REPORT DANIELE NIEDDU – ESERCIZIO 09/11/2024

Esercizio:

L'esercizio consisteva nel provare i comandi riportati sotto, e da questi cercare di estrapolare informazioni utili per la ricerca di vulnerabilità.

Comandi usati:

1. nmap -sn -PE <target>

2. netdiscover -r <target>

3. crackmapexec <target>

4. nmap <target> –top-ports 10 –open

5. nmap <target> -p- -sV –reason –dns-server ns

6. us -mT -Iv <target>:a -r 3000 -R 3 && us -mU -Iv <target>:a -r 3000 -R 3

7. nmap -sS -sV -T4 <target>

8. hping3 –scan known <target>

9. nc -nvz <target> 1-1024

10. nc -nv <target> 22

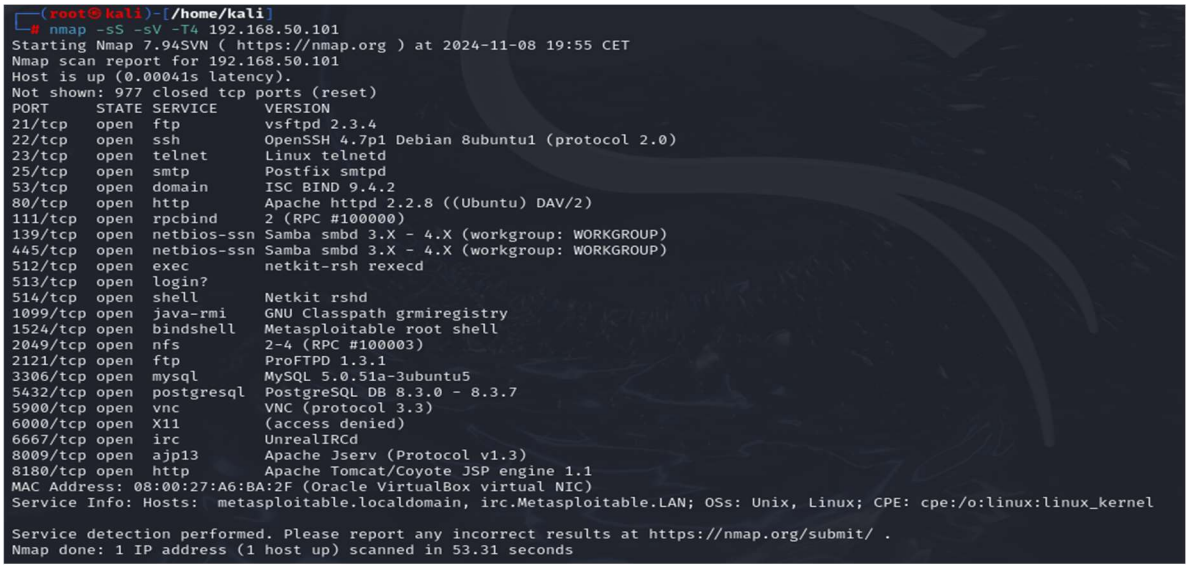
11. nmap -sV <target>

12. db_import <file.xml> (For Metasploit Framework)

13. nmap -f –mtu=512 <target>

14. masscan <network> -p80 –banners –source-ip <target>

Risultati ottenuti:



```
┌──(root㉿kali)-[/home/kali]
└─# crackmapexec smb 192.168.50.101 --shares
SMB         192.168.50.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True
)
SMB         192.168.50.101  445    METASPLOITABLE   [-] Error enumerating shares: STATUS_ACCESS_DENIED

┌──(root㉿kali)-[/home/kali]
└─# crackmapexec smb 192.168.50.101 --users
SMB         192.168.50.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True
)
SMB         192.168.50.101  445    METASPLOITABLE   [-] Error enumerating domain users using dc ip 192.168.50.101: socket connectio
n error while opening: [Errno 111] Connection refused
SMB         192.168.50.101  445    METASPLOITABLE   [*] Trying with SAMRPC protocol
SMB         192.168.50.101  445    METASPLOITABLE   [+] Enumerated domain user(s)
SMB         192.168.50.101  445    METASPLOITABLE   [+] Enumerated domain user(s)
```

```
┌──(root㉿kali)-[/home/kali]
└─# crackmapexec smb 192.168.50.101 --groups
SMB         192.168.50.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True
)
SMB         192.168.50.101  445    METASPLOITABLE   [-] Error enumerating domain group using dc ip 192.168.50.101: socket connectio
n error while opening: [Errno 111] Connection refused
```

```
┌──(root㉿kali)-[/home/kali]
└─# us -mT -Iv 192.168.50.101:a -r 3000 -R 3 && us -mU -Iv 192.168.50.101:a -r 3000 -R 3
adding 192.168.50.101/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.50.101:8787  ttl 64
TCP open 192.168.50.101:5900  ttl 64
TCP open 192.168.50.101:39532  ttl 64
TCP open 192.168.50.101:139  ttl 64
TCP open 192.168.50.101:23  ttl 64
TCP open 192.168.50.101:42955  ttl 64
TCP open 192.168.50.101:53  ttl 64
TCP open 192.168.50.101:2049  ttl 64
TCP open 192.168.50.101:25  ttl 64
TCP open 192.168.50.101:1099  ttl 64
TCP open 192.168.50.101:6667  ttl 64
TCP open 192.168.50.101:1524  ttl 64
TCP open 192.168.50.101:3632  ttl 64
TCP open 192.168.50.101:80  ttl 64
TCP open 192.168.50.101:512  ttl 64
TCP open 192.168.50.101:6697  ttl 64
TCP open 192.168.50.101:8009  ttl 64
TCP open 192.168.50.101:445  ttl 64
TCP open 192.168.50.101:6000  ttl 64
TCP open 192.168.50.101:5432  ttl 64
TCP open 192.168.50.101:111  ttl 64
TCP open 192.168.50.101:8180  ttl 64
TCP open 192.168.50.101:514  ttl 64
TCP open 192.168.50.101:21  ttl 64
TCP open 192.168.50.101:22  ttl 64
TCP open 192.168.50.101:513  ttl 64
TCP open 192.168.50.101:38320  ttl 64
TCP open 192.168.50.101:49934  ttl 64
TCP open 192.168.50.101:2121  ttl 64
TCP open 192.168.50.101:3306  ttl 64
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.101 -top-ports 100 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 19:41 CET
Nmap scan report for 192.168.50.101
Host is up (0.00059s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 08:00:27:A6:BA:2F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvz 192.168.50.101 1-1024
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.101 -p- -sV -reason -dns-server ns
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 19:42 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers w
th --dns-servers
Stats: 0:03:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.53% done; ETC: 19:46 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.00038s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  shell       syn-ack ttl 64 Netkit rshd
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown     syn-ack ttl 64
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
38320/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
39532/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
42955/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
49934/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
MAC Address: 08:00:27:A6:BA:2F (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 235.99 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvz 192.168.50.101 1-1024
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open

┌──(root㉿kali)-[/home/kali]
└─# nc -nv 192.168.50.101 22
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:06 CET
Nmap scan report for 192.168.50.101
Host is up (0.00053s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:A6:BA:2F (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.63 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -f -mtu=512 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:14 CET
Nmap scan report for 192.168.50.101
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:A6:BA:2F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sF -p1-100 -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:23 CET
Nmap scan report for 192.168.50.101
Host is up (0.00032s latency).
Not shown: 94 closed tcp ports (reset)
PORT   STATE         SERVICE
21/tcp open|filtered ftp
22/tcp open|filtered ssh
23/tcp open|filtered telnet
25/tcp open|filtered smtp
53/tcp open|filtered domain
80/tcp open|filtered http
MAC Address: 08:00:27:A6:BA:2F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -v -v -Pn 192.168.50.101
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:26 CET
Initiating ARP Ping Scan at 20:26
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 20:26, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:26
Completed Parallel DNS resolution of 1 host. at 20:26, 0.00s elapsed
Initiating SYN Stealth Scan at 20:26
Scanning 192.168.50.101 [1000 ports]
Discovered open port 22/tcp on 192.168.50.101
Discovered open port 21/tcp on 192.168.50.101
Discovered open port 3306/tcp on 192.168.50.101
Discovered open port 111/tcp on 192.168.50.101
Discovered open port 80/tcp on 192.168.50.101
Discovered open port 5900/tcp on 192.168.50.101
Discovered open port 23/tcp on 192.168.50.101
Discovered open port 445/tcp on 192.168.50.101
Discovered open port 139/tcp on 192.168.50.101
Discovered open port 25/tcp on 192.168.50.101
Discovered open port 53/tcp on 192.168.50.101
Discovered open port 2049/tcp on 192.168.50.101
Discovered open port 1524/tcp on 192.168.50.101
Discovered open port 8180/tcp on 192.168.50.101
Discovered open port 512/tcp on 192.168.50.101
Discovered open port 1099/tcp on 192.168.50.101
Discovered open port 513/tcp on 192.168.50.101
Discovered open port 514/tcp on 192.168.50.101
Discovered open port 2121/tcp on 192.168.50.101
Discovered open port 5432/tcp on 192.168.50.101
Discovered open port 8009/tcp on 192.168.50.101
Discovered open port 6000/tcp on 192.168.50.101
Discovered open port 6667/tcp on 192.168.50.101
Completed SYN Stealth Scan at 20:26, 0.71s elapsed (1000 total ports)
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.00045s latency).
Scanned at 2024-11-08 20:26:00 CET for 1s
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 64
22/tcp   open  ssh          syn-ack ttl 64
23/tcp   open  telnet       syn-ack ttl 64
25/tcp   open  smtp         syn-ack ttl 64
53/tcp   open  domain       syn-ack ttl 64
80/tcp   open  http         syn-ack ttl 64
111/tcp  open  rpcbind      syn-ack ttl 64
139/tcp  open  netbios-ssn  syn-ack ttl 64
445/tcp  open  microsoft-ds syn-ack ttl 64
512/tcp  open  exec         syn-ack ttl 64
513/tcp  open  login        syn-ack ttl 64
514/tcp  open  shell        syn-ack ttl 64
1099/tcp open  rmiregistry  syn-ack ttl 64
1524/tcp open  ingreslock   syn-ack ttl 64
2049/tcp open  nfs          syn-ack ttl 64
2121/tcp open  ccproxy-ftp  syn-ack ttl 64
3306/tcp open  mysql        syn-ack ttl 64
5432/tcp open  postgresql   syn-ack ttl 64
5900/tcp open  vnc          syn-ack ttl 64
6000/tcp open  X11          syn-ack ttl 64
6667/tcp open  irc          syn-ack ttl 64
8009/tcp open  ajp13        syn-ack ttl 64
8180/tcp open  unknown      syn-ack ttl 64
MAC Address: 08:00:27:A6:BA:2F (Oracle VirtualBox virtual NIC)
```

Con i dati ottenuti, facendo una ricerca online, si possono scoprire alcune vulnerabilità come quelle riportate sotto:

FTP (vsftpd 2.3.4)

Questa versione di vsftpd ha una backdoor nota. Se un attaccante si connette utilizzando :) come parte del nome utente, può ottenere una shell sulla porta 6200.

Telnet (Linux telnetd)

L'uso di Telnet è di per sé rischioso poiché invia i dati non crittografati, facilitando attacchi di intercettazione. Inoltre, può essere soggetto a brute-forcing di credenziali.

Samba (139/tcp e 445/tcp)

Samba smbd 3.X - 4.X è vulnerabile a numerosi attacchi. Una delle vulnerabilità più conosciute è "Samba CVE-2007-2447", che permette l'esecuzione di comandi remoti tramite un exploit chiamato "Samba usermap script".

Bindshell (1524/tcp)

Questa porta spesso rappresenta un bind shell già aperto e accessibile senza bisogno di autenticazione. Può fornire accesso diretto al sistema remoto.

MySQL (3306/tcp)

Potrebbero essere sfruttabili password di default o configurazioni non sicure (ad esempio, l'accesso root senza password). Potenziali escalation di privilegi tramite query SQL non sicure.

ProFTPD (2121/tcp)

Vulnerabilità: Alcune versioni di ProFTPD hanno una vulnerabilità RCE (Remote Command Execution) tramite l'utilizzo di moduli come mod_copy.

PostgreSQL (5432/tcp)

Potrebbe essere configurato con credenziali deboli o accesso anonimo. Inoltre, potenziali attacchi di SQL Injection o accesso amministrativo non protetto.

UnrealIRCd (6667/tcp)

È noto per una backdoor inserita in alcune versioni compromesse del codice sorgente. L'exploit consente l'esecuzione di comandi remoti.

RSH (512/tcp, 513/tcp, 514/tcp)

rsh (Remote Shell) utilizza connessioni non crittografate, rendendolo vulnerabile agli attacchi di intercettazione e di spoofing.

Apache HTTPD (80/tcp, 8180/tcp)

Potrebbe essere soggetto a diversi tipi di attacchi, come directory traversal, buffer overflow o accesso non autorizzato.

NFS (2049/tcp)

Configurazioni di NFS non sicure possono consentire il mounting delle directory esportate, che può permettere un'escalation di privilegi.