S5L3

Report scansione Nmap su Windows e Metaspoitable

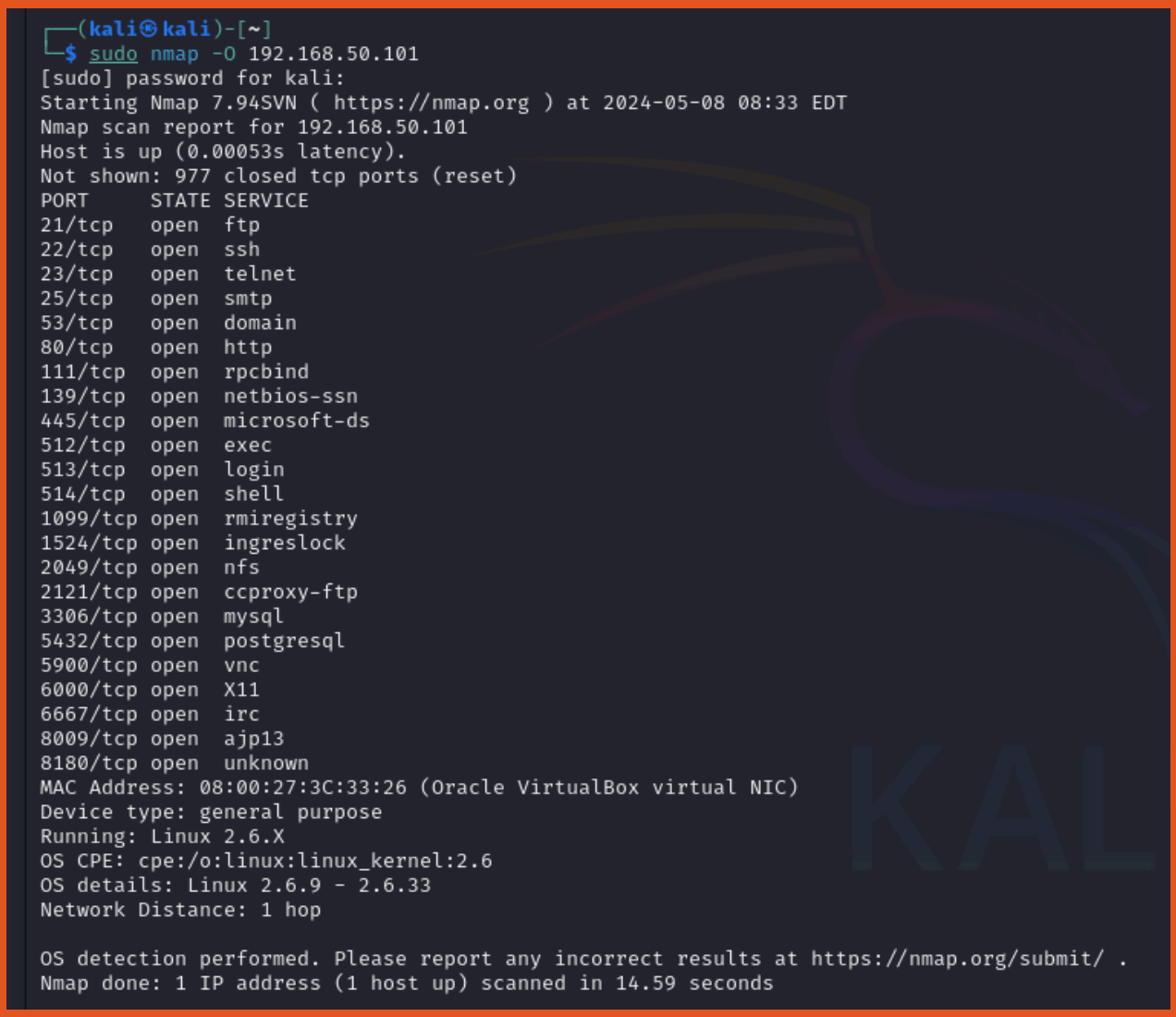
Introduzione

Il seguente report documenta le scansioni effettuate utilizzando il tool Nmap sui sistemi target Metasploitable e Windows 7, l'obiettivo era valutare la sicurezza di rete di questi sistemi attraverso diverse tecniche di scansione per identificare servizi attivi, porte aperte e le relative versioni del software in esecuzione, oltre a confrontare le tecniche di scansione SYN e TCP Connect.

Metodologia

- OS Fingerprinting (nmap -O): Questa tecnica è stata utilizzata per dedurre il sistema operativo del host basandosi sui pacchetti TCP/IP inviati dal target durante la scansione.
- SYN Scan (nmap -sS): Questo metodo invia pacchetti SYN verso una lista di porte per determinare lo stato di ciascuna. Non completa la connessione TCP, aspettando pacchetti SYN-ACK come conferma di porte aperte.
- TCP Connect Scan (nmap -sT): A differenza del SYN Scan, questa tecnica stabilisce una connessione TCP completa, il che può essere più rilevabile ma fornisce conferme affidabili dello stato delle porte.
- Version Detection (nmap -sV): Analizza le risposte dai servizi attivi per determinare la versione del software in esecuzione, utilizzando specifiche sequenze di pacchetti.

Risultati scan Metaspoitable



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 08:33 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00053s 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:33:26 (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 14.59 seconds
```

Nella scansione Nmap su un sistema Metasploitable, ho utilizzato diversi comandi come spiegati nella metodologia con le relative funzioni.
Risultati:

- IP del Target: 192.168.50.101
- Sistema Operativo Rilevato: Linux 2.6.x
- Porte Aperte e Servizi:
  - FTP (21/tcp): vsftpd 2.3.4
  - SSH (22/tcp): OpenSSH 4.7p1 Debian 8ubuntu1
  - Telnet (23/tcp): Linux telnetd
  - SMTP (25/tcp): Postfix smtpd
  - DNS (53/tcp): ISC BIND 9.4.2
  - HTTP (80/tcp): Apache httpd 2.2.8 (Ubuntu)
  - RPC (111/tcp): rpcbind
  - NetBIOS (139/tcp): netbios-ssn
  - Microsoft DS (445/tcp): microsoft-ds
  - Numerosi altri servizi come MySQL, PostgreSQL, VNC, e più, indicando un'ampia varietà di applicazioni e protocolli in esecuzione, ciascuno con le proprie implicazioni e potenziali vulnerabilità.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 08:37 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000096s 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:33:26 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

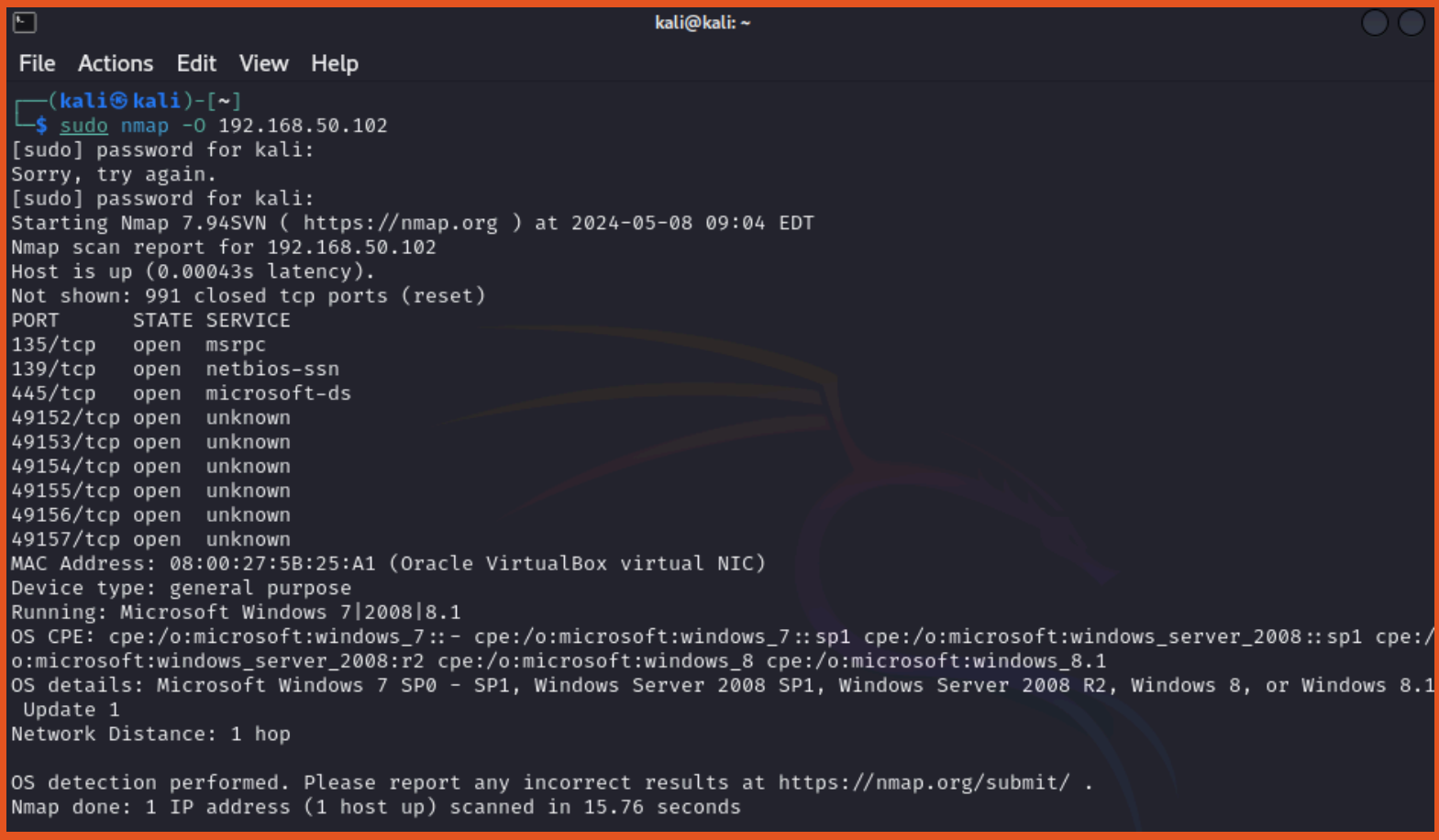
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 08:39 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00023s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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:33:26 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 08:50 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00045s 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?
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.60 seconds
```

Risultati scansione Windows



Come prima cosa per assicurarmi che pingassero le due macchine ho dovuto per prima cosa disattivare il firewall.
Successivamente ho utilizzato l'opzione -O per identificare il sistema operativo del target. La scansione ha confermato che il sistema operativo è Windows 7, questo tipo di informazione è cruciale per comprendere le specifiche vulnerabilità legate alla versione del sistema operativo e per pianificare attacchi di test di penetrazione appropriati.

- Ip del target:192.168.50.102
- Porte aperte e servizi rilevati (TCP Connect -sT):
  - MSRPC (135/tcp): Un protocollo che permette la comunicazione tra processi e operazioni di gestione remota su network Microsoft.
  - NetBIOS-SSN (139/tcp): Utilizzato per il servizio di nomi e la registrazione in reti Microsoft.
  - Microsoft-ds (445/tcp): Protocollo Server Message Block (SMB) utilizzato per la condivisione di file e stampanti.

L'esposizione di queste porte suggerisce la possibilità di sfruttare vulnerabilità legate a servizi Windows non sicuri o mal configurati, questa scansione mi ha permesso di ottenere un quadro chiaro delle potenziali falle di sicurezza, facilitando la preparazione di test di penetrazione mirati per valutare ulteriormente la robustezza del sistema contro attacchi esterni

Una valida ragione per i risultati ottenuti dalla scansione sulla macchina Windows 7 potrebbe essere la presenza di configurazioni di sicurezza robuste, come firewall personalizzati o regole di sicurezza del network che bloccano o filtrano i pacchetti inviati durante una scansione. Questi strumenti di sicurezza sono spesso configurati per minimizzare l'esposizione a possibili attacchi esterni, specialmente sui porti e servizi più comuni e notoriamente vulnerabili.
Soluzioni per continuare le scansioni:

- Utilizzo di Tecniche di Scansione Avanzate:
  - Scansione Stealth (SYN Scan): Potreste utilizzare una scansione SYN stealth (-sS) per tentare di bypassare i firewall che potrebbero bloccare le scansioni più invasive come quelle di TCP Connect. Questo tipo di scansione invia pacchetti SYN senza completare la connessione TCP, rendendola meno rilevabile.
  - Fragmentation (-f): Questa opzione frammenta i pacchetti inviati in modo che siano meno riconoscibili da IDS (Intrusion Detection Systems) e firewall configurati per analizzare pacchetti di dimensioni standard.
  - Decoy Scanning (-D): Potreste usare indirizzi IP di decoy insieme al vostro per confondere i dispositivi di sicurezza e mascherare la fonte effettiva della scansione.
- **Utilizzo di Script Nmap:**
  - Nmap offre una vasta gamma di script (NSE - Nmap Scripting Engine) che possono essere utilizzati per eseguire scansioni più sofisticate e mirate, questi script possono aiutare a rilevare servizi specifici, configurazioni di sicurezza, o vulnerabilità note che non sono facilmente identificabili con scansioni standard.