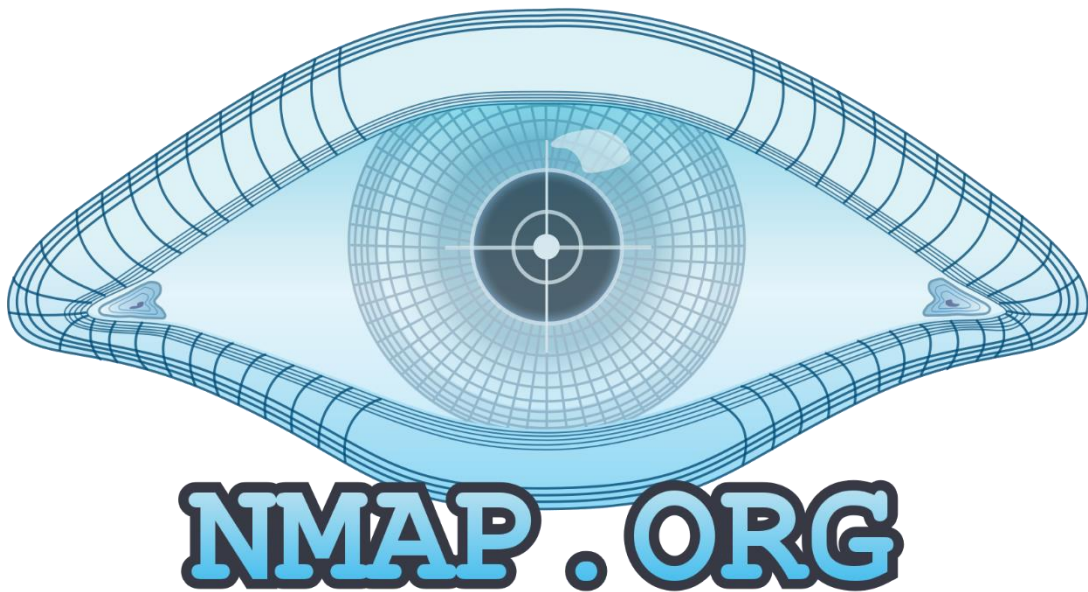




ANÁLISIS DE VULNERABILIDADES CON NMAP

TAREA 1



ERIC SERRANO MARÍN

UD3
HACKING ÉTICO

Contenido

ANÁLISIS DE VULNERABILIDAD	2
1. Ejecución de escaneo de vulnerabilidades específico.	2
2. Ejecución de escaneo de vulnerabilidades general.	3
CONCLUSIÓN.....	3
RECOPIACIÓN DE INFORMACIÓN CON NSE.....	4
1. Identifica los servicios SMB y SNMP.	5
2. Ejecuta scripts para SMB.	5
3. Ejecuta scripts para SMNP.	8
4. Escaneo de servicios adicionales.	9
Conclusiones de la Evaluación de Vulnerabilidades y Servicios Adicionales.	9

ANÁLISIS DE VULNERABILIDAD

En base a los datos obtenidos en las anteriores tareas (puertos abiertos, servicios), realiza un escaneo de vulnerabilidades empleando Nmap contra las dos máquinas vulnerables Metasploitable3.

Intenta ceñirte a aquellos servicios y puertos que has descubierto en primer lugar.

Tras esto realiza un scan sin especificar servicios y puertos, sencillamente lanza un escaneo de vulnerabilidades contra la máquina para ver si habías omitido algún protocolo, servicio, etc.

Podrás observar que Nmap nos proporciona el CVE de las vulnerabilidades que ha encontrado, incluso a veces nos sugeriría un posible exploit a emplear.

1. Ejecución de escaneo de vulnerabilidades específico.

```
nmap --script vuln -oX informe_vuln_WinUbun.xml -p 21,22,80,445,3306  
192.168.56.102 192.168.56.101
```

No tengo comando, pero en el archivo html que voy a pegar aquí aparece el comando que he hecho como prueba, es que he pasado al siguiente comando sin sacarlo.

```
sudo xsltproc informe_vuln_WinUbun.xml -o 1. Ejecución de escaneo de  
vulnerabilidades específico
```



```
(kali㉿kali)-[~]  
$ sudo xsltproc informe_vuln_WinUbun.xml -o 1. Ejecución de escaneo de vulnerabilidades específico.html
```

[Enlace al archivo HTML.](#)

[Un gif por si acaso no apetece descargarse el archivo.](#)

2. Ejecución de escaneo de vulnerabilidades general.

`sudo nmap --script vuln -oX VulnGeneral.xml 192.168.56.102 192.168.56.101`

```
(kali@kali)-[~]
$ sudo nmap --script vuln -oX VulnGeneral.xml 192.168.56.102 192.168.56.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 12:40 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Stats: 0:01:37 elapsed; 0 hosts completed (2 up), 2 undergoing Script Scan
NSE Timing: About 94.31% done; ETC: 12:42 (0:00:05 remaining)
Stats: 0:03:59 elapsed; 0 hosts completed (2 up), 2 undergoing Script Scan
NSE Timing: About 99.72% done; ETC: 12:44 (0:00:01 remaining)
Nmap scan report for 192.168.56.102
Host is up (0.00023s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
|_ssl-dh-params:
|_VULNERABLE:
|_Diffie-Hellman Key Exchange Insufficient Group Strength
|_State: VULNERABLE
|_Transport Layer Security (TLS) services that use Diffie-Hellman groups
|_of insufficient strength, especially those using one of a few commonly
|_shared groups, may be susceptible to passive eavesdropping attacks.
|_Check results:
|_WEAK DH GROUP 1
```

`sudo xsltproc VulnGeneral.xml -o 2. Ejecución de escaneo de vulnerabilidades general`

```
(kali@kali)-[~]
$ sudo xsltproc VulnGeneral.xml -o 2. Ejecución de escaneo de vulnerabilidades general.html
```

[Enlace al archivo HTML.](#)

[Un gif por si acaso no le apetece descargarse el archivo.](#)

CONCLUSIÓN

- La Máquina Ubuntu (192.168.56.101) presenta varias vulnerabilidades, incluyendo posibles inyecciones de SQL.
- La Máquina Windows (192.168.56.102) tiene vulnerabilidades significativas, como la ejecución remota de código a través de SMB (MS17-010) y vulnerabilidades de denegación de servicio.

Para más información mirar el informe HTML.

RECOPIACIÓN DE INFORMACIÓN CON NSE

Concretamente vamos a emplear los scripts relacionados con SMB y SNMP.

Haciendo como objetivo a nuestro sistema Windows de nuestro entorno de aprendizaje Metasploitable3, realiza una recopilación de información mediante los scripts de Nmap.

Utiliza tanto los scripts del protocolo SMB como del protocolo SNMP. No has de emplear todos, tan solo aquellos que se limiten a darnos información.

Deberás indagar un poco en los scripts para averiguar cuáles son útiles para este propósito.

Por ejemplo: aquellos scripts de la categoría “brute” están destinados al ataque por fuerza bruta de contraseñas, por lo que en principio no sería de nuestro interés.

Entrega un reporte de los resultados obtenidos. Deben constar los resultados y los métodos empleados. Fíjate en los tipos de datos que es capaz de descubrir (usuarios, programas y sus versiones, SO, procesos, archivos compartidos, hardware, x64-x86, etc.)

Consideraciones a tener en cuenta:

- SMB: habitualmente los servicios asociados a este protocolo escuchan por los puertos 445, 139.
- SNMP: habitualmente los servicios asociados a este protocolo escuchan por los puertos 161 y 162. A diferencia de SMP, SNMP trabaja con UDP.

Estos dos protocolos asociados a Windows han sido objeto de muchos ataques debido a sus vulnerabilidades pasadas, a día de hoy se siguen descubriendo, por lo que siempre es interesante realizar un scan de ellos.

Especialmente SNMP suele estar mal configurado por defecto, por lo que, si nuestro objetivo es un sistema Windows, podemos tener suerte.

Busca algún otro servicio o protocolo empleado en alguna de las dos máquinas y recopila información sobre él.

1. Identifica los servicios SMB y SNMP.

```
cd /usr/share/nmap/scripts
```

```
ls smb*
```

```
(kali@kali)-[~]
└─$ cd /usr/share/nmap/scripts
(kali@kali)-[/usr/share/nmap/scripts]
└─$ ls smb*
smb2-capabilities.nse  smb-brute.nse  smb-enum-processes.nse  smb-enum-users.nse  smb-os-discovery.nse  smb-security-mode.nse  smb-vuln-cv
smb2-security-mode.nse  smb-double-pulsar-backdoor.nse  smb-enum-services.nse  smb-flood.nse  smb-print-text.nse  smb-server-stats.nse  smb-vuln-cv
smb2-time.nse  smb-enum-domains.nse  smb-enum-sessions.nse  smb-ls.nse  smb-protocols.nse  smb-system-info.nse  smb-vuln-ms
smb2-vuln-uptime.nse  smb-enum-groups.nse  smb-enum-shares.nse  smb-mbenum.nse  smb-psexec.nse  smb-vuln-conficker.nse  smb-vuln-ms
```

```
ls snmp*
```

```
(kali@kali)-[/usr/share/nmap/scripts]
└─$ ls snmp*
snmp-brute.nse  snmp-info.nse  snmp-ios-config.nse  snmp-processes.nse  snmp-win32-services.nse  snmp-win32-software.nse
snmp-hh3c-logins.nse  snmp-interfaces.nse  snmp-netstat.nse  snmp-sysdescr.nse  snmp-win32-shares.nse  snmp-win32-users.nse
```

2. Ejecuta scripts para SMB.

Para la Máquina Ubuntu (192.168.56.101):

smb-enum-domains.nse: Enumera dominios SMB.

```
(kali@kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script smb-enum-domains.nse 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 13:58 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00029s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp    open  microsoft-ds
631/tcp    open  ipp
3000/tcp   closed ppp
3306/tcp   open  mysql
8080/tcp   open  http-proxy
8181/tcp   closed intermapper
MAC Address: 08:00:27:42:51:79 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-domains:
| METASPLOITABLE3-UB1404
| Groups: n/a
| Users: chewbacca
| Creation time: unknown
| Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
| Account lockout disabled
| Builtin
| Groups: n/a
| Users: n/a
| Creation time: unknown
| Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
| Account lockout disabled
Nmap done: 1 IP address (1 host up) scanned in 7.87 seconds
```

smb-enum-users.nse: Enumera usuarios SMB.

```
(kali@kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script smb-enum-users.nse 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 13:59 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00030s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3000/tcp  closed ppp
3306/tcp  open  mysql
8080/tcp  open  http-proxy
8181/tcp  closed intermapper
MAC Address: 08:00:27:42:51:79 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-users:
|   METASPLOITABLE3-UB1404\chewbacca (RID: 1000)
|   Full name:
|   Description:
|   Flags: Normal user account
|_

Nmap done: 1 IP address (1 host up) scanned in 9.01 seconds
```

smb-enum-shares.nse: Enumera recursos compartidos SMB.

```
Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\192.168.56.101\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (metasploitable3-ub1404 server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.56.101\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.56.101\public:
|     Type: STYPE_DISKTREE
|     Comment: WWW
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\www\html\
|     Anonymous access: <none>
|     Current user access: <none>
|_

Nmap done: 1 IP address (1 host up) scanned in 23.59 seconds
```

smb-enum-sessions.nse: Enumera sesiones SMB.

```
Host script results:
| smb-enum-sessions:
|_ <nobody>
```

Para la Máquina Windows (192.168.56.102):

smb-vuln-ms17-010.nse: Verifica la vulnerabilidad MS17-010 (Ejecución remota de código).

```
Host script results:
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
| Disclosure date: 2017-03-14
| References:
| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ NT STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 19.18 seconds
```

smb-vuln-ms10-054.nse: Verifica la vulnerabilidad MS10-054.

```
Host script results:
|_ smb-vuln-ms10-054: false
```

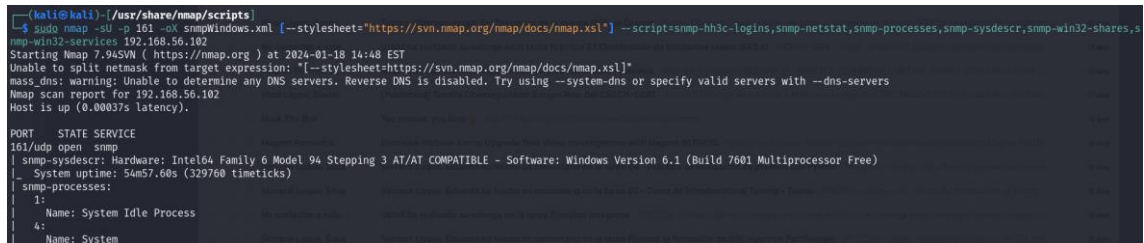
smb-vuln-ms10-061.nse: Verifica la vulnerabilidad MS10-061.

```
Host script results:
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```


3. Ejecuta scripts para SNMP.

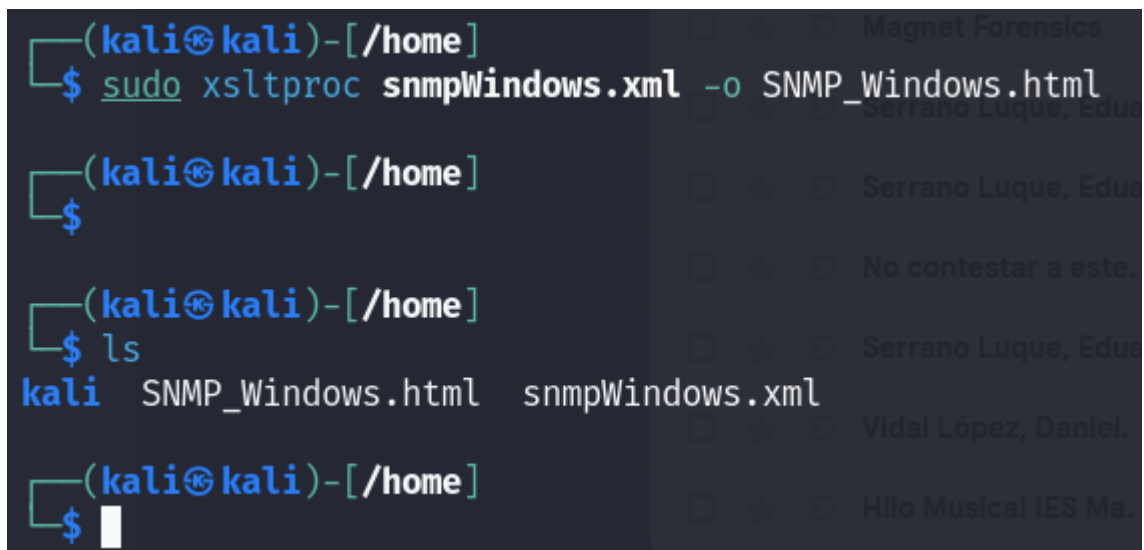
Para la Máquina Windows (192.168.56.102):

```
sudo nmap -sU -p 161 -oX snmpWindows.xml [--stylesheet="https://svn.nmap.org/nmap/docs/nmap.xsl"] --script=snmp-hh3c-logins,snmp-netstat,snmp-processes,snmp-sysdescr,snmp-win32-shares,snmp-win32-services 192.168.56.102
```



```
(kali@kali)-[/usr/share/nmap/scripts]
$ sudo nmap -sU -p 161 -oX snmpWindows.xml [--stylesheet="https://svn.nmap.org/nmap/docs/nmap.xsl"] --script=snmp-hh3c-logins,snmp-netstat,snmp-processes,snmp-sysdescr,snmp-win32-shares,snmp-win32-services 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 14:48 EST
Unable to split netmask from target expression: "[--stylesheet=https://svn.nmap.org/nmap/docs/nmap.xsl]"
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00037s latency).
PORT      STATE SERVICE
161/udp   open  snmp
snmp-sysdescr: Hardware: Intel64 Family 6 Model 94 Stepping 3 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free)
System uptime: 54m57.60s (329760 timeticks)
snmp-processes:
1: Name: System Idle Process
4: Name: System
```

```
sudo xsltproc snmpWindows.xml -o SNMP_Windows.html
```



```
(kali@kali)-[/home]
$ sudo xsltproc snmpWindows.xml -o SNMP_Windows.html
(kali@kali)-[/home]
$ ls
kali  SNMP_Windows.html  snmpWindows.xml
```

[Reporte SNMP Windows.](#)

[Gif.](#)

Para la Máquina Ubuntu (192.168.56.101):

He probado todos los scripts de SNMP y ninguno me ha funcionado.

4. Escaneo de servicios adicionales.

sudo nmap -p- --open -sV -sC -oX servicios_adicionales.xml 192.168.56.101 192.168.56.102

```
(kali@kali)-[/home]
$ sudo nmap -p- --open -sV -sC -oX servicios_adicionales.xml 192.168.56.101 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 15:13 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
```

sudo xsltproc servicios_adicionales.xml -o servicios_adicionales.html

```
(kali@kali)-[/home]
$ sudo xsltproc servicios_adicionales.xml -o servicios_adicionales.html
(kali@kali)-[/home]
$ ls
kali servicios_adicionales.html servicios_adicionales.xml snmpUbuntu.xml SNMP_Windows.html snmpWindows.xml
(kali@kali)-[/home]
$
```

[Reporte servicios adicionales.](#)

[Gif.](#)

Conclusiones de la Evaluación de Vulnerabilidades y Servicios Adicionales.

192.168.56.101 (Máquina Ubuntu):

- Se destacan servicios como ProFTPD (FTP), OpenSSH (SSH), Apache HTTP Server, Samba smbd, CUPS (Common Unix Printing System), MySQL, WEBrick HTTPd, UnrealIRCd (IRC), Jetty, y otros.
- Las versiones de software y banners asociados a estos servicios han sido recopiladas.
- Se ha encontrado información detallada sobre la configuración de algunos servicios, como los títulos de las páginas web, contenido de directorios, y detalles de la configuración de Samba.

192.168.56.102 (Máquina Windows):

- Destacan servicios como Microsoft FTPd, OpenSSH (SSH), Microsoft IIS HTTPd, Microsoft Windows RPC, MySQL, Java RMI, Apache Tomcat, Microsoft HTTPAPI, Jenkins TcpSlaveAgentListener, y otros.
- Las versiones de software y banners han sido recopiladas para su análisis.
- Se ha obtenido información detallada sobre la configuración de servicios como RDP (Remote Desktop Protocol), GlassFish Server, Apache Tomcat, Jenkins, entre otros.

Observaciones Generales:

- Ambas máquinas presentan una variedad significativa de servicios y protocolos activos.
- Se han identificado posibles puntos de vulnerabilidad y configuraciones que podrían representar riesgos de seguridad.