

XYZ Corp VAPT Report

August 22, 2022

WHITE HATS organization

White Hat Street, White Hat State, White Hat Nation - 007007



Submission by: Goutham Vyasroimath Keshava Murthy

Assignment: AEP CS - Ethical Hacking and VAPT

Cohort: PGP AEP CS May 2022 Cohort

Contents

[1. Disclaimer 2](#_Toc112072879)

[2. In-Scope 2](#_Toc112072880)

[3. Out-Of-Scope 2](#_Toc112072881)

[4. Executive Report 3](#_Toc112072882)

[**4.1.** **Vulnerability summary** 3](#_Toc112072883)

[**4.2.** **Vulnerability severity summary** 3](#_Toc112072884)

[**4.3.** **Vulnerability assessment inference** 3](#_Toc112072885)

[**4.4.** **Estimation & next steps** 3](#_Toc112072886)

[5. Technical Report 4](#_Toc112072887)

[**5.1.** **Testing methodology** 4](#_Toc112072888)

[**5.2.** **Linux vulnerability list** 4](#_Toc112072889)

[**5.3.** **Linux reverse shell exploit** 4](#_Toc112072890)

[**5.4.** **Windows reverse shell exploit** 5](#_Toc112072891)

[**5.5.** **Vulnerabilities & exploit list with solution** 6](#_Toc112072892)

[**5.6.** **Reverse shell exploit & solution** 6](#_Toc112072893)

[6. APPENDIX - Tool Wise Scanning Data 7](#_Toc112072894)

[**6.1.** Nessus Advanced Scans 7](#_Toc112072895)

[**6.2.** Nmap Version Summary Scans 8](#_Toc112072896)

[**6.3.** Nmap Vulners Scan 10](#_Toc112072897)

[**6.4.** Nmap Vulscan Scan 12](#_Toc112072898)

[**6.5.** Reverse shell exploit 16](#_Toc112072899)

# Disclaimer

White Hats Organization was officially contacted by XYZ Corp for conducting vulnerability assessment and security testing (*henceforth referred to as VAPT*) of the 2 servers (1 Windows and 1 Linux server) using Kali Linux as one of the tools.

Vulnerability assessment and testing has been conducted within purview of laws governing the jurisdiction with proper permissions from XYZ Corp.

**Assignment specific call-out**:

I have taken permission from Gaurav & Imran to use personal labs in addition to Simplilearn labs for this assignment

# In-Scope

* Scope of this assessment has been to identify vulnerabilities in 1 Windows and 1 Linux Server of XYZ Corp by utilizing Kali Linux and other tools

**Target servers (victim servers)**

|  |  |  |
| --- | --- | --- |
| Server OS | IP Address | Functionality |
| Windows 10 | 192.168.100 OR 192.168.1.33 OR 172.31.56.14 | Administration Server |
| Linux | 192.168.101 OR 172.31.61.40 OR 192.168.1.105 | Administration Server |

**Testing tool (Kali Linux)**

|  |  |  |
| --- | --- | --- |
| Server OS | IP Address | Functionality |
| Kali Linux | 192.168.102 OR 192.168.1.103 OR 192.168.1.106 | Testing server |

# Out-Of-Scope

* Any target servers other than the 1 Windows & 1 Linux server.
* Tools cost
  + XYZ Corp has not given permission for White Hats Organization to use tools with license cost. If White Hats Organization uses licensed tools to conduct security assessment and testing, cost will not be paid by XYZ Corp

# Executive Report

XYZ Corp engaged White Hats Organization to perform penetration testing for their servers. The testing was performed on the targets reported under scope section.

Target servers are used for storing data for administration purposes

# **Vulnerability summary**

|  |  |  |
| --- | --- | --- |
| Total vulnerabilities | Windows server | Linux Servers |
| 8 | 1 reverse shell exploit (common for both) | * 7 vulnerabilities * 1 reverse shell exploit (common for both) |

# **Vulnerability severity summary**

|  |  |  |
| --- | --- | --- |
| Severity | Number of issues | Source system |
| 0 Day | 0 | Linux |
| Critical | 0 | Linux |
| High | 8 | Linux + Windows |
| Medium | 0 | Linux |
| Low | 0 | Linux |

# **Vulnerability assessment inference**

* Windows server is comparatively more secure than Linux server.
* There is corrective action to be taken for both Windows & Linux servers

# **Estimation & next steps**

* Ballpark effort to fix the issues is medium. Accurate estimation for fixing issues will be provided by White Hats Organization after due diligence phase
* Below list of tools were leveraged for VAPT
* Kali Linux
* Nmap
* Nmap vulscan
* Nmap vulners
* Nessus
* Metasploit framework

# Technical Report

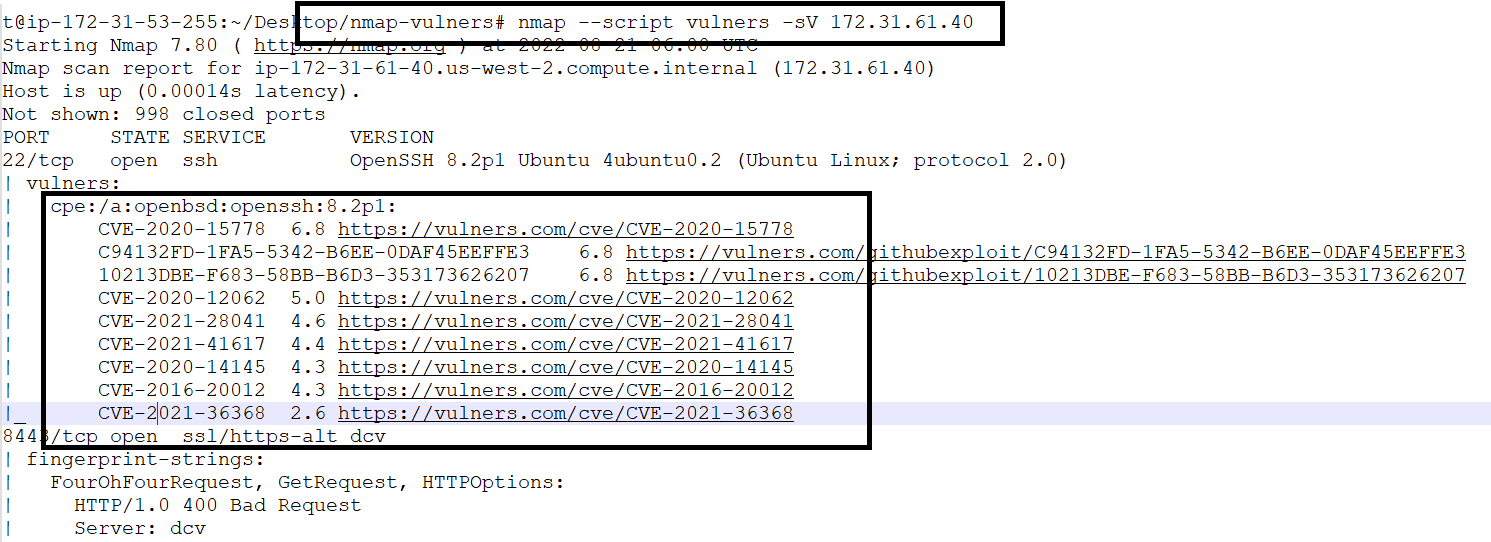
# **Testing methodology**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Phases involved** | | | | |
| **Information Gathering and Reconnaissance** | **Scanning and Enumeration** | **Vulnerability Assessment** | **Exploitation** | **Analysis and Reporting** |

* As depicted above, White Hats Organization has carried out standard phases of VAPT. We have leveraged tools which do not incur license cost.
* Nmap Vulners and Vulscan utilities proved to be useful in unearthing CVEs related to Linux
* Please see Tool Wise Scanning Data section for more details of data collected

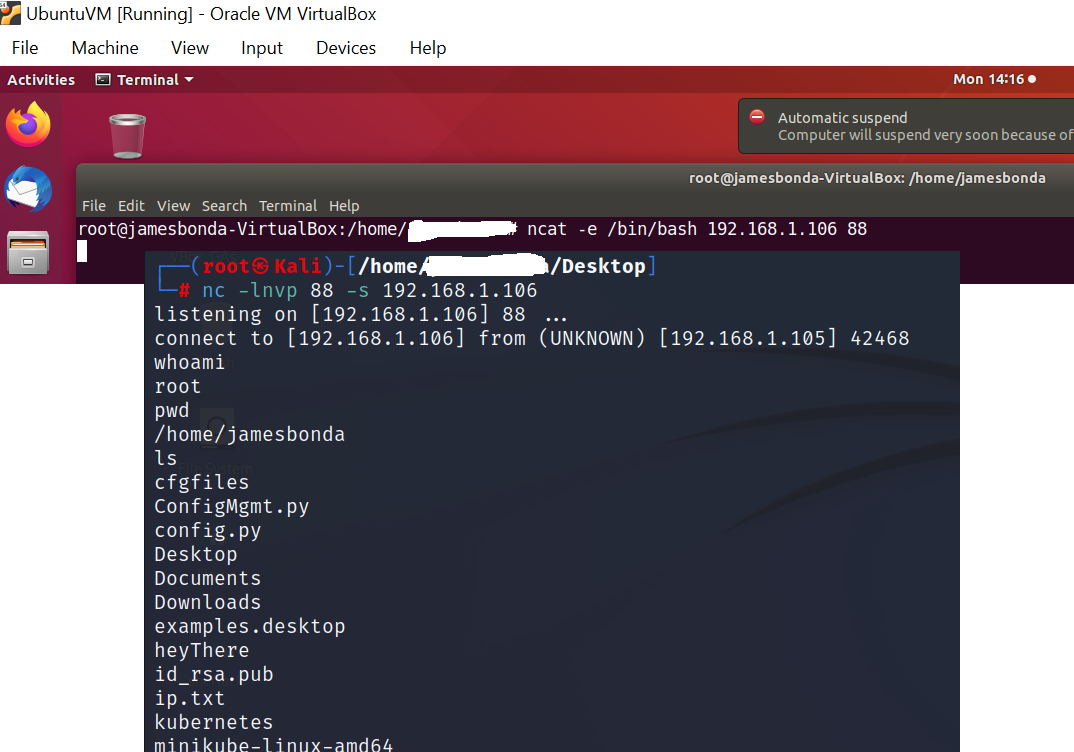
# **Linux vulnerability list**

Below list of vulnerabilities are found out from the utility **Nmap Vulners** as shown below



# **Linux reverse shell exploit**

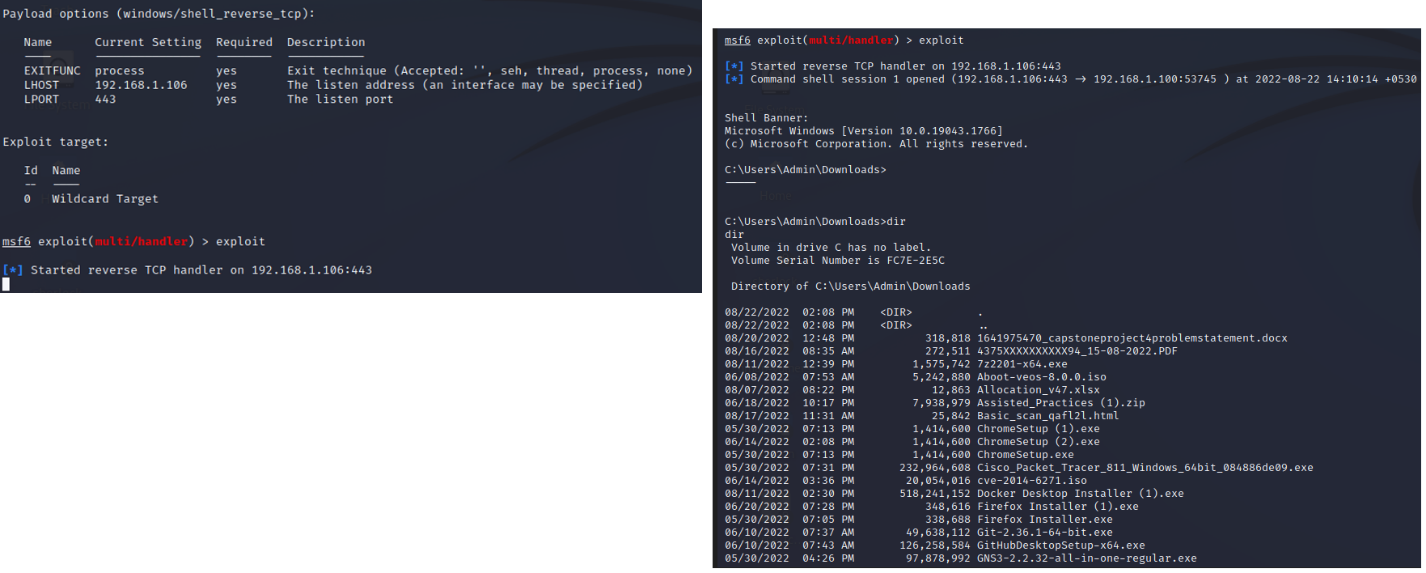
For below exploit, reverse shell commands were used



# **Windows reverse shell exploit**

Msfvenom was used to create an exe file. File was hosted on apache server.

Windows machine access apache server and downloaded the exe file, clicked on it to provide Windows remote access to Kali Linux machine



# **Vulnerabilities & exploit list with solution**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability | Server | Severity | Name - Description | Mitigation |
| CVE-2020-15778 | Linux | High | scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function | Use of rsync in the place of scp for better security. More details about supported alternatives available at: https://access.redhat.com/articles/5284081 |
| CVE-2020-12062 | Linux | High | The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure | Use Openssh release-8.3 |
| CVE-2021-28041 | Linux | High | sh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios | Use Openssh release-8.5 |
| CVE-2021-41617 | Linux | High | sshd in OpenSSH 6.2 through 8.x before 8.8, allows privilege escalation | Use Openssh release-8.8 |
| CVE-2020-14145 | Linux | High | OpenSSH 5.7 through 8.4 has an information leak | Use Openssh release greater than 8.5\_p1 |
| CVE-2016-20012 | Linux | High | OpenSSH through 8.7 allows remote attackers to test combination of username and public key | Patch available through https://github.com/openssh/openssh-portable/pull/270 |
| CVE-2021-36368 | Linux | High | OpenSSH before 8.9.allows attacker to meddle with FIDO authentication | Use Openssh 1:8.9p1-1 |

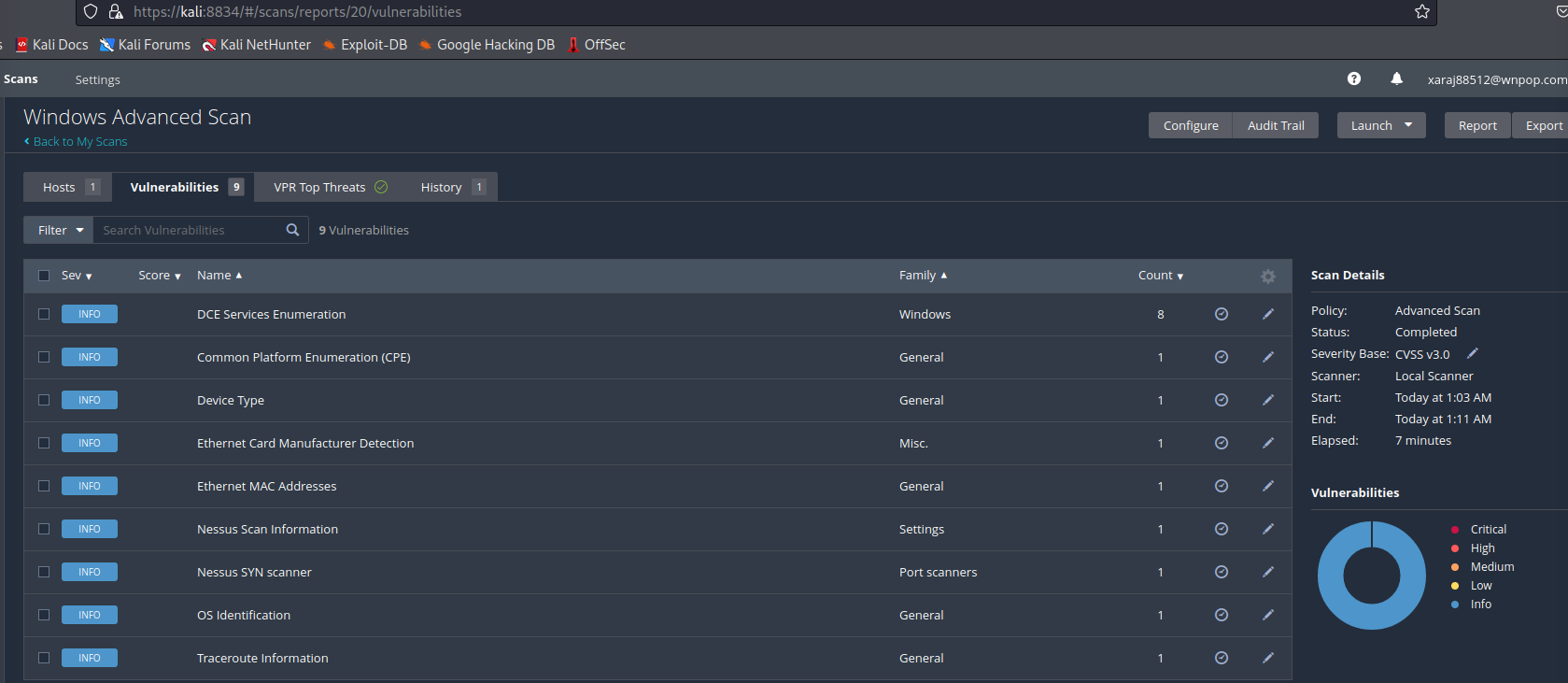
# **Reverse shell exploit & solution**

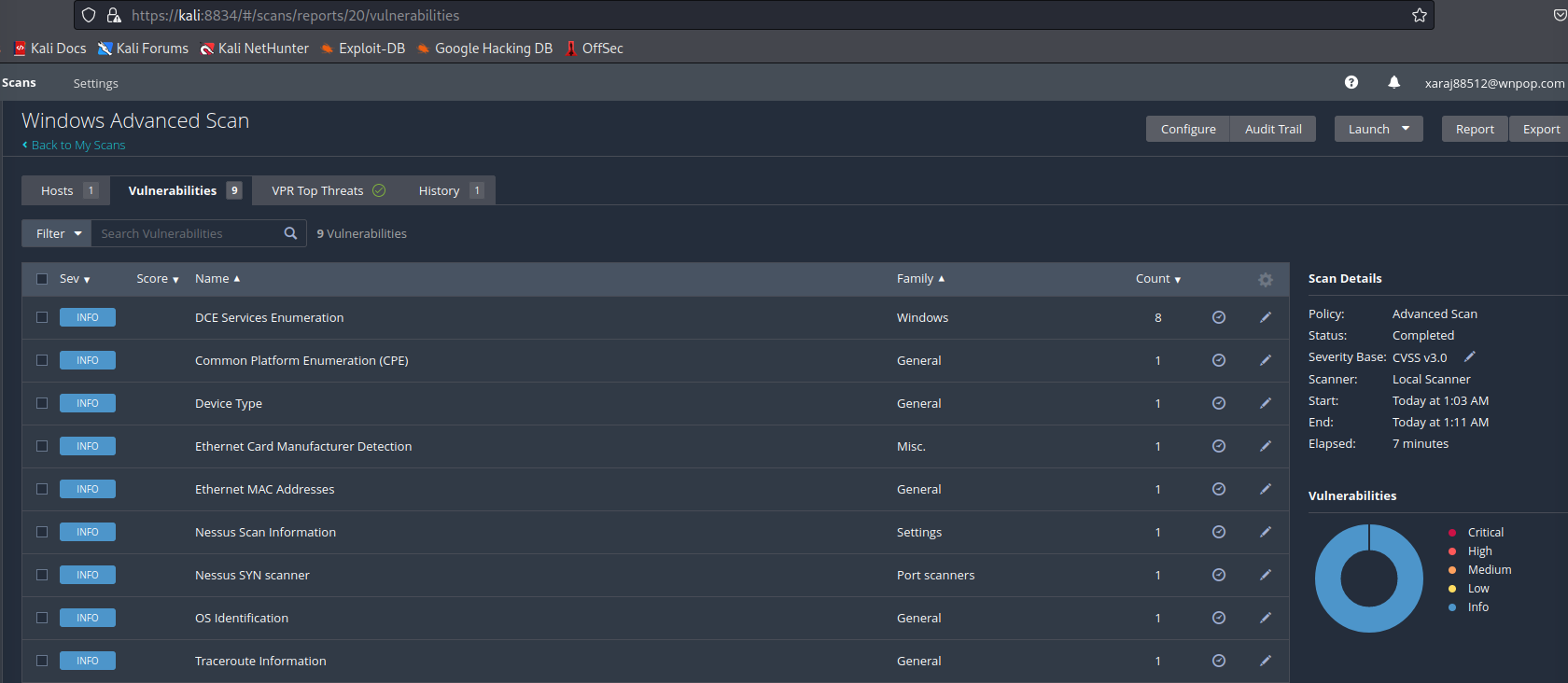
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exploit | Server | Severity | Name - Description | Mitigation |
| Reverse shell | Linux | High | Opens a connection to a remote machine giving access | * Lock all outgoing connectivity * Set up a proxy server * Remove unnecessary interpreters * Prevent exploits such as code injection vulnerabilities |
| Reverse shell | Windows | High | Opens a connection to a remote machine giving access | * Lock all outgoing connectivity * Set up a proxy server * Remove unnecessary interpreters * Prevent exploits such as code injection vulnerabilities |

# APPENDIX - Tool Wise Scanning Data

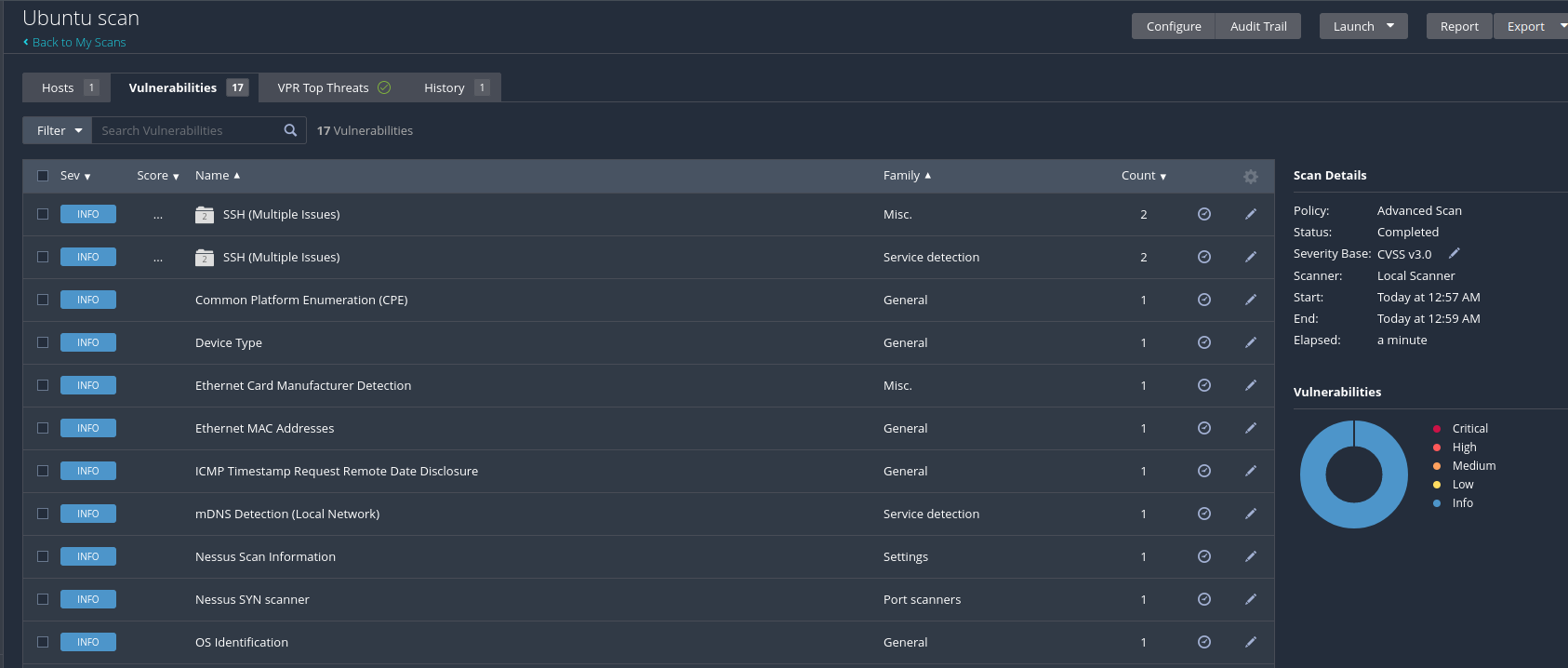
# Nessus Advanced Scans

**Windows Server**

****

****

**Linux Server**

****

# Nmap Version Summary Scans

**Windows server**

└─# nmap -sT -A 192.168.1.100

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-21 08:02 IST

Nmap scan report for 192.168.1.100

Host is up (0.0013s latency).

Not shown: 996 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

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

445/tcp open microsoft-ds?

2179/tcp open vmrdp?

MAC Address: CC:2F:71:C4:7A:5C (Intel Corporate)

Device type: general purpose

Running: Microsoft Windows 10

OS CPE: cpe:/o:microsoft:windows\_10

OS details: Microsoft Windows 10 1709 - 1803, Microsoft Windows 10 1709 - 1909

Network Distance: 1 hop

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

Host script results:

| smb2-time:

| date: 2022-08-21T02:32:55

|\_ start\_date: N/A

| smb2-security-mode:

| 3.1.1:

|\_ Message signing enabled but not required

|\_nbstat: NetBIOS name: DESKTOP-B2LAJI9, NetBIOS user: <unknown>, NetBIOS MAC: cc:2f:71:c4:7a:5c (Intel Corporate)

TRACEROUTE

HOP RTT ADDRESS

1 1.33 ms 192.168.1.100

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

Nmap done: 1 IP address (1 host up) scanned in 38.90 seconds

**Linux server**

└─# nmap -sT -A 192.168.1.101

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-21 08:01 IST

Nmap scan report for 192.168.1.101

Host is up (0.0021s latency).

Not shown: 999 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 86:c7:72:b5:5e:27:29:73:54:14:ec:c2:bc:af:93:0b (RSA)

| 256 34:af:4a:4a:da:ef:0b:41:bb:cc:7f:fd:55:2f:1e:bf (ECDSA)

|\_ 256 6a:2e:09:bf:c7:0a:01:92:40:b1:11:45:4c:21:04:d8 (ED25519)

MAC Address: 08:00:27:73:47:D9 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 4.X|5.X

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5

OS details: Linux 4.15 - 5.6

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE

HOP RTT ADDRESS

1 2.13 ms 192.168.1.101

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

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds

# Nmap Vulners Scan

**Windows server (no vulnerabilities found)**

t@ip-172-31-53-255:~/Desktop/nmap-vulners# nmap --script vulners -sV 172.31.56.14

Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-21 06:12 UTC

Nmap scan report for ip-172-31-56-14.us-west-2.compute.internal (172.31.56.14)

Host is up (0.0036s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

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

445/tcp open microsoft-ds?

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

8443/tcp open ssl/https-alt dcv

| fingerprint-strings:

| FourOhFourRequest, GetRequest, HTTPOptions:

| HTTP/1.0 400 Bad Request

| Server: dcv

| Date: Sun, 21 Aug 2022 06:12:35 GMT

| Content-Length: 0

| RTSPRequest, SIPOptions:

| HTTP/1.1 400 Bad Request

| Server: dcv

|\_ Content-Length: 0

|\_http-server-header: dcv

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-Port8443-TCP:V=7.80%T=SSL%I=7%D=8/21%Time=6301CCD3%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,61,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer:\x20dcv

SF:\r\nDate:\x20Sun,\x2021\x20Aug\x202022\x2006:12:35\x20GMT\r\nContent-Le

SF:ngth:\x200\r\n\r\n")%r(HTTPOptions,61,"HTTP/1\.0\x20400\x20Bad\x20Reque

SF:st\r\nServer:\x20dcv\r\nDate:\x20Sun,\x2021\x20Aug\x202022\x2006:12:35\

SF:x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,61,"HTTP/1

SF:\.0\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nDate:\x20Sun,\x2021\x

SF:20Aug\x202022\x2006:12:35\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RT

SF:SPRequest,3C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nC

SF:ontent-Length:\x200\r\n\r\n")%r(SIPOptions,3C,"HTTP/1\.1\x20400\x20Bad\

SF:x20Request\r\nServer:\x20dcv\r\nContent-Length:\x200\r\n\r\n");

MAC Address: 0E:3A:3B:4C:11:8F (Unknown)

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

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

Nmap done: 1 IP address (1 host up) scanned in 136.36 seconds

**Linux server (vulnerabilities found)**

t@ip-172-31-53-255:~/Desktop/nmap-vulners# nmap --script vulners -sV 172.31.61.40

Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-21 06:00 UTC

Nmap scan report for ip-172-31-61-40.us-west-2.compute.internal (172.31.61.40)

Host is up (0.00014s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)

| vulners:

| cpe:/a:openbsd:openssh:8.2p1:

| CVE-2020-15778 6.8 https://vulners.com/cve/CVE-2020-15778

| C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 \*EXPLOIT\*

| 10213DBE-F683-58BB-B6D3-353173626207 6.8 https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 \*EXPLOIT\*

| CVE-2020-12062 5.0 https://vulners.com/cve/CVE-2020-12062

| CVE-2021-28041 4.6 https://vulners.com/cve/CVE-2021-28041

| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617

| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145

| CVE-2016-20012 4.3 https://vulners.com/cve/CVE-2016-20012

|\_ CVE-2021-36368 2.6 https://vulners.com/cve/CVE-2021-36368

8443/tcp open ssl/https-alt dcv

| fingerprint-strings:

| FourOhFourRequest, GetRequest, HTTPOptions:

| HTTP/1.0 400 Bad Request

| Server: dcv

| Date: Sun, 21 Aug 2022 06:00:14 GMT

| Content-Length: 0

| RTSPRequest, SIPOptions:

| HTTP/1.1 400 Bad Request

| Server: dcv

|\_ Content-Length: 0

|\_http-server-header: dcv

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-Port8443-TCP:V=7.80%T=SSL%I=7%D=8/21%Time=6301C9EE%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,61,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer:\x20dcv

SF:\r\nDate:\x20Sun,\x2021\x20Aug\x202022\x2006:00:14\x20GMT\r\nContent-Le

SF:ngth:\x200\r\n\r\n")%r(HTTPOptions,61,"HTTP/1\.0\x20400\x20Bad\x20Reque

SF:st\r\nServer:\x20dcv\r\nDate:\x20Sun,\x2021\x20Aug\x202022\x2006:00:14\

SF:x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,61,"HTTP/1

SF:\.0\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nDate:\x20Sun,\x2021\x

SF:20Aug\x202022\x2006:00:14\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RT

SF:SPRequest,3C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nC

SF:ontent-Length:\x200\r\n\r\n")%r(SIPOptions,3C,"HTTP/1\.1\x20400\x20Bad\

SF:x20Request\r\nServer:\x20dcv\r\nContent-Length:\x200\r\n\r\n");

MAC Address: 0E:54:84:6D:75:3B (Unknown)

Service Info: OS: 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 131.31 seconds

# Nmap Vulscan Scan

**Windows server (no vulnerabilities found)**

t@ip-172-31-53-255:~/Desktop/vulscan# nmap --script vulscan -sV 172.31.56.14

Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-21 06:16 UTC

Nmap scan report for ip-172-31-56-14.us-west-2.compute.internal (172.31.56.14)

Host is up (0.00012s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

| vulscan: VulDB - https://vuldb.com:

| No findings

|

| MITRE CVE - https://cve.mitre.org:

| No findings

|

| SecurityFocus - https://www.securityfocus.com/bid/:

| No findings

|

| IBM X-Force - https://exchange.xforce.ibmcloud.com:

| No findings

|

| Exploit-DB - https://www.exploit-db.com:

| No findings

|

| OpenVAS (Nessus) - http://www.openvas.org:

| No findings

|

| SecurityTracker - https://www.securitytracker.com:

| No findings

|

| OSVDB - http://www.osvdb.org:

| No findings

|\_

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

| vulscan: VulDB - https://vuldb.com:

| No findings

|

| MITRE CVE - https://cve.mitre.org:

| No findings

|

| SecurityFocus - https://www.securityfocus.com/bid/:

| No findings

|

| IBM X-Force - https://exchange.xforce.ibmcloud.com:

| No findings

|

| Exploit-DB - https://www.exploit-db.com:

| No findings

|

| OpenVAS (Nessus) - http://www.openvas.org:

| No findings

|

| SecurityTracker - https://www.securitytracker.com:

| No findings

|

| OSVDB - http://www.osvdb.org:

| No findings

|\_

445/tcp open microsoft-ds?

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

| vulscan: VulDB - https://vuldb.com:

| No findings

|

| MITRE CVE - https://cve.mitre.org:

| No findings

|

| SecurityFocus - https://www.securityfocus.com/bid/:

| No findings

|

| IBM X-Force - https://exchange.xforce.ibmcloud.com:

| No findings

|

| Exploit-DB - https://www.exploit-db.com:

| No findings

|

| OpenVAS (Nessus) - http://www.openvas.org:

| No findings

|

| SecurityTracker - https://www.securitytracker.com:

| No findings

|

| OSVDB - http://www.osvdb.org:

| No findings

|\_

8443/tcp open ssl/https-alt dcv

| fingerprint-strings:

| FourOhFourRequest, GetRequest, HTTPOptions:

| HTTP/1.0 400 Bad Request

| Server: dcv

| Date: Sun, 21 Aug 2022 06:17:07 GMT

| Content-Length: 0

| RTSPRequest, SIPOptions:

| HTTP/1.1 400 Bad Request

| Server: dcv

|\_ Content-Length: 0

|\_http-server-header: dcv

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-Port8443-TCP:V=7.80%T=SSL%I=7%D=8/21%Time=6301CDE3%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,61,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer:\x20dcv

SF:\r\nDate:\x20Sun,\x2021\x20Aug\x202022\x2006:17:07\x20GMT\r\nContent-Le

SF:ngth:\x200\r\n\r\n")%r(HTTPOptions,61,"HTTP/1\.0\x20400\x20Bad\x20Reque

SF:st\r\nServer:\x20dcv\r\nDate:\x20Sun,\x2021\x20Aug\x202022\x2006:17:07\

SF:x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,61,"HTTP/1

SF:\.0\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nDate:\x20Sun,\x2021\x

SF:20Aug\x202022\x2006:17:07\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RT

SF:SPRequest,3C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nC

SF:ontent-Length:\x200\r\n\r\n")%r(SIPOptions,3C,"HTTP/1\.1\x20400\x20Bad\

SF:x20Request\r\nServer:\x20dcv\r\nContent-Length:\x200\r\n\r\n");

MAC Address: 0E:3A:3B:4C:11:8F (Unknown)

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

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

Nmap done: 1 IP address (1 host up) scanned in 136.53 seconds

**Linux server (no vulnerabilities found)**

t@ip-172-31-53-255:~/Desktop/vulscan# nmap --script vulscan -sV 172.31.61.40

Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-21 05:58 UTC

Nmap scan report for ip-172-31-61-40.us-west-2.compute.internal (172.31.61.40)

Host is up (0.00017s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)

| vulscan: VulDB - https://vuldb.com:

| No findings

|

| MITRE CVE - https://cve.mitre.org:

| No findings

|

| SecurityFocus - https://www.securityfocus.com/bid/:

| No findings

|

| IBM X-Force - https://exchange.xforce.ibmcloud.com:

| No findings

|

| Exploit-DB - https://www.exploit-db.com:

| No findings

|

| OpenVAS (Nessus) - http://www.openvas.org:

| No findings

|

| SecurityTracker - https://www.securitytracker.com:

| No findings

|

| OSVDB - http://www.osvdb.org:

| No findings

|\_

8443/tcp open ssl/https-alt dcv

| fingerprint-strings:

| FourOhFourRequest, GetRequest, HTTPOptions:

| HTTP/1.0 400 Bad Request

| Server: dcv

| Date: Sun, 21 Aug 2022 05:58:47 GMT

| Content-Length: 0

| RTSPRequest, SIPOptions:

| HTTP/1.1 400 Bad Request

| Server: dcv

|\_ Content-Length: 0

|\_http-server-header: dcv

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-Port8443-TCP:V=7.80%T=SSL%I=7%D=8/21%Time=6301C997%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,61,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer:\x20dcv

SF:\r\nDate:\x20Sun,\x2021\x20Aug\x202022\x2005:58:47\x20GMT\r\nContent-Le

SF:ngth:\x200\r\n\r\n")%r(HTTPOptions,61,"HTTP/1\.0\x20400\x20Bad\x20Reque

SF:st\r\nServer:\x20dcv\r\nDate:\x20Sun,\x2021\x20Aug\x202022\x2005:58:47\

SF:x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,61,"HTTP/1

SF:\.0\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nDate:\x20Sun,\x2021\x

SF:20Aug\x202022\x2005:58:47\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RT

SF:SPRequest,3C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nC

SF:ontent-Length:\x200\r\n\r\n")%r(SIPOptions,3C,"HTTP/1\.1\x20400\x20Bad\

SF:x20Request\r\nServer:\x20dcv\r\nContent-Length:\x200\r\n\r\n");

MAC Address: 0E:54:84:6D:75:3B (Unknown)

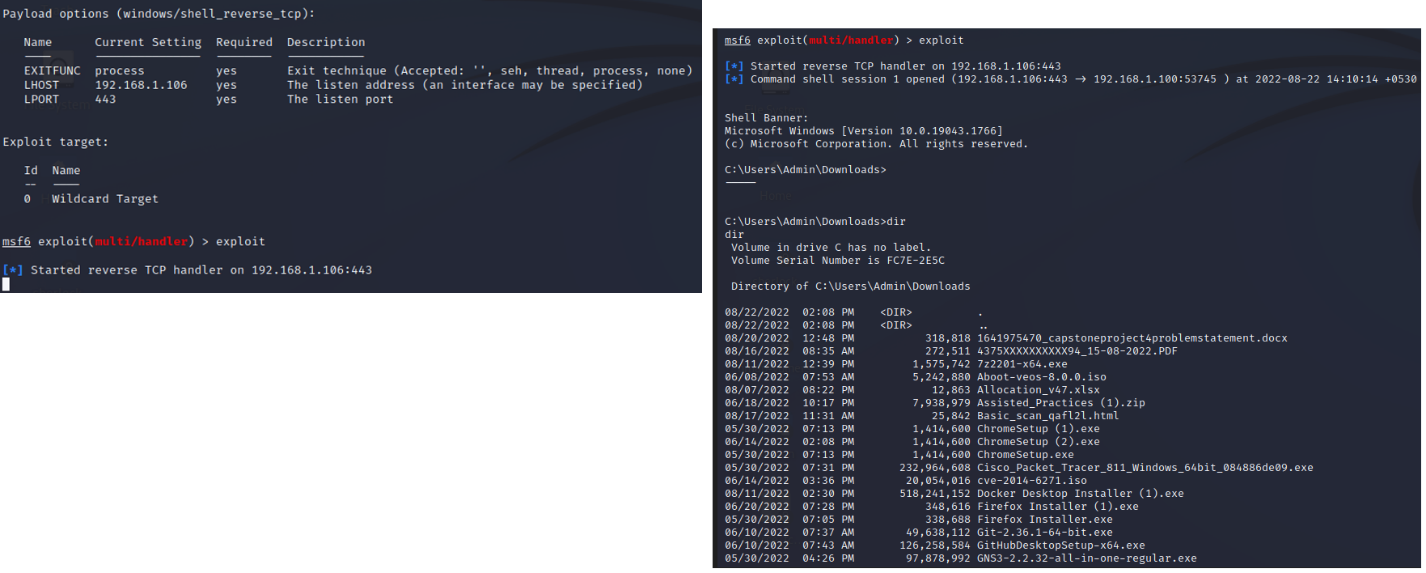
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 130.73 seconds

# Reverse shell exploit

**Windows server (exploitable)**



**Linux server (exploitable)**

