M3-W11D4 – pratica

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

Questo esercizio può essere utile per lo studente per prendere dimestichezza con i vari comandi di nmap. Poiché su Linux è un potente tool di scansione della rete, si richiede di utilizzare i seguenti comandi e trascrivere i vari risultati su un report:

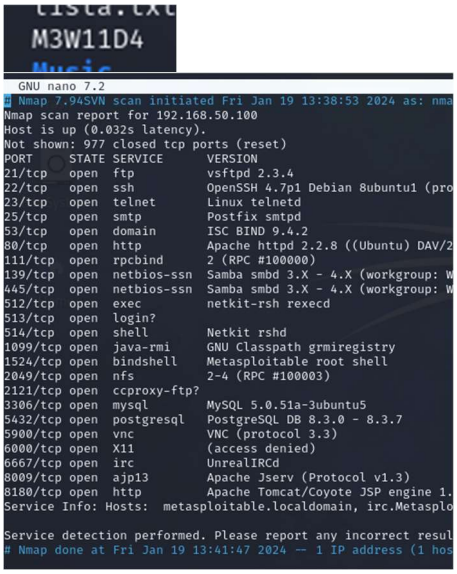
TCP: #	nmap -sS ip address
scansione completa: #	nmap -sV ip address
output su file: #	nmap -sV -oN file.txt ip address
scansione su porta: #	nmap -sS -p 8080 ip address
scansione tutte le porte: #	nmap -sS -p ip address
scansione UDP: #	nmap -sU -r -v ip address
scansione sistema operativo: #	nmap -O ip address
scansione versione servizi: #	nmap -sV ip address
scansione common 100 ports: #	nmap -F ip address
scansione tramite ARP: #	nmap -PR ip address
scansione tramite PING: #	nmap -sP ip address
scansione senza PING: #	nmap -PN ip address

Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

Infine, disegnare 3-4 grafici delle scansioni effettuate, esplicitando le varie fasi di syn, syn/ack ecc.

nmap -sS 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ **sudo nmap -sS 192.168.50.100** [sudo] password for kali: Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 13:24 EST Nmap scan report for 192.168.50.100 Host is up (0.41s 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 1.98 seconds	Esecuzione meno invasiva. Solo SYN senza completare la procedura di handshake TCP. Più veloce.

nmap -sT 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ sudo nmap -sT 192.168.50.100 Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 14:51 EST Nmap scan report for 192.168.50.100 Host is up (0.023s 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 Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds	Esecuzione invasiva. Completare la procedura di handshake TCP. Più lento.

nmap -sV -oN M3W11D4 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ **sudo nmap -sV -oN M3W11D4 192.168.50.100** Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 13:38 EST Nmap scan report for 192.168.50.100 Host is up (0.032s 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 174.64 seconds	Qui oltre alla scansione come quella precedente viene generato anche un report. Nome report M3W11D4 

nmap -sS -p 8080 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ **sudo nmap -sS -p 8080 192.168.50.100** Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 13:46 EST Nmap scan report for 192.168.50.100 Host is up (0.0033s latency). PORT STATE SERVICE 8080/tcp closed http-proxy Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds	Si scansiona la singola porta. In questo casosi scansiona solo la porta **8080**
nmap -sS -p- 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ sudo nmap -sS -p- 192.168.50.100 Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 13:51 EST Nmap scan report for 192.168.50.100 Host is up (0.043s latency). Not shown: 65505 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 3632/tcp open distccd 5432/tcp open postgresql 5900/tcp open vnc 6000/tcp open X11 6667/tcp open irc 6697/tcp open ircs-u 8009/tcp open ajp13 8180/tcp open unknown 8787/tcp open msgsrvr 37762/tcp open unknown 38654/tcp open unknown 38814/tcp open unknown 51766/tcp open unknown Nmap done: 1 IP address (1 host up) scanned in 40.11 seconds	Scansione completa di tutte le porte. Ricordarsi di mettere **-p-**

sudo nmap -sU -r -v 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ sudo nmap -sU -r -v 192.168.50.100 Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 14:00 EST Initiating Ping Scan at 14:00 Scanning 192.168.50.100 [4 ports] Completed Ping Scan at 14:00, 0.09s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 14:00 Completed Parallel DNS resolution of 1 host. at 14:00, 0.01s elapsed Initiating UDP Scan at 14:00 Scanning 192.168.50.100 [1000 ports] Discovered open port 53/udp on 192.168.50.100 Discovered open port 111/udp on 192.168.50.100 Increasing send delay for 192.168.50.100 from 0 to 50 due to max_successful_tryno increase to 4 Increasing send delay for 192.168.50.100 from 50 to 100 due to max_successful_tryno increase to 5 Increasing send delay for 192.168.50.100 from 100 to 200 due to max_successful_tryno increase to 6 Increasing send delay for 192.168.50.100 from 200 to 400 due to max_successful_tryno increase to 7 Discovered open port 137/udp on 192.168.50.100 Increasing send delay for 192.168.50.100 from 400 to 800 due to 11 out of 21 dropped probes since last increase. UDP Scan Timing: About 4.66% done; ETC: 14:11 (0:10:35 remaining) UDP Scan Timing: About 7.69% done; ETC: 14:13 (0:12:12 remaining) Discovered open port 2049/udp on 192.168.50.100 UDP Scan Timing: About 25.13% done; ETC: 14:15 (0:11:31 remaining) UDP Scan Timing: About 31.01% done; ETC: 14:15 (0:10:43 remaining) UDP Scan Timing: About 36.98% done; ETC: 14:15 (0:09:55 remaining) UDP Scan Timing: About 41.91% done; ETC: 14:15 (0:09:06 remaining) UDP Scan Timing: About 47.17% done; ETC: 14:15 (0:08:18 remaining) UDP Scan Timing: About 52.64% done; ETC: 14:15 (0:07:29 remaining) UDP Scan Timing: About 57.82% done; ETC: 14:15 (0:06:41 remaining) UDP Scan Timing: About 63.01% done; ETC: 14:15 (0:05:53 remaining) UDP Scan Timing: About 68.11% done; ETC: 14:16 (0:05:05 remaining) UDP Scan Timing: About 73.30% done; ETC: 14:16 (0:04:16 remaining) UDP Scan Timing: About 78.47% done; ETC: 14:16 (0:03:27 remaining) UDP Scan Timing: About 83.54% done; ETC: 14:16 (0:02:39 remaining) UDP Scan Timing: About 88.73% done; ETC: 14:16 (0:01:49 remaining) UDP Scan Timing: About 93.92% done; ETC: 14:16 (0:00:59 remaining) Completed UDP Scan at 14:16, 984.70s elapsed (1000 total ports) Nmap scan report for 192.168.50.100 Host is up (0.0029s latency). Not shown: 993 closed udp ports (port-unreach) PORT STATE SERVICE 53/udp open domain 68/udp open|filtered dhcpc 69/udp open|filtered tftp 111/udp open rpcbind 137/udp open netbios-ns 138/udp open|filtered netbios-dgm 2049/udp open nfs Read data files from: /usr/bin/../share/nmap Nmap done: 1 IP address (1 host up) scanned in 984.90 seconds Raw packets sent: 1379 (66.029KB) | Rcvd: 1008 (74.889KB)	Scansione porte UDP

sudo nmap -O 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ sudo nmap -O 192.168.50.100 [sudo] password for kali: Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 14:39 EST Nmap scan report for 192.168.50.100 Host is up (0.0069s 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 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 OS detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds	Verifica sistemi operativi.

nmap -sV 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ **sudo nmap -sV 192.168.50.100** Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 13:31 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 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 174.77 seconds	Verifica i servizi

nmap -F 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ sudo nmap -F 192.168.50.100 Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 14:40 EST Nmap scan report for 192.168.50.100 Host is up (0.0089s latency). Not shown: 82 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 513/tcp open login 514/tcp open shell 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 8009/tcp open ajp13 Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds	Scansione rapida, poco invadente

nmap -PR 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ sudo nmap -PR 192.168.50.100 Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 14:41 EST Nmap scan report for 192.168.50.100 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 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 0.69 seconds	Scansione ARP
nmap -sP 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ sudo nmap -sP 192.168.50.100 Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 14:43 EST Nmap scan report for 192.168.50.100 Host is up (0.0025s latency). Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds	Si comporta come un PING

nmap -PN 192.168.50.100	
┌──(kali㉿kali)-[~] └─$ sudo nmap -PN 192.168.50.100 Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 14:45 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 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 0.51 seconds	Non esegue il ping.

Cybersecurity Analyst 2023