

Modulo 3 Esercitazione 6 - Russo Alessio

1. Scanning di Metasploitable tramite Kali Linux, Step 1: OS Fingerprinting: scanning per vedere Sistema Operativo della macchina Analizzata per valutare eventuali vulnerabilità note, l'OS fingerprinting si effettua da kali tramite i comandi:

`nmap -O {IPTARGET}`

- Ifconfig su metasploitable per vedere indirizzo IP:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:db:80:98
          inet addr:192.168.49.101  Bcast:192.168.49.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedb:8098/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:128 (128.0 B)  TX bytes:8425 (8.2 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:154 errors:0 dropped:0 overruns:0 frame:0
          TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50237 (49.0 KB)  TX bytes:50237 (49.0 KB)
```

- Nmap -O {iptarget} da kali linux:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 14:59 CET
Nmap scan report for 192.168.49.101
Host is up (0.0036s 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    filtered  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), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
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 2.95 seconds
```

2. STEP 2 di uno scan e la SYN scan: `nmap -sS`, `-ST` (TCP connect): `-sS` scanning sul SYN e la scansione si stoppa con REST, poco invasiva;

```
root@kali:~# nmap -sS 192.168.49.101
Failed to resolve/decode supposed IPv4 source address "s": No address associated with hostname
QUITTING!

root@kali:~# nmap -sS 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 15:03 CET
Nmap scan report for 192.168.49.101
Host is up (0.016s 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    filtered 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 1.61 seconds
```

`-sT` test TCP completo quindi fata il 3 way handshake, più invasive rispetto alla `-sS`

```
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds

root@kali:~# nmap -sT 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 15:06 CET
Nmap scan report for 192.168.49.101
Host is up (0.025s 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    filtered 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 1.43 seconds
```

3. Scan -sV, utilizzato per eseguire una scansione di versione dei servizi su host di destinazione

```
zsh: suspended nmap -sV 192.168.49.101

(root@kali)~[/home/kali]
# nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 15:13 CET
Nmap scan report for 192.168.49.101
Host is up (0.014s 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    filtered http
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  ccproxy-ftp?
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 174.03 seconds
```

4. Nmap -A 192.168.48.101: Questa scansione fornirà informazioni complete, compreso il rilevamento del sistema operativo, la scansione delle versioni dei servizi, la scansione degli script Nmap e altro ancora.

```
└─# nmap -A 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 15:48 CET
Nmap scan report for 192.168.49.101
Host is up (0.0051s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|  STAT:
| FTP server status:
|  Connected to 192.168.50.100
|  Logged in as ftp
|  TYPE: ASCII
|  No session bandwidth limit
|  Session timeout in seconds is 300
|  Control connection is plain text
|  Data connections will be plain text
|  vsFTPd 2.3.4 - secure, fast, stable
```

|_End of status
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp filtered http
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 33095/udp mountd
| 100005 1,2,3 44892/tcp mountd
| 100021 1,3,4 53040/tcp nlockmgr
| 100021 1,3,4 53812/udp nlockmgr
| 100024 1 50301/udp status
|_ 100024 1 55235/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (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 ccproxy-ftp?
3306/tcp open mysql?
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing
outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2024-01-21T14:52:16+00:00; +20s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)

6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

Host script results:

|_clock-skew: mean: 1h40m20s, deviation: 2h53m13s, median: 19s
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2024-01-21T09:51:19-05:00
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)

TRACEROUTE (using port 587/tcp)

HOP	RTT	ADDRESS
1	1.89 ms	192.168.50.1
2	4.47 ms	192.168.49.101

OS and Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 239.18 seconds