S5L3 SCANSIONE DEI SERVIZI CON NMAP

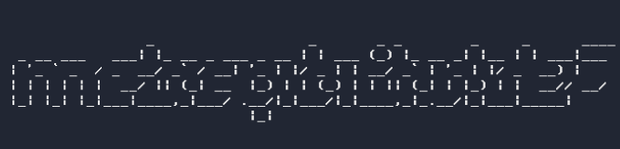
Utilizzando delle tecniche di scansione con Nmap su Kali Linux, effettuiamo delle scansioni su Metasploitable e su Windows7.

Per poter comunicare tra di loro impostiamo le 3 macchine sulla stessa rete:

Kali 192.168.50.100

Metaspoitable 192.168.50.101

Wndows7 192.168.50.102



Andiamo ora a fare le scansioni sulle macchine.

Partiamo da meta dove effettuiamo un:

- ***OS fingerprint***
- ***Syn Scan***
- ***TCP connect***
- ***Version detection***

Le diverse scansioni di Nmap ci offrono approcci diversi per raccogliere le informazioni sui servizi e sul sistema operativo in esecuzione su un host.

OS Fingerprint identifica il sistema operativo analizzando i suoi comportamenti e le risposte ai pacchetti inviati durante la scansione.

Syn Scan rileva le porte aperte su un host inviando pacchetti SYN e analizzando le risposte. Se la risposta è un SYN/ACK, la porta viene considerata aperta, se è un RST, viene considerata chiusa.

TCP Connect rileva le porte aperte stabilendo connessioni incomplete con i servizi sulle porte, rispetto a Syn Scan completa l'handshake TCP per determinare lo stato della porta.

Version Detecion identifica le versioni dei servizi in esecuzione sulle porte aperte, si concentra sulla raccolta di informazioni specifiche sulle versioni dei servizi.

Le differenze principali tra la scansione la SYN Scan e TCP Connect:

Scansione SYN (Scansione TCP SYN):

Invia pacchetti SYN senza stabilire una connessione completa.
E' un tipo di scansione meno intrusiva, ed è meno probabile che venga registrata nei log.
E' più veloce, meno intrusiva, ma può generare alcuni falsi positivi o negativi.

La scelta tra le due tecniche dipende dalla necessità di precisione, velocità e livello di intrusione consentito nella rete o nei dispositivi che stai esaminando.

Scansione TCP Connect:

Stabilisce connessioni complete con i dispositivi di destinazione.

Rispetto alla scansione Syn Scan è più intrusiva ed è più probabile che venga registrata nei log del dispositivo scansionato.

Quindi in conclusione è più accurata ma potenzialmente più lenta e facilmente rilevabile.

```
┌──(franco㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:03 CET
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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:CB:4F:27 (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 15.12 seconds
```

Come abbiamo già anticipato la scansione SYN non completa l'handshake TCP, ma si basa sulle risposte ricevute per determinare lo stato delle porte.

Al contrario, la scansione TCP Connect tenta di stabilire una connessione completa con i servizi, offrendo una visione più accurata dello stato delle porte, ma potrebbe essere più lenta e più intrusiva. La scelta tra le due dipende dalle esigenze specifiche della scansione in corso: velocità, precisione e livello di intrusione consentito.

```
┌──(franco㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:08 CET
Nmap scan report for 192.168.50.101
Host is up (0.00048s 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:CB:4F:27 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.69 seconds
```

```
┌──(franco㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:08 CET
Nmap scan report for 192.168.50.101
Host is up (0.0016s 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:CB:4F:27 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
```

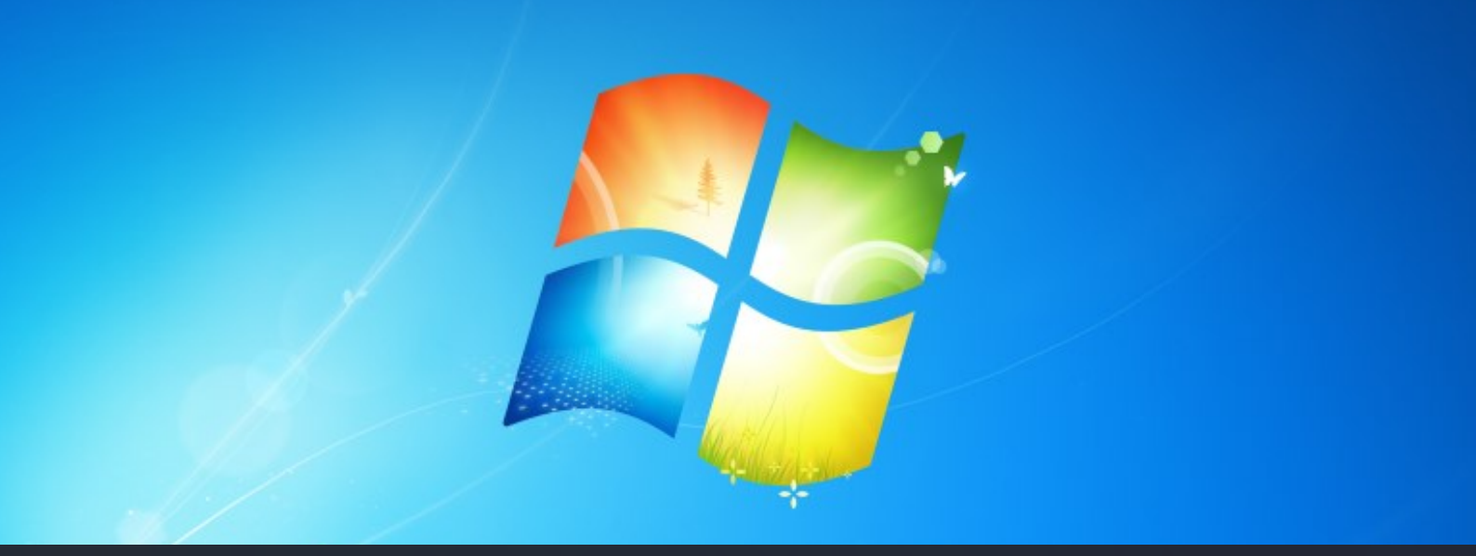
```
┌──(franco㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:10 CET
Nmap scan report for 192.168.50.101
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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:CB:4F:27 (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 193.53 seconds
```

```
┌──(franco㉿kali)-[~]
└─$ sudo nmap 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:27 CET
Nmap scan report for 192.168.50.101
Host is up (0.00040s 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  microsof0
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:CB:4F:27 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-12-20T04:28:01-05:00

Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds
```



```
┌──(franco㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:14 CET
Nmap scan report for 192.168.50.102
Host is up (0.00095s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:5F:81:8F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_serv
er_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:wi
ndows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows
 8, or Windows 8.1 Update 1
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 15.70 seconds
```

```
┌──(franco㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sS 192.168.50.102
[sudo] password for franco:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 16:23 CE
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:5F:81:8F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.44 seconds
```

```
┌──(franco㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sT 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 16:28 CET
Nmap scan report for 192.168.50.102
Host is up (0.0030s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:5F:81:8F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.72 seconds
```

```
┌──(franco㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:17 CET
Nmap scan report for 192.168.50.102
Host is up (0.0010s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:5F:81:8F (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.23 seconds
```

```
┌──(franco㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap 192.168.50.102 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:34 CET
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsof0
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:5F:81:8F (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Windows7-PC
|   NetBIOS computer name: WINDOWS7-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-12-20T11:35:11+01:00

Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds
```

Quesito extra

La scansione sulla macchina di Windows 7 non fornisce risultati accurati, ovvero non rileva i servizi in ascolto.

I potenziali problemi potrebbero essere i seguenti:

Il Firewall attivo che potrebbe bloccare le richieste di scansione, impedendo l'identificazione corretta dei servizi.

Le protezioni antivirus o i strumenti di sicurezza potrebbero limitare l'accesso alle informazioni sui servizi in esecuzione.

Mancanza di privilegi necessario potrebbe essere un'altra causa che ci impedisce l'ottenimento delle informazioni dettagliate sui servizi.

Qualche soluzione a riguardo potrebbe essere:

La disattivazione temporanea del firewall e configurazione di qualche regola aggiuntiva per consentire a Nmap di eseguire la scansione.

La disattivazione temporanea dell'antivirus.

Esecuzione di Nmap con tutti i privilegi elevati come quelli di amministratore.

Opzioni di scansione di Nmap specifiche per poter essere adattate alla situazione.