**Q.1:**

└─# cat /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

\_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin

systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin

systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false

tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false

strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin

ntp:x:107:112::/nonexistent:/usr/sbin/nologin

messagebus:x:108:113::/nonexistent:/usr/sbin/nologin

redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin

rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin

iodine:x:111:65534::/run/iodine:/usr/sbin/nologin

miredo:x:112:65534::/var/run/miredo:/usr/sbin/nologin

\_rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin

usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin

tcpdump:x:115:121::/nonexistent:/usr/sbin/nologin

rtkit:x:116:122:RealtimeKit,,,:/proc:/usr/sbin/nologin

sshd:x:117:65534::/run/sshd:/usr/sbin/nologin

statd:x:118:65534::/var/lib/nfs:/usr/sbin/nologin

postgres:x:119:124:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash

avahi:x:120:126:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin

stunnel4:x:121:127::/var/run/stunnel4:/usr/sbin/nologin

Debian-snmp:x:122:128::/var/lib/snmp:/bin/false

speech-dispatcher:x:123:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false

sslh:x:124:129::/nonexistent:/usr/sbin/nologin

nm-openvpn:x:125:130:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin

nm-openconnect:x:126:131:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin

pulse:x:127:132:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin

saned:x:128:135::/var/lib/saned:/usr/sbin/nologin

inetsim:x:129:137::/var/lib/inetsim:/usr/sbin/nologin

colord:x:130:138:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin

geoclue:x:131:139::/var/lib/geoclue:/usr/sbin/nologin

lightdm:x:132:140:Light Display Manager:/var/lib/lightdm:/bin/false

king-phisher:x:133:141::/var/lib/king-phisher:/usr/sbin/nologin

kali:x:1000:1000:Kali,,,:/home/kali:/usr/bin/zsh

systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

debian-tor:x:134:144::/var/lib/tor:/bin/false

**Q.2:**

**─# awk -F: '{print $1}' /etc/passwd**

**root**

**daemon**

**bin**

**sys**

**sync**

**games**

**man**

**lp**

**mail**

**news**

**uucp**

**proxy**

**www-data**

**backup**

**list**

**irc**

**gnats**

**nobody**

**\_apt**

**systemd-timesync**

**systemd-network**

**systemd-resolve**

**mysql**

**tss**

**strongswan**

**ntp**

**messagebus**

**redsocks**

**rwhod**

**iodine**

**miredo**

**\_rpc**

**usbmux**

**tcpdump**

**rtkit**

**sshd**

**statd**

**postgres**

**avahi**

**stunnel4**

**Debian-snmp**

**speech-dispatcher**

**sslh**

**nm-openvpn**

**nm-openconnect**

**pulse**

**saned**

**inetsim**

**colord**

**geoclue**

**lightdm**

**king-phisher**

**kali**

**systemd-coredump**

**debian-tor**

**Q.3:**

**└─# wfuzz -c -z file,/usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://172.17.0.7/FUZZ**

**/usr/lib/python3/dist-packages/wfuzz/\_\_init\_\_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**\* Wfuzz 3.1.0 - The Web Fuzzer \***

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Target: http://172.17.0.7/FUZZ**

**Total requests: 951**

**=====================================================================**

**ID Response Lines Word Chars Payload**

**=====================================================================**

**000000194: 301 9 L 28 W 309 Ch "config"**

**000000332: 301 9 L 28 W 311 Ch "external"**

**000000279: 301 9 L 28 W 307 Ch "docs"**

**Total time: 0**

**Processed Requests: 951**

**Filtered Requests: 948**

**Requests/sec.: 0**

**└─# wfuzz --script=robots -z list,robots.txt http://www.webscantest.com/FUZZ**

**/usr/lib/python3/dist-packages/wfuzz/\_\_init\_\_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**\* Wfuzz 3.1.0 - The Web Fuzzer \***

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Target: http://www.webscantest.com/FUZZ**

**Total requests: 1**

**=====================================================================**

**ID Response Lines Word Chars Payload**

**=====================================================================**

**000000001: 403 10 L 30 W 296 Ch "robots.txt"**

**Total time: 0.574525**

**Processed Requests: 1**

**Filtered Requests: 0**

**Requests/sec.: 1.740567**

**Q.4:**

Wordlist was created/opened: /root/.local/share/legion/tmp/legion-6\_2ps399-tool-output/legion-usernames.txt

Wordlist was created/opened: /root/.local/share/legion/tmp/legion-6\_2ps399-tool-output/legion-passwords.txt

Loading settings file..

runStagedNmap called for stage 1

Queuing: nmap -T4 -sV -sSU -p T:80,81,443,4443,8080,8081,8082 172.17.0.7 -oA /root/.local/share/legion/tmp/legion-wtr605p3-running/nmap/20221010200519451592-nmapstage1

runCommand called for stage 1

runCommand connected for stage 1

Process 1 is done!

runStagedNmap called for stage 2

Queuing: nmap -T4 -sV -n -sSU -O -p T:25,135,137,139,445,1433,3306,5432,U:137,161,162,1434 172.17.0.7 -oA /root/.local/share/legion/tmp/legion-wtr605p3-running/nmap/20221010200528742867-nmapstage2

runCommand called for stage 2

runCommand connected for stage 2

Parsing nmap xml file: /root/.local/share/legion/tmp/legion-6\_2ps399-tool-output/nmap/20221010200519451592-nmapstage1.xml

nmap xml report read successfully!

Adding db\_host

Processing h 172.17.0.7

Found db\_host during os/ports/service processing

'os\_nodes' to process: 0

'ports' to process: 7

Processing port obj 80

Processing port obj 81

Processing port obj 443

Processing port obj 4443

Processing port obj 8080

Processing port obj 8081

Processing port obj 8082

Finished in 0.7064385414123535 seconds.

Scheduler started!

Running tools for: http on 172.17.0.7:80

-----------------------------------------------

Scheduler ended!

Saving screenshot as: 20221010200529984620-screenshot-172.17.0.7-80.png

Process 2 is done!

runStagedNmap called for stage 3

Queuing: nmap -sV --script=./scripts/nmap/vulners.nse -vvvv 172.17.0.7 -oA /root/.local/share/legion/tmp/legion-wtr605p3-running/nmap/20221010200532589418-nmapstage3

runCommand called for stage 3

runCommand connected for stage 3

Parsing nmap xml file: /root/.local/share/legion/tmp/legion-6\_2ps399-tool-output/nmap/20221010200528742867-nmapstage2.xml

nmap xml report read successfully!

Found db\_host already in db

Processing h 172.17.0.7

Found db\_host during os/ports/service processing

'os\_nodes' to process: 0

'ports' to process: 12

Processing port obj 25

Processing port obj 135

Processing port obj 137

Processing port obj 139

Processing port obj 445

Processing port obj 1433

Processing port obj 3306

Processing port obj 5432

Processing port obj 137

Processing port obj 161

Processing port obj 162

Processing port obj 1434

Finished in 0.15488481521606445 seconds.

Scheduler started!

-----------------------------------------------

Scheduler ended!

Finished.

Process 3 is done!

runStagedNmap called for stage 4

Queuing: nmap -T4 -sV -n -sSU -p T:23,21,22,110,111,2049,3389,8080,U:500,5060 172.17.0.7 -oA /root/.local/share/legion/tmp/legion-wtr605p3-running/nmap/20221010200542551392-nmapstage4

runCommand called for stage 4

runCommand connected for stage 4

Parsing nmap xml file: /root/.local/share/legion/tmp/legion-6\_2ps399-tool-output/nmap/20221010200532589418-nmapstage3.xml

nmap xml report read successfully!

Found db\_host already in db

Processing h 172.17.0.7

Found db\_host during os/ports/service processing

'os\_nodes' to process: 0

'ports' to process: 1

Processing port obj 80

Processing script obj <parsers.Script.Script object at 0x7ff56c589be0>

Adding l1ScriptObj obj http-server-header

Processing script obj <parsers.Script.Script object at 0x7ff56c589100>

Adding l1ScriptObj obj vulners

Finished in 0.5411064624786377 seconds.

Scheduler started!

Running tools for: http on 172.17.0.7:80

-----------------------------------------------

Scheduler ended!

Process 5 is done!

runStagedNmap called for stage 5

Queuing: nmap -T4 -sV -n -sSU -p T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-2048,2050-3305,3307-3388,3390-5431,5433-8079,8081-29999 172.17.0.7 -oA /root/.local/share/legion/tmp/legion-wtr605p3-running/nmap/20221010200545924238-nmapstage5

runCommand called for stage 5

runCommand connected for stage 5

Saving screenshot as: 20221010200544440562-screenshot-172.17.0.7-80.png

Finished.

Parsing nmap xml file: /root/.local/share/legion/tmp/legion-6\_2ps399-tool-output/nmap/20221010200542551392-nmapstage4.xml

nmap xml report read successfully!

Found db\_host already in db

Processing h 172.17.0.7

Found db\_host during os/ports/service processing

'os\_nodes' to process: 0

'ports' to process: 10

Processing port obj 21

Processing port obj 22

Processing port obj 23

Processing port obj 110

Processing port obj 111

Processing port obj 2049

Processing port obj 3389

Processing port obj 8080

Processing port obj 500

Processing port obj 5060

Finished in 0.07292556762695312 seconds.

Scheduler started!

-----------------------------------------------

Scheduler ended!

Process 6 is done!

runStagedNmap called for stage 6

Queuing: nmap -T4 -sV -n -sSU -p T:30000-65535 172.17.0.7 -oA /root/.local/share/legion/tmp/legion-wtr605p3-running/nmap/20221010200549226463-nmapstage6

runCommand called for stage 6

Parsing nmap xml file: /root/.local/share/legion/tmp/legion-6\_2ps399-tool-output/nmap/20221010200545924238-nmapstage5.xml

nmap xml report read successfully!

Found db\_host already in db

Processing h 172.17.0.7

Found db\_host during os/ports/service processing

'os\_nodes' to process: 0

'ports' to process: 0

Finished in 0.018777132034301758 seconds.

Scheduler started!

-----------------------------------------------

Scheduler ended!

Process 8 is done!

Parsing nmap xml file: /root/.local/share/legion/tmp/legion-6\_2ps399-tool-output/nmap/20221010200549226463-nmapstage6.xml

nmap xml report read successfully!

Found db\_host already in db

Processing h 172.17.0.7

Found db\_host during os/ports/service processing

'os\_nodes' to process: 0

'ports' to process: 0

Finished in 0.03825521469116211 seconds.

Scheduler started!

-----------------------------------------------

Scheduler ended!

**Q.5:**

─# nmap -sU -sV 192.168.56.101 -p 161

Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-10 20:08 EDT

Nmap scan report for 192.168.56.101

Host is up (0.00023s latency).

PORT STATE SERVICE VERSION

161/udp open snmp SNMPv1 server (public)

MAC Address: 08:00:27:46:8C:27 (Oracle VirtualBox virtual NIC)

Service Info: Host: vagrant-2008R2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 8.28 seconds

└─# snmp-check 192.168.56.101

snmp-check v1.9 - SNMP enumerator

Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.56.101:161 using SNMPv1 and community 'public'

[\*] System information:

Host IP address : 192.168.56.101

Hostname : vagrant-2008R2

Description : Hardware: AMD64 Family 25 Model 33 Stepping 0 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free)

Contact : -

Location : -

Uptime snmp : 00:23:02.92

Uptime system : 00:22:29.82

System date : 2022-10-10 19:08:53.1

Domain : WORKGROUP

[\*] User accounts:

Guest

greedo

vagrant

han\_solo

kylo\_ren

boba\_fett

chewbacca

ben\_kenobi

jabba\_hutt

artoo\_detoo

c\_three\_pio

darth\_vader

leia\_organa

jarjar\_binks

Administrator

luke\_skywalker

anakin\_skywalker

lando\_calrissian

[\*] Network information:

IP forwarding enabled : no

Default TTL : 128

TCP segments received : 0

TCP segments sent : 0

TCP segments retrans : 0

Input datagrams : 45

Delivered datagrams : 136

Output datagrams : 128

[\*] Network interfaces:

Interface : [ up ] Software Loopback Interface 1

Id : 1

Mac Address : :::::

Type : softwareLoopback

Speed : 1073 Mbps

MTU : 1500

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (SSTP)

Id : 2

Mac Address : :::::

Type : unknown

Speed : 1073 Mbps

MTU : 4091

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (L2TP)

Id : 3

Mac Address : :::::

Type : unknown

Speed : 1073 Mbps

MTU : 1460

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (PPTP)

Id : 4

Mac Address : :::::

Type : unknown

Speed : 1073 Mbps

MTU : 1464

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (PPPOE)

Id : 5

Mac Address : :::::

Type : ppp

Speed : 1073 Mbps

MTU : 1494

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (IPv6)

Id : 6

Mac Address : f0:8f:20:52:41:53

Type : ethernet-csmacd

Speed : 1073 Mbps

MTU : 1500

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (Network Monitor)

Id : 7

Mac Address : f0:8f:20:52:41:53

Type : ethernet-csmacd

Speed : 1073 Mbps

MTU : 1500

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (IP)

Id : 8

Mac Address : f0:8f:20:52:41:53

Type : ethernet-csmacd

Speed : 1073 Mbps

MTU : 1500

In octets : 0

Out octets : 0

Interface : [ down ] RAS Async Adapter

Id : 9

Mac Address : 20:41:53:59:4e:ff

Type : ppp

Speed : 0 Mbps

MTU : 0

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (IKEv2)

Id : 10

Mac Address : 00:00:00:00:00:00

Type : unknown

Speed : 0 Mbps

MTU : 1480

In octets : 0

Out octets : 0

Interface : [ up ] Intel(R) PRO/1000 MT Network Connection

Id : 11

Mac Address : 08:00:27:46:8c:27

Type : ethernet-csmacd

Speed : 1000 Mbps

MTU : 1500

In octets : 4958

Out octets : 19952

Interface : [ up ] Microsoft ISATAP Adapter

Id : 12

Mac Address : 00:00:00:00:00:00

Type : unknown

Speed : 0 Mbps

MTU : 1280

In octets : 0

Out octets : 0

Interface : [ up ] Intel(R) PRO/1000 MT Network Connection-QoS Packet Scheduler-0000

Id : 13

Mac Address : 08:00:27:46:8c:27

Type : ethernet-csmacd

Speed : 1000 Mbps

MTU : 1500

In octets : 4958

Out octets : 19952

Interface : [ up ] Intel(R) PRO/1000 MT Network Connection-WFP LightWeight Filter-0000

Id : 14

Mac Address : 08:00:27:46:8c:27

Type : ethernet-csmacd

Speed : 1000 Mbps

MTU : 1500

In octets : 4958

Out octets : 19952

Interface : [ up ] WAN Miniport (IPv6)-QoS Packet Scheduler-0000

Id : 15

Mac Address : f0:8f:20:52:41:53

Type : ethernet-csmacd

Speed : 1073 Mbps

MTU : 1500

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (IP)-QoS Packet Scheduler-0000

Id : 16

Mac Address : f0:8f:20:52:41:53

Type : ethernet-csmacd

Speed : 1073 Mbps

MTU : 1500

In octets : 0

Out octets : 0

Interface : [ up ] WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000

Id : 17

Mac Address : f0:8f:20:52:41:53

Type : ethernet-csmacd

Speed : 1073 Mbps

MTU : 1500

In octets : 0

Out octets : 0

[\*] Network IP:

Id IP Address Netmask Broadcast

1 127.0.0.1 255.0.0.0 1

11 192.168.56.101 255.255.255.0 1

[\*] Routing information:

Destination Next hop Mask Metric

127.0.0.0 127.0.0.1 255.0.0.0 306

127.0.0.1 127.0.0.1 255.255.255.255 306

127.255.255.255 127.0.0.1 255.255.255.255 306

192.168.56.0 192.168.56.101 255.255.255.0 266

192.168.56.101 192.168.56.101 255.255.255.255 266

192.168.56.255 192.168.56.101 255.255.255.255 266

224.0.0.0 127.0.0.1 240.0.0.0 306

255.255.255.255 127.0.0.1 255.255.255.255 306

[\*] TCP connections and listening ports:

Local address Local port Remote address Remote port State

0.0.0.0 135 0.0.0.0 0 listen

0.0.0.0 3389 0.0.0.0 0 listen

0.0.0.0 49152 0.0.0.0 0 listen

0.0.0.0 49153 0.0.0.0 0 listen

0.0.0.0 49154 0.0.0.0 0 listen

0.0.0.0 49155 0.0.0.0 0 listen

0.0.0.0 49156 0.0.0.0 0 listen

0.0.0.0 49157 0.0.0.0 0 listen

192.168.56.101 139 0.0.0.0 0 listen

[\*] Listening UDP ports:

Local address Local port

0.0.0.0 123

0.0.0.0 161

0.0.0.0 500

0.0.0.0 4500

0.0.0.0 5355

192.168.56.101 137

192.168.56.101 138

[\*] Network services:

Index Name

0 Power

1 Server

2 IP Helper

3 DNS Client

4 DHCP Client

5 Workstation

6 SNMP Service

7 Windows Time

8 Plug and Play

9 Print Spooler

10 Task Scheduler

11 Windows Update

12 Remote Registry

13 Windows Firewall

14 COM+ Event System

15 Windows Event Log

16 IPsec Policy Agent

17 Group Policy Client

18 Network Connections

19 RPC Endpoint Mapper

20 Software Protection

21 Network List Service

22 User Profile Service

23 Base Filtering Engine

24 Microsoft FTP Service

25 TCP/IP NetBIOS Helper

26 Cryptographic Services

27 Diagnostic System Host

28 Certificate Propagation

29 Remote Desktop Services

30 SPP Notification Service

31 Shell Hardware Detection

32 Diagnostic Policy Service

33 Security Accounts Manager

34 Network Location Awareness

35 Windows Font Cache Service

36 Remote Procedure Call (RPC)

37 DCOM Server Process Launcher

38 Remote Desktop Configuration

39 Application Host Helper Service

40 Network Store Interface Service

41 Distributed Link Tracking Client

42 System Event Notification Service

43 World Wide Web Publishing Service

44 Windows Management Instrumentation

45 Windows Process Activation Service

46 Distributed Transaction Coordinator

47 IKE and AuthIP IPsec Keying Modules

48 Windows Licensing Monitoring Service

49 Desktop Window Manager Session Manager

50 Windows Remote Management (WS-Management)

51 Remote Desktop Services UserMode Port Redirector

[\*] Processes:

Id Status Name Path Parameters

1 running System Idle Process

4 running System

124 running conhost.exe \??\C:\Windows\system32\

212 running smss.exe \SystemRoot\System32\

280 running csrss.exe %SystemRoot%\system32\ ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User

332 running csrss.exe %SystemRoot%\system32\ ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User

340 running wininit.exe

368 running winlogon.exe

428 running services.exe C:\Windows\system32\

436 running lsass.exe C:\Windows\system32\

444 running lsm.exe C:\Windows\system32\

496 running slui.exe

536 running svchost.exe

612 running svchost.exe

692 running svchost.exe

748 running svchost.exe

796 running svchost.exe

844 running svchost.exe

884 running svchost.exe

1008 running svchost.exe

1048 running spoolsv.exe

1088 running svchost.exe

1112 running svchost.exe

1300 running conhost.exe \??\C:\Windows\system32\

1336 running taskhost.exe

1528 running powercfg.exe C:\Windows\System32\ -energy -auto

1544 running svchost.exe

1568 running snmp.exe C:\Windows\System32\

1612 running svchost.exe C:\Windows\system32\ -k iissvcs

1640 running wlms.exe C:\Windows\system32\wlms\

1648 running svchost.exe

1760 running cmd.exe C:\Windows\system32\

1772 running explorer.exe C:\Windows\

1776 running dwm.exe C:\Windows\system32\

1904 running msdtc.exe

1908 running sppsvc.exe

2016 running svchost.exe

2044 running svchost.exe

[\*] Storage information:

Description : ["C:\\ Label:Windows 2008R2 Serial Number 2476a374"]

Device id : [#<SNMP::Integer:0x0000557f75004520 @value=1>]

Filesystem type : ["unknown"]

Device unit : [#<SNMP::Integer:0x0000557f750026f8 @value=4096>]

Memory size : 100.00 GB

Memory used : 7.97 GB

Description : ["D:\\ Label:data Serial Number 6e9bf1e4"]

Device id : [#<SNMP::Integer:0x0000557f750c15d0 @value=2>]

Filesystem type : ["unknown"]

Device unit : [#<SNMP::Integer:0x0000557f74fff818 @value=4096>]

Memory size : 10.00 GB

Memory used : 3.15 GB

Description : ["Virtual Memory"]

Device id : [#<SNMP::Integer:0x0000557f750be588 @value=3>]

Filesystem type : ["unknown"]

Device unit : [#<SNMP::Integer:0x0000557f750bc940 @value=65536>]

Memory size : 2.00 GB

Memory used : 339.00 MB

Description : ["Physical Memory"]

Device id : [#<SNMP::Integer:0x0000557f750af830 @value=4>]

Filesystem type : ["unknown"]

Device unit : [#<SNMP::Integer:0x0000557f750adbe8 @value=65536>]

Memory size : 1023.50 MB

Memory used : 324.12 MB

[\*] File system information:

Index : 1

Mount point :

Remote mount point : -

Access : 1

Bootable : 1

[\*] Device information:

Id Type Status Descr

1 unknown running Microsoft XPS Document Writer

2 unknown running Unknown Processor Type

3 unknown unknown Software Loopback Interface 1

4 unknown unknown WAN Miniport (SSTP)

5 unknown unknown WAN Miniport (L2TP)

6 unknown unknown WAN Miniport (PPTP)

7 unknown unknown WAN Miniport (PPPOE)

8 unknown unknown WAN Miniport (IPv6)

9 unknown unknown WAN Miniport (Network Monitor)

10 unknown unknown WAN Miniport (IP)

11 unknown unknown RAS Async Adapter

12 unknown unknown WAN Miniport (IKEv2)

13 unknown unknown Intel(R) PRO/1000 MT Network Connection

14 unknown unknown Microsoft ISATAP Adapter

15 unknown unknown Intel(R) PRO/1000 MT Network Connection-QoS Packet Scheduler-000

16 unknown unknown Intel(R) PRO/1000 MT Network Connection-WFP LightWeight Filter-0

17 unknown unknown WAN Miniport (IPv6)-QoS Packet Scheduler-0000

18 unknown unknown WAN Miniport (IP)-QoS Packet Scheduler-0000

19 unknown unknown WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000

20 unknown running Fixed Disk

21 unknown running Fixed Disk

22 unknown running IBM enhanced (101- or 102-key) keyboard, Subtype=(0)

[\*] IIS server information:

TotalBytesSentLowWord : 0

TotalBytesReceivedLowWord : 0

TotalFilesSent : 0

CurrentAnonymousUsers : 0

CurrentNonAnonymousUsers : 0

TotalAnonymousUsers : 0

TotalNonAnonymousUsers : 0

MaxAnonymousUsers : 0

MaxNonAnonymousUsers : 0

CurrentConnections : 0

MaxConnections : 0

ConnectionAttempts : 0

LogonAttempts : 0

Gets : 0

Posts : 0

Heads : 0

Others : 0

CGIRequests : 0

BGIRequests : 0

NotFoundErrors : 0

**Q.6:**

└─# rdesktop 192.168.56.101

Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses and invalid security certificate which can not be trusted for

the following identified reasons(s);

1. Certificate issuer is not trusted by this system.

Issuer: CN=vagrant-2008R2

Review the following certificate info before you trust it to be added as an exception.

If you do not trust the certificate the connection atempt will be aborted:

Subject: CN=vagrant-2008R2

Issuer: CN=vagrant-2008R2

Valid From: Sat Sep 3 22:26:43 2022

To: Sun Mar 5 21:26:43 2023

Certificate fingerprints:

sha1: 1bd3e0972b0da719117b64096e17a1e584fe21e4

sha256: bbfde7d1a5e354e5930a26e44408ae2d5c6f73a3ae14e87de8ed8f70c69bd72c

Do you trust this certificate (yes/no)? y

ATTENTION! The server uses and invalid security certificate which can not be trusted for

the following identified reasons(s);

1. Certificate issuer is not trusted by this system.

Issuer: CN=vagrant-2008R2

Review the following certificate info before you trust it to be added as an exception.

If you do not trust the certificate the connection atempt will be aborted:

Subject: CN=vagrant-2008R2

Issuer: CN=vagrant-2008R2

Valid From: Sat Sep 3 22:26:43 2022

To: Sun Mar 5 21:26:43 2023

Certificate fingerprints:

sha1: 1bd3e0972b0da719117b64096e17a1e584fe21e4

sha256: bbfde7d1a5e354e5930a26e44408ae2d5c6f73a3ae14e87de8ed8f70c69bd72c

Do you trust this certificate (yes/no)? y

ATTENTION! The server uses and invalid security certificate which can not be trusted for

the following identified reasons(s);

1. Certificate issuer is not trusted by this system.

Issuer: CN=vagrant-2008R2

Review the following certificate info before you trust it to be added as an exception.

If you do not trust the certificate the connection atempt will be aborted:

Subject: CN=vagrant-2008R2

Issuer: CN=vagrant-2008R2

Valid From: Sat Sep 3 22:26:43 2022

To: Sun Mar 5 21:26:43 2023

Certificate fingerprints:

sha1: 1bd3e0972b0da719117b64096e17a1e584fe21e4

sha256: bbfde7d1a5e354e5930a26e44408ae2d5c6f73a3ae14e87de8ed8f70c69bd72c

Do you trust this certificate (yes/no)? yes

Failed to initialize NLA, do you have correct Kerberos TGT initialized ?

Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.

Connection established using SSL.

Protocol(warning): process\_pdu\_logon(), Unhandled login infotype 1

Clipboard(error): xclip\_handle\_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request

A screenshot of a computer

Description automatically generated

Graphical user interface, website

Description automatically generated

**Q.7:**

I think that my biggest key takeaway from this practical exercise is that it really highlights the issue of ports being open that can allow access points for hackers to access another individual’s pc. Just like the example above with Port #3389 listening which was discovered using nmap and the Metasploit-3 VM’s IP. Like the assignment says, the user and password could be harvested using a brute force method of SQL injecting attack. With these tools at an individual’s disposal, they could easily remote into a pc and start gaining access to private information. Another takeaway for me is how to use Legion for a vulnerability analysis that uses a few different tools. Using Legion can be quicker than using each individual tool to run a test which can save time over inputting each tool.

**Q.8:**

Graphical user interface, application

Description automatically generated