Esercizio W11D4
Network
192.168.1.0
192.168.32.0
Host
Pfsense: 192.168.1.1
Kali: 192.168.1.100
Meta: 192.168.32.100

TCP: # nmap -sS ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.32.100
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:29 EST
Nmap scan report for 192.168.32.100
Host is up (0.022s 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
Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

Scansione completa: # nmap -sV ip address

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:41 EST
Nmap scan report for 192.168.32.100
Host is up (0.027s latency).
Not shown: 977 closed tcp ports (conn-refused)
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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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
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 11.99 seconds
```

Output su file: # nmap -sV -oN file.txt ip address

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -oN file.txt 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:46 EST
Nmap scan report for 192.168.32.100
Host is up (0.051s latency).
Not shown: 977 closed tcp ports (conn-refused)
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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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
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 12.11 seconds

┌──(kali㉿kali)-[~]
└─$ ls -l
total 464
drwxr-xr-x 2 kali kali   4096 Dec  7 21:34 Desktop
drwxr-xr-x 2 kali kali   4096 Oct 27 13:24 Documents
drwxr-xr-x 2 kali kali   4096 Jan 18 14:23 Downloads
-rw-r--r-- 1 kali kali   1705 Jan 19 13:47 file.txt
-rwxr-xr-x 1 kali kali 224755 Dec 17 18:10 gameshell-save.sh
-rw-r--r-- 1 kali kali 203144 Nov 30 14:02 gameshell.sh
drwxr-xr-x 2 kali kali   4096 Oct 27 13:24 Music
-rw-r--r-- 1 kali kali    521 Jan 18 14:22 nessus
drwxr-xr-x 2 kali kali   4096 Oct 27 13:24 Pictures
drwxr-xr-x 2 kali kali   4096 Oct 27 13:24 Public
-rw-r--r-- 1 root root    819 Jan 16 13:49 scanMeta
drwxr-xr-x 2 kali kali   4096 Oct 27 13:24 Templates
drwxr-xr-x 2 kali kali   4096 Oct 27 13:24 Videos

┌──(kali㉿kali)-[~]
└─$ more file.txt
# Nmap 7.94 scan initiated Fri Jan 19 13:46:56 2024 as: nmap -sV -oN file.txt 192.168.32.100
Nmap scan report for 192.168.32.100
Host is up (0.051s latency).
Not shown: 977 closed tcp ports (conn-refused)
```

Commentato [LR1]: Il comando ha creato un file di testo popolato con il risultato della scansione nmap -sV sul target

```
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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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
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 at Fri Jan 19 13:47:08 2024 -- 1 IP address (1 host up) scanned in 12.11 seconds
```

Scansione su porta: # nmap -sS -p 8080 ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 8080 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:54 EST
Nmap scan report for 192.168.32.100
Host is up (0.0027s latency).
PORT     STATE  SERVICE
8080/tcp closed http-proxy
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Scansione tutte le porte: # nmap -sS -p- ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p- 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 14:15 EST
Nmap scan report for 192.168.32.100
Host is up (0.071s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
36198/tcp open  unknown
44391/tcp open  unknown
45207/tcp open  unknown
50526/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 48.60 seconds
```

Scansione UDP: # nmap -sU -r -v ip address

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -r -v 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 14:18 EST
Initiating Ping Scan at 14:18
Scanning 192.168.32.100 [4 ports]
Completed Ping Scan at 14:18, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:18
Completed Parallel DNS resolution of 1 host. at 14:18, 0.00s elapsed
Initiating UDP Scan at 14:18
Scanning 192.168.32.100 [1000 ports]
Discovered open port 53/udp on 192.168.32.100
Discovered open port 111/udp on 192.168.32.100
Increasing send delay for 192.168.32.100 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.32.100 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.32.100 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.32.100 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.32.100 from 400 to 800 due to 11 out of 12 dropped probes since last increase.
Discovered open port 137/udp on 192.168.32.100
UDP Scan Timing: About 3.67% done; ETC: 14:32 (0:13:34 remaining)
UDP Scan Timing: About 7.54% done; ETC: 14:34 (0:14:18 remaining)
UDP Scan Timing: About 19.93% done; ETC: 14:35 (0:13:31 remaining)
Discovered open port 2049/udp on 192.168.32.100
UDP Scan Timing: About 25.69% done; ETC: 14:35 (0:12:38 remaining)
UDP Scan Timing: About 31.36% done; ETC: 14:35 (0:11:45 remaining)
UDP Scan Timing: About 36.03% done; ETC: 14:35 (0:10:52 remaining)
UDP Scan Timing: About 41.70% done; ETC: 14:35 (0:09:57 remaining)
UDP Scan Timing: About 47.06% done; ETC: 14:35 (0:09:05 remaining)
UDP Scan Timing: About 52.32% done; ETC: 14:35 (0:08:13 remaining)
UDP Scan Timing: About 57.68% done; ETC: 14:35 (0:07:19 remaining)
UDP Scan Timing: About 62.92% done; ETC: 14:35 (0:06:24 remaining)
UDP Scan Timing: About 68.28% done; ETC: 14:35 (0:05:29 remaining)
UDP Scan Timing: About 73.42% done; ETC: 14:35 (0:04:36 remaining)
UDP Scan Timing: About 78.78% done; ETC: 14:35 (0:03:41 remaining)
UDP Scan Timing: About 84.04% done; ETC: 14:36 (0:02:46 remaining)
UDP Scan Timing: About 89.40% done; ETC: 14:36 (0:01:51 remaining)
UDP Scan Timing: About 94.48% done; ETC: 14:35 (0:00:57 remaining)
Completed UDP Scan at 14:36, 1074.71s elapsed (1000 total ports)
Nmap scan report for 192.168.32.100
Host is up (0.011s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
1020/udp open|filtered unknown
2049/udp open          nfs
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1074.90 seconds
           Raw packets sent: 1482 (68.290KB) | Rcvd: 1094 (79.771KB)
```

Scansione sistema operativo: # nmap -O ip address

```
└─# nmap -O 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-25 12:13 EST
Nmap scan report for 192.168.32.100
Host is up (0.0042s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds
```

Scansione versione servizi: # nmap -sV ip address

```
└─# nmap -sV 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-25 12:15 EST
Nmap scan report for 192.168.32.100
Host is up (0.019s 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  tcpwrapped
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
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 12.34 seconds
```

Scansione common 100 ports: # nmap -F ip address

```
└─# nmap -F 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-25 12:16 EST
Nmap scan report for 192.168.32.100
Host is up (0.011s 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
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Scansione tramite ARP: # nmap -PR ip address

```
└─# nmap -PR 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-25 12:18 EST
Nmap scan report for 192.168.32.100
Host is up (0.013s 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
Nmap done: 1 IP address (1 host up) scanned in 0.85 seconds
```

Scansione tramite PING: # nmap -sP ip addres

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-25 12:19 EST
Nmap scan report for 192.168.32.100
Host is up (0.0018s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Scansione senza PING: # nmap -PN ip address

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PN 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-25 12:19 EST
Nmap scan report for 192.168.32.100
Host is up (0.015s 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
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```