


ESERCITAZIONE WEEK 10 DAY 5



Esercizio
Info Gathering

Traccia

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

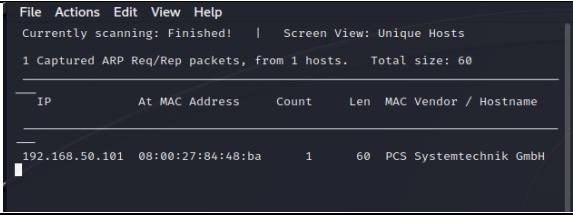
Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report.

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

3

Report

Macchina target: Metasploitable

Strumenti	Risultati
sudo nmap -sn -PE 192.168.50.101	Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:30 EST Nmap scan report for 192.168.50.101 Host is up (0.00024s latency). MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
sudo netdiscover -r 192.168.50.101	
sudo crackmapexec 192.168.50.101	[*] First time use detected [*] Creating home directory structure [*] Creating default workspace [*] Initializing SMB protocol database [*] Initializing RDP protocol database [*] Initializing MSSQL protocol database [*] Initializing WINRM protocol database [*] Initializing SSH protocol database [*] Initializing LDAP protocol database [*] Initializing FTP protocol database [*] Copying default configuration file [*] Generating SSL certificate usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose] {smb,rdp,mssql,winrm,ssh,ldap,ftp} ...

	crackmapexec: error: argument protocol: invalid choice: '192.168.50.101' (choose from 'smb', 'rdp', 'mssql', 'winrm', 'ssh', 'ldap', 'ftp')
sudo nmap 192.168.50.101 -top-ports 10 -open	<p>Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:36 EST</p> <p>Nmap scan report for 192.168.50.101</p> <p>Host is up (0.00032s latency).</p> <p>Not shown: 3 closed tcp ports (reset)</p> <p>PORT STATE SERVICE</p> <p>21/tcp open ftp</p> <p>22/tcp open ssh</p> <p>23/tcp open telnet</p> <p>25/tcp open smtp</p> <p>80/tcp open http</p> <p>139/tcp open netbios-ssn</p> <p>445/tcp open microsoft-ds</p> <p>MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)</p> <p>Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds</p>
sudo nmap 192.168.50.101 -p -sV -reason -dns-server ns	<p>Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:37 EST</p> <p>Error #486: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"</p> <p>QUITTING!</p>
sudo nmap -sS -sV -T4 192.168.50.101	<p>Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:39 EST</p> <p>Nmap scan report for 192.168.50.101</p> <p>Host is up (0.000061s latency).</p> <p>Not shown: 977 closed tcp ports (reset)</p> <p>PORT STATE SERVICE VERSION</p> <p>21/tcp open ftp vsftpd 2.3.4</p> <p>22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)</p> <p>23/tcp open telnet Linux telnetd</p> <p>25/tcp open smtp Postfix smtpd</p> <p>53/tcp open domain ISC BIND 9.4.2</p> <p>80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)</p> <p>111/tcp open rpcbind 2 (RPC #100000)</p> <p>139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)</p> <p>445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)</p> <p>512/tcp open exec netkit-rsh rexecd</p> <p>513/tcp open login?</p> <p>514/tcp open shell Netkit rshd</p> <p>1099/tcp open java-rmi GNU Classpath grmiregistry</p> <p>1524/tcp open bindshell Metasploitable root shell</p> <p>2049/tcp open nfs 2-4 (RPC #100003)</p> <p>2121/tcp open ftp ProFTPD 1.3.1</p> <p>3306/tcp open mysql MySQL 5.0.51a-3ubuntu5</p> <p>5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7</p> <p>5900/tcp open vnc VNC (protocol 3.3)</p> <p>6000/tcp open X11 (access denied)</p>

	<p>6667/tcp open irc UnrealIRCd</p> <p>8009/tcp open ajp13 Apache Jserv (Protocol v1.3)</p> <p>8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1</p> <p>MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)</p> <p>Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel</p> <p>Service detection performed. Please report any incorrect results at https://nmap.org/submit/.</p> <p>Nmap done: 1 IP address (1 host up) scanned in 65.55 seconds</p>																																																												
sudo nc -nvz 192.168.50.101 1-1024	<p>(UNKNOWN) [192.168.50.101] 514 (shell) open</p> <p>(UNKNOWN) [192.168.50.101] 513 (login) open</p> <p>(UNKNOWN) [192.168.50.101] 512 (exec) open</p> <p>(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open</p> <p>(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open</p> <p>(UNKNOWN) [192.168.50.101] 111 (sunrpc) open</p> <p>(UNKNOWN) [192.168.50.101] 80 (http) open</p> <p>(UNKNOWN) [192.168.50.101] 53 (domain) open</p> <p>(UNKNOWN) [192.168.50.101] 25 (smtp) open</p> <p>(UNKNOWN) [192.168.50.101] 23 (telnet) open</p> <p>(UNKNOWN) [192.168.50.101] 22 (ssh) open</p> <p>(UNKNOWN) [192.168.50.101] 21 (ftp) open</p>																																																												
sudo nc -nv 192.168.50.101 22	<p>(UNKNOWN) [192.168.50.101] 22 (ssh) open</p> <p>SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1</p>																																																												
sudo nmap -sV 192.168.50.101	<p>Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:44 EST</p> <p>Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan</p> <p>Parallel DNS resolution of 1 host. Timing: About 0.00% done</p> <p>Nmap scan report for 192.168.50.101</p> <p>Host is up (0.000075s latency).</p> <p>Not shown: 977 closed tcp ports (reset)</p> <table><thead><tr><th>PORT</th><th>STATE</th><th>SERVICE</th><th>VERSION</th></tr></thead><tbody><tr><td>21/tcp</td><td>open</td><td>ftp</td><td>vsftpd 2.3.4</td></tr><tr><td>22/tcp</td><td>open</td><td>ssh</td><td>OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)</td></tr><tr><td>23/tcp</td><td>open</td><td>telnet</td><td>Linux telnetd</td></tr><tr><td>25/tcp</td><td>open</td><td>smtp</td><td>Postfix smtpd</td></tr><tr><td>53/tcp</td><td>open</td><td>domain</td><td>ISC BIND 9.4.2</td></tr><tr><td>80/tcp</td><td>open</td><td>http</td><td>Apache httpd 2.2.8 ((Ubuntu) DAV/2)</td></tr><tr><td>111/tcp</td><td>open</td><td>rpcbind</td><td>2 (RPC #100000)</td></tr><tr><td>139/tcp</td><td>open</td><td>netbios-ssn</td><td>Samba smbd 3.X - 4.X (workgroup: WORKGROUP)</td></tr><tr><td>445/tcp</td><td>open</td><td>netbios-ssn</td><td>Samba smbd 3.X - 4.X (workgroup: WORKGROUP)</td></tr><tr><td>512/tcp</td><td>open</td><td>exec</td><td>netkit-rsh rexecd</td></tr><tr><td>513/tcp</td><td>open</td><td>login?</td><td></td></tr><tr><td>514/tcp</td><td>open</td><td>shell</td><td>Netkit rshd</td></tr><tr><td>1099/tcp</td><td>open</td><td>java-rmi</td><td>GNU Classpath grmiregistry</td></tr><tr><td>1524/tcp</td><td>open</td><td>bindshell</td><td>Metasploitable root shell</td></tr></tbody></table>	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
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																																																										

	<p>2049/tcp open nfs 2-4 (RPC #100003)</p> <p>2121/tcp open ftp ProFTPD 1.3.1</p> <p>3306/tcp open mysql MySQL 5.0.51a-3ubuntu5</p> <p>5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7</p> <p>5900/tcp open vnc VNC (protocol 3.3)</p> <p>6000/tcp open X11 (access denied)</p> <p>6667/tcp open irc UnrealIRCd</p> <p>8009/tcp open ajp13 Apache Jserv (Protocol v1.3)</p> <p>8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1</p> <p>MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)</p> <p>Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel</p> <p>Service detection performed. Please report any incorrect results at https://nmap.org/submit/.</p> <p>Nmap done: 1 IP address (1 host up) scanned in 65.42 seconds</p>
<pre>sudo nmap -f -mtu=512 192.168.50.101</pre>	<p>Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:46 EST</p> <p>Nmap scan report for 192.168.50.101</p> <p>Host is up (0.000084s latency).</p> <p>Not shown: 977 closed tcp ports (reset)</p> <p>PORT STATE SERVICE</p> <p>21/tcp open ftp</p> <p>22/tcp open ssh</p> <p>23/tcp open telnet</p> <p>25/tcp open smtp</p> <p>53/tcp open domain</p> <p>80/tcp open http</p> <p>111/tcp open rpcbind</p> <p>139/tcp open netbios-ssn</p> <p>445/tcp open microsoft-ds</p> <p>512/tcp open exec</p> <p>513/tcp open login</p> <p>514/tcp open shell</p> <p>1099/tcp open rmiregistry</p> <p>1524/tcp open ingreslock</p> <p>2049/tcp open nfs</p> <p>2121/tcp open ccproxy-ftp</p> <p>3306/tcp open mysql</p> <p>5432/tcp open postgresql</p> <p>5900/tcp open vnc</p> <p>6000/tcp open X11</p> <p>6667/tcp open irc</p> <p>8009/tcp open ajp13</p> <p>8180/tcp open unknown</p> <p>MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)</p> <p>Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds</p>

