REPORT W11D4 PEPPOLI

Tecniche di scansione con **Nmap**

Tabella Excel riassunto scansioni

Riassunto generale di ogni scansione
Ip target, Sistema operativo target, tipo di scansione, comando nmap,
numero di porte aperte e caratteristiche particolari riscontrate.

	Ip target	s.o. target	tipo scansione	comando	porte aperte	Caratteristiche particolari
1	192.168.1.101	Metasploitable	TCP	nmap -sS ip_address	23	MAC address: 08:00:27:44:05:C4
2			Scansione completa	nmap -sV ip_address	23	MAC address: 08:00:27:44:05:C4, service, version
3			Output su file	nmap -sV -oN file.txt ip_address	23	MAC address: 08:00:27:44:05:C4, service, version, salvataggio dell'output su file
4			Scansione su porta	nmap -sS -p 8080 ip_address	0	MAC address: 08:00:27:44:05:C4, service
5			Scansione su tutte le porte	nmap -sS -p- ip_address	30	MAC address: 08:00:27:44:05:C4, service, tutte e 65535 le porte
6			Scansione UDP	nmap -sU -r -v ip_address	6	MAC address: 08:00:27:44:05:C4, lunga scansione
7			Scansione sistema operativo	nmap -O ip_address	23	MAC address: 08:00:27:44:05:C4, service, Aggressive OS guesser, Network distance
8			Scansione versione servizi	nmap -sV ip_address	23	MAC address: 08:00:27:44:05:C4, service, version
9			Scansione common 100 ports	nmap -F ip_address	18	MAC address: 08:00:27:44:05:C4, service, scansione delle 100 porte più comuni
10			Scansione tramite ARP	nmap -PR ip_address	23	MAC address: 08:00:27:44:05:C4, service
11			Scansione tramite PING	nmap -sP ip_address		MAC address: 08:00:27:44:05:C4
12			Scansione senza PING	nmap -pN ip_address		MAC address: 08:00:27:44:05:C4

Prima scansione, TCP

Seconda scansione, completa

```
└─# nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:33 CET
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 30.43% done; ETC: 19:33 (0:00:14 remaining)
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 47.83% done; ETC: 19:33 (0:00:07 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 19:33 (0:00:03 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 19:33 (0:00:05 remaining)
Nmap scan report for 192.168.1.101
Host is up (0.0074s 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: 08:00:27:44:05:C4 (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 17.18 seconds
```

Terza scansione, su porta 8080

```
└─# nmap -sS -p 8080 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:39 CET
Nmap scan report for 192.168.1.101
Host is up (0.0070s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:44:05:C4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Quarta scansione, tutte le porte

```
└─# nmap -sS -p- 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:46 CET
Nmap scan report for 192.168.1.101
Host is up (0.00064s 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
39206/tcp open  unknown
44178/tcp open  unknown
44543/tcp open  unknown
50702/tcp open  unknown
MAC Address: 08:00:27:44:05:C4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.40 seconds
```

Quinta scansione, sistema operativo

```
└─# nmap -O 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 20:02 CET
Nmap scan report for 192.168.1.101
Host is up (0.0041s 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: 08:00:27:44:05:C4 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.31 (94%), Linux 2.6.9 - 2.6.24 (94%), Linux 2.6.9 - 2.6.30 (94%), L
inux 2.6.9 - 2.6.33 (94%), Linux 2.6.13 - 2.6.32 (94%), Linux 2.6.18 - 2.6.32 (93%), Linux 2.6.21 (9
3%), Linux 2.6.22 (embedded, ARM) (93%), Linux 2.6.22 - 2.6.23 (93%), Linux 2.6.22 (Ubuntu 8.04 Serv
er Edition) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds
```

Sesta scansione, tramite PING

```
└─# nmap -sP 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 20:09 CET
Nmap scan report for 192.168.1.101
Host is up (0.00059s latency).
MAC Address: 08:00:27:44:05:C4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Settima scansione, UDP prima parte

```
└─# nmap -sU -r -v 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:52 CET
Initiating ARP Ping Scan at 19:52
Scanning 192.168.1.101 [1 port]
Completed ARP Ping Scan at 19:52, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:52
Completed Parallel DNS resolution of 1 host. at 19:52, 0.00s elapsed
Initiating UDP Scan at 19:52
Scanning 192.168.1.101 [1000 ports]
Discovered open port 111/udp on 192.168.1.101
Discovered open port 53/udp on 192.168.1.101
Discovered open port 137/udp on 192.168.1.101
Discovered open port 2049/udp on 192.168.1.101
Increasing send delay for 192.168.1.101 from 0 to 50 due to 11 out of 22 dropped probes since last i
ncrease.
Increasing send delay for 192.168.1.101 from 50 to 100 due to max_successful_tryno increase to 4
```

Settima scansione, UDP seconda parte

```
Discovered open port 2049/udp on 192.168.1.101
Increasing send delay for 192.168.1.101 from 0 to 50 due to 11 out of 22 dropped probes since last i
ncrease.
Increasing send delay for 192.168.1.101 from 50 to 100 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.1.101 from 100 to 200 due to max_successful_tryno increase to 5
UDP Scan Timing: About 21.07% done; ETC: 19:54 (0:01:56 remaining)
Increasing send delay for 192.168.1.101 from 200 to 400 due to max_successful_tryno increase to 6
UDP Scan Timing: About 20.89% done; ETC: 19:57 (0:03:51 remaining)
Increasing send delay for 192.168.1.101 from 400 to 800 due to 11 out of 12 dropped probes since las
t increase.
Increasing send delay for 192.168.1.101 from 800 to 1000 due to 11 out of 11 dropped probes since la
st increase.
UDP Scan Timing: About 22.46% done; ETC: 19:59 (0:05:14 remaining)
UDP Scan Timing: About 23.65% done; ETC: 20:01 (0:06:31 remaining)
UDP Scan Timing: About 24.95% done; ETC: 20:02 (0:07:34 remaining)
UDP Scan Timing: About 26.24% done; ETC: 20:03 (0:08:29 remaining)
UDP Scan Timing: About 27.70% done; ETC: 20:05 (0:09:11 remaining)
UDP Scan Timing: About 23.97% done; ETC: 20:09 (0:12:44 remaining)
UDP Scan Timing: About 25.95% done; ETC: 20:10 (0:13:36 remaining)
UDP Scan Timing: About 28.23% done; ETC: 20:12 (0:14:32 remaining)
UDP Scan Timing: About 33.73% done; ETC: 20:15 (0:15:35 remaining)
UDP Scan Timing: About 49.29% done; ETC: 20:20 (0:14:24 remaining)
UDP Scan Timing: About 56.75% done; ETC: 20:22 (0:12:57 remaining)
UDP Scan Timing: About 62.97% done; ETC: 20:23 (0:11:23 remaining)
UDP Scan Timing: About 68.64% done; ETC: 20:23 (0:09:50 remaining)
UDP Scan Timing: About 74.23% done; ETC: 20:24 (0:08:14 remaining)
UDP Scan Timing: About 79.79% done; ETC: 20:25 (0:06:36 remaining)
UDP Scan Timing: About 85.13% done; ETC: 20:25 (0:04:55 remaining)
UDP Scan Timing: About 90.41% done; ETC: 20:25 (0:03:13 remaining)
UDP Scan Timing: About 95.49% done; ETC: 20:26 (0:01:31 remaining)
Completed UDP Scan at 20:36, 2619.58s elapsed (1000 total ports)
Nmap scan report for 192.168.1.101
Host is up (0.0071s latency).
Not shown: 994 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
2049/udp open          nfs
MAC Address: 08:00:27:44:05:C4 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2619.75 seconds
           Raw packets sent: 4045 (171.842KB) | Rcvd: 1196 (85.802KB)
```