

Vulnerability and Threat Analysis

RIS430 NAA

Group Project

Vulnerability Assessment Report

Prepared By Group 10,

Khondoker Ishmum Muhammad (155895212)

Aryan Santosh Saindane (136235215)

Ananthu Krishna Vadakkeppatt (154290217)

Syed Mujahid Hamid Ali (161202213)

Assignment 5.....	00
Vulnerability Assessment Report.....	00
 Executive Summary.....	03
 Scope Of Engagement.....	04
 Vulnerability Assessment Methodology.....	12
 Risk Assessment Methodology Reflection Report.....	13
 Vulnerability Assessment And Patching Report.....	14
Conclusion.....	36

Executive Summary

In this report, we will be assessing vulnerabilities found while attempting scans on the home network devices. This assessment was done between August 8th 2023 and 13th August 2023 in Toronto, Canada. We have made use of two LAN segments that are 192.168.110.0 /24 and 192.168.99.0/24. 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.

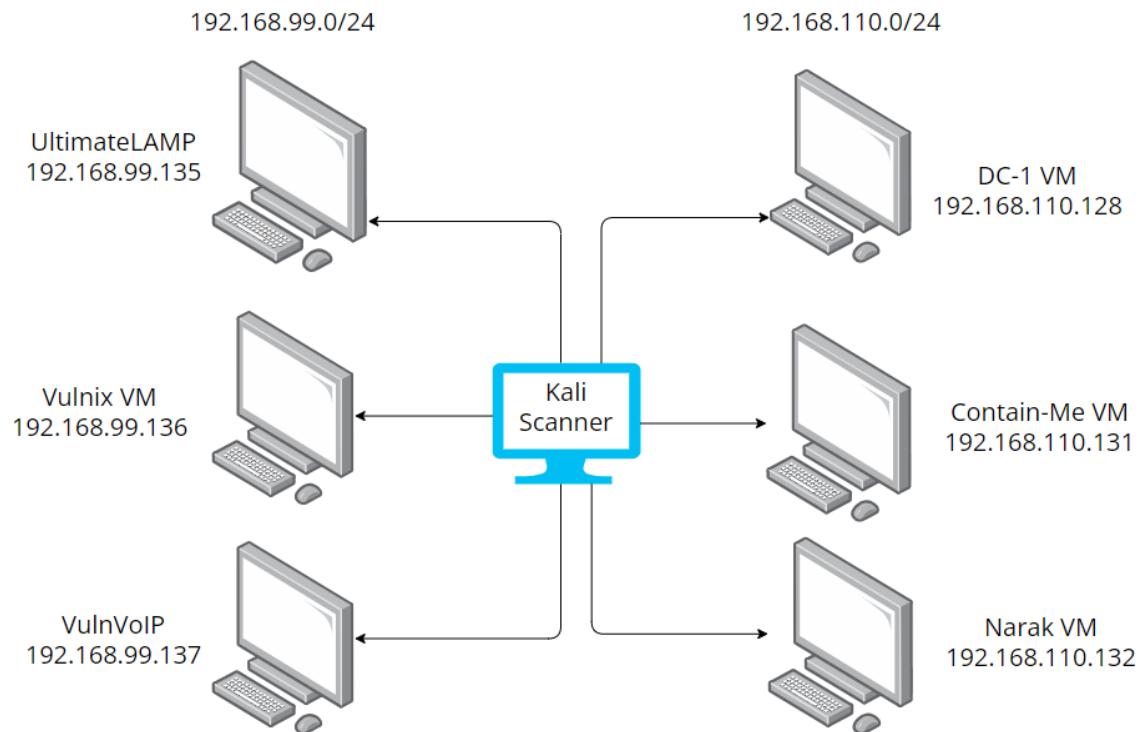
Across the whole assessment, we analyzed a lot of vulnerabilities which will be elaborated in the report ahead. Moreover, students from our group have only performed scans on local networks.

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	192.168.110.	255.255.255.0 - /24	Scanner to find vulnerabilities in the network infrastructure.
DC-1 VM	Vulnerable virtual machine	192.168.110.128	255.255.255.0 - /24	Acts as a victim that has a lot of vulnerable services running in the machine.
Contain-Me	Vulnerable virtual machine	192.168.110.131.	255.255.255.0 - /24	Acts as a victim that has a lot of vulnerable services running in the machine.
Narak	Vulnerable Virtual machine	192.168.110.132	255.255.255.0 - /24	Acts as a victim that has a lot of vulnerable services running in the machine.
UltimateLAMP	Vulnerable Virtual Machine	192.168.99.35	255.255.255.0 - /24	Acts as a victim that has a lot of vulnerable services running in the machine.
Vulnix VM	Vulnerable Virtual Machine	192.168.99.36	255.255.255.0/4	Acts as a victim that has a lot of vulnerable services running in the machine.
VulnVoIP	Vulnerable Virtual Machine	192.168.99.37	255.255.255.0/4	Acts as a victim that has a lot of vulnerable services running in the machine.

Important Notes

We have used two VLANS in this assignment. One has the network 192.168.110.0/24 and the other is 192.168.99.0/24.

The first network has the vulnerable VM's DC-1, Contain-me and Narak. The second network has the virtual machines UltimateLAMP, Vulnix VM and VulnVoIP,

Network Host Discovery

This screenshot shows a Kali Linux desktop environment with multiple windows open. In the foreground, a Mozilla Firefox browser window displays the Nessus Essentials interface at <https://kali:8834/#/scans/reports/17/hosts>. The main page shows 'Host Discovery' results for a scan with 6 hosts. One host entry is expanded, showing details for 'Group 10' and several discovered users: Khondoker Ishmmu Muhammad (155895212), Aryan Santosh Saindane (136235215), Ananthu Krishna Vadakeppatt (154290217), and Syed Mujahid Hamid Ali (161202213). To the right of the host list is a 'Scan Details' panel and a 'Vulnerabilities' section with a donut chart. On the left, there's a sidebar with 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. A news feed on the left sidebar mentions 'Cross-Site Scripting in Microsoft Teams via Dynam...'. The desktop taskbar at the bottom shows various application icons.

This screenshot shows a Kali Linux virtual machine running in VMware Workstation. The host machine's desktop is visible in the background, showing a similar Nessus Essentials interface. The VM's desktop shows a Mozilla Firefox browser window displaying the Nessus Essentials interface at <https://kali:8834/#/scans/reports/76/hosts>. The main page shows 'Host Discovery' results for a scan with 6 hosts. One host entry is expanded, showing details for 'Group 10' and several discovered users: Khondoker Ishmmu Muhammad (155895212), Aryan Santosh Saindane (136235215), Ananthu Krishna Vadakeppatt (154290217), and Syed Mujahid Hamid Ali (161202213). To the right of the host list is a 'Scan Details' panel and a 'Vulnerabilities' section with a donut chart. On the left, there's a sidebar with 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. The desktop taskbar at the bottom shows various application icons.

Nessus Scans

The screenshot displays the Nessus Essentials interface in a Mozilla Firefox browser. The main window shows a list of 'My Scans' with four entries:

Name	Schedule	Last Scanned
Host Discovery	On Demand	Today at 9:03 AM
Narak	On Demand	Today at 6:58 AM
Contain-Me	On Demand	Today at 4:43 AM
DC-1	On Demand	August 12 at 9:16 AM

A Notepad window is open, displaying a list of scanned hosts under 'Group 10':

```
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkepatt (154290217)
Syed Mujahid Hamid Ali (161202213)
```

The bottom part of the screenshot shows a VMware Workstation interface with a Kali Linux VM running. The taskbar shows various application icons, and the system tray indicates it's 9:05 AM, sunny, and 96°F.

Nmap scan report for 192.168.110.128

Host is up (pingable).

Scanning completed at 2023-08-12 09:16 (ET) (0:00:07 elapsed)

OS: Linux Kernel 3.2 on Debian 7.0 (wheezy)

Ports: 22/tcp open ssh

Vulnerabilities: 30

Severity	CVSS	VPR	Name	Family	Count
Critical	10.0		Unix Operating System Unsupported Version Detection	General	1
Mixed	PHP (Multiple Issues)	CGI abuses	3
Mixed	Drupal (Multiple Issues)	CGI abuses	2
Medium	6.1	5.7	jQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	1
Medium	5.3		web.config File Information Disclosure	CGI abuses	1
Mixed	SSH (Multiple Issues)	Misc.	6
Info	Apache HTTP Server (Multiple Issues)	Web Servers	2
Info	HTTP (Multiple Issues)	Web Servers	2
Info	RPC (Multiple Issues)	RPC	2
Info	SSH (Multiple Issues)	General	2
Info	SSH (Multiple Issues)	Service detection	2

Host Details:

- IP: 192.168.110.128
- MAC: 00:0C:29:ED:AC:79
- OS: Linux Kernel 3.2 on Debian 7.0 (wheezy)
- Start: August 12 at 9:09 AM
- End: August 12 at 9:16 AM
- Elapsed: 7 minutes
- KB: Download

Vulnerabilities:

Nmap scan report for 192.168.110.132

Host is up (pingable).

Scanning completed at 2023-08-12 09:16 (ET) (0:00:07 elapsed)

OS: Linux Kernel 4.15 on Ubuntu 18.04 (bionic)

Ports: 22/tcp open ssh

Vulnerabilities: 20

Severity	CVSS	VPR	Name	Family	Count
Info	HTTP (Multiple Issues)	Web Servers	3
Info	SSH (Multiple Issues)	Misc.	2
Info	SSH (Multiple Issues)	Service detection	2
Info			Nessus SYN scanner	Port scanners	2
Info			Service Detection	Service detection	2
Info			Apache HTTP Server Version	Web Servers	1
Info			Backported Security Patch Detection (WWW)	General	1
Info			Common Platform Enumeration (CPE)	General	1
Info			Device Type	General	1
Info			Ethernet Card Manufacturer Detection	Misc.	1
Info			Ethernet MAC Addresses	General	1

Host Details:

- IP: 192.168.110.132
- MAC: 00:0C:29:9B:54:B5
- OS: Linux Kernel 4.15 on Ubuntu 18.04 (bionic)
- Start: Today at 6:51 AM
- End: Today at 6:58 AM
- Elapsed: 7 minutes
- KB: Download

Vulnerabilities:

Nessus Essentials / Folders / View Scan — Mozilla Firefox

https://kali:8834/#/scans/reports/8/hosts/2/vulnerabilities

Contain-Me / 192.168.110.131

Vulnerabilities 20

Group 10:

Severity	CVSS	VPR	Name	Family	Count	Action
INFO	SSH (Multiple Issues)	Misc.	4	○
INFO	SSH (Multiple Issues)	Service detection	4	○
INFO	HTTP (Multiple Issues)	Web Servers	3	○
INFO			Nessus SYN scanner	Port scanners	4	○
INFO			Service Detection	Service detection	3	○
INFO			SSH Protocol Versions Supported	General	2	○
INFO			Apache HTTP Server Version	Web Servers	1	○
INFO			Backported Security Patch Detection (WWW)	General	1	○
INFO			Common Platform Enumeration (CPE)	General	1	○
INFO			Device Type	General	1	○
INFO			Ethernet Card Manufacturer Detection	Misc.	1	○

Host Details

- IP: 192.168.110.131
- MAC: 00:0C:29:8D:8B:B8
- OS: Linux Kernel 4.15 on Ubuntu 18.04 (bionic)
- Start: Today at 4:35 AM
- End: Today at 4:43 AM
- Elapsed: 8 minutes
- KB: Download

Vulnerabilities

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Nessus Essentials / Folders / View Scan — Mozilla Firefox

https://kali:8834/#/scans/reports/61/hosts/2/vulnerabilities

UltimateLAMP / 192.168.99.135

Vulnerabilities 18

Khondoker Ishmu... (155895212)

Severity	CVSS	VPR	Name	Family	Count	Action
Critical	10.0		Unix Operating System Unsupported Version Detection	General	1	○
Mixed	HTTP (Multiple Issues)	Web Servers	4	○
Mixed	Apache HTTP Server (Multiple Issues)	Web Servers	3	○
Info	PHP (Multiple Issues)	Web Servers	2	○
Info			Backported Security Patch Detection (WWW)	General	1	○
Info			Common Platform Enumeration (CPE)	General	1	○
Info			Device Type	General	1	○
Info			Drupal Software Detection	CGI abuses	1	○
Info			Ethernet Card Manufacturer Detection	Misc.	1	○
Info			Ethernet MAC Addresses	General	1	○
Info			ICMP Timestamp Request Remote Date Disclosure	General	1	○

Host Details

- IP: 192.168.99.135
- Mac: 00:0C:29:82:7F:24
- OS: Linux Kernel 2.6 on Ubuntu 5.10 (breezy)
- Start: August 12 at 5:27 AM
- End: August 12 at 5:43 AM
- Elapsed: 16 minutes
- KB: Download

Vulnerabilities

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Kali-vm - VMware Workstation

File Edit View VM Tabs Help

Vulnix 192.168.99.136

Scans Settings

Vulnerabilities 38

Filter Search Vulnerabilities 38 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	Actions
Critical	10.0 *		NFS Exported Share Information Disclosure	RPC	1	○ ⚒
Critical	10.0		Unix Operating System Unsupported Version Detection	General	1	○ ⚒
Critical	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	○ ⚒
High	7.5		NFS Shares World Readable	RPC	1	○ ⚒
Mixed	SSL (Multiple Issues)	General	37	○ ⚒
Mixed	OpenSSL (Multiple Issues)	Misc.	10	○ ⚒
Mixed	IETF Md5 (Multiple Issues)	General	9	○ ⚒
Medium	5.0 *		Finger Service Remote Information Disclosure	Misc.	1	○ ⚒
Mixed	TLS (Multiple Issues)	Service detection	8	○ ⚒
Mixed	SSH (Multiple Issues)	Misc.	6	○ ⚒
Info	TLS (Multiple Issues)	General	7	○ ⚒

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Host Details

- IP: 192.168.99.136
- Mac: 00:0C:29:B7:B1:A5
- OS: Linux Kernel 3.0 on Ubuntu 12.04 (precise)
- Start: August 12 at 5:52 AM
- End: August 12 at 6:31 AM
- Elapsed: 40 minutes
- KB: Download

Vulnerabilities

9:19 AM 2023-08-13

Kali-vm - VMware Workstation

File Edit View VM Tabs Help

VulnVoIP 192.168.99.137

Scans Settings

Vulnerabilities 19

Filter Search Vulnerabilities 19 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	Actions
Mixed	SSH (Multiple Issues)	Misc.	6	○ ⚒
Info	RPC (Multiple Issues)	RPC	2	○ ⚒
Info	SSH (Multiple Issues)	General	2	○ ⚒
Info	SSH (Multiple Issues)	Service detection	2	○ ⚒
Info			RPC Services Enumeration	Service detection	4	○ ⚒
Info			Nessus SYN scanner	Port scanners	3	○ ⚒
Info			Common Platform Enumeration (CPE)	General	1	○ ⚒
Info			Device Type	General	1	○ ⚒
Info			Ethernet Card Manufacturer Detection	Misc.	1	○ ⚒
Info			Ethernet MAC Addresses	General	1	○ ⚒
Info			ICMP Timestamp Request Remote Date Disclosure	General	1	○ ⚒

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Host Details

- IP: 192.168.99.137
- Mac: 00:0C:29:2A:BB:C9
- OS: Linux Kernel 2.6
- Start: August 12 at 6:46 AM
- End: August 12 at 6:51 AM
- Elapsed: 5 minutes
- KB: Download

Vulnerabilities

9:19 AM 2023-08-13

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, netdiscover and Nessus . Nmap firstly was used to run a simple scan across the network of the vulnerable machine so as to get an idea of the open ports and services that 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. We then made a patchin report that gives you a brief overview of how these vulnerabilities can be patched in such a way that there are no loopholes that an attacker could possibly exploit.

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.

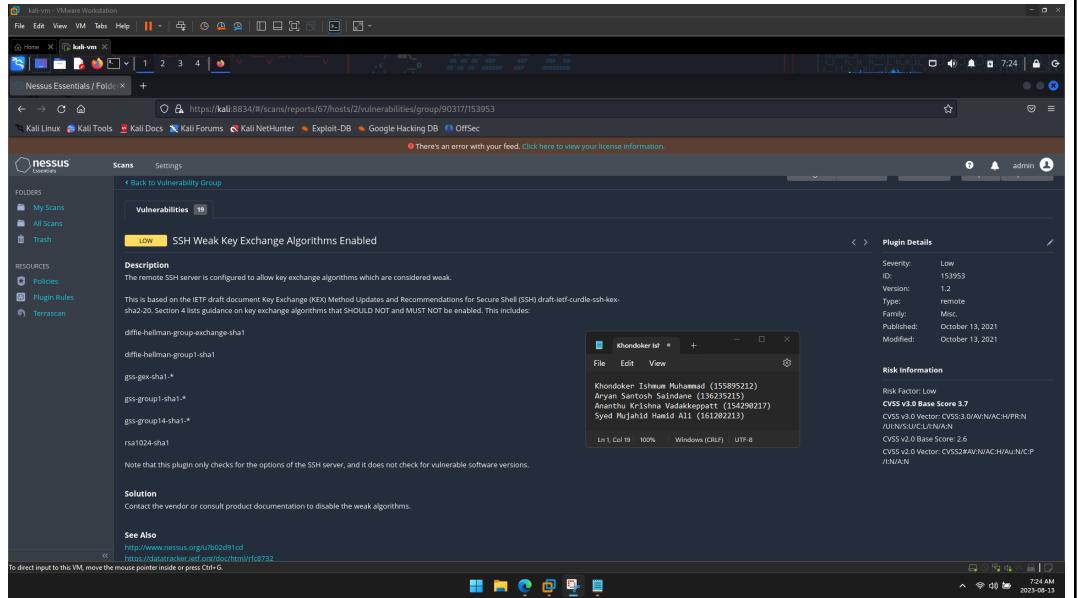
Likelihood	Info	Low	Medium	High	Critical
Critical	Info	Low	Medium	High	Critical
High	Info	Low	Medium	High	Critical
Medium	Info	Low	Medium	Medium	High
Low	Info	Low	Low	Low	Medium
Info	Info	Info	Info	Low	Low

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	VulnVoIP VM	SSH Weak Key Exchange Algorithms Enabled	Low
V2	Vulnix VM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Low
V3	Vulnix VM	SSH Weak Key Exchange Algorithms Enabled	Low
V4	DC-1 VM	SSH Server CBC Mode Ciphers Enabled	Low
V5	DC-1 VM	SSH Weak MAC Algorithms Enabled	Low
V6	UltimateLAMP VM	HTTP TRACE / TRACK Methods Allowed	Medium
V7	Vulnix VM	SSL Certificate Cannot Be Trusted	Medium
V8	VulnVoIP VM	SSH Weak Algorithms Supported	Medium
V9	DC-1 VM	JQuery 1.2 < 3.5.0 Multiple XSS	Medium
V10	DC-1 VM	web.config File Information Disclosure	Medium
V11	Vulnix VM	NFS Shares World Readable	High
V12	Vulnix VM	SSL Medium Strength Cipher Suites Supported (SWEET32)	High
V13	Vulnix VM	OpenSSL Heartbeat Information Disclosure (Heartbleed)	High
V14	DC-1	PHP < 7.3.24 Multiple Vulnerabilities	High

V15	DC-1	Drupal Database Abstraction API SQLi	High
V16	UltimateLAMP VM	Unix Operating System Unsupported Version Detection	Critical
V17	Vulnix VM	SSL Version 2 and 3 Protocol Detection	Critical
V18	Vulnix VM	NFS Exported Share Information Disclosure	Critical
V19	DC-1 VM	Unix Operating System Unsupported Version Detection	Critical
V20	DC-1 VM	PHP Unsupported Version Detection	Critical

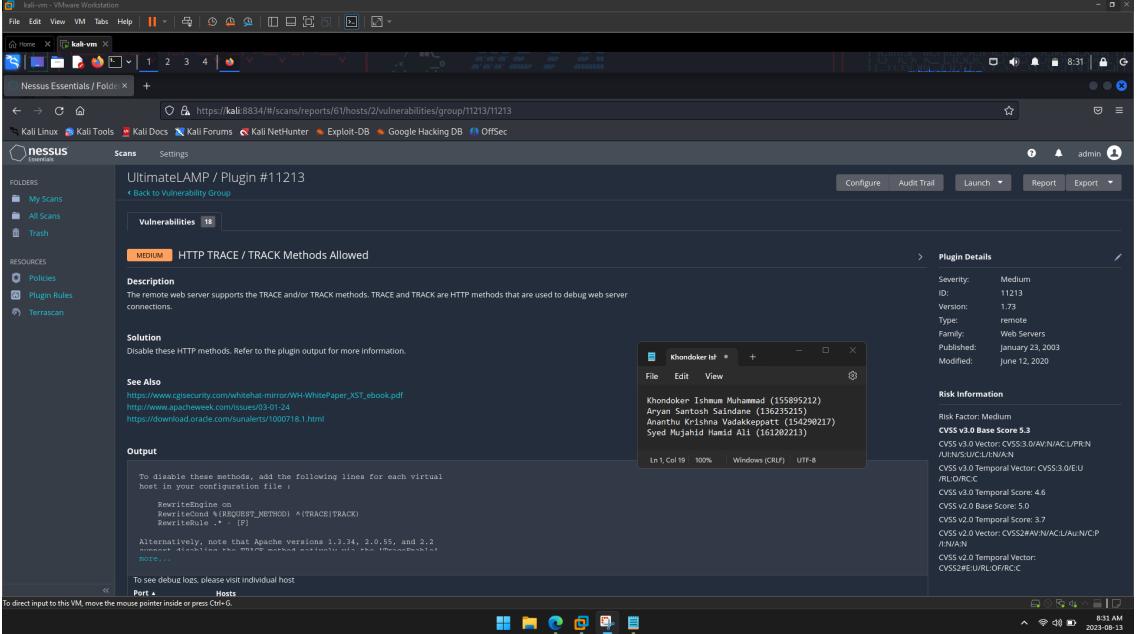
VulnVoIP VM		
Low	V1 - SSH Weak Key Exchange Algorithms Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	<p>The remote SSH server allows weak key exchange algorithms as mentioned in the IETF draft document "Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)." The document provides guidance on which key exchange algorithms should not be enabled. The algorithms listed in Section 4 that should not be used include:</p> <ul style="list-style-type: none"> • Diffie-hellman-group-exchange-sha1 • Diffie-hellman-group1-sha1 • gss-gex-sha1-* • gss-group1-sha1-* • gss-group14-sha1-* • rsa1024-sha1 	
CVSS Score	3.7	
Affected Scope	192.168.99.137	
Proof of Concept	<p>We were able to get information about this Vulnerability from a Nessus scan on the host.</p> 	
Reference	https://www.tenable.com/plugins/nessus/153953	

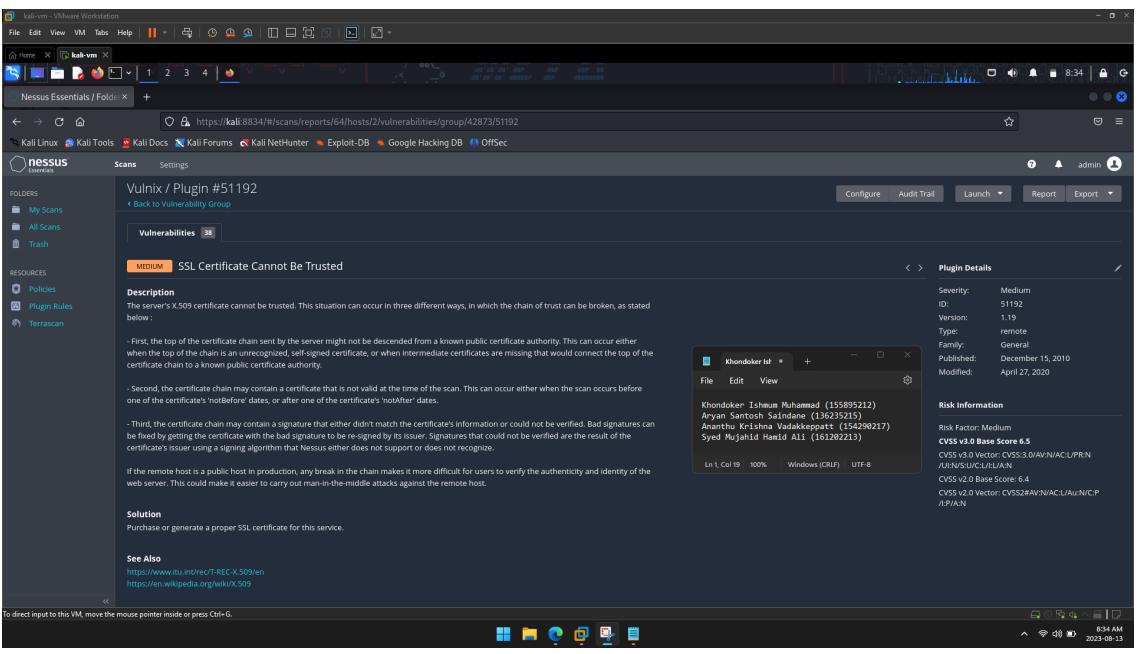
Vulnix VM	
Low	V2 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Risk Assessment	Impact: Low Likelihood: Medium
Description	<p>The remote host has a vulnerability called POODLE, which is a man-in-the-middle information disclosure issue. This vulnerability exists in SSL 3.0 due to how it handles padding during message decryption with block ciphers in cipher block chaining (CBC) mode. Attackers could exploit this to decrypt a specific byte of cipher text in about 256 attempts, given they make a victim application repeatedly send the same data over new SSL 3.0 connections.</p> <p>Even if both a client and a service support newer TLS versions, a connection can be downgraded to SSL 3.0. The TLS Fallback SCSV mechanism can prevent version rollback attacks, but only if both the client and service support it. Sites still using SSLv3 are recommended to enable this mechanism. This vulnerability is inherent to the SSLv3 specification itself, not any specific SSL implementation. To fully mitigate this vulnerability, SSLv3 should be disabled.</p>
CVSS Score	3.4
Affected Scope	192.168.99.136
Proof of Concept	<p>We were able to know about this vulnerability through a Nessus scan on the host.</p>
Reference	https://www.tenable.com/plugins/nessus/78479

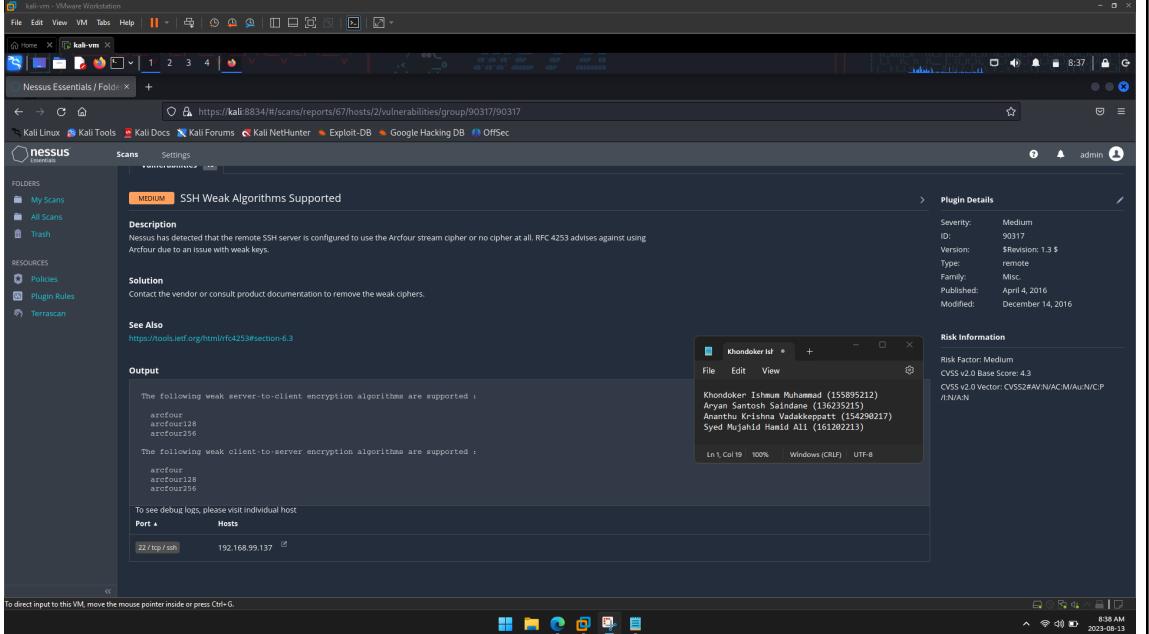
Vulnix VM		
Low	V3 - SSH Weak Key Exchange Algorithms Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	<p>The remote SSH server has been set up with key exchange algorithms that are considered weak according to the IETF draft document "Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)". This document, specifically in Section 4, provides recommendations on which key exchange algorithms should not be enabled. The list includes algorithms like diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, gss-gex-sha1-, gss-group1-sha1-, gss-group14-sha1-*, and rsa1024-sha1. These algorithms are discouraged due to their vulnerability and lack of security.</p>	
CVSS Score	3.7	
Affected Scope	192.168.99.136	
Proof of Concept	<p>We were able to know about this vulnerability through a Nessus scan.</p>	
Reference	https://www.tenable.com/plugins/nessus/153953	

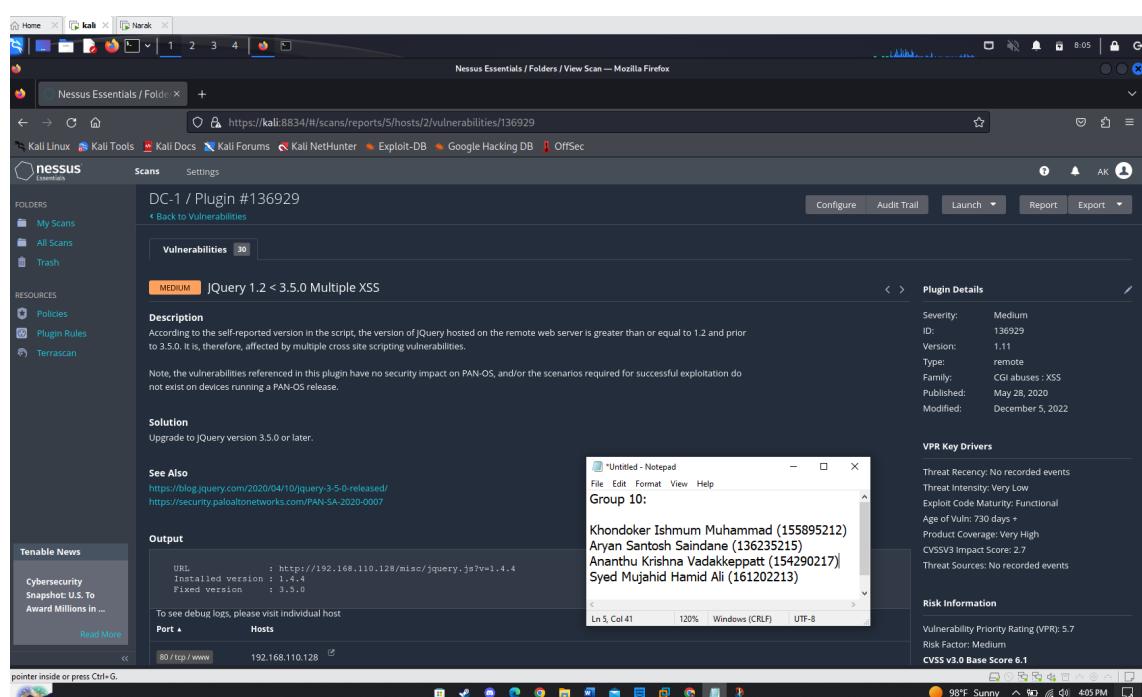
DC-1 VM		
Low	V4 - SSH Server CBC Mode Ciphers Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	<p>The SSH server in question has been set up to use Cipher Block Chaining (CBC) encryption. CBC is a method of encryption that can be susceptible to certain types of attacks, potentially allowing an attacker to retrieve the original plaintext message from the encrypted ciphertext. It's worth noting that this warning is related to the encryption configuration itself and doesn't specifically assess the presence of software vulnerabilities. As a result, there might be a risk associated with using CBC encryption in this SSH server configuration.</p>	
CVSS Score	2.6	
Affected Scope	192.168.110.	
Proof of Concept		
Reference	https://www.tenable.com/plugins/nessus/70658	

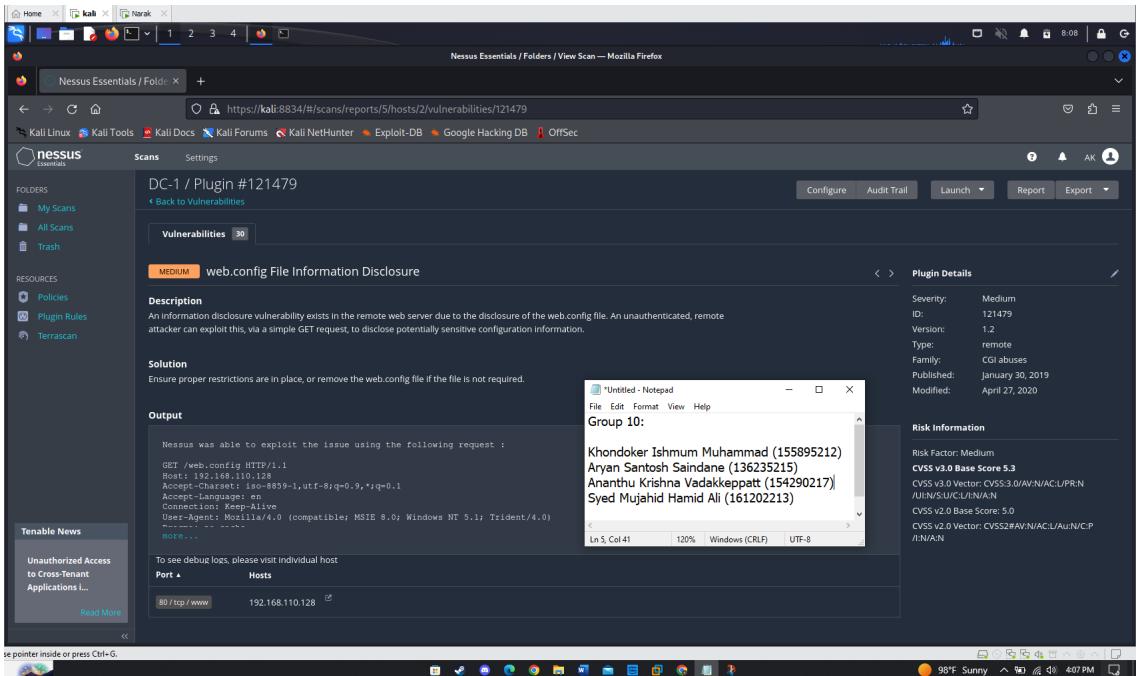
DC-1 VM		
Low	V5 - SSH Weak MAC Algorithms Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	<p>The remote SSH server is set up to permit the use of either MD5 or 96-bit MAC (Message Authentication Code) algorithms. Both of these options are considered weak from a security standpoint. This weakness stems from the vulnerabilities associated with MD5 and short MAC lengths, which can potentially make the SSH communication susceptible to various attacks. It's important to recognize that this observation focuses solely on the configuration choices of the SSH server and does not evaluate potential vulnerabilities stemming from software versions.</p>	
CVSS Score	2.6	
Affected Scope	192.168.110.	
Proof of Concept	We were able to identify this vulnerability using a nessus scan.	
Reference	https://www.tenable.com/plugins/nessus/71049	

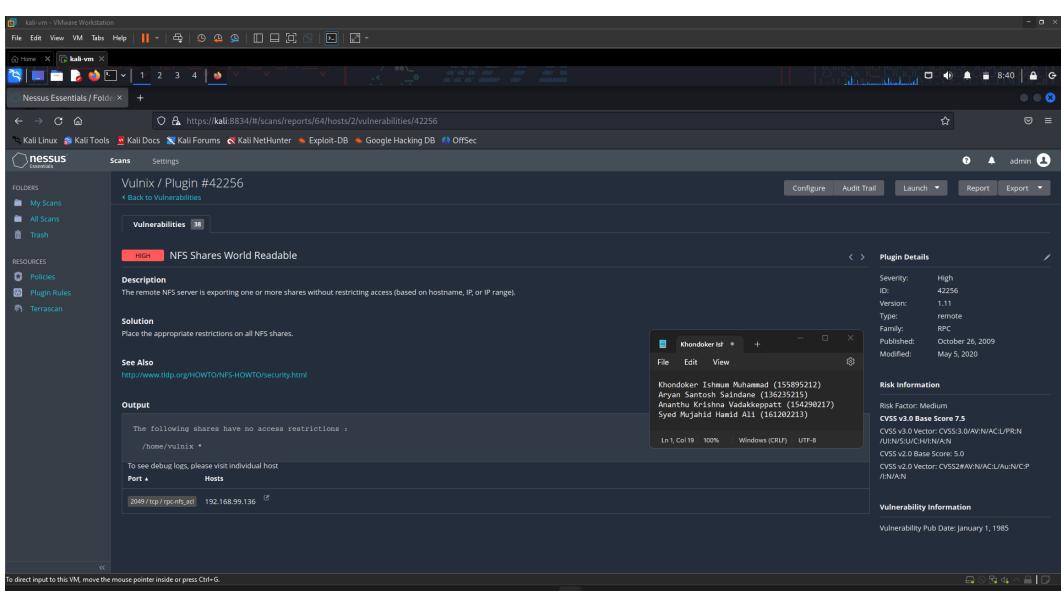
UltimateLAMP VM	
Medium	V6 - HTTP TRACE / TRACK Methods Allowed
Risk Assessment	Impact: Medium Likelihood: Medium
Description	The remote web server allows the use of the TRACE and/or TRACK methods, which are HTTP methods used for debugging web server connections.
CVSS Score	5.3
Affected Scope	192.168.99.135
Proof of Concept	 <p>The screenshot shows the Nessus application interface. The main window displays the 'UltimateLAMP / Plugin #11213' page. The 'Vulnerabilities' tab is selected, showing one result for 'HTTP TRACE / TRACK Methods Allowed'. The 'Description' section states: 'The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.' The 'Solution' section provides instructions to disable these methods in the Apache configuration. The 'See Also' section lists several URLs for further reading. The 'Output' section contains the Apache configuration code to disable TRACE and TRACK methods. A tooltip window is overlaid on the 'Plugin Details' section, showing information about the vulnerability, including the author (Khondoker Ishmu...), severity (Medium), ID (11213), version (1.79), type (remote), family (Web Servers), and publication date (January 23, 2003). The tooltip also lists risk factors and temporal vectors.</p>
Reference	https://www.tenable.com/plugins/nessus/11213

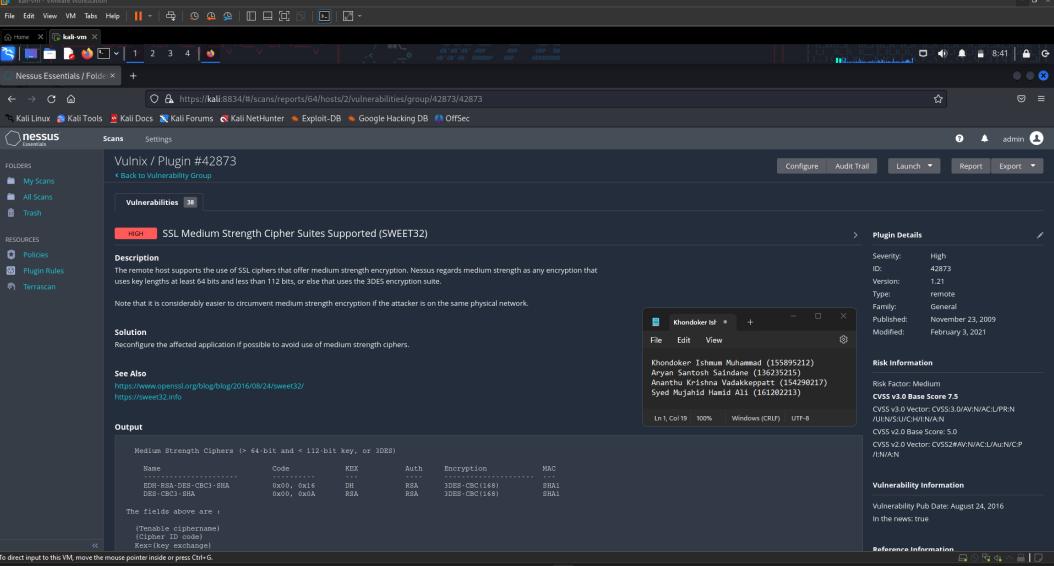
Vulnix VM	
Medium	V7 - SSL Certificate Cannot Be Trusted
Risk Assessment	Impact: Medium Likelihood: Medium
Description	<p>The server's X.509 certificate trust issues can arise in three ways:</p> <ol style="list-style-type: none"> 1. The certificate chain's top might not be linked to a recognized public certificate authority. This could be due to an unknown self-signed top certificate or missing intermediate certificates. 2. The chain might include a certificate that's invalid during scanning, either before its 'notBefore' date or after its 'notAfter' date. 3. The chain might have an unverifiable or mismatched signature, possibly due to unsupported signing algorithms by Nessus. <p>For public production hosts, any break in the chain can undermine users' ability to verify the web server's authenticity, potentially aiding man-in-the-middle attacks.</p>
CVSS Score	6.5
Affected Scope	192.168.99.136
Proof of Concept	
Reference	https://www.tenable.com/plugins/nessus/51192

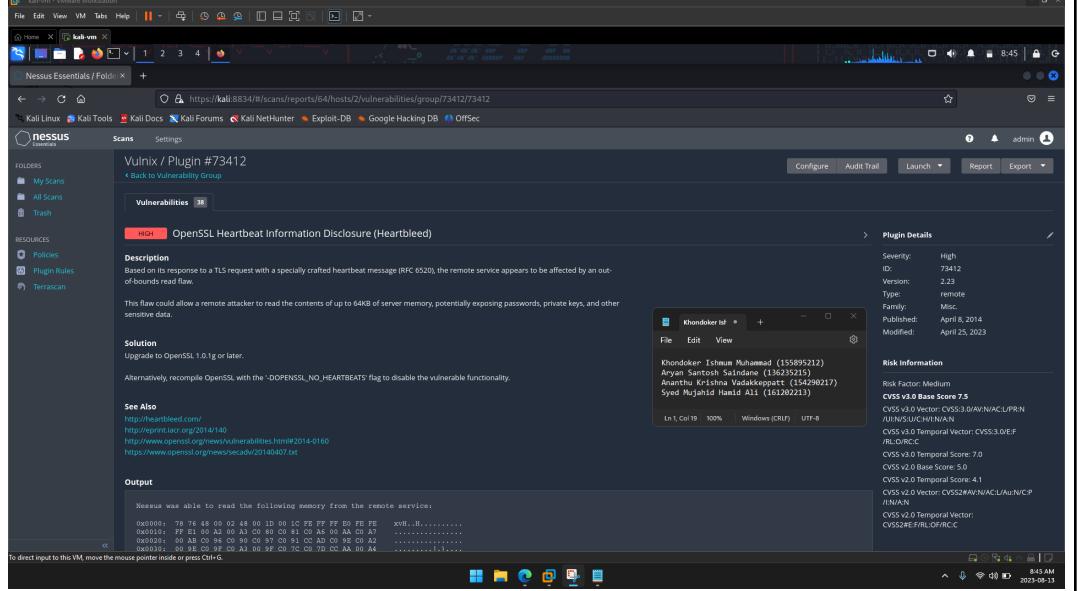
VulnVoIP VM	
Medium	V8 - SSH Weak Algorithms Supported
Risk Assessment	Impact: Medium Likelihood: Medium
Description	Nessus has identified an issue with the remote SSH server's configuration. It is either using the insecure Arcfour stream cipher or no cipher at all, which goes against the recommendations in RFC 4253. This is because Arcfour has a vulnerability related to weak keys.
CVSS Score	4.3
Affected Scope	192.168.99.137
Proof of Concept	
Reference	https://www.tenable.com/plugins/nessus/90317

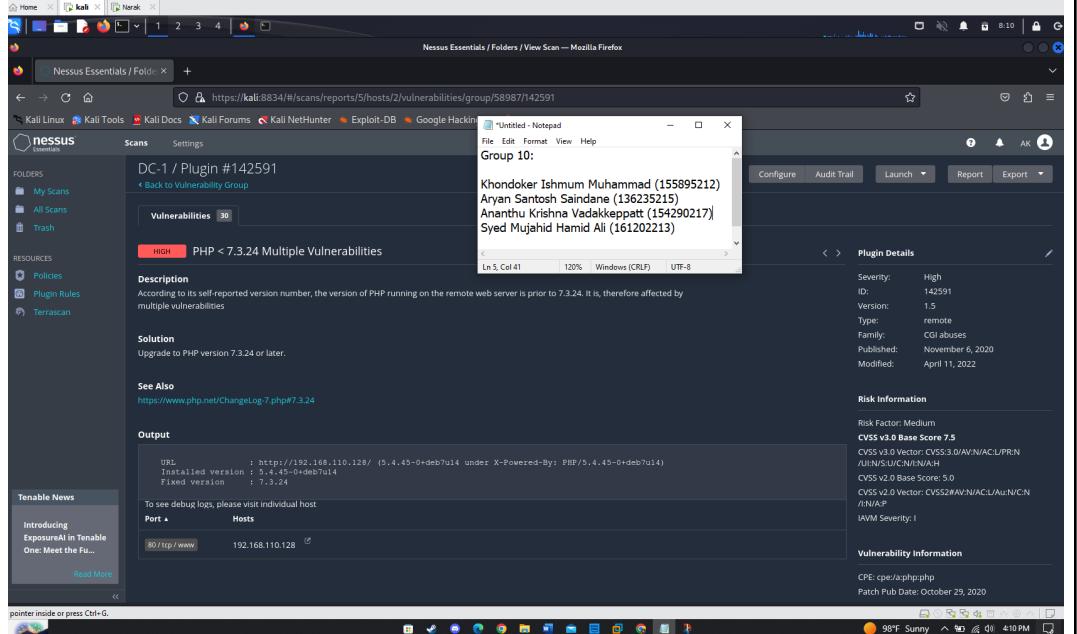
DC-1 VM	
Medium	V9 - JQuery 1.2 < 3.5.0 Multiple XSS
Risk Assessment	Impact: Medium Likelihood: Medium
Description	Based on the version reported in the script, the remote web server is using a version of jQuery that falls between 1.2 and 3.5.0. This version range is known to be impacted by multiple cross-site scripting (XSS) vulnerabilities. These vulnerabilities could potentially allow attackers to inject malicious code into web pages viewed by users, leading to security breaches.
CVSS Score	4.3
Affected Scope	192.168.110.128
Proof of Concept	
Reference	https://www.tenable.com/plugins/nessus/136929

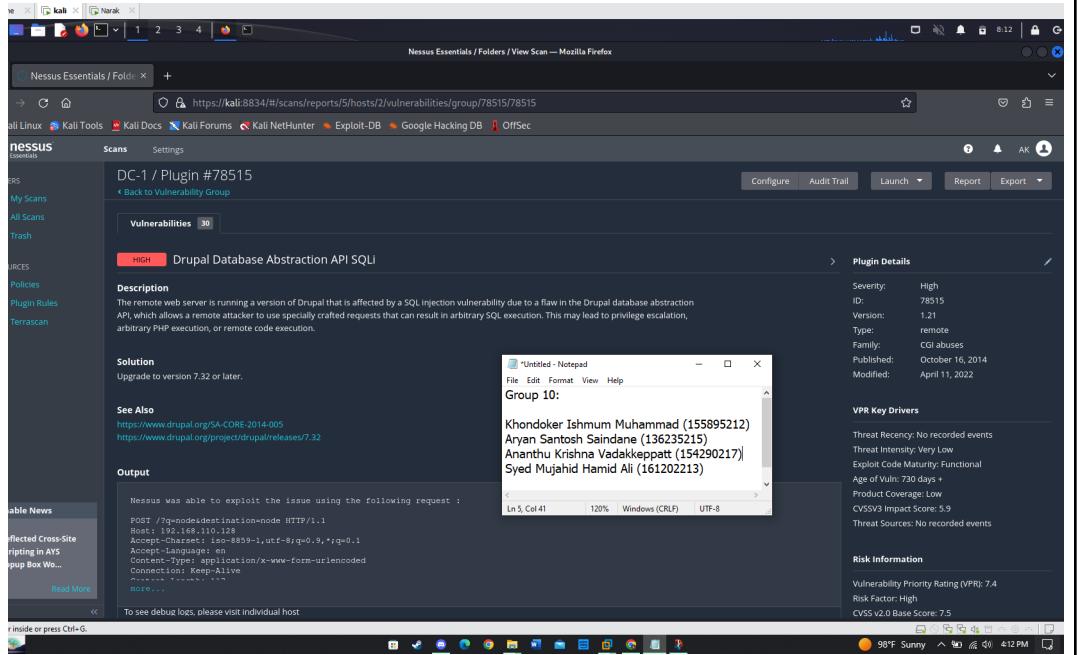
DC-1 VM	
Medium	V10 - web.config File Information Disclosure
Risk Assessment	Impact: Medium Likelihood: Medium
Description	An information disclosure vulnerability has been identified in the remote web server. This vulnerability arises from the inadvertent exposure of the "web.config" file. An attacker who is not authenticated and is remote can exploit this vulnerability by sending a basic GET request to the server. This action can lead to the unintended disclosure of potentially sensitive configuration details.
CVSS Score	5
Affected Scope	192.168.110.128
Proof of Concept	 <p>The screenshot shows the Nessus Essentials interface. A specific vulnerability report is open for host 192.168.110.128, identified as DC-1 / Plugin #121479. The vulnerability is categorized as MEDIUM and titled "web.config File Information Disclosure". The "Description" section states: "An information disclosure vulnerability exists in the remote web server due to the disclosure of the web.config file. An unauthenticated, remote attacker can exploit this, via a simple GET request, to disclose potentially sensitive configuration information." The "Solution" section advises ensuring proper restrictions are in place or removing the web.config file if it's not required. The "Output" section displays the exploit command: "curl -A 'Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)' -H 'Host: 192.168.110.128' -H 'Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1' -H 'Accept-Language: en' -H 'Connection: Keep-Alive' -H 'User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)'. . .". A Notepad window is overlaid on the interface, showing a list of names: Khondoker Ishmmum Muhammad (155895212), Aryan Santosh Saindane (136235215), Ananthu Krishna Vadakkepatt (154290217), and Syed Mujahid Hamid Ali (161202213). The Nessus interface also includes a sidebar with "Tenable News" and "Unauthorized Access to Cross-Tenant Applications ...".</p>
Reference	https://www.tenable.com/plugins/nessus/121479

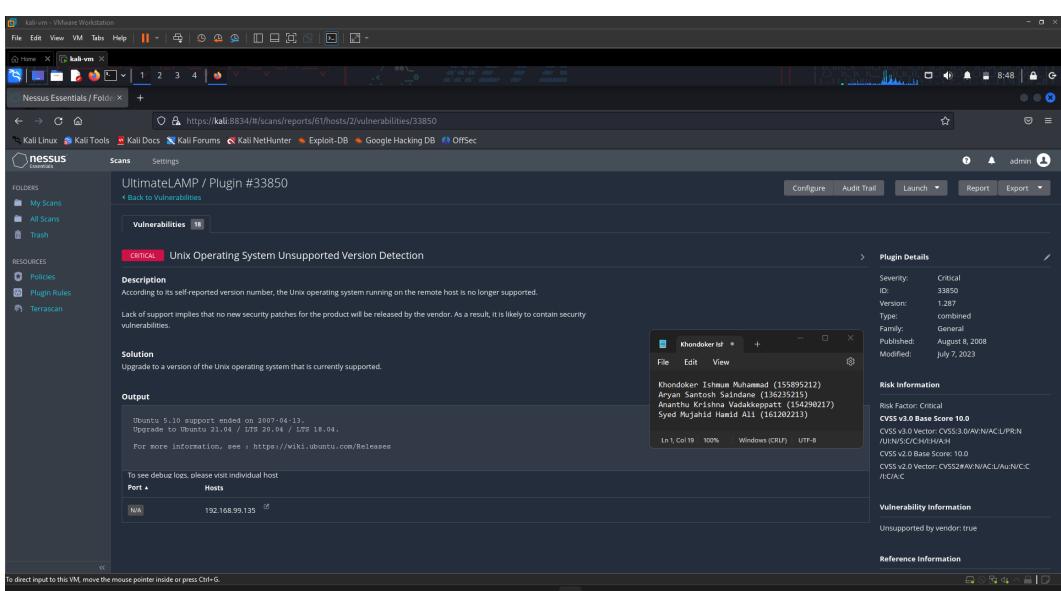
Vulnix VM		
High	V11 - NFS Shares World Readable	
Risk Assessment	Impact: Critical	Likelihood: Medium
Description	The NFS server is allowing access to one or more shares without any restrictions based on hostname, IP address, or IP range.	
CVSS Score	9.3	
Affected Scope	192.168.99.136	
Proof of Concept	 <p>The screenshot shows the Nessus interface with a scan report for host 192.168.99.136. A specific vulnerability is highlighted: 'NFS Shares World Readable' (Plugin #42256). The description states: 'The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range)'. The solution section suggests placing appropriate restrictions on all NFS shares. The output section shows that the share '/home/vulnix' has no access restrictions. The 'Plugin Details' panel provides technical details like ID, Version, Type, and Published date. The 'Risk Information' panel shows the risk factor as Medium and CVSS scores. The 'Vulnerability Information' panel notes the publication date as January 1, 1985.</p>	
Reference	https://www.tenable.com/plugins/nessus/42256	

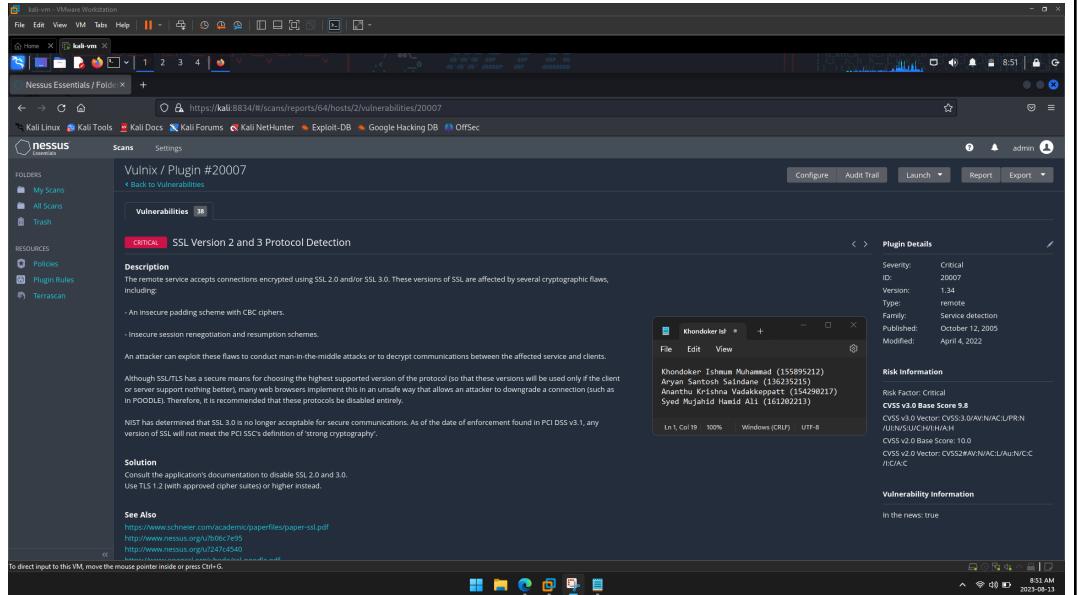
Vulnix VM																																
High	V12 - SSL Medium Strength Cipher Suites Supported (SWEET32)																															
Risk Assessment	Impact: High	Likelihood: Medium																														
Description	The remote host allows the use of SSL ciphers with medium strength encryption, defined as encryption with key lengths between 64 and 112 bits, or the use of the 3DES encryption suite. However, medium strength encryption can be more easily bypassed if the attacker is on the same physical network.																															
CVSS Score	7.5																															
Affected Scope	192.168.99.136																															
Proof of Concept	 <p>The screenshot shows the Nessus interface with the following details:</p> <ul style="list-style-type: none"> Vulnerability Group: Vulnix / Plugin #42873 Description: The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Solution: Reconfigure the affected application if possible to avoid use of medium strength ciphers. See Also: https://www.openssl.org/blog/lib/2016/09/24/sweet32/, https://sweet32.info Output: A table titled "Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)" lists cipher suites: <table border="1"> <thead> <tr> <th>Name</th> <th>Code</th> <th>KEX</th> <th>Auth</th> <th>Encryption</th> <th>MAC</th> </tr> </thead> <tbody> <tr> <td>ECDHE-RSA-CHACHA20-POLY1305</td> <td>0x00, 0x01</td> <td>IM</td> <td>RSA</td> <td>TLS-ECDHE-CHACHA20-POLY1305</td> <td>SHA384</td> </tr> <tr> <td>ECDHE-RSA-CHACHA20-POLY1305-SHA256</td> <td>0x00, 0x01</td> <td>IM</td> <td>RSA</td> <td>TLS-ECDHE-CHACHA20-POLY1305-SHA256</td> <td>SHA256</td> </tr> <tr> <td>DHE-RSA-CHACHA20-POLY1305-SHA256</td> <td>0x00, 0x0A</td> <td>RSA</td> <td>RSA</td> <td>TLS-DHE-RSA-CHACHA20-POLY1305-SHA256</td> <td>SHA256</td> </tr> <tr> <td>DHE-RSA-CBC3-SHA</td> <td>0x00, 0x0A</td> <td>RSA</td> <td>RSA</td> <td>TLS-DHE-RSA-CBC3-SHA</td> <td>SHA1</td> </tr> </tbody> </table> 		Name	Code	KEX	Auth	Encryption	MAC	ECDHE-RSA-CHACHA20-POLY1305	0x00, 0x01	IM	RSA	TLS-ECDHE-CHACHA20-POLY1305	SHA384	ECDHE-RSA-CHACHA20-POLY1305-SHA256	0x00, 0x01	IM	RSA	TLS-ECDHE-CHACHA20-POLY1305-SHA256	SHA256	DHE-RSA-CHACHA20-POLY1305-SHA256	0x00, 0x0A	RSA	RSA	TLS-DHE-RSA-CHACHA20-POLY1305-SHA256	SHA256	DHE-RSA-CBC3-SHA	0x00, 0x0A	RSA	RSA	TLS-DHE-RSA-CBC3-SHA	SHA1
Name	Code	KEX	Auth	Encryption	MAC																											
ECDHE-RSA-CHACHA20-POLY1305	0x00, 0x01	IM	RSA	TLS-ECDHE-CHACHA20-POLY1305	SHA384																											
ECDHE-RSA-CHACHA20-POLY1305-SHA256	0x00, 0x01	IM	RSA	TLS-ECDHE-CHACHA20-POLY1305-SHA256	SHA256																											
DHE-RSA-CHACHA20-POLY1305-SHA256	0x00, 0x0A	RSA	RSA	TLS-DHE-RSA-CHACHA20-POLY1305-SHA256	SHA256																											
DHE-RSA-CBC3-SHA	0x00, 0x0A	RSA	RSA	TLS-DHE-RSA-CBC3-SHA	SHA1																											
Reference	https://www.tenable.com/plugins/nessus/42873																															

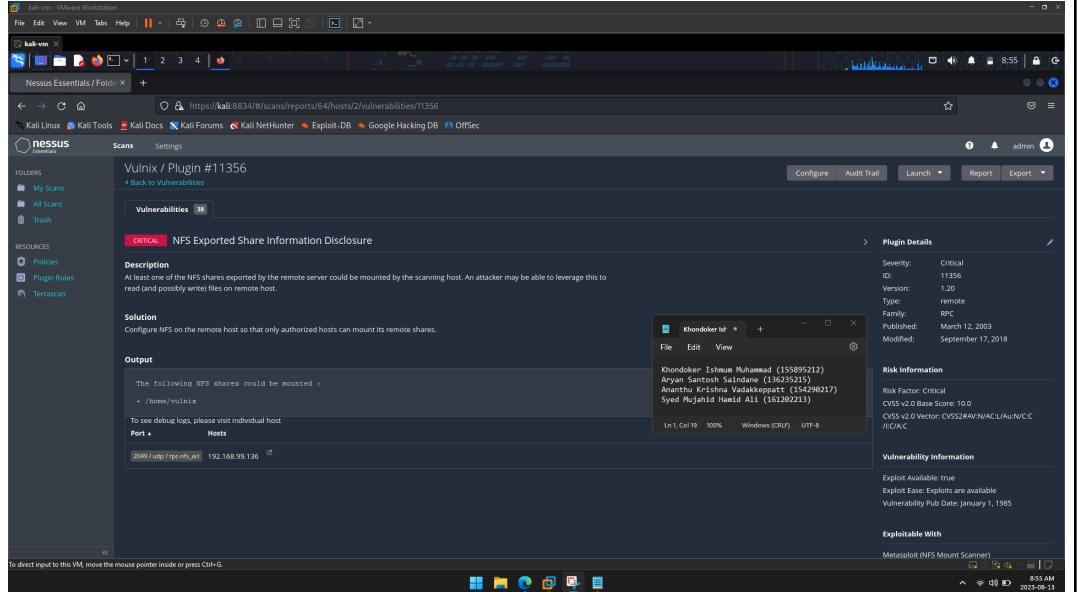
Vulnix VM	
High	V13 - OpenSSL Heartbeat Information Disclosure (Heartbleed)
Risk Assessment	Impact: High Likelihood: Medium
Description	The remote service is vulnerable to an out-of-bounds read flaw triggered by a specially crafted heartbeat message in a TLS request (RFC 6520). This flaw could be exploited by a remote attacker to access up to 64KB of server memory, potentially exposing sensitive information like passwords and private keys.
CVSS Score	7.5
Affected Scope	192.168.99.136
Proof of Concept	 <p>The screenshot shows the Nessus Essentials interface with the following details:</p> <ul style="list-style-type: none"> Scan Details: Vulnix / Plugin #73412 Vulnerability Type: HIGH - OpenSSL Heartbeat Information Disclosure (Heartbleed) Description: Based on its response to a TLS request with a specially crafted heartbeat message (RFC 6520), the remote service appears to be affected by an out-of-bounds read flaw. Solution: Upgrade to OpenSSL 1.0.1g or later. Alternatively, recompile OpenSSL with the '-DOPENSSL_NO_HEARTBEATS' flag to disable the vulnerable functionality. See Also: <ul style="list-style-type: none"> http://nmap.org/heartbleed.cgi/ http://reprint.lasr.org/2014/140 http://www.openssl.org/news/vulnerabilities.html#2014-0160 https://www.openssl.org/news/secadv/20140407.txt Output: Nessus was able to read the following memory from the remote service: <pre> 0x0000: 78 F6 86 93 02 48 00 10 A1 1C FE FF FF B9 PE FE xvi..H. 0x0001: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0x0002: 60 AB C0 94 C0 90 C0 97 C0 91 C0 AD C0 98 C0 A2 0x0003: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0x0004: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 </pre>
Reference	https://www.tenable.com/plugins/nessus/73412

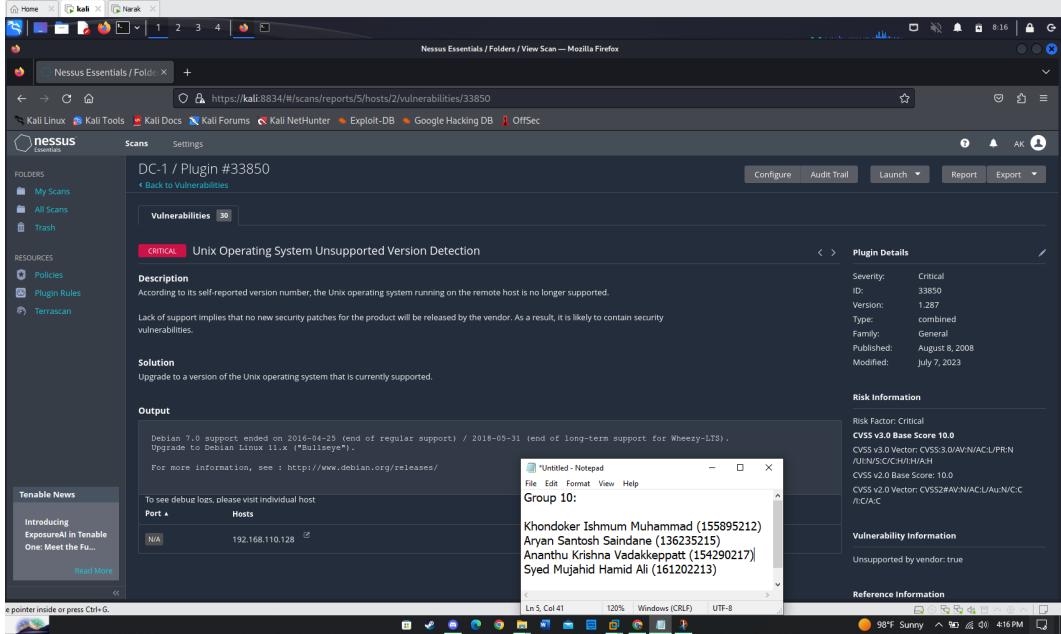
DC-1 VM	
High	V14 - PHP < 7.3.24 Multiple Vulnerabilities
Risk Assessment	Impact: Critical Likelihood: High
Description	The PHP version on the remote web server is reported to be older than 7.3.24. This version is known to be affected by several vulnerabilities. Without specifying the exact vulnerabilities, it's important to note that using an outdated PHP version can expose the server to potential security risks, as older versions might have known security flaws that could be exploited by attackers.
CVSS Score	5
Affected Scope	192.168.110.128
Proof of Concept	 <p>The screenshot shows the Nessus Essentials interface. A central window displays a plugin titled "DC-1 / Plugin #142591" which identifies multiple vulnerabilities in PHP versions prior to 7.3.24. The interface includes a sidebar with "Folders" (My Scans, All Scans, Trash), "Resources" (Policies, Plugin Rules, Terrascan), and a "Tenable News" section. The bottom status bar shows system information like CPU, RAM, and battery level.</p>
Reference	https://www.tenable.com/plugins/nessus/142591

DC-1 VM	
High	V15 - Drupal Database Abstraction API SQLi
Risk Assessment	Impact: Critical Likelihood: High
Description	The version of Drupal installed on the remote web server is susceptible to a SQL injection vulnerability. This vulnerability stems from a flaw in the Drupal database abstraction API. An attacker can exploit this vulnerability by sending specially crafted requests to the server. When successful, this can lead to the execution of arbitrary SQL commands, potentially resulting in various malicious outcomes such as privilege escalation, arbitrary execution of PHP code, or even remote code execution on the affected system.
CVSS Score	7.5
Affected Scope	192.168.110.128
Proof of Concept	
Reference	https://www.tenable.com/plugins/nessus/78515

UltimateLAMP VM	
Critical	V16 - Unix Operating System Unsupported Version Detection
Risk Assessment	Impact: Critical Likelihood: Critical
Description	The remote host is running an unsupported version of the Unix operating system, which means it won't receive any new security patches from the vendor. This makes it susceptible to security vulnerabilities.
CVSS Score	10
Affected Scope	192.168.99.135
Proof of Concept	 <p>The screenshot shows the Nessus application interface. The main window displays a critical vulnerability report titled "UltimateLAMP / Plugin #33850". The report details an unsupported Unix version detection on host 192.168.99.135. The report includes sections for Description, Solution, and Output. The Solution section suggests upgrading to a supported version. The Output section provides technical details about the unsupported version. The right side of the interface shows the "Plugin Details" panel, which lists the plugin's metadata such as Severity (Critical), ID (33850), Version (1.287), and Family (General). It also shows the Risk Information, Vulnerability Information, and Reference Information sections.</p>
Reference	https://www.tenable.com/plugins/nessus/33850

Vulnix VM		
Critical	V17 - SSL Version 2 and 3 Protocol Detection	
Risk Assessment	Impact: Critical	Likelihood: High
Description	<p>The remote service accepts connections encrypted using insecure versions of SSL (SSL 2.0 and SSL 3.0), which have cryptographic vulnerabilities like insecure padding schemes and session renegotiation issues. These flaws can be exploited by attackers to perform man-in-the-middle attacks and decrypt communications between the service and clients. Many web browsers also have unsafe implementations that allow attackers to downgrade connections. It's recommended to disable these protocols entirely. The National Institute of Standards and Technology (NIST) has deemed SSL 3.0 as insecure for secure communications, and any version of SSL is considered inadequate for meeting strong cryptography standards as defined by PCI SSC after the enforcement date in PCI DSS v3.1.</p>	
CVSS Score	9.8	
Affected Scope	192.168.99.136	
Proof of Concept	<p>We were able to find this vulnerability from the advanced scans conducted by Nessus.</p> 	
Reference	https://www.tenable.com/plugins/nessus/20007	

Vulnix VM	
Critical	V18 - NFS Exported Share Information Disclosure
Risk Assessment	Impact: Critical Likelihood: High
Description	The scanning host can mount one of the NFS shares from the remote server, potentially allowing an attacker to access and manipulate files on the remote host.
CVSS Score	10
Affected Scope	192.168.99.136
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"> Scan Details: Vulnix / Plugin #11356 Vulnerability Type: CRITICAL Description: At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host. Solution: Configure NFS on the remote host so that only authorized hosts can mount its remote shares. Output: The following NFS shares could be mounted: <ul style="list-style-type: none"> /home/vulnix To see debug logs, please visit individual host Hosts: 192.168.99.136 Plugin Details: <ul style="list-style-type: none"> Severity: Critical ID: 11356 Version: 1.20 Type: Remote Family: RPC Published: March 12, 2003 Modified: September 17, 2018 Risk Information: <ul style="list-style-type: none"> Risk Factor: Critical CVSS v2.0 Base Score: 10.0 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C ICV: A Vulnerability Information: <ul style="list-style-type: none"> Exploit Available: true Exploit Ease: Exploits are available Vulnerability Pub Date: January 1, 1985 Exploitables With: Metasploit (NFS Mount Scanner)
Reference	https://www.tenable.com/plugins/nessus/11356

DC-1 VM		
Critical	V19 - Unix Operating System Unsupported Version Detection	
Risk Assessment	Impact: Critical	Likelihood: High
Description	<p>The Unix operating system installed on the remote host is reported to be in a state of no longer being supported. This means that the vendor has ceased providing new security patches or updates for the product. Consequently, the operating system is more susceptible to containing security vulnerabilities. As there won't be any new patches released to address potential security issues, the system is at a heightened risk of being exploited by attackers who could take advantage of these vulnerabilities.</p>	
CVSS Score	10	
Affected Scope	192.168.110.128	
Proof of Concept	<p>We were able to find this vulnerability from the advanced scans conducted by Nessus.</p> 	
Reference	https://www.tenable.com/plugins/nessus/33850	

DC-1 VM	
Critical	V20 - PHP Unsupported Version Detection
Risk Assessment	Impact: Critical Likelihood: High
Description	The PHP installation on the remote host is indicated to be in a state of no longer receiving support. This signifies that the vendor has ceased providing new security patches or updates for the PHP version in question. Consequently, the PHP installation is more susceptible to housing security vulnerabilities. Because no new patches will be released to address potential security issues, the installation is at an elevated risk of being exploited by malicious actors who could leverage these vulnerabilities.
CVSS Score	10
Affected Scope	192.168.110.128
Proof of Concept	
Reference	https://www.tenable.com/plugins/nessus/156255

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.