CSPT0524IT – W10D4

Enumerazione Servizi

Evasione Firewall

1. *Enumerazione Servizi*

Command 01: *Scopri host attivi con ICMP senza fare port-scanning*

```
# nmap -sn -PE 192.168.51.0/24
```

Command 02: *Scopri host attivi con ARP, scansiona tutta la rete dall'interno*

```
# netdiscover -r 192.168.51.0/24
```

Command 03: Scansione credenziali Active Directory, SMB, SSH

```
# crackmapexec  192.168.51.0/24
```

Command 04: Identifica le prime 10 porte aperte (più comuni)

```
# nmap 192.168.51.101 --top-ports 10 --open
```

Command 05: Scansiona tutte le 65 535 porte, determina versioni servizi, il motivo della porta e specifica un dns

```
# nmap 192.168.51.101 -p- -sV --reason --dns-server ns
```

Command 06: Test di performance o reattività della rete inviando 3000 pacchetti in TCP e UDP

```
# us -mT -lv 192.168.51.101:a -r 3000 -R 3 && us -mU -lv 192.168.51.101:a -r 3000 -R 3
```

Command 07: Scansione veloce Syn per rilevare le versioni dei servizi

```
# nmap -sS -sV -T4 192.168.51.101
```

Command 08: Scansione porte conosciute inviando pacchetti ICMP, TCP e UDP

```
# hping3 --scan known 192.168.51.101
```

Command 09: Verifica le prime 1024 porte aperte (range)

nc -nvz 192.168.51.101 1-1024

Command 10: Test di connessione su una porta specifica

nc -nv 192.168.51.101 22

Command 11: Identifica versione servizi su porte aperte (le piu conosciute)

nmap -sV 192.168.51.101

Command 12: NON ESEGUITO

db_import <filename.xml>

Command 13: Invia pacchetti frammentati per bypassare/eludere Firewall e IDS

nmap -f --mtu=512 192.168.51.101

Command 14: Identifica in una rete, il numero di host con la porta 80 aperta

masscan 192.168.51.0/24 -p80 --banners --source-ip 192.168.51.101

SERVIZI IDENTIFICATI

Porta	Stato	Servizio	Versione Servizio
21	open	ftp	vsftpd 2.3.4
22	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	open	telnet	Linux telnetd
25	open	smtp	Postfix smtpd
53	open	domain	ISC BIND 9.4.2
80	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	open	rpcbind	2 (RPC #100000)
139	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	open	exec	netkit-rsh rexecd
513	open	login?	Unknown
514	open	shell	Netkit rshd
1099	open	java-rmi	GNU Classpath grmiregistry
1524	open	bindshell	Metasploitable root shell
2049	open	nfs	2-4 (RPC #100003)
2121	open	ccproxy-ftp?	Unknown
3306	open	mysql	MySQL 5.0.51a-3ubuntu5
3632	open	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	open	vnc	VNC (protocol 3.3)
6000	open	X11	(access denied)
6667	open	irc	UnrealIRCd
6697	open	irc	UnrealIRCd
8009	open	ajp13	Apache Jserv (Protocol v1.3)
8180	open	http	Apache Tomcat/Coyote JSP engine 1.1
8787	open	drb	Ruby DRb RMI (Ruby 1.8 path /usr/lib/ruby/1.8/drb)
32859	open	nlockmgr	1-4 (RPC #100021)
50476	open	java-rmi	GNU Classpath grmiregistry
51233	open	status	1 (RPC #100024)
59425	open	mountd	1-3 (RPC #100005)

2. *Evasione Firewall*

Command 01:

-sF scansione FIN, tecnica di scansione furtiva che invia pacchetti TCP con solo il flag FIN impostato. È utile per cercare porte aperte senza stabilire connessioni complete, e spesso viene utilizzata per aggirare i firewall o i sistemi di rilevamento intrusioni che bloccano le scansioni convenzionali. Se il target non risponde, la porta è aperta

```
nmap -sF -p1-100 -T4 192.168.51.101
```

Command 02:

-sS: Scansione SYN, che invia pacchetti TCP SYN per verificare lo stato delle porte (aperta, chiusa, filtrata).

- **-v -v**: Abilita due livelli di verbosità, mostrando dettagli aggiuntivi sull'output della scansione.
- **-Pn**: Disabilita il "ping" iniziale per verificare se l'host è online. Presuppone che l'host sia raggiungibile, evitando di scartarlo se non risponde ai ping.
- **172.25.0.14**: Target della scansione.

```
nmap -sS -v -v -Pn 172.25.0.14
```

Command 03:

-sS: Scansione SYN.

- **-v -v**: Verbosità.
- **-Pn**: Evita il ping iniziale.
- **-g 88**: Usa la porta **88** (porta sorgente) per i pacchetti generati da Nmap. Questo parametro può essere utilizzato per bypassare alcuni firewall o regole di filtraggio.
- **172.25.0.1**: Target della scansione.

```
nmap -sS -v -v -Pn -g 88 172.25.0.1
```

Command 04:

-p 22,25,135: Specifica la scansione delle porte **22 (SSH)**, **25 (SMTP)** e **135 (RPC)**.

- **-Pn**: Disabilita il ping iniziale.
- **-v**: Verbosità.
- **-b XXX.YY.111.2**: **Scansione FTP bounce**, che tenta di sfruttare un server FTP vulnerabile (all'indirizzo XXX.YY.111.2) per scansionare un target (scanme.nmap.org).

```
nmap -p 22,25,135 -Pn -v -b XXX.YY.111.2 scanme.nmap.org
```

Command 05:

-n: Non risolve i nomi DNS per velocizzare la scansione.

- **-sn**: Disabilita la scansione delle porte; esegue solo un **ping scan** per verificare quali host sono attivi.
- **-PE**: Usa l'Echo Request ICMP (ping standard) per identificare gli host attivi.
- **-T4**: Imposta un livello di velocità elevato per la scansione.
- **10.10.10.0/24**: Scansiona la sottorete (range) **10.10.10.0-10.10.10.255**.

  nmap -n -sn -PE -T4 10.10.10.0/24

Command 06:

-vv: Verbosità elevata.

- **-n**: Nessuna risoluzione DNS.
- **-sn**: Ping scan (non scansiona le porte).
- **-PE**: Usa pacchetti ICMP Echo Request (ping).
- **-T4**: Scansione rapida.
- **--packet-trace**: Mostra i dettagli di ogni pacchetto inviato e ricevuto.

  nmap -vv -n -sn -PE -T4 --packet-trace 10.10.10.7

Command 07:

-vv: Verbosità elevata.

- **-n**: Nessuna risoluzione DNS.
- **-Pn**: Nessun ping iniziale.
- **-sI 10.10.6.30:445**: Usa il **"Zombie scan"** (Idle scan). Qui, l'host **10.10.6.30** è usato come zombie, sfruttando la porta 445 (SMB), per eseguire una scansione stealth sul target.
- **-p 25**: Scansiona la porta 25 (SMTP).
- **10.10.6.60**: Target della scansione.

  nmap -vv -n -Pn -sI 10.10.6.30:445 -p 25 10.10.6.60

Command 08:

-n: Nessuna risoluzione DNS.

- **-sn**: Ping scan (non scansiona le porte).
- **-PE**: Usa pacchetti ICMP Echo Request.
- **--ip-options "L 10.10.6.60"**: Specifica opzioni IP personalizzate nei pacchetti (in questo caso, il flag "L").
- **--reason**: Mostra il motivo per cui ogni host è considerato attivo/inattivo.
- **10.10.6.30**: Target della scansione.

  nmap -n -sn -PE --ip-options "L 10.10.6.60" --reason 10.10.6.30

Command 09:

-vv: Verbosità elevata.

- **-n**: Nessuna risoluzione DNS.

- **-sS**: Scansione SYN.
- **-Pn**: Nessun ping iniziale.
- **--ip-options "L 10.10.6.60"**: Usa opzioni IP personalizzate nei pacchetti.
- **--reason**: Mostra il motivo per cui ogni porta viene segnalata come aperta/chiusa/filtrata.
- **10.10.10.7**: Target della scansione.

```
nmap -vv -n -sS -Pn --ip-options "L 10.10.6.60" --reason 10.10.10.7
```