TECNICHE DI SCANSIONE CON #NMAP, TARGET:

#WINDOWS7

MODIFICARE LE IMPOSTAZIONI IN MODO CHE LE DUE MACCHINE SIANO SULLA STESSA RETE.
PRODURRE UN REPORT CONTENENTE LE SEGUENTI INFO:

- **IP ADDRESS**
- **SISTEMA OPERATIVO**
- **PORTE APERTE**
- **SERVIZI IN ASCOLTO CON VERSIONE**
- **DESCRIZIONE DEI SERVIZI**

(https://www-poftut.com/nmap-output)
(nmap -oN report1 IP)

SI RICHIEDE DI EFFETTUARE LE SEGUENTI SCANSIONI SUL TARGET METASPLOITABLE:

- **OS FINGERPRINT**
- **SYN SCAN**
- **VERSION DETECTION**

QUESITO EXTRA: QUALE POTREBBE ESSERE UNA VALIDA RAGIONE PER SPIEGARE IL RISULTATO OTTENUTO DALLA SCANSIONE SULLA MACCHINA WINDOWS 7? CHE TIPO DI SOLUZIONE POTRESTE PROPORRE PER CONTINUARE LE SCANSIONI?

AL FINE DELL'ESERCIZIO SERVE CHE LE DUE MACCHINE (KALI E WINDOWS7) SIANO SULLA STESSA RETE, CONTROLLO QUINDI CON IPCONFIG DA COMMAND PROMPT CHE L'IP DI WINDOWS7 SIA 192.168.50.102, MENTRE QUELLO DI KALI LINUX RESTA 192.168.50.100. RIAVVIO IL SERVIZIO NETWORKING SU KALI CON SUDO SERVICE NETWORKING RESTART PER SICUREZZA.

#IP ADDRESS E VERSIONE OS KALI LINUX:

IP

```
┌──(root㉿kali)-[/home/django]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
 group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
state UP group default qlen 1000
    link/ether 08:00:27:fa:dd:14 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
       valid_lft 83038sec preferred_lft 83038sec
    inet6 fe80::a00:27ff:fefa:dd14/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
state UP group default qlen 1000
    link/ether 08:00:27:62:34:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe62:3451/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

```
┌──(root㉿kali)-[/home/django]
└─# cat /etc/xrelease
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.3"
VERSION="2023.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"

┌──(root㉿kali)-[/home/django]
└─# cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.3"
VERSION="2023.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
```

#IP ADDRESS WINDOWS7 + PING VERSO KALI:

PING

IP

```
Command Prompt
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Win7>ping 192.168.50.100

Pinging 192.168.50.100 with 32 bytes of data:
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time=1ms TTL=64
Reply from 192.168.50.100: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.50.100:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\Win7>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::38ff:a4f7:d164:cadf%11
   IPv4 Address. . . . . . . . . . . : 192.168.50.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1

Tunnel adapter isatap.{0A64898F-0786-4096-876D-52DBE55926CB}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Win7>_
```

#REPORT SULLE MACCHINE:

- ifconfig O ip -a PER VEDERE IP/MAC ADDRESS DELLE MACCHINE LINUX / ipconfig SUL PROMPT COMANDI PER WINDOWS7 (NELLE IMG PRECEDENTI)
- ESEGUO UN OS FINGERPRINT CON NMAP PER CONOSCERE IL SISTEMA OPERATIVO (nmap -O <IP>)
- ESEGUO UNO STEALTH SCAN E UNO CON VERSION DETECTION CON NMAP PER IDENTIFICARE LE PORTE APERTE, IL SERVIZIO IN ASCOLTO ASSOCIATO E LA SUA VERSIONE (nmap -sS <IP> / nmap -sV <IP>)

```
┌──(root㉿kali)-[/home/django]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:38 EST
Nmap scan report for 192.168.50.102
Host is up (0.00086s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:D3:39:4A (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
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 22.27 seconds
```

```
┌──(root㉿kali)-[/home/django]
└─# ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.921 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.27 ms
^C
── 192.168.50.102 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.921/1.094/1.267/0.173 ms

┌──(root㉿kali)-[/home/django]
└─# nmap -sV 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:34 EST
Nmap scan report for 192.168.50.102
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:D3:39:4A (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.83 seconds

┌──(root㉿kali)-[/home/django]
└─# nmap -sS 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 10:35 EST
Nmap scan report for 192.168.50.102
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:D3:39:4A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.43 seconds
```

IL REPORT DELLA SCANSIONE OS FINGERPRINTING CON LO SWITCH -O HA RESTITUITO COME RISULTATO I SISTEMI OPERATIVI PIÙ PROBABILI ANALIZZANDO I PACCHETTI DI RISPOSTA RICEVUTI DAL TARGET, STIMANDO CHE L'OS TARGET SIA PROBABILMENTE WINDOWS (7, EMBEDDED STANDARD 7, 8.1 UPDATE 1, XP SP3, SERVER 2012) O ALTRO.
POSSIAMO PERÒ NOTARE DALLO SCAN CHE SU 1000 PORTE ANALIZZATE, 1000 SONO FILTRATE. QUESTO A CAUSA DI UNA PROTEZIONE CHE SAPPIAMO ESSERE IL FIREWALL DI WINDOWS.
BISOGNA QUINDI ELUDERE IL FIREWALL CON TECNICHE SPECIFICHE, COME AD ESEMPIO CONFIGURARE PER L'INVIO DEI PACCHETTI UNA PORTA SORGENTE NOTA (AD ES. HTTP-80 o HTTPS-443) CON IL COMANDO --source-port 80 (oppure 443) IN MODO TALE CHE IL FIREWALL RITENGA IL TRAFFICO NON SOSPETTO. SI PUÒ ANCHE INTERVENIRE SUL FIREWALL DI WINDOWS7 STESSO, CREANDO/MODIFICANDO REGOLE INBOUND PER PERMETTERE IL TRAFFICO DALLA MACCHINA KALI. INFATTI VEDIAMO I SEGUENTI RISULTATI:

```
┌──(root㉿kali)-[/home/django]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 15:10 EST
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  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:D3:39:4A (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_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_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 2.81 seconds
```

```
┌──(django㉿kali)-[~]
└─$ sudo su
[sudo] password for django:
┌──(root㉿kali)-[/home/django]
└─# nmap -sS 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 15:08 EST
Nmap scan report for 192.168.50.102
Host is up (0.00060s 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:D3:39:4A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

```
┌──(root㉿kali)-[/home/django]
└─# nmap -sV 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 15:09 EST
Nmap scan report for 192.168.50.102
Host is up (0.00072s 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:D3:39:4A (Oracle VirtualBox virtual NIC)
Service Info: Host: WIN7-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 60.77 seconds
```