath	Vulnerable
5. Invasion: Runner	Protected
6. Invasion: RawDisk	Vulnerable
7. Invasion: PhysicalMemory	Protected
8. Invasion: FileDrop	Vulnerable
9. Invasion: DebugControl	Protected
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Protected
13. Injection: Services	Vulnerable
14. Injection: ProcessInject	Protected
15. Injection: KnownDlls	Vulnerable
16. Injection: DupHandles	Protected
17. Injection: CreateRemoteThread	Protected
18. Injection: APC dll injection	Protected
19. Injection: AdvancedProcessTermination	Protected
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Vulnerable
22. Impersonation: OLE automation	Protected
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Vulnerable
25. Impersonation: Coat	Vulnerable
26. Impersonation: BITS	Protected
27. Hijacking: WinlogonNotify	Protected
28. Hijacking: Userinit	Vulnerable
29. Hijacking: UIHost	Protected
30. Hijacking: SupersedeServiceDll	Vulnerable
31. Hijacking: StartupPrograms	Vulnerable
32. Hijacking: ChangeDebuggerPath	Protected
33. Hijacking: AppinitDlls	Protected
34. Hijacking: ActiveDesktop	Protected

Score	210/340

ANEXO 4

Solicitud al Sr. Rector de la Universidad Técnica de Ambato Luis Amoroso Mora para la realización del presente proyecto de tesis.



Ambato, 30 de enero de 2012

Ingeniero M.Sc.
Luis Amoroso Mora
RECTOR UNIVERSIDAD TÉCNICA DE AMBATO

UNIVERSIDAD TECNICA DE AMBATO
RECTORADO
Constancia de Recepción
30 ENE. 2012
16:06 — I 00128
Hora — Nº. de trámite
Firma de responsabilidad

Presente

Reciba un cordial saludo, a la vez que me permito solicitar comedidamente, se sirva autorizarme a mi **JIJÓN RAMOS MAURO DARIO** con cédula de ciudadanía **1804151775**, estudiante del Seminario de Graduación de la carrera de Ingeniería en Sistemas Computacionales e Informáticos de la Facultad, realizar los estudios de **"CAPTURA Y ANÁLISIS DE LOS ATAQUES INFORMÁTICOS EN LOS SERVIDORES DE LA UNIVERSIDAD TÉCNICA DE AMBATO MEDIANTE LA IMPLANTACIÓN DE UNA HONEYNET PARA LA OPTIMIZACIÓN DE LA SEGURIDAD INFORMÁTICA"** como parte del proyecto de tesis, y dicho estudio sea realizado como complemento al ámbito del proyecto de investigación: **"EVALUACION DE LAS SEGURIDADES DE LA INFRAESTRUCTIRA TECNOLOGICA DE LA DIRECCION DE SISTEMAS INFORMATICOS Y REDES DE TELECOMUNICACION DE LA UNIVERSIDAD TECNICA DE AMBATO POR MEDIO DE PRUEBAS DE INTRUSION"** que el Ing. Luis Solís se encuentra realizando; con el propósito de ampliar los criterios de seguridad informática a los servidores de la UTA.

Por la favorable atención que se designe dar al presente, anticipo mi agradecimiento

INTERESADO (A)

Atentamente

JIJÓN RAMOS MAURO DARIO

CI: 180415177-5

31/01/12

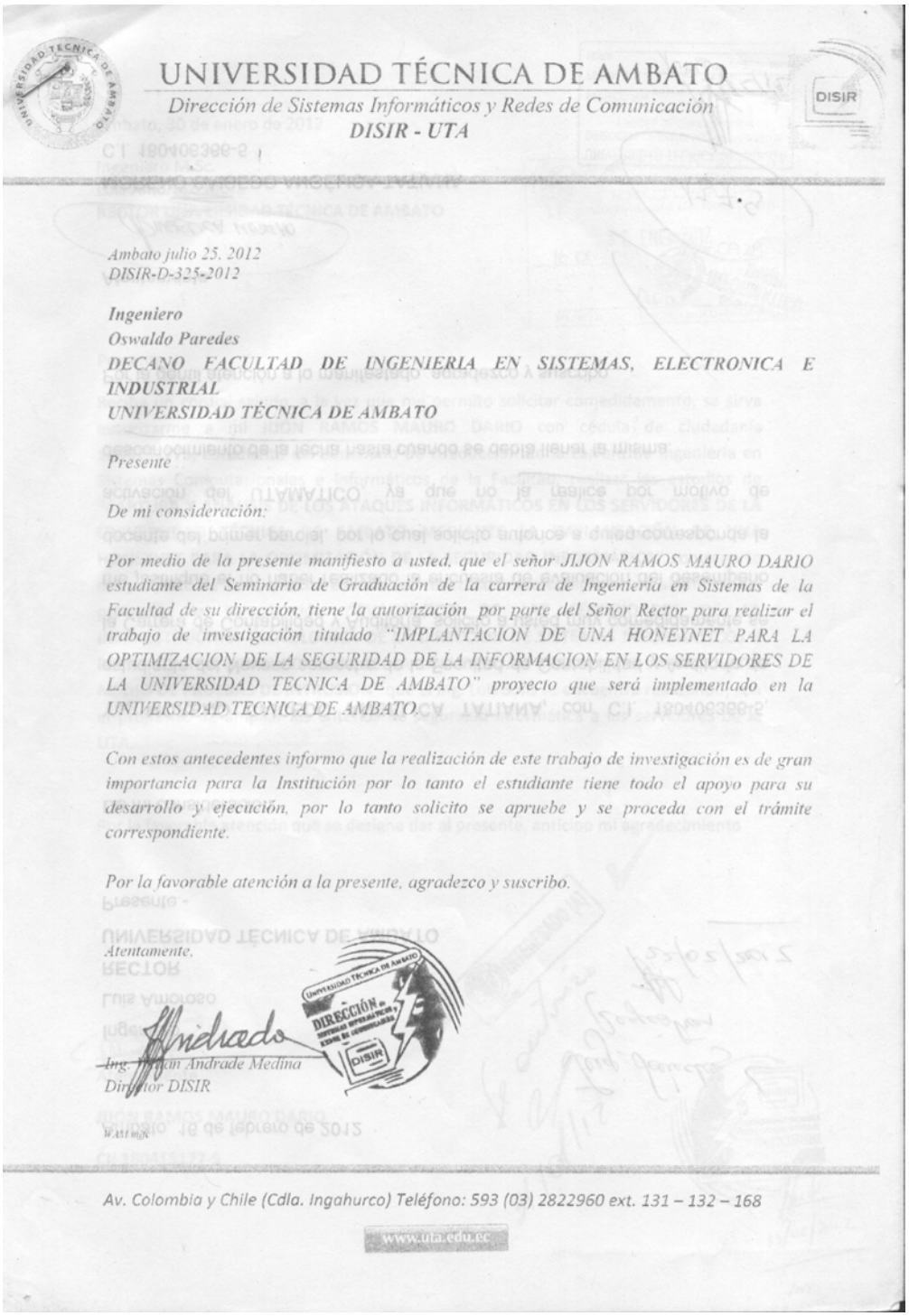
DIRECCIÓN DISIR

13/02/2012

INT.

ANEXO 5

Autorización del Sr. Rector de la Universidad Técnica de Ambato Luis Amoroso Mora para la realización del presente proyecto de tesis.



UNIVERSIDAD TÉCNICA DE AMBATO

Dirección de Sistemas Informáticos y Redes de Comunicación

DISIR - UTA

DISIR

Ambato julio 25, 2012
DISIR-D-325-2012

Ingeniero
Oswaldo Paredes
DECANO FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRONICA E INDUSTRIAL
UNIVERSIDAD TÉCNICA DE AMBATO

Presente

De mi consideración:

Por medio de la presente manifiesto a usted, que el señor JIJON RAMOS MAURO DARIO estudiante del Seminario de Graduación de la carrera de Ingeniería en Sistemas de la Facultad de su dirección, tiene la autorización por parte del Señor Rector para realizar el trabajo de investigación titulado "IMPLANTACION DE UNA HONEYNET PARA LA OPTIMIZACION DE LA SEGURIDAD DE LA INFORMACION EN LOS SERVIDORES DE LA UNIVERSIDAD TECNICA DE AMBATO" proyecto que será implementado en la UNIVERSIDAD TECNICA DE AMBATO.

Con estos antecedentes informo que la realización de este trabajo de investigación es de gran importancia para la Institución por lo tanto el estudiante tiene todo el apoyo para su desarrollo y ejecución, por lo tanto solicito se apruebe y se proceda con el trámite correspondiente.

Por la favorable atención a la presente, agradezco y suscribo.

Atentamente,

DIRECCIÓN DISIR

Ing. Vivian Andrade Medina
Director DISIR

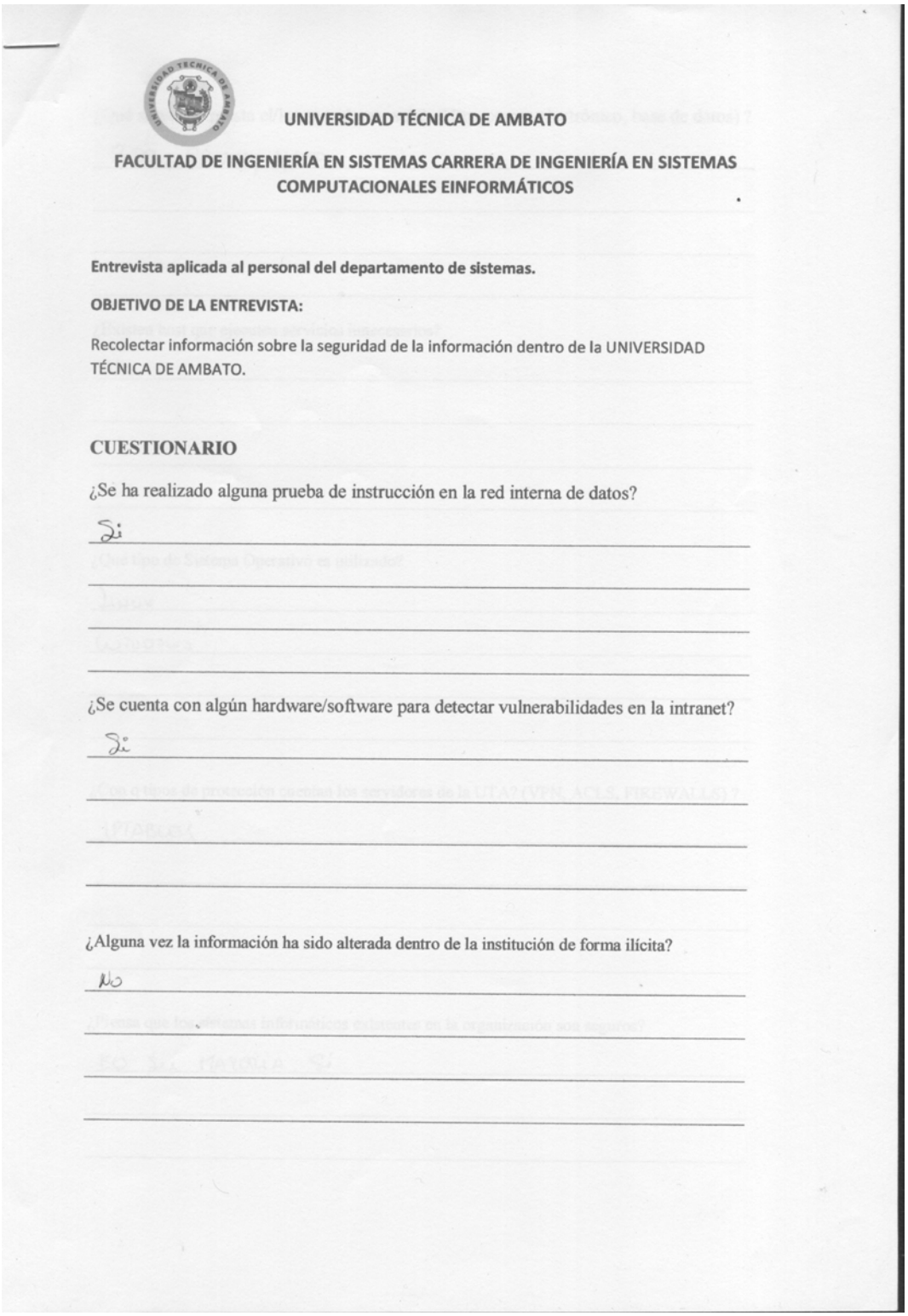
WASI/mjk

Av. Colombia y Chile (Cdla. Ingahurco) Teléfono: 593 (03) 2822960 ext. 131 – 132 – 168

www.uta.edu.ec

ANEXO 6

Encuestas realizadas a los administradores de red de la Universidad Técnica de Ambato.



UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES EINFORMÁTICOS

Entrevista aplicada al personal del departamento de sistemas.

OBJETIVO DE LA ENTREVISTA:

Recolectar información sobre la seguridad de la información dentro de la UNIVERSIDAD TÉCNICA DE AMBATO.

CUESTIONARIO

¿Se ha realizado alguna prueba de instrucción en la red interna de datos?

Si

¿Se cuenta con algún hardware/software para detectar vulnerabilidades en la intranet?

Si

¿Alguna vez la información ha sido alterada dentro de la institución de forma ilícita?

No

¿Qué servicios presta el/los servidores web? (Http, correo electrónico, base de datos) ?

BDD, PROXY, HTTP.

¿Existen host que ejecuten servicios innecesarios?

NO

¿Qué tipo de Sistema Operativo es utilizado?

LINUX

WINDOWS

¿Con q tipos de protección cuentan los servidores de la UTA? (VPN, ACLS, FIREWALLS) ?

IPTABLES

¿Piensa que los sistemas informáticos existentes en la organización son seguros?

EN SU MAYORÍA, SÍ

¿Cantidad de servidores con los que se cuenta?

2

¿Durante cuánto tiempo han estado operativos los servidores?

3 AÑOS

¿Cuenta con algún tipo de encriptación para asegurar los datos importantes?

NO

¿A qué tipo de amenazas o de ataques se han expuesto los servidores últimamente?

NINGUNA

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES EINFORMÁTICOS

Entrevista aplicada al personal del departamento de sistemas.

OBJETIVO DE LA ENTREVISTA:

Recolectar información sobre la seguridad de la información dentro de la UNIVERSIDAD TÉCNICA DE AMBATO.

CUESTIONARIO

¿Se ha realizado alguna prueba de instrucción en la red interna de datos?

No

¿Se cuenta con algún hardware/software para detectar vulnerabilidades en la intranet?

Si, software

¿Alguna vez la información ha sido alterada dentro de la institución de forma ilícita?

No

¿Qué servicios presta el/los servidores web? (Http, correo electrónico, base de datos) ?

- Correo electrónico
- Autenticación de usuarios
- Aulas virtuales, etc.

¿Existen host que ejecuten servicios innecesarios?

No

¿Qué tipo de Sistema Operativo es utilizado?

Plataforma Linux y Windows

¿Con q tipos de protección cuentan los servidores de la UTA? (VPN, ACLS, FIREWALLS) ?

- Firewalls
- VLANS
- Antivirus

¿Piensa que los sistemas informáticos existentes en la organización son seguros?

Parcialmente

¿Cantidad de servidores con los que se cuenta?

Diez.

¿Durante cuánto tiempo han estado operativos los servidores?

Varios desde 2005; han ido variando en función del tiempo

¿Cuenta con algún tipo de encriptación para asegurar los datos importantes?

No la totalidad, el acceso a usuarios parcialmente

¿A qué tipo de amenazas o de ataques se han expuesto los servidores últimamente?

Virus informáticos

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES EINFORMÁTICOS

Entrevista aplicada al personal del departamento de sistemas.

OBJETIVO DE LA ENTREVISTA:

Recolectar información sobre la seguridad de la información dentro de la UNIVERSIDAD TÉCNICA DE AMBATO.

CUESTIONARIO

¿Se ha realizado alguna prueba de instrucción en la red interna de datos?

SI

¿Se cuenta con algún hardware/software para detectar vulnerabilidades en la intranet?

SI

¿Alguna vez la información ha sido alterada dentro de la institución de forma ilícita?

NO

¿Qué servicios presta el/los servidores web? (Http, correo electrónico, base de datos) ?

HTTP ; HTTPS ; BASE DE DATOS

¿Existen host que ejecuten servicios innecesarios?

NO

¿Qué tipo de Sistema Operativo es utilizado?

LINUX ; WINDOWS

¿Con q tipos de protección cuentan los servidores de la UTA? (VPN, ACLS, FIREWALLS) ?

FIREWALL

¿Piensa que los sistemas informáticos existentes en la organización son seguros?

SE HACE LO POSIBLE

¿Cantidad de servidores con los que se cuenta?

15

¿Durante cuánto tiempo han estado operativos los servidores?

9 AÑOS

¿Cuenta con algún tipo de encriptación para asegurar los datos importantes?

¿A qué tipo de amenazas o de ataques se han expuesto los servidores últimamente?

ANEXO 7

Ubicación Universidad Técnica de Ambato, campus Huachi