

ESERCIZIO W11D1

Secondo la traccia sul sito, dobbiamo effettuare diverse tipologie di scansioni su Metasploitable, controllando le differenze eventuali che emergono tra reti diverse e uguali.

Gli scan di nmap saranno i seguenti:

- OS fingerprinting (-O)
- Syn Scan (-sS)
- TCP connect (-sT)
- Version detection (-sV)

Configurazioni reti su pfsense

Prima di procedere settiamo le macchine virtuali con l'assegnazione di indirizzi offerti dal DHCP di pfsense.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
#address 192.168.32.100/24
#netmask 255.255.255.0
#gateway 192.168.32.1
```

Configurazione normale Kali Linux

Metasploitable2 [In esecuzione] - Oracle VM VirtualBox

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
iface eth0 inet dhcp
#address 192.168.32.101
#netmask 255.255.255.0
#network 192.168.50.0
#broadcast 192.168.50.255
#gateway 192.168.32.1
```

Configurazione pfsense Metasploitable

Analisi pfsense

Su terminale scriviamo uno ad uno tutti i tipi di scan, andando per ordine come riportato sulla lista in alto.

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 09:30 EST
Nmap scan report for 192.168.50.100
Host is up (0.0019s 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 2.88 seconds
```

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 09:38 EST
Nmap scan report for 192.168.50.100
Host is up (0.0022s 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 0.74 seconds
```

SYN scan pfsense
Meta

```
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 09:40 EST
Nmap scan report for 192.168.50.100
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (conn-refused)
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 0.31 seconds
```

TCP scan
pfsense Meta

```

(kali@kali)-[~]
$ sudo nmap -sV 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 09:42 EST
Nmap scan report for 192.168.50.100
Host is up (0.0017s 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 rshexec
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 12.35 seconds

```

Version detection
pfsense Meta

Analisi rete interna

```

(kali@kali)-[~]
$ sudo nmap -O 192.168.32.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 06:50 EST
Nmap scan report for 192.168.32.101
Host is up (0.00077s 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: 08:00:27:3C:14:F7 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 15.31 seconds

```

OS fingerprinting
Metasploitable

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 06:58 EST
Nmap scan report for 192.168.32.101
Host is up (0.00058s 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: 08:00:27:3C:14:F7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

SYN scan
Metasploitable

```
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.32.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 08:46 EST
Nmap scan report for 192.168.32.101
Host is up (0.0039s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 08:00:27:3C:14:F7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds
```

TCP scan
Metasploitable

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 08:50 EST
Nmap scan report for 192.168.32.101
Host is up (0.00019s 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: 08:00:27:3C:14:F7 (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 68.82 seconds
```

Version detection
Metasploitable

Risultati

Da ciò che emerge, in entrambi casi, gli scan mostra gli stessi risultati. L'unica cosa che cambia sono il metodo utilizzato, gli hop e la latenza del sistema target. Lascio qui sotto la tabella.

IP	SISTEMA	PORTE APERTE	SERVIZI IN ASCOLTO CON VERSIONE	DESCRIZIONE DEI SERVIZI	LATENZA E HOP

192.168.50.100 (pfsense)	LINUX 2.6.X	21, 22, 23 , 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2048, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180	(Lista dei servizi in ascolto nei greenshot)	(elenco descrizioni più in basso)	-O(0.0019s) -sS(0.0022s) -sT(0.0015s) -sV(0.0017s) 2 Hops
192.168.32.100 (rete interna)	LINUX 2.6.X	21, 22, 23 , 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2048, 2121, 3306, 5432, 5900,	(Lista dei servizi in ascolto nei greenshot)	(elenco descrizioni più in basso)	- O(0.00077s) - sS(0.00058s) -sT(0.0039s) - sV(0.00019s) 1 Hop

		6000, 6667, 8009, 8180			
--	--	---------------------------------	--	--	--

Descrizione servizi

ftp: (file transfer protocol) un protocollo di comunicazione standard usato per lo scambio di file da un server a un client.

ssh: (secure shell) un protocollo di comunicazione che permette di stabilire una connessione sicura e cifrata.

telnet: un protocollo client-server che consente di cominciare una connessione tra client e server e di trasmettere dati.

smtp: (simple mail transfer protocol) un protocollo utilizzato per l'invio dei messaggi di posta elettronica.

domain: si riferisce al servizio dns, ovvero il traduttore di nomi di dominio in indirizzi IP.

http: (hyper text transfer protocol) il protocollo che si occupa di caricare le risorse richieste dal client in una pagina web.

rpcbind: si tratta di un server che converte i numeri di programma RPC in indirizzi universali. L'RPC consente a un programma di un sistema di richiedere un servizio ad un programma di un altro sistema.

netbios-ssn: un interfaccia di comunicazione che consente alle applicazioni su computer diversi di comunicare tra di loro.

exec: una funzione di sistema che sostituisce il codice in esecuzione dal lato utente con quelli di un altro programma contenuto in un file eseguibile specificato.

login?: un protocollo di autenticazione che permette agli utenti di accedere ad un sistema informatico grazie all'ausilio di username e password.

shell: un servizio syslog che riceve messaggi di log da dispositivi di rete e sistemi operativi.

java-rmi: (java remote method invocation) consente ai programmatori di creare applicazioni su base java, i cui oggetti possono essere invocati da altre macchine virtuali java, su host diversi.

bind-shell: una shell remota che consente a un utente di connettersi e interagire con un sistema remoto.

nfs: un file system che consente a client di utilizzare la rete per accedere a directory condivise da server remoti.

mysql: un sistema di gestione di database relazionali open source che utilizza SQL (structured query language).

postgresql: fornisce supporto a diverse funzioni di SQL, come trigger, chiavi esterne, subquery etc

vnc: un software di accesso e controllo remoto utilizzato per l'amministrazione del proprio computer a distanza.

X11: il sistema x Window è un framework di base per la creazione di interfacce utente grafiche su openVMS.

Irc: (internet relay chat un servizio di chat che permette agli utenti di comunicare tra di loro quasi in tempo reale, utilizzando internet.

ajp13: (Apache jServ Protocol) un protocollo binario usato per la comunicazione tra server web e un container servelet.

