Esplorazione di Nmap

Macchine utilizzate: pfSense, CyberOps Workstation.

Configurazione della rete: Rete Interna, gestita da **pfSense**, che in questo caso è stato utilizzato come Router.

Cos'è Nmap?

Nmap è uno strumento utilizzato per l'esplorazione e la sicurezza delle reti.

Per cosa viene usato nmap?

Viene utilizzato principalmente per avere informazioni dettagliate specifiche per una rete. In particolare permette di eseguire:
Scansioni delle porte aperte.
Identificazione del sistema operativo.
Rilevamento dei servizi attivi.
Scansione di rete.

Utilizzo dei comandi **Nmap**.

```
[analyst@secOps ~]$ nmap -A -T4 scanwe.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 09:46 EDT
```

Qual è il comando nmap usato?

Il comando usato è **nmap -A -T4 scanwe.nmap.org**.

Cosa fa l'opzione A?

L'opzione **-A** effettua una scansione aggressiva.
E' utile per determinare il sistema operativo dell'host, la versione dei servizi attivi e le porte aperte.

Cosa fa l'opzione T4?

L’opzione **-T4** determina la velocità della scansione.
I valori utilizzabili sono da 0 a 5, con progressione di velocità fino ad avere la velocità più aggressiva al quinto valore. In questo caso la scansione è molto rapida.

Quali porte e servizi sono aperti?

Durante la scansione **Nmap** ha rilevato diverse porte aperte che registrano diversi servizi in esecuzione al loro interno, tra i quali:

Port 22 relativa al servizio **SSH**.

```
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)
```

Port 25 relativa al servizio **SMTP.**

```
25/tcp  open  smtp    Postfix smtpd
```

Port 80 relativa al servizio **HTTP**.

```
80/tcp  open  http    Apache httpd 2.4.6
```

Port 443 relativa al servizio **TCP**.

```
443/tcp open  ssl/ssl Apache httpd (SSL-only mode)
```

Scansiona la tua rete.

Con l'utilizzo del comando **ip config**, è stato possibile visualizzare l'IP e l'interfaccia di rete della macchina.

```
link/ether 08:00:27:5f:e4:06 brd ff:ff:ff:ff:ff:ff
inet 192.168.56.11/24 brd 192.168.56.255 scope global dynamic enp0s3
```

A quale rete appartiene la tua VM?

La vm in questo caso appartiene ad una rete interna, con indirizzo IP **privato**.
La vm appartiene alla rete 192.168.56.0/24, configurata con **pfSense**.

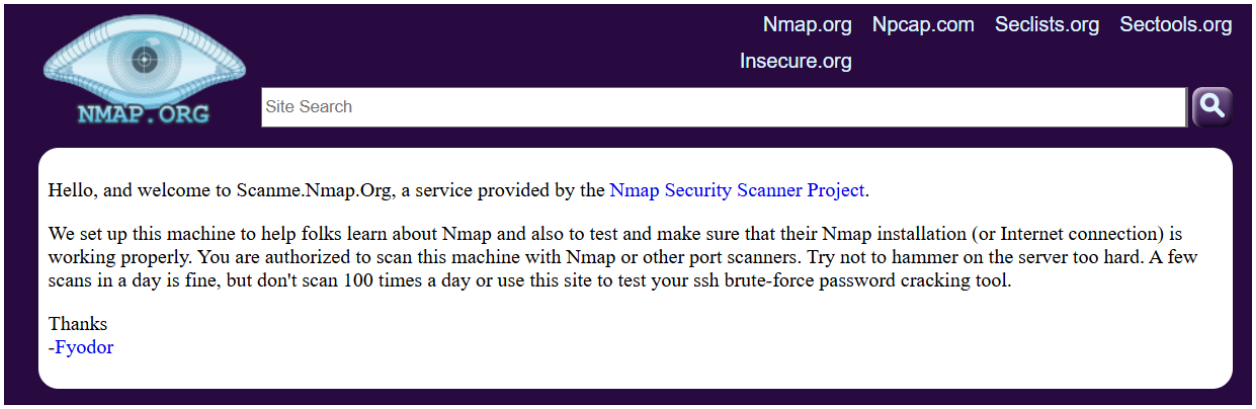
E' stata successivamente effettuata la scansione di questa rete, utilizzando il comando visto sopra in precedenza.

Quanti host sono attivi?

Il comando ci ha fornito 2 Host attivi sulla rete:

Con i seguenti indirizzi **IPv4**: 192.168.56.1 e 192.168.56.11.
Il primo è l'indirizzo IP del Gateway predefinito, il secondo è quello della VM.

Scopo del sito



Il sito è stato messo a disposizione per testare il tool **Nmap**, in modo da poter verificarne la sua funzionalità.
Presenta infatti un'autorizzazione a chiunque voglia effettuare delle prove del tool con il sito come target.

Risultati del comando nmap -A -T4 scanme.nmap.org.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 10:22 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 996 filtered ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; pro
tocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
```

Quali porte e servizi sono aperti?

Le porte aperte sono:

La 22, con il servizio ssh attivo.

80, con il servizio http attivo.

9929, con il Server di Nping echo attivo.

31337 aperta ma nessuna informazione riguardo il servizio attivo.

Quali porte e servizi sono filtrati?

Non sono state identificate porte filtrate.

Qual è l'indirizzo IP del server?

L'indirizzo IP del server è 45.33.32.156.

```
Nmap scan report for scanme.nmap.org (45.33.32.156)
```

Qual è il sistema operativo?

Il Sistema Operativo rilevato risulta Linux.

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Come può Nmap aiutare con la sicurezza della rete?

Nmap aiuta a scoprire porte aperte, servizi, versioni software, sistemi operativi, vulnerabilità e mappare la rete per migliorare la sicurezza, in quanto si può verificare quali di questi sarebbero identificabili e di conseguenza ridurre l'esposizione agli attacchi prendendo le giuste contromisure.

Come può Nmap essere usato da un attore malevolo come strumento nefasto?

Un attaccante potrebbe usarlo per identificare punti deboli, raccogliere informazioni, pianificare attacchi mirati, bypassare firewall e fare ricognizione furtiva.