

# **Vulnerability and Threat Analysis**

**RIS430 NAA**

**Assignment 5**

## **Vulnerability Assessment Report**

**Prepared By Group 10,**

**Khondoker Ishmum Muhammad (155895212)**

**Aryan Santosh Saindane (136235215)**

**Ananthu Krishna Vadakkeppatt (154290217)**

**Syed Mujahid Hamid Ali (161202213)**

<b>Assignment 5.....</b>	<b>00</b>
<b>Vulnerability Assessment Report.....</b>	<b>00</b>
<b>    Executive Summary.....</b>	<b>03</b>
<b>    Scope Of Engagement.....</b>	<b>04</b>
<b>    Vulnerability Assessment Methodology.....</b>	<b>12</b>
<b>    Risk Assessment Methodology Reflection Report.....</b>	<b>13</b>
<b>    Vulnerability Assessment And Patching Report.....</b>	<b>14</b>
<b>Conclusion.....</b>	<b>34</b>

## **Executive Summary**

---

In this report, we will be assessing vulnerabilities found while attempting scans on the home network devices. This assessment was done between 1st August 2023 and 6th August 2023 in Toronto, Canada. The LAN segment had the IP network of 192.168.1.0 /24 and VLANs had an IP network of 10.6.6.0/24. Another network of 192.168.99.0/24 was also used for assessing the Lupin One VM. At the time of the assessment, the infrastructure was operational and being used. This report includes a high-level summary of our test results, a description of the assessment, and extensive technical details for each risk or vulnerability discovered. The publication also contains general approaches to enhancing security posture as well as techniques for correcting each finding.

Across the whole assessment, we analyzed a lot of vulnerabilities which will be elaborated in the report ahead. Moreover, students from our group have only performed scans on local networks.

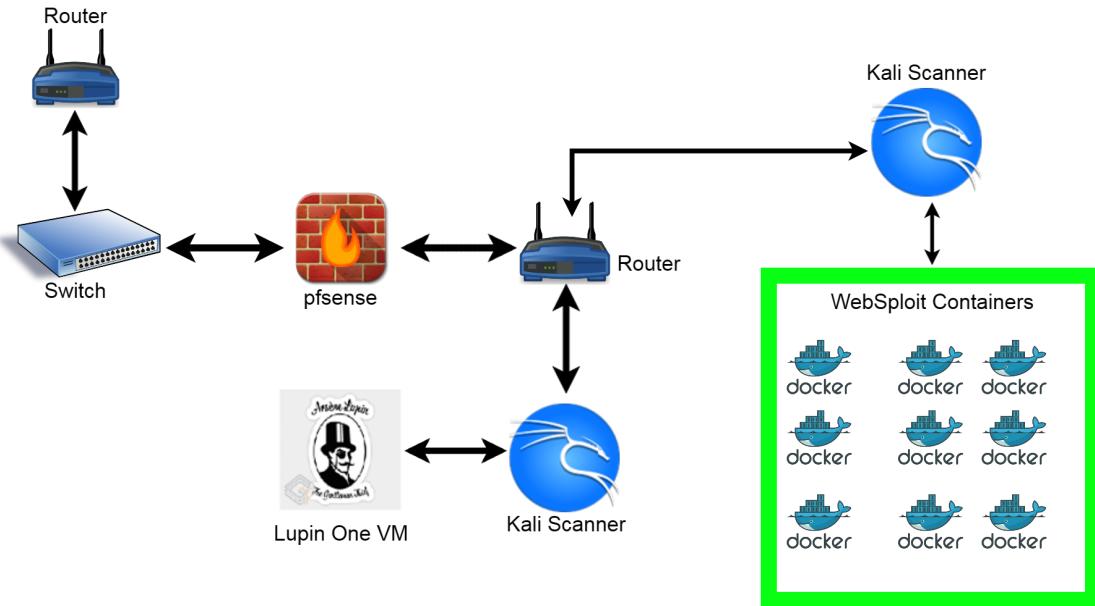
The purpose of this report is to highlight critical vulnerabilities present in the devices under assessment. Leaving these devices in their current state poses significant risks to the organization's security and operations. The maintainer of these devices is strongly advised to take immediate action by analyzing the detailed list of vulnerabilities provided further in this document and initiating the necessary Patching measures promptly.

The assessment's findings are based on the current network and topology configurations. Changes in the network environment or device positioning might alter the risk landscape and introduce new vulnerabilities. Therefore, it is crucial to periodically reassess the devices' security and adapt Patching strategies accordingly.

# Scope Of Engagement

---

## Network Infrastructure



## Network Layout Information

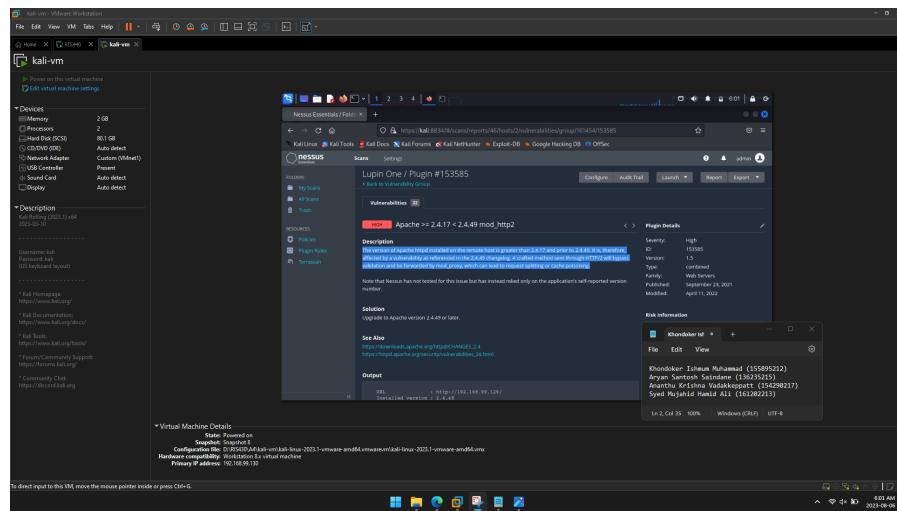
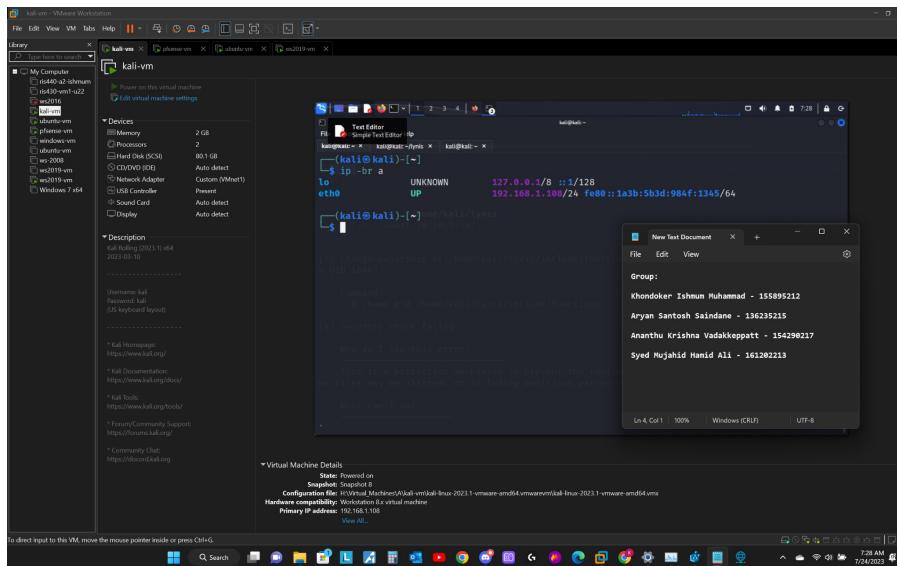
Hardware Inventory & Software Inventory				
Machines	Software & Services	IP Address	Subnet Mask - CIDR	Role
Kali Scanner (1)	Nessus	192.168.1.108	255.255.255.0 - /24	Scanner to find vulnerabilities in the network infrastructure.
Websploit VM	Contains the docker environment with vulnerable services	10.6.6.0	255.255.255.0 - /24	Acts as a victim that has a lot of vulnerable services running in the machine.
Kali Scanner (2)	Nessus	192.168.1.130	255.255.255.0 - /24	Scanner to find vulnerabilities in the Lupin One VM.
LupinOne VM	-	192.168.99.129	255.255.255.0 - /24	
Pfsense router/firewall VM	- Firewall - Routing - Forwarding	192.168.1.101	255.255.255.0 - /24	Router and Firewall to protect the vlan and for routing.

## Few Important Notes

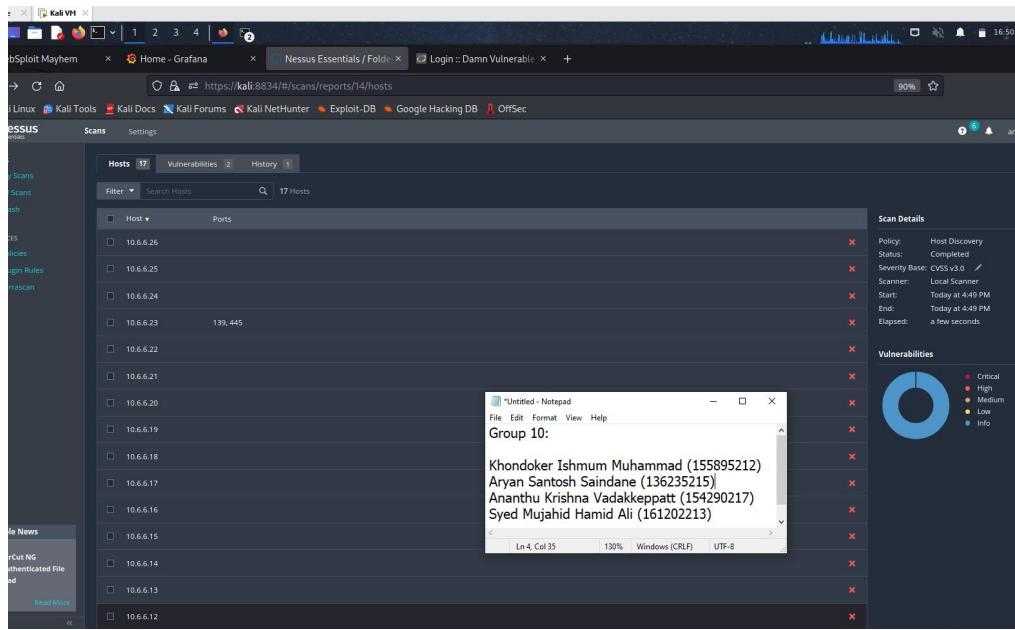
The VLAN contains the devices such as the Kali machine that was used to run the websploit services and the Lupin One machine.

For the LAN, we were allowed to run various tests using tools such as Nmap, Nessus on the network 10.6.6.0/24 that was a virtual network created for the docker containers created by the websploit application.

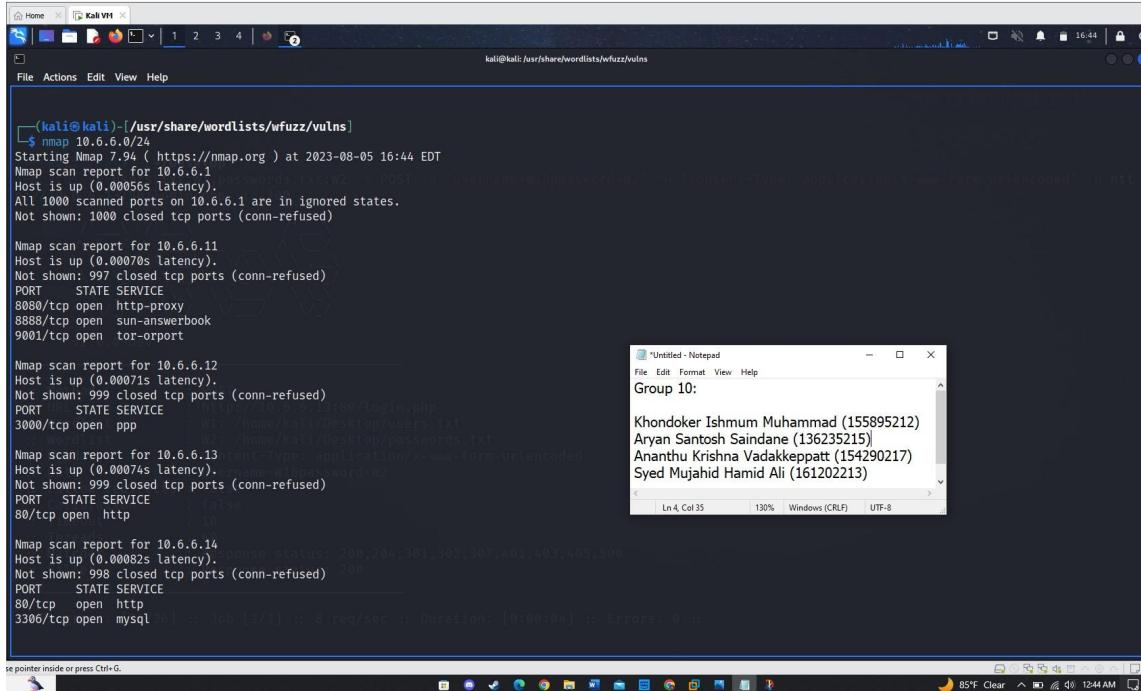
## Kali scanner



# Docker Network Host Discovery



# Nmap Scans to perform service discovery across the Network.



```
(kali㉿kali)-[~/usr/share/wordlists/wfuzz/vulns]
$ nmap 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-05 16:44 EDT
Nmap scan report for 10.6.6.11
Host is up (0.00056s latency).
All 1000 scanned ports on 10.6.6.11 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 10.6.6.11
Host is up (0.00078s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
8888/tcp  open  sun-answerbook
9001/tcp  open  tor-orport

Nmap scan report for 10.6.6.12
Host is up (0.00071s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3000/tcp  open  ppp
3306/tcp  open  mysql

Nmap scan report for 10.6.6.13
Host is up (0.00074s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
80/tcp    open  http

Nmap scan report for 10.6.6.14
Host is up (0.00082s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql

Nmap scan report for 10.6.6.15
Host is up (0.00091s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
9090/tcp  open  zeus-admin

Nmap scan report for 10.6.6.16
Host is up (0.00100s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

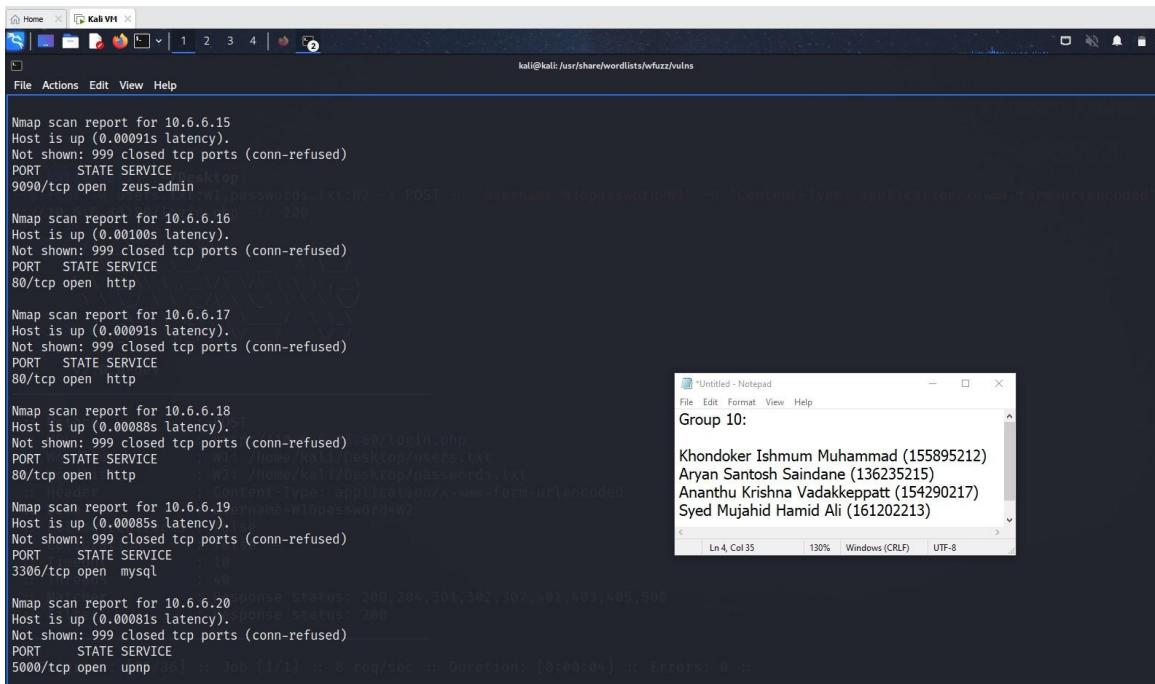
Nmap scan report for 10.6.6.17
Host is up (0.00091s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 10.6.6.18
Host is up (0.00088s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 10.6.6.19
Host is up (0.00085s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 10.6.6.20
Host is up (0.00081s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
5000/tcp  open  upnp

Nmap scan report for 10.6.6.21
Host is up (0.00081s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
5000/tcp  open  upnp
```



```
Nmap scan report for 10.6.6.15
Host is up (0.00091s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
9090/tcp  open  zeus-admin

Nmap scan report for 10.6.6.16
Host is up (0.00100s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 10.6.6.17
Host is up (0.00091s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 10.6.6.18
Host is up (0.00088s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 10.6.6.19
Host is up (0.00085s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 10.6.6.20
Host is up (0.00081s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
5000/tcp  open  upnp

Nmap scan report for 10.6.6.21
Host is up (0.00081s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
5000/tcp  open  upnp
```

```
Home Kali VM
File Actions Edit View Help
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
5000/tcp open upnp

Nmap scan report for 10.6.6.21
Host is up (0.00070s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open http

Nmap scan report for 10.6.6.22
Host is up (0.00067s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open http

Nmap scan report for 10.6.6.23
Host is up (0.00073s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
53/tcp open domain
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Usernames: W1,password-W2

Nmap scan report for 10.6.6.24
Host is up (0.00070s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
3000/tcp open ppp

Nmap scan report for 10.6.6.25
Host is up (0.00067s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open http

Nmap done: 256 IP addresses (17 hosts up) scanned in 3.05 seconds
kali@kali: /usr/share/wordlists/wfuzz/vulns
```

pointer inside or press Ctrl+G.

The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window displays Nmap scan results for hosts 10.6.6.21, 10.6.6.22, 10.6.6.23, and 10.6.6.25. Host 10.6.6.23 is found to have an open Microsoft-DNS port (445). Host 10.6.6.25 is found to have an open HTTP port (80). A Notepad window titled "Untitled - Notepad" is open in the background, showing a list of names and their corresponding ID numbers, likely extracted from the scan results. The desktop taskbar at the bottom shows various application icons, and the system tray indicates the date and time as 12:46 AM.

```
Home Kali VM
File Actions Edit View Help
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open http

Nmap scan report for 10.6.6.23
Host is up (0.00073s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
53/tcp open domain
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Usernames: W1,password-W2

Nmap scan report for 10.6.6.24
Host is up (0.00070s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
3000/tcp open ppp

Nmap scan report for 10.6.6.25
Host is up (0.00067s latency).
Not shown: 1000 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open http

Nmap done: 256 IP addresses (17 hosts up) scanned in 3.05 seconds
kali@kali: /usr/share/wordlists/wfuzz/vulns
```

pointer inside or press Ctrl+G.

This screenshot is nearly identical to the one above, showing the same Nmap scan results for hosts 10.6.6.21 through 10.6.6.25. The Notepad window in the background contains the same list of names and IDs. The desktop environment, including the taskbar and system tray, remains consistent with the previous screenshot.

kali-vm - VMware Workstation

File Edit View VM Tabs Help

Home X Ubuntu-42S430-shard-0 X kali-vm X LuarOne X

root@kali:~[~]

```
root@kali:~[~]
# nmap -sA 192.168.99.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-03 07:41 EDT
Nmap scan report for 192.168.99.129
Host is up (0.0004s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3070 4d:a4:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
|   256  bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
|_  256 ac:18:ec:cc:c3:5c:05:1f:5f:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp    open  http    Apache httpd 2.4.48 ((Debian))
|_http-server-header: Apache/2.4.48 (Debian)
| http-robots.txt: 1 disallowed entry
|_ /myfiles
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:D0:D7:A3 (VMware)
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 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.44 ms 192.168.99.129

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 21.61 seconds
```

To direct input to this VM, click inside or press Ctrl-G.

File Edit View

Khondoker ls

File Edit View

Khondoker Ishum Muhammad (155895212)  
Aryan Santosh Saindane (136235215)  
Ananthu Krishna Vadakeppatt (154290217)  
Syed Mujahid Hamid Ali (161202213)

Ln 2, Col 35 100% Windows (CRLF) UTF-8

7:44 AM 2023-08-03

# Nessus Scans

Notice: Your scanning limit of 16 was reached, and 1 host was removed from this scan. License more.

**Scan Details**

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	August 4 at 4:19 AM
End:	August 4 at 4:25 AM
Elapsed:	6 minutes

**Vulnerabilities**

Critical	High	Medium	Low	Info
1	1	1	1	1

Websploit VM

**Scan Details**

Host	Vulnerabilities
Khondoker Ishmum Muhammad (155895212)	10
Aryan Santosh Saindane (136235215)	1
Ananthu Krishna Vadakeppatt (154290217)	1
Syed Mujahid Hamid Ali (161202213)	1

**Vulnerabilities**

Critical	High	Medium	Low	Info
10	0	0	0	0

Lupin One VM

## **Vulnerability Assessment Methodology**

---

A vulnerability assessment is a layered approach of identifying and listing various security flaws that can be identified from an organization's IT infrastructure. The main goal of a vulnerability assessment report is to make sure organizations are able to act against malicious threats before they are able to cause any serious damage. This vulnerability assessment report follows the guidelines and standards provided as well as maintained by the National Institute of Standards and Technology (NIST).

Throughout this vulnerability assessment report we have made use of various open source tools such as Nmap, Nessus, sqlmap, skipfish, wfuzz, ffuf and nikto. Nmap firstly was used to run a simple scan across the docker network so as to detect the open ports and the services that they were running on it. Along with it, we also ran a Nessus advanced scan on the network that allowed us to get a comprehensive overview of the vulnerabilities that were affecting these networks.

After we had a fair idea of the vulnerabilities that were present throughout the networks we used tools such as sqlmap, skipfish, wfuzz, ffuf and nikto to gain a more advanced overview as to where we can find these vulnerabilities and how we can possibly fix them. Sqlmap and skipfish were used to test the services for vulnerabilities. Additionally, wfuzz, ffuf and nikto were also used to discover common vulnerabilities using the technique of fuzzing.

We have also used another tool named ZAP that was useful to identify web server vulnerabilities when running tests across various services.

# Risk Assessment Methodology Reflection Report

---

This risk assessment is based on the standardized risk assessment methodology that is laid out by the National Institute of Standards and Technology (NIST) from the “ NIST Special Publication 800-30 Revision 1”. It focuses on the combination of likelihood and impact. The higher the likelihood the more adverse the impact would be.

Likelihood	Info	Low	Medium	High	Critical
Critical	Info	Low	Medium	High	Critical
High	Info	Low	Medium	High	Critical
Medium	Info	Low	Medium	Medium	High
Low	Info	Low	Low	Low	Medium
Info	Info	Info	Info	Low	Low

# Vulnerability Assessment And Patching Report

---

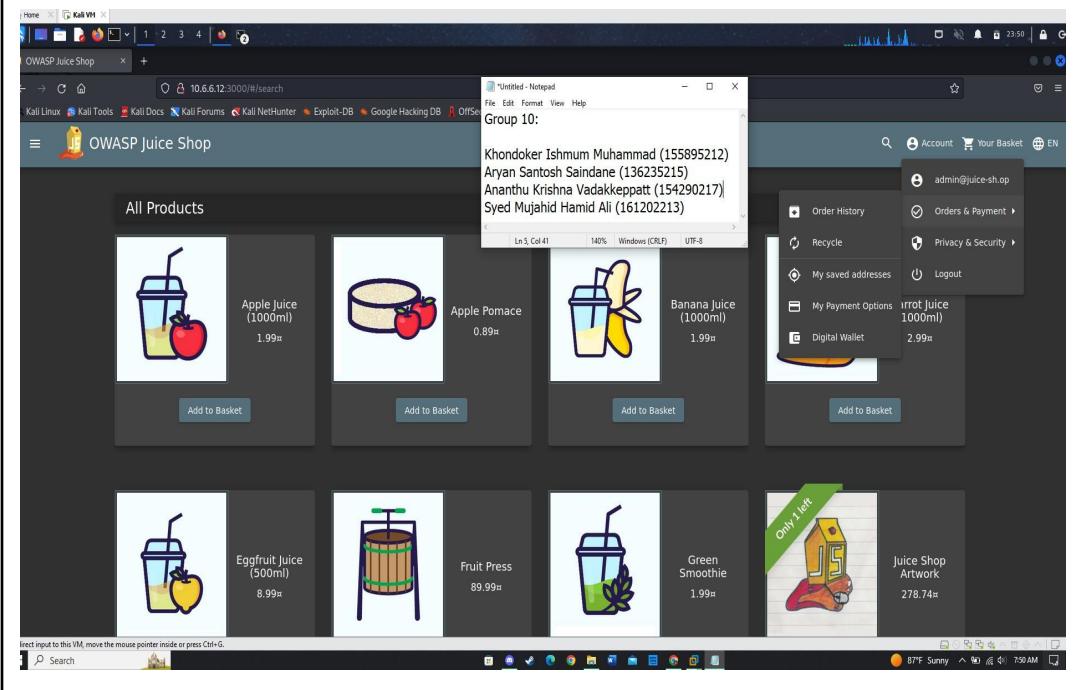
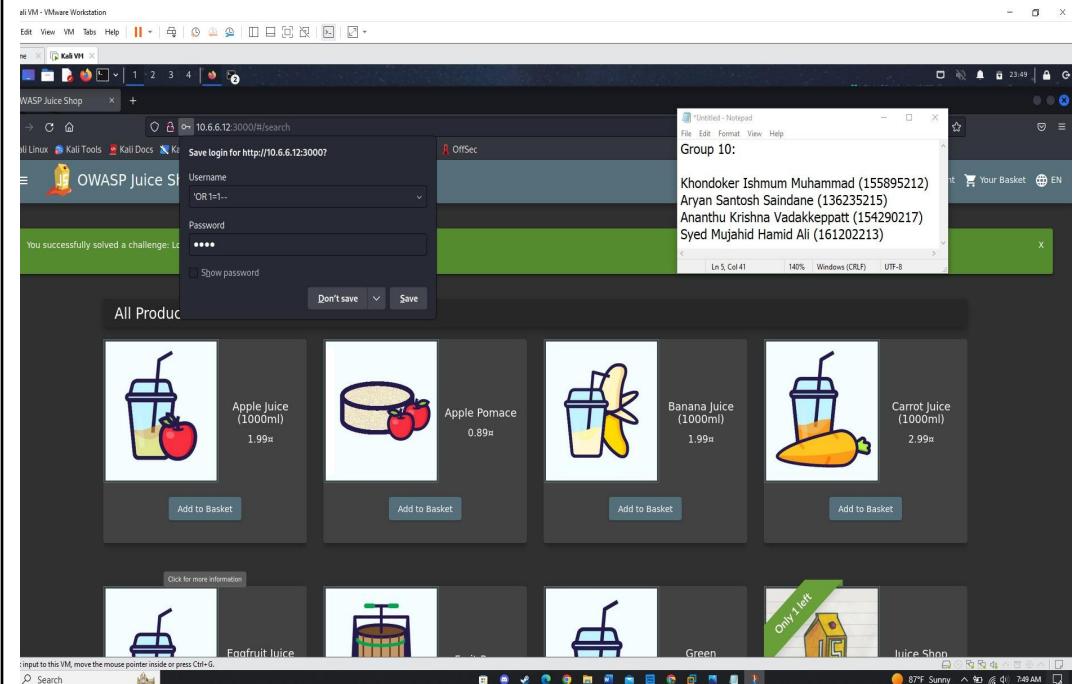
The following is the list of vulnerabilities that we were able to find on all of the operating systems across this assignment:

Vulnerabilities			
Vulnerability ID	Machine	Vulnerability Name	Risk Level
V1	Websploit VM	SQL Injection	Low
V2	Websploit VM	Web Server Transmits Cleartext Credentials	Low
V3	Websploit VM	Web.config File Information Disclosure	Medium
V4	Websploit VM	SMB Signing not required	Medium
V5	Websploit VM	OpenSSL 1.02 < 1.0.2zg	High
V6	LupinOne VM	Apache >= 2.4.17 < 2.4.49 mod_http2	High
V7	Websploit VM	Microsoft Windows SMB Shares Unprivileged Access	High
V8	Websploit VM	Apache Solr 7.4.0 <= 7.7.3 / 8.0.0 <= 8.11.0 RCE	Critical
V9	LupinOne VM	Apache 2.4.x < 2.4.55	Critical
V10	LupinOne VM	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	Critical

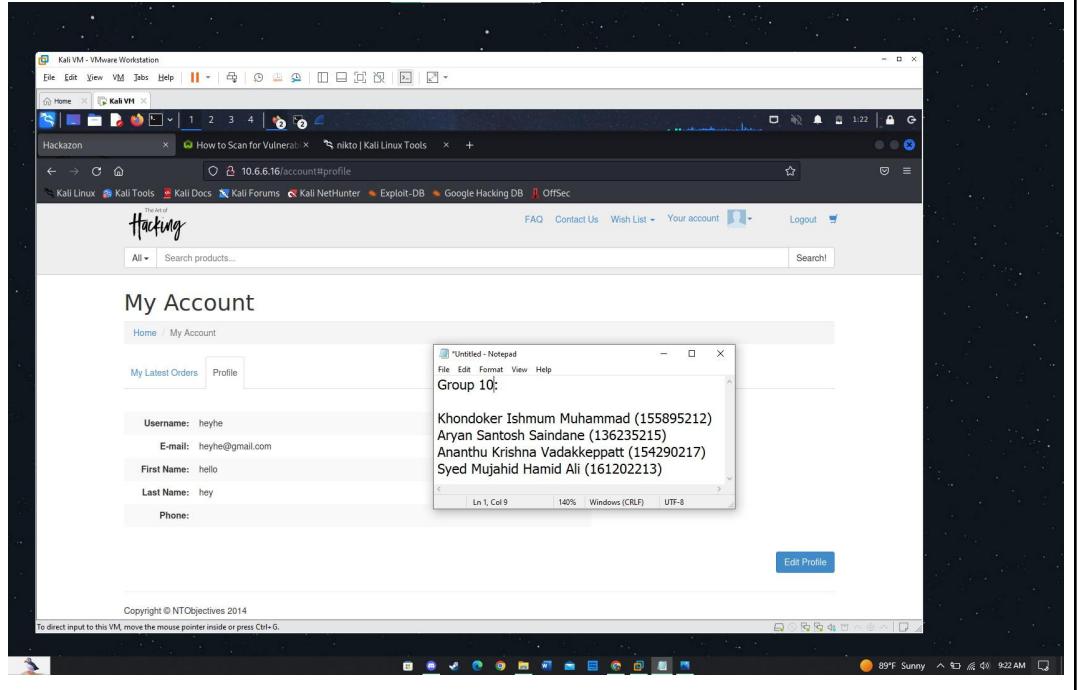
Websploit VM		
Low	V1 - SQL Injection	
Risk Assessment	Impact: Medium	Likelihood: Low
Description	SQL injection is a type of attack where an attacker is able to interact with the queries that are made by a specific application to its database. This vulnerability has the potential to cause data breaches and misuse of sensitive information limited to a few.	
CVSS Score	N/A	
Affected Scope	10.6.6.12	

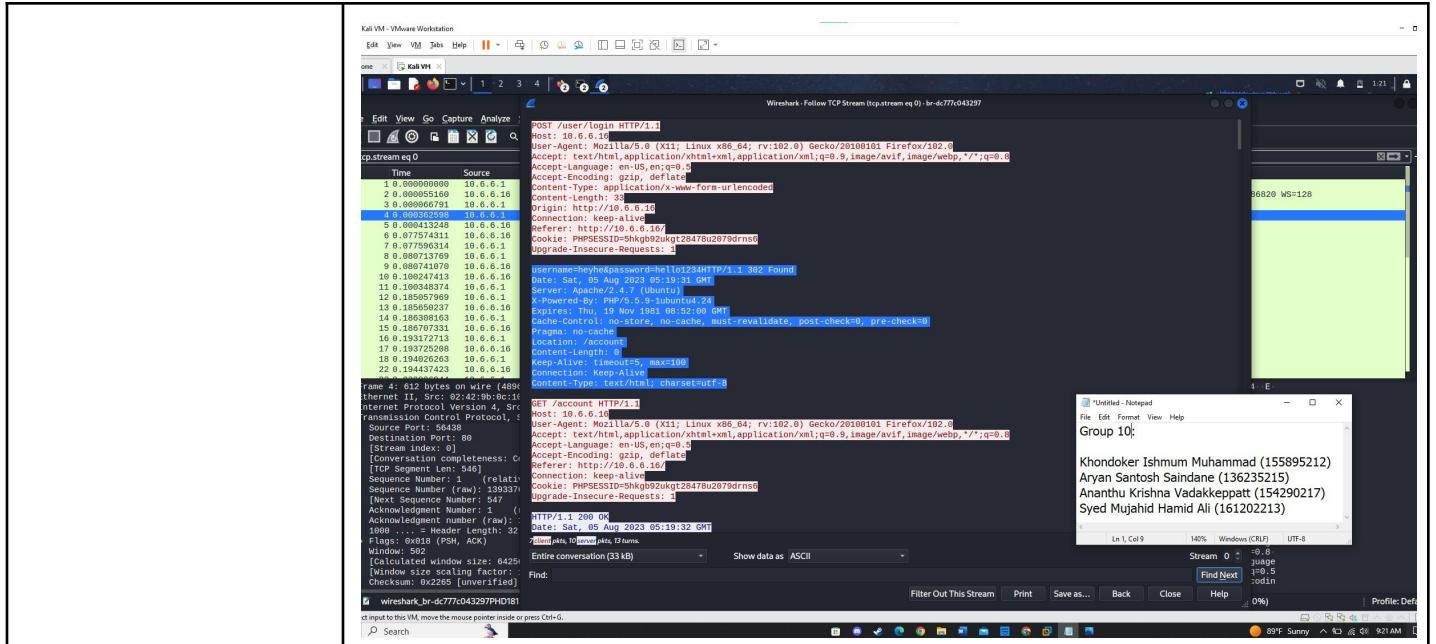
## Proof of Concept

Here we made use of a malicious query that bypasses the security measures and allowed us to login.

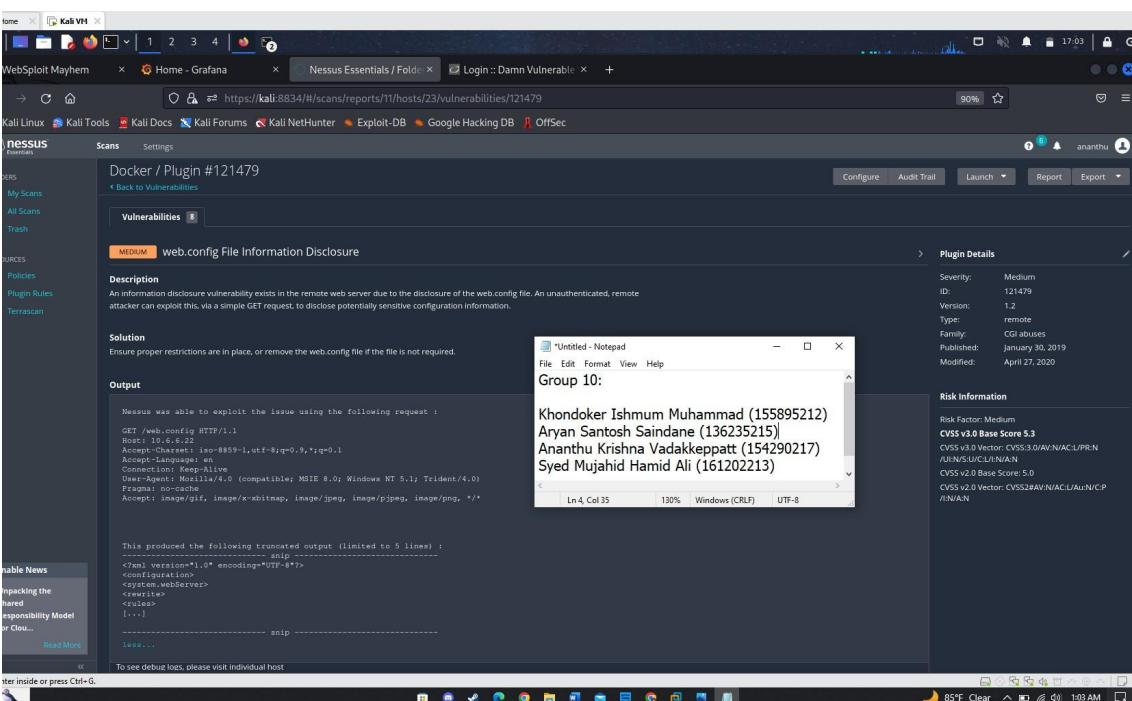


Patching	The usage of parameterized queries and proper statements, third party authentication, password hashing, updating and patching softwares are some of the ways we can make sure an attacker never gets the chance to exploit this vulnerability.
Reference	<a href="https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-sql-injection#:~:text=SQL%20Injection%20is%20a%20code,delete%20records%20in%20a%20database.">https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-sql-injection#:~:text=SQL%20Injection%20is%20a%20code,delete%20records%20in%20a%20database.</a>

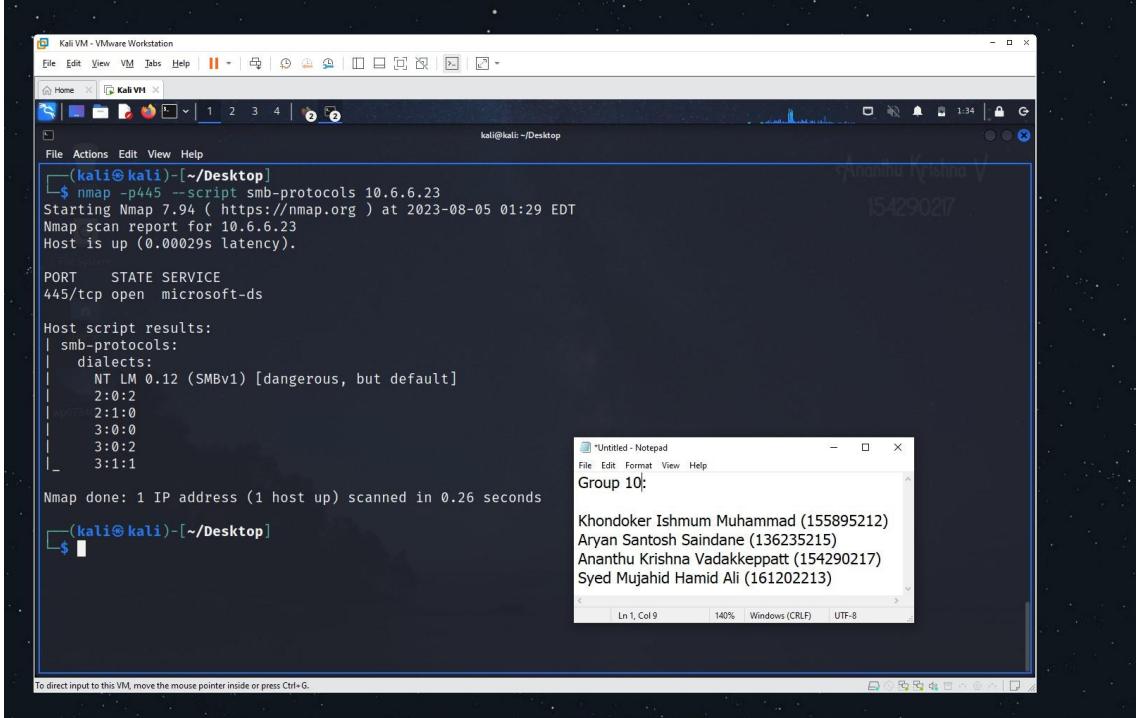
Websploit VM		
Low	V2 - Web Server Transmits Cleartext Credentials	
Risk Assessment	Impact: Low	Likelihood: Low
Description	The web traffic that is being transferred is not encrypted and is passed on to the remote web server. This could eventually result in exposing sensitive credentials as anyone who can intercept the traffic is able to see the data as it has not been encrypted.	
CVSS Score	2.6	
Affected Scope	10.6.6.16	
Proof of Concept	<p>Here we logged in with the details shown below and a simple wireshark scan that was started could pick up the data that was transferred.</p>  <p>The screenshot shows a Kali Linux desktop environment. A browser window is open at <a href="http://10.6.6.16/account#profile">http://10.6.6.16/account#profile</a>, displaying a 'My Account' page with user information: Username: heyhe, E-mail: heyhe@gmail.com, First Name: hello, Last Name: hey, and Phone: (empty). Below the form, a note states "Group 10:" followed by a list of names and IDs: Khondoker Ishnum Muhammad (155895212), Aryan Santosh Saindane (136235215), Ananthu Krishna Vadakkepatt (154290217), and Syed Mujahid Hamid Ali (161202213). A Notepad window titled 'Untitled - Notepad' is overlaid on the browser, containing the same list of names and IDs. The desktop taskbar at the bottom shows various application icons.</p>	

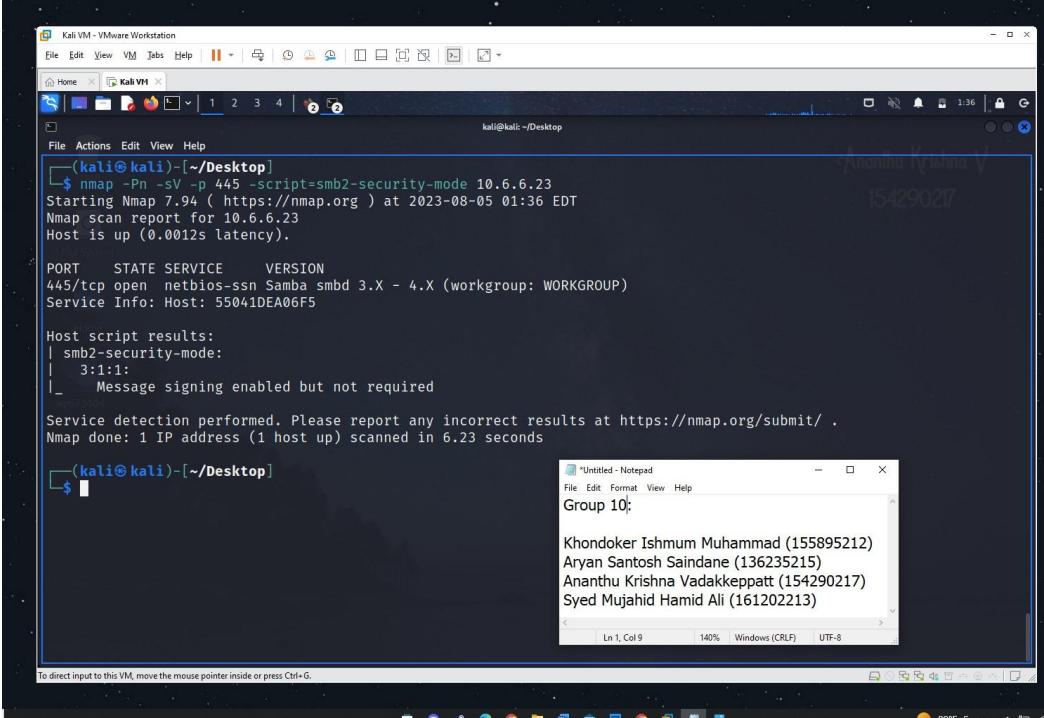
	
Patching	Applications should make use of SSL or TLS encryption techniques that would protect everything that is transferred from the client to the server. Thus, encrypting details from the client side will help us prevent an attacker from exploiting this vulnerability.
Reference	<a href="https://www.tenable.com/plugins/nessus/26194">https://www.tenable.com/plugins/nessus/26194</a>

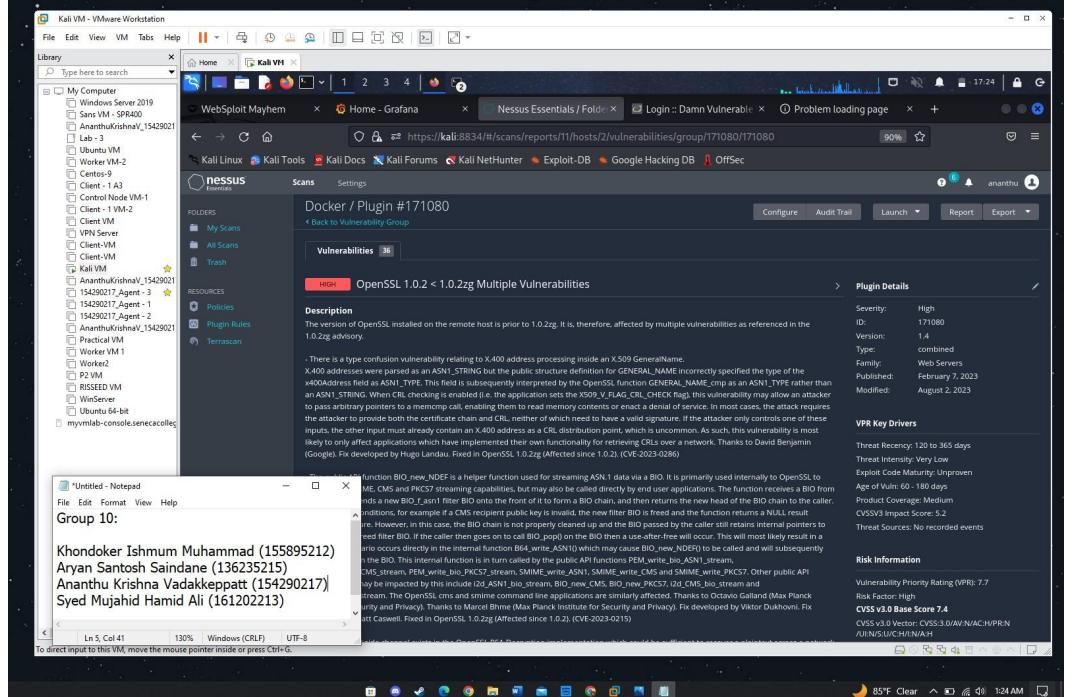
## Websploit VM

Medium	V3 - Web.config File Information Disclosure	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	In this vulnerability the remote web server is impacted by a security risk because of the disclosure of the web.config file. An attacker could take advantage of this vulnerability that would leak sensitive information related to the configuration settings of the system. This can be done by a simple GET request .	
CVSS Score	5.3	
Affected Scope	10.6.6.22	
Proof of Concept	We were able to find this vulnerability from the Nessus advanced scan we did run. Additionally, we also did confirm that this vulnerability existed by using the fuzzing technique.	
 <p>The screenshot shows a Kali Linux desktop environment. A browser window displays a Nessus scan report for Docker / Plugin #121479. The report details a 'web.config File Information Disclosure' vulnerability with a medium severity rating. It includes sections for Description, Solution, and Output, along with a note about exploitability via a simple GET request. To the right of the report, there is a Notepad window showing exploit code and a Risk Information panel.</p>		

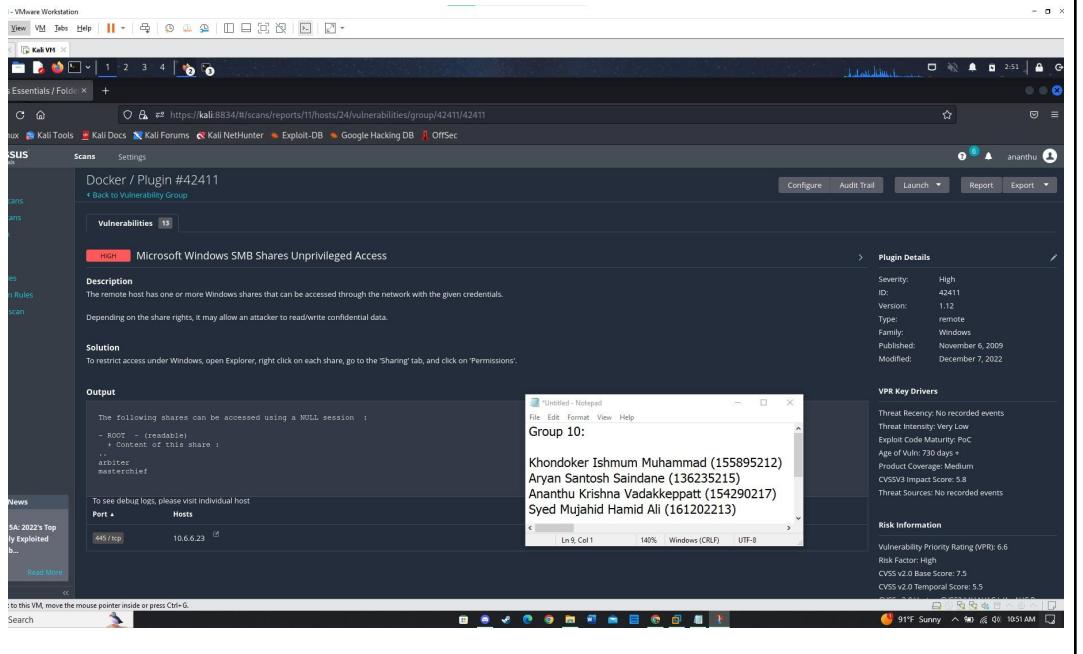
Patching	In order to patch this vulnerability, we would have to ensure that proper restrictions are placed on this configuration in such a way that it cannot be accessed by hosts outside the network. Another option would be to get rid of the file if there isn't a particular use for it.
Reference	<a href="https://www.tenable.com/plugins/nessus/121479">https://www.tenable.com/plugins/nessus/121479</a>

Websploit VM	
Medium	V4 - SMB Signing not required
Risk Assessment	Impact: Medium      Likelihood: Medium
Description	SMB is a service used for file sharing and other services. If attackers were able to get access to it, they would be able to direct man in the middle attacks that would intercept and modify the SMB traffic. They would have access to sensitive files that would allow them to inject malware that would perform other malicious activities on the infected system. This feature needs to be enabled because it makes sure that the attacks did not tamper with the smb packets. This can prevent MITM attacks.
CVSS Score	5.3
Affected Scope	10.6.6.23
Proof of Concept	<p>By running a couple of Nmap scans on the host, we were able to confirm that the SMB signing feature was enabled but wasn't necessary.</p>  <p>The terminal window shows the following Nmap command and output:</p> <pre>(kali㉿kali)-[~/Desktop] \$ nmap -p445 --script smb-protocols 10.6.6.23 Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-05 01:29 EDT Nmap scan report for 10.6.6.23 Host is up (0.00029s latency).  PORT      STATE SERVICE 445/tcp    open  microsoft-ds  Host script results:   smb-protocols:     dialects:       NT LM 0.12 (SMBv1) [dangerous, but default]         2.0:2         2.1:0         3.0:0         3.0:2         3.1:1  Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds (kali㉿kali)-[~/Desktop]</pre> <p>A separate Notepad window titled "Untitled - Notepad" contains a list of names and their corresponding IDs:</p> <pre>Khondoker Ishnum Muhammad (155895212) Aryan Santosh Saindane (136235215) Ananthu Krishna Vadakkepatt (154290217) Syed Mujahid Hamid Ali (161202213)</pre>

	 <p>The screenshot shows a terminal window running an nmap scan on port 445 of a host at 10.6.6.23. The output indicates that SMB security mode is enabled. Below the terminal is a Notepad window titled "Untitled - Notepad" containing a list of user accounts and their corresponding Windows IDs:</p> <pre> Group 10: Khondoker Ishmum Muhammad (155895212) Aryan Santosh Saindane (136235215) Ananthu Krishna Vadakkeppatt (154290217) Syed Mujahid Hamid Ali (161202213) </pre>
Patching	In order to make sure that this vulnerability is not made use of by any attacker, would have to enforce rules on the machine that makes sure that it only accepts digitally signed communications. This policy can be found in the Microsoft Network Server and would make sure that this vulnerability is mitigated.
Reference	<a href="http://www.nessus.org/u?df39b8b3">http://www.nessus.org/u?df39b8b3</a> <a href="http://technet.microsoft.com/en-us/library/cc731957.aspx">http://technet.microsoft.com/en-us/library/cc731957.aspx</a> <a href="http://www.nessus.org/u?74b80723">http://www.nessus.org/u?74b80723</a> <a href="https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html">https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html</a> <a href="http://www.nessus.org/u?a3cac4ea">http://www.nessus.org/u?a3cac4ea</a>

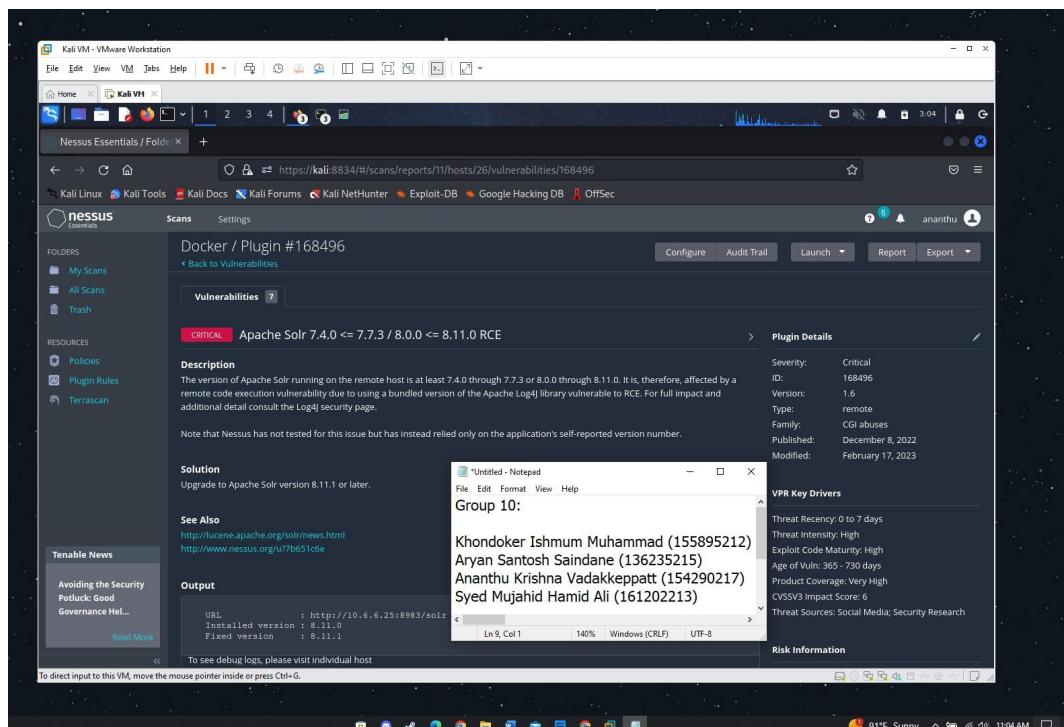
Websploit VM	
High	V5 - OpenSSL 1.02 < 1.0.2zg
Risk Assessment	Impact: High   Likelihood: High
Description	In this case, the machine is running an outdated version of OpenSSL that is prior to 1.02.zg which is why there are multiple vulnerabilities that are linked to it. This vulnerability could have numerous implications such as websites could suffer from data breaches, malware injections and so on.
CVSS Score	7.1
Affected Scope	10.6.6.1
Proof of Concept	<p>We were able to find this vulnerability from the advanced scans conducted by Nessus.</p> 
Patching	As the OpenSSL service has been outdated in this vulnerability, we'll have to make sure to keep it updated. This would ensure that we have dealt with this vulnerability and keep the machine safe from additional threats.

Reference	<a href="https://www.tenable.com/plugins/nessus/171080">https://www.tenable.com/plugins/nessus/171080</a>
-----------	---

Websploit VM		
High	V6 - Microsoft Windows SMB Shares Unprivileged Access	
Risk Assessment	Impact: Critical	Likelihood: High
Description	<p>Here, this host machine has multiple shares that are based on a network. This data can be accessed by anyone who has the credentials that can allow an attacker to read and write over the sensitive information.</p>	
CVSS Score	7.5	
Affected Scope	10.6.6.23	
Proof of Concept	<p>We detected this vulnerability from the advanced nessus scan that we had conducted. We also confirmed this using the help of the Nmap scan.</p> 	

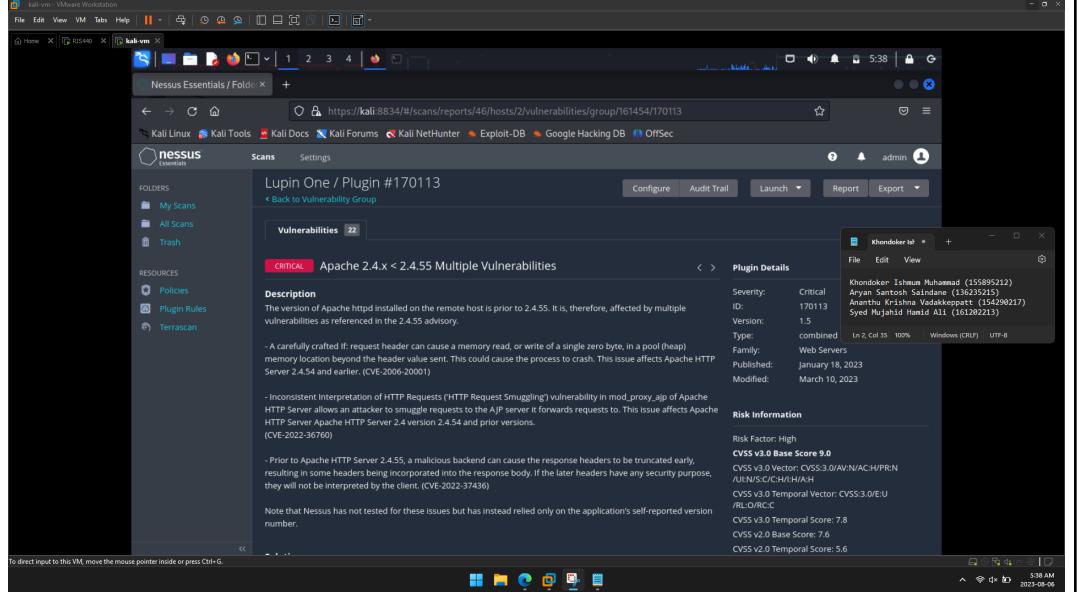
Patching	To make sure that this vulnerability does not resurface we would need to ensure that the permissions of each share under the sharing tab is set properly such that the security is tight.
Reference	<a href="https://www.tenable.com/plugins/nessus/42411">https://www.tenable.com/plugins/nessus/42411</a>

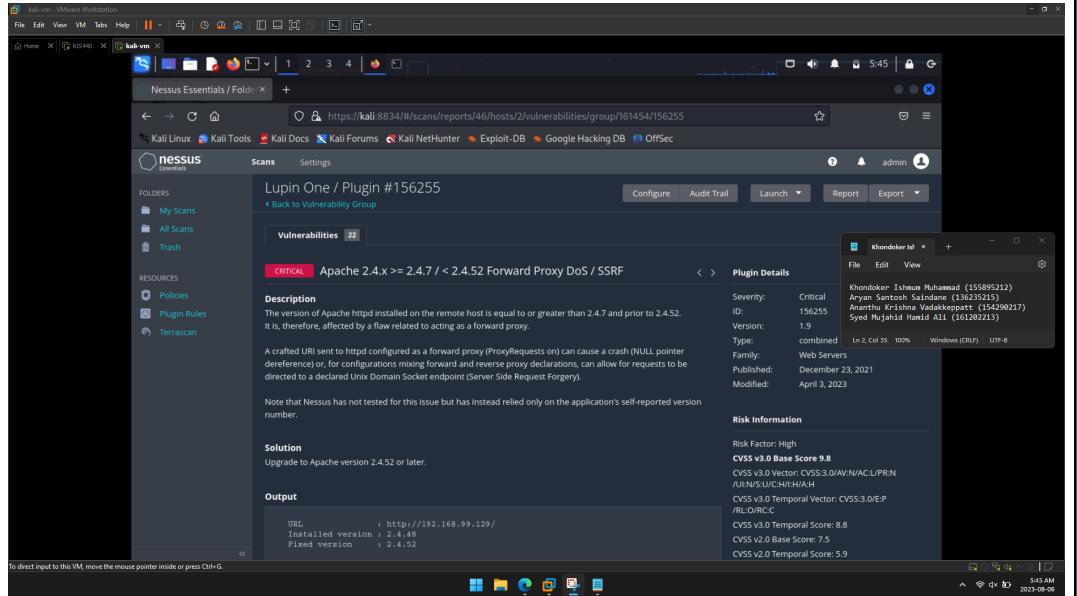
Lupin One VM		
High	V7 - Apache >= 2.4.17 < 2.4.49 mod_http2	
Risk Assessment	Impact: High	Likelihood: Medium
Description	The remote host has an Apache httpd version greater than 2.4.17 and before 2.4.49, which is vulnerable. The vulnerability allows a crafted HTTP/2 method to bypass validation and be forwarded by mod_proxy, potentially leading to request splitting or cache poisoning.	
CVSS Score	7.5	
Affected Scope	192.168.99.129	
Proof of Concept	We were able to find this vulnerability from the advanced scans conducted by Nessus.	
Patching	To patch it, we would simply need to update the Apache service running on Lupin One to version 2.4.49 or later.	
Reference	<a href="https://www.tenable.com/plugins/nessus/153585">https://www.tenable.com/plugins/nessus/153585</a>	

Websploit VM		
Critical	V8 - Apache Solr 7.4.0 <= 7.7.3 / 8.0.0 <= 8.11.0 RCE	
Risk Assessment	Impact: Critical	Likelihood: High
Description	<p>This vulnerability occurs as the Apache Solr version is outdated. It is therefore affected by a remote code execution vulnerability because of the bundled version of Apache Log4J library that is vulnerable to RCE.</p>	
CVSS Score	9.3	
Affected Scope	10.6.6.25	
Proof of Concept	<p>We were able to identify this vulnerability from the scans, also confirmed the host was running the service using nmap and finally verified that the host is running an outdated version of Apache Solr.</p> 	

	<pre>(kali㉿kali)-[~] \$ nmap -T4 -A -p 10.6.6.25 Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-05 03:05 EDT Nmap scan report for 10.6.6.25 Host is up (0.00013s latency). Not shown: 65534 closed tcp ports (conn-refused) PORT      STATE SERVICE VERSION 8983/tcp  open  http    Apache Solr   http-title: Solr Admin  _Requested resource was http://10.6.6.25:8983/solr/ Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds</pre>
	<p>The screenshot shows the Apache Solr dashboard at <a href="http://10.6.6.25:8983/solr/">10.6.6.25:8983/solr/</a>. The interface includes sections for Instance, Versions, and JVM. The JVM section displays the following configuration:</p> <pre>JVM Runtime Oracle Corporation OpenJDK 64-Bit Server VM 18.0.1_25.25-b14 Processors 4 Args -DSTOP KEY=solrrocks -DSTOP PORT=7983 -Djetty.home=/opt/solr/server -Djetty.port=8983 -Dsolr.data.home= -Dsolr.default.configdir=/opt/solr/server/solr/configsets/_default/conf -Dsolr.install.dir=/opt/solr -Dsolr.jetty.inetaccess.excludes= -Dsolr.jetty.inetaccess.includes=</pre>
Patching	The only way to make sure that we counter this vulnerability is to keep the Apache Solr version up to date with the latest updates and patches.

Reference	<a href="https://www.tenable.com/plugins/nessus/168496">https://www.tenable.com/plugins/nessus/168496</a>
-----------	---

Lupin One VM		
Critical	V9 - Apache 2.4.x < 2.4.55	
Risk Assessment	Impact: Critical	Likelihood: High
Description	<p>Multiple vulnerabilities can affect this machine, as it has an Apache installed whose version is prior to 2.4.55. An If: request header can cause a crash by reading or writing a single zero byte in a pool (heap) memory location beyond the header value sent.</p> <p>There is a vulnerability in mod_proxy_ajp that allows an attacker to smuggle requests to the AJP server it forwards requests to, due to inconsistent interpretation of HTTP requests.</p>	
CVSS Score	9.0	
Affected Scope	192.168.99.129	
Proof of Concept	<p>We were able to find this vulnerability from the advanced scans conducted by Nessus.</p>  <p>The screenshot shows the Nessus application window. The main pane displays the details of a critical vulnerability for Apache 2.4.x &lt; 2.4.55. The description states that the Apache httpd installed on the remote host is prior to 2.4.55, making it vulnerable to multiple issues. It mentions CVE-2006-20001 and CVE-2022-37430. The right pane shows the plugin details, including the author (Khondaker Ishamul Haque), severity (Critical), ID (170113), version (1.5), type (combined), family (Web Servers), and risk information. The risk factor is listed as High, with a CVSS v3.0 Base Score of 9.0.</p>	
Patching	To patch it, we would need to update the Apache service running on Lupin One to version 2.4.55 or later.	
Reference	<a href="https://www.tenable.com/plugins/nessus/170113">https://www.tenable.com/plugins/nessus/170113</a>	

Lupin One VM		
Critical	V10 - Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	
Risk Assessment	Impact: Critical	Likelihood: High
Description	<p>The remote host has an Apache httpd server version equal to or greater than 2.4.7 and prior to 2.4.52. It is vulnerable to a flaw related to acting as a forward proxy. A specially crafted URI sent to the server, when configured as a forward proxy (ProxyRequests on), can lead to a crash (NULL pointer dereference) or allow requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).</p>	
CVSS Score	9.8	
Affected Scope	192.168.99.129	
Proof of Concept	<p>We were able to find this vulnerability from the advanced scans conducted by Nessus.</p>  <p>The screenshot shows the Nessus interface with the following details:</p> <ul style="list-style-type: none"> <li><b>Scan Name:</b> Lupin One / Plugin #156255</li> <li><b>Vulnerabilities:</b> 22 (CRITICAL)</li> <li><b>Description:</b> Apache 2.4.x &gt;= 2.4.7 / &lt; 2.4.52 Forward Proxy DoS / SSRF. The description states that the version of Apache httpd installed on the remote host is equal to or greater than 2.4.7 and prior to 2.4.52. It is, therefore, affected by a flaw related to acting as a forward proxy. A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).</li> <li><b>Solution:</b> Upgrade to Apache version 2.4.52 or later.</li> <li><b>Output:</b> URL: http://192.168.99.129/. Installed Version: 2.4.46. Fixed Version: 2.4.52.</li> <li><b>Plugin Details:</b> <ul style="list-style-type: none"> <li>Severity: Critical</li> <li>ID: 156255</li> <li>Version: 1.9</li> <li>Type: combined</li> <li>Family: Web Servers</li> <li>Published: December 23, 2021</li> <li>Modified: April 3, 2023</li> </ul> </li> <li><b>Risk Information:</b> <ul style="list-style-type: none"> <li>Risk Factor: High</li> <li>CVSS v3.0 Base Score: 9.8</li> <li>CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:U/PR:N/UF:N/S:U/C:H/I:H/A:H</li> <li>CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/R:LC/R:CC</li> <li>CVSS v2.0 Base Score: 8.8</li> <li>CVSS v2.0 Score: 7.5</li> <li>CVSS v2.0 Temporal Score: 5.9</li> </ul> </li> </ul>	
Patching	To patch it, we would need to update the Apache service running on Lupin One to version 2.4.52 or later.	
Reference	<a href="https://www.tenable.com/plugins/nessus/156255">https://www.tenable.com/plugins/nessus/156255</a>	

## **Conclusion**

---

In conclusion, this report helped us figure out all the vulnerabilities while performing scans on the home network devices. There were a plethora of vulnerabilities in the Virtual Machines ranging from low to critical.

The present state of the devices exposes the organization to multiple security risks. The maintainer must prioritize the immediate analysis and Patching of the critical vulnerabilities outlined in the main report.

The urgency of addressing these vulnerabilities cannot be overstated. To mitigate the risks effectively, the maintainer must conduct a thorough analysis of each vulnerability's impact on the devices and the broader network infrastructure. Immediate Patching actions should be planned and executed to reduce the attack surface and enhance the overall security posture.

Taking prompt action to address these issues will enhance the devices' resilience against cyber threats and safeguard the organization's assets and reputation.