W10D4 – Pratica

DATA
Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Fase di raccolta informazioni

Traccia:

https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/

Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina **metasploitable** e produrre un report.

Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

- 1. nmap -sn -PE <target>
- 2. netdiscover -r <target>
- 3. crackmapexec <target>
- 4. nmap <target> –top-ports 10 –open
- 5. nmap <target> -p- -sV –reason –dns-server ns
- 6. us -mT -lv <target>:a -r 3000 -R 3 && us -mU -lv <target>:a -r 3000 -R 3
- 7. nmap -sS -sV -T4 <target>
- 8. hping3 –scan known <target>
- 9. nc -nvz <target> 1-1024
- 10. nc -nv <target> 22
- 11. nmap -sV <target>
- 12. db_import <file.xml> (For Metasploit Framework)
- 13. nmap -f –mtu=512 <target>
- 14. masscan <network> -p80 –banners –source-ip <target>
- Never ending process……..

└─$ nmap 192.168.50.100 -top-port 10 -open

Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-21 11:56 EST
Nmap scan report for 192.168.50.100
Host is up (0.013s latency).
Not shown: 3 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

—$ sudo nmap -sS -sV -T4 192.168.50.100

[sudo] password for kali:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-21 12:01 EST
Nmap scan report for 192.168.50.100
Host is up (0.020s 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 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 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 174.28 seconds

└─$ nmap 192.168.50.100 -p- -sV -reason -dns-server ns

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 11:57 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.100
Host is up, received syn-ack (0.011s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT     STATE SERVICE     REASON  VERSION
21/tcp   open  ftp         syn-ack vsftpd 2.3.4
22/tcp   open  ssh         syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      syn-ack Linux telnetd
25/tcp   open  smtp        syn-ack Postfix smtpd
53/tcp   open  domain      syn-ack ISC BIND 9.4.2
80/tcp   open  http        syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     syn-ack
139/tcp  open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        syn-ack netkit-rsh rexecd
513/tcp  open  login?      syn-ack
514/tcp  open  shell       syn-ack Netkit rshd
1099/tcp open  java-rmi    syn-ack GNU Classpath grmiregistry
1524/tcp open  bindshell   syn-ack Metasploitable root shell
2049/tcp open  rpcbind     syn-ack
2121/tcp open  ccproxy-ftp? syn-ack
3306/tcp open  mysql       syn-ack MySQL 5.0.51a-3ubuntu5
3632/tcp open  distccd     syn-ack distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open  postgresql  syn-ack PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         syn-ack VNC (protocol 3.3)
6000/tcp open  X11         syn-ack (access denied)
6667/tcp open  irc         syn-ack UnrealIRCd
6697/tcp open  irc         syn-ack UnrealIRCd
8009/tcp open  ajp13       syn-ack Apache Jserv (Protocol v1.3)
8180/tcp open  unknown     syn-ack
8787/tcp open  drb         syn-ack Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
34333/tcp open unknown     syn-ack
36112/tcp open rpcbind     syn-ack
37014/tcp open rpcbind     syn-ack
56035/tcp open rpcbind     syn-ack
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 122.88 seconds
```

└─$ sudo nmap -f -mtu=512 192.168.50.100

Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-21 12:07 EST
Nmap scan report for 192.168.50.100
Host is up (0.0098s 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

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds

└─$ sudo us -mT -Iv 192.168.50.100:a -r 3000 -R 3 && us -mU -Iv 192.168.50.100:a -r 3000 -R 3

```
[sudo] password for kali:
adding 192.168.50.100/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.50.100:5900  ttl 63
TCP open 192.168.50.100:22  ttl 63
TCP open 192.168.50.100:445  ttl 63
TCP open 192.168.50.100:23  ttl 63
TCP open 192.168.50.100:6000  ttl 63
TCP open 192.168.50.100:1524  ttl 63
TCP open 192.168.50.100:139  ttl 63
TCP open 192.168.50.100:2121  ttl 63
TCP open 192.168.50.100:8009  ttl 63
TCP open 192.168.50.100:56035  ttl 63
TCP open 192.168.50.100:2049  ttl 63
sender statistics 2863.2 pps with 196608 packets sent total
TCP open 192.168.50.100:37014  ttl 63
listener statistics 18536 packets recieved 0 packets droped and 0 interface drops
TCP open                 ssh[   22]        from 192.168.50.100  ttl 63
TCP open              telnet[   23]        from 192.168.50.100  ttl 63
TCP open           netbios-ssn[  139]        from 192.168.50.100  ttl 63
TCP open          microsoft-ds[  445]        from 192.168.50.100  ttl 63
TCP open           ingreslock[ 1524]        from 192.168.50.100  ttl 63
TCP open              shilp[ 2049]        from 192.168.50.100  ttl 63
TCP open         scientia-ssdb[ 2121]        from 192.168.50.100  ttl 63
TCP open              winvnc[ 5900]        from 192.168.50.100  ttl 63
TCP open                 x11[ 6000]        from 192.168.50.100  ttl 63
TCP open             unknown[ 8009]        from 192.168.50.100  ttl 63
TCP open             unknown[37014]        from 192.168.50.100  ttl 63
TCP open             unknown[56035]        from 192.168.50.100  ttl 63
adding 192.168.50.100/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minute, 12 Seconds
Send [Error   socktrans.c:123] bind() path `/var/lib/unicornscan/send' fails: Address already in us
Send exiting cant create listener socket: system error Address already in use
Recv [Error   socktrans.c:123] bind() path `/var/lib/unicornscan/listen' fails: Address already in se
Recv exiting cant create listener socket: system error Address already in use
```

└─$ nmap -sV 192.168.50.100

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 12:06 EST
Nmap scan report for 192.168.50.100
Host is up (0.019s 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  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 174.42 seconds
```

Riepilogo:
Molte porte sono aperte e molti servizi attivi, versioni softare vecchie con possibili problemi di sicurezza.

Cybersecurity Analyst 2023