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)

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.

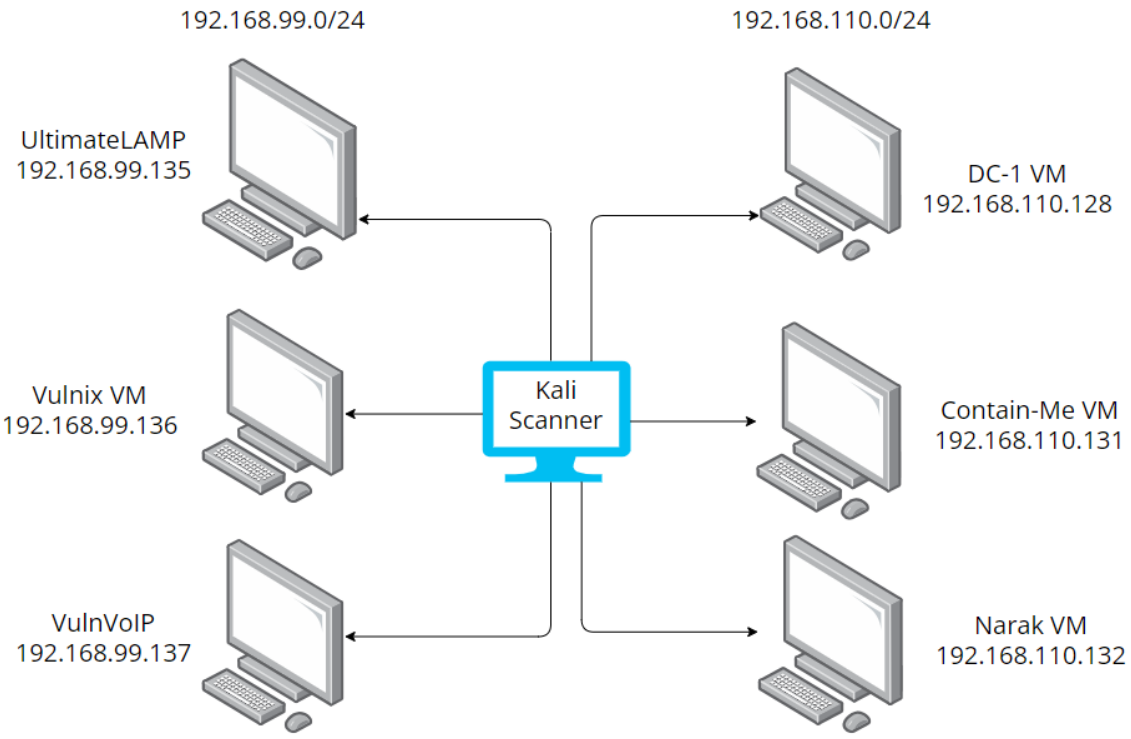
Across the whole assessment, we analyzed a lot of vulnerabilities which will be elaborated in the report ahead. Moreover, students from our group have only performed scans on local networks.

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

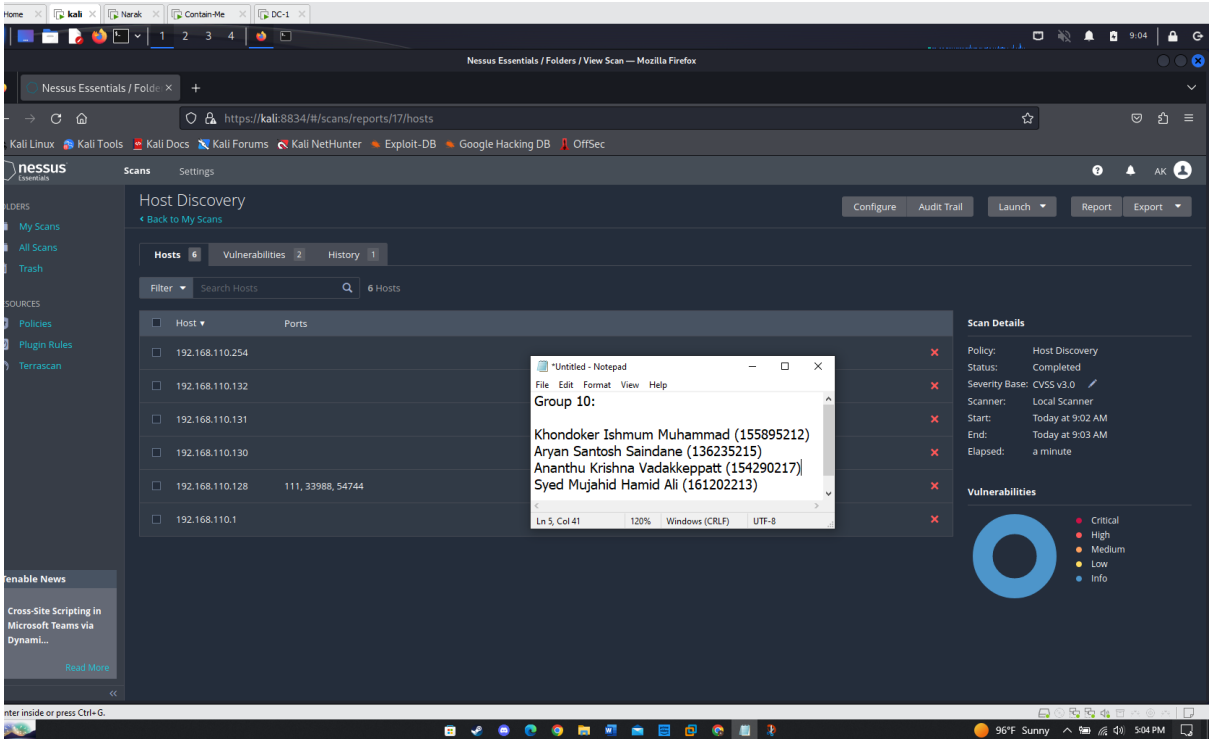
Hardware Inventory & Software Inventory				
Machines	**Software & Services**	**IP Address**	**Subnet Mask - CIDR**	**Role**
Kali Scanner (1)	Nessus	192.168.110.	255.255.255.0 - /24	Scanner to find vulnerabilities in the network infrastructure.
DC-1 VM	Vulnerable virtual machine	192.168.110.128	255.255.255.0 - /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	255.255.255.0/24	Acts as a victim that has a lot of vulnerable services running in the machine.
VulnVoIP	Vulnerable Virtual Machine	192.168.99.37	255.255.255.0/24	Acts as a victim that has a lot of vulnerable services running in the machine.

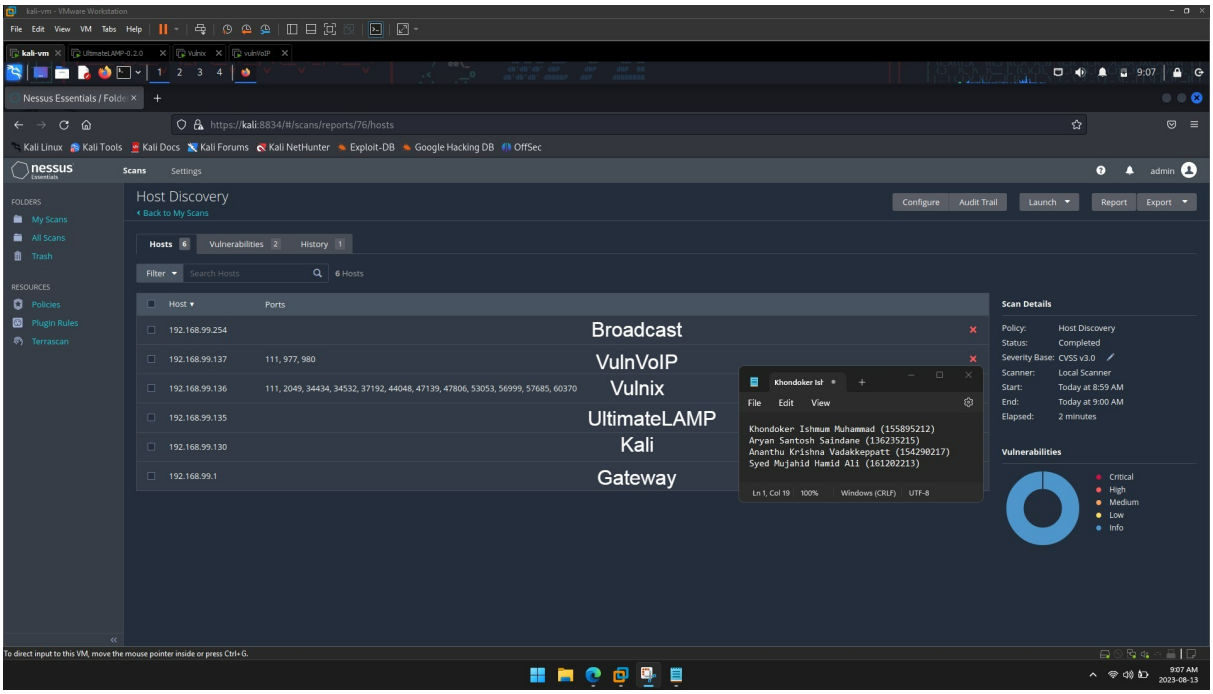
Important Notes

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.

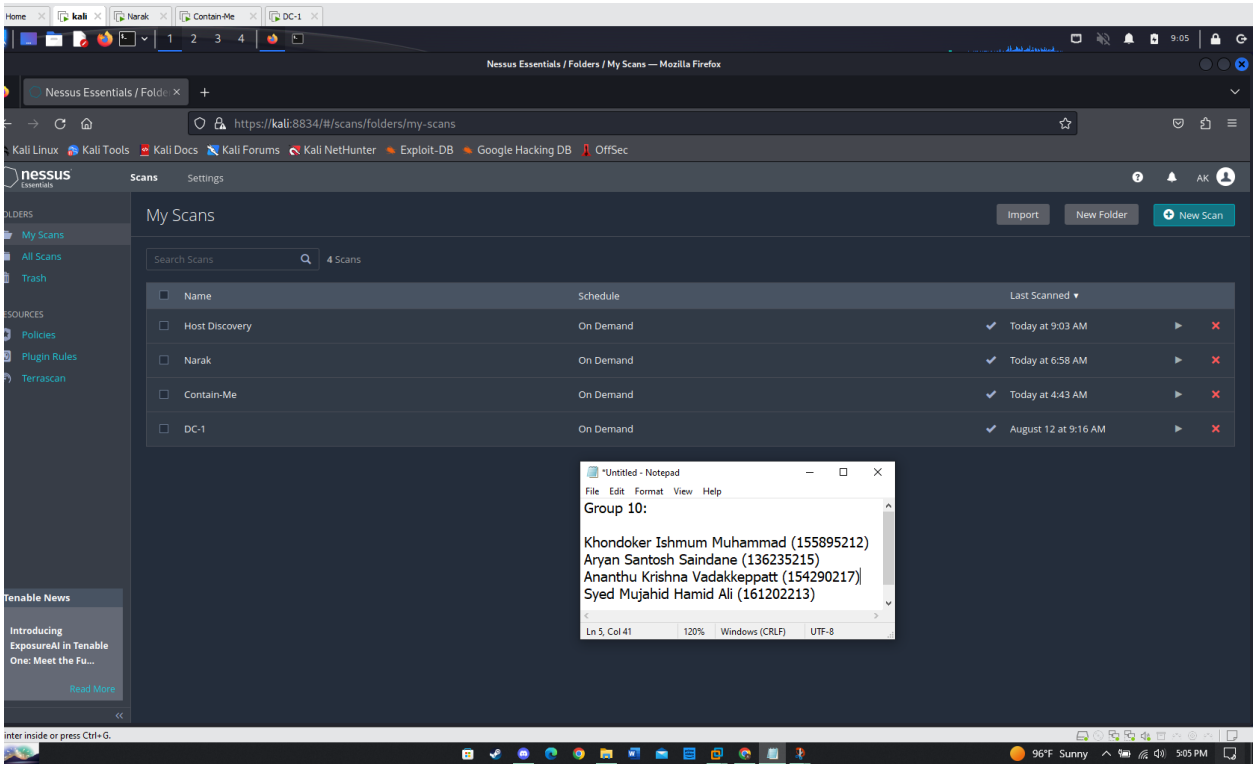
The first network has the vulnerable VM's DC-1. Contain-me and Narak. The second network has the virtual machines UltimateLAMP, Vulnix VM and VulnVoIP,

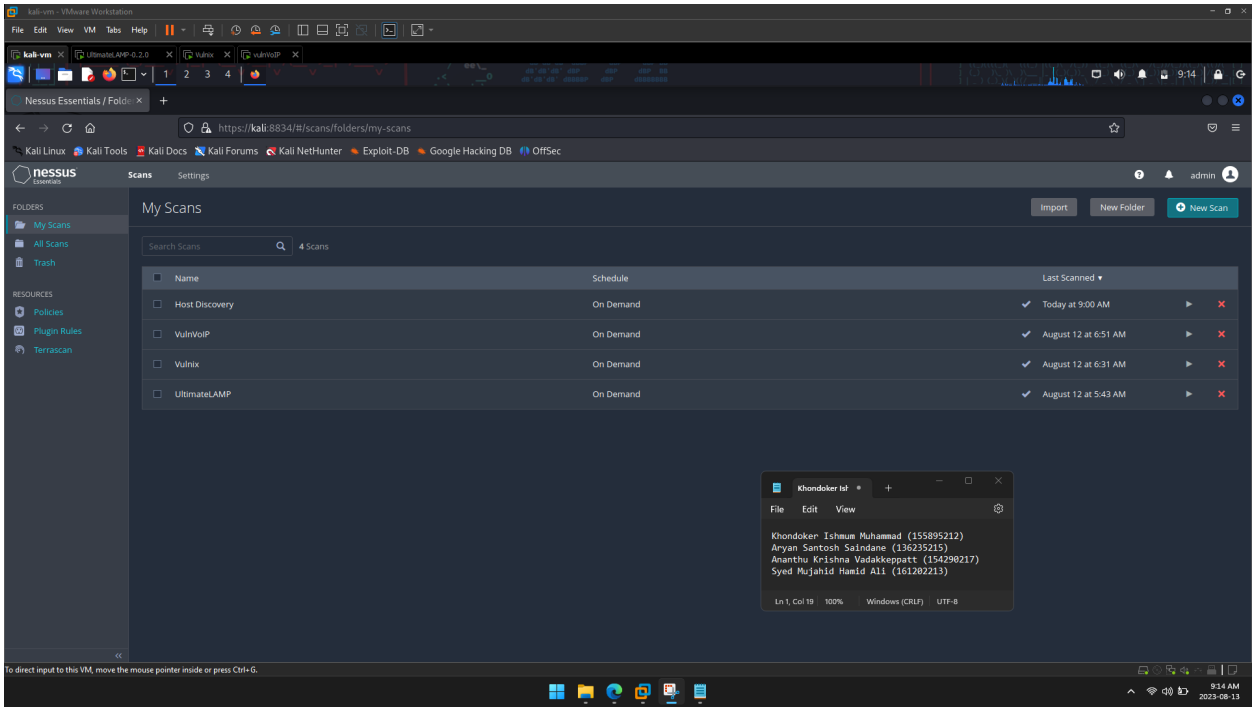
Network Host Discovery

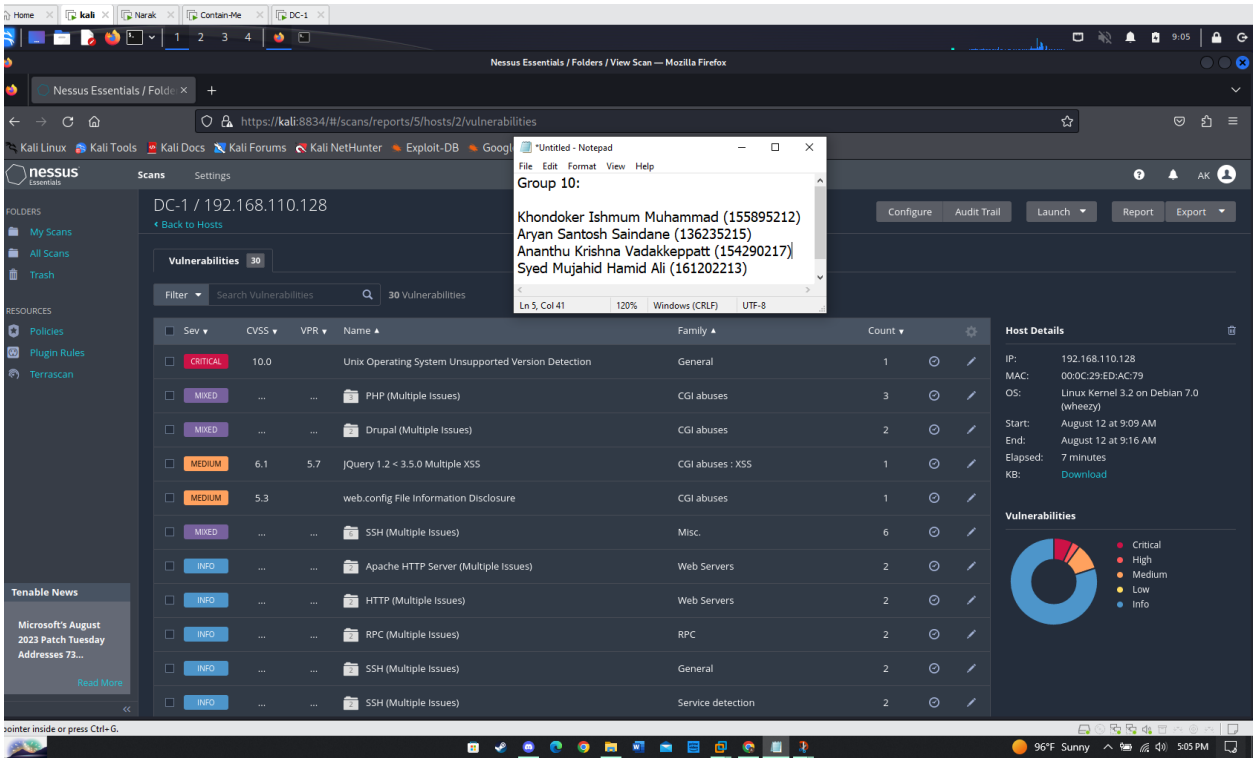


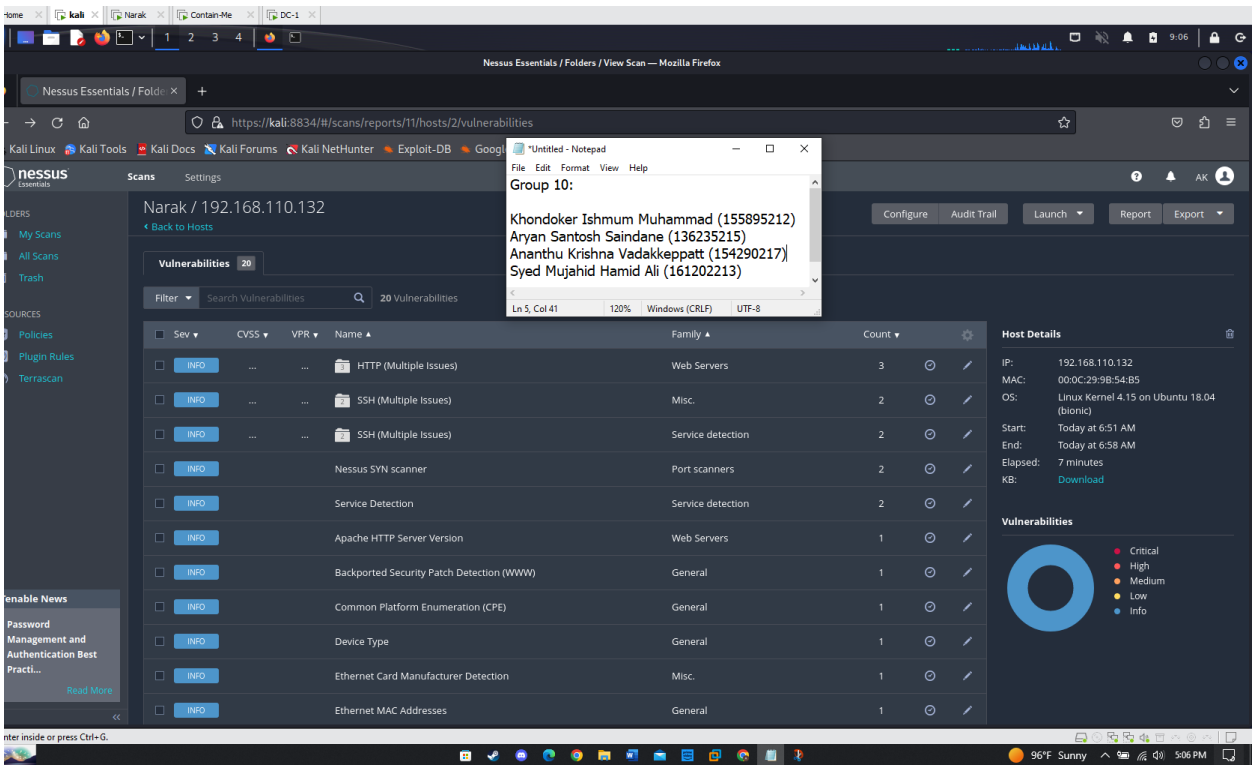


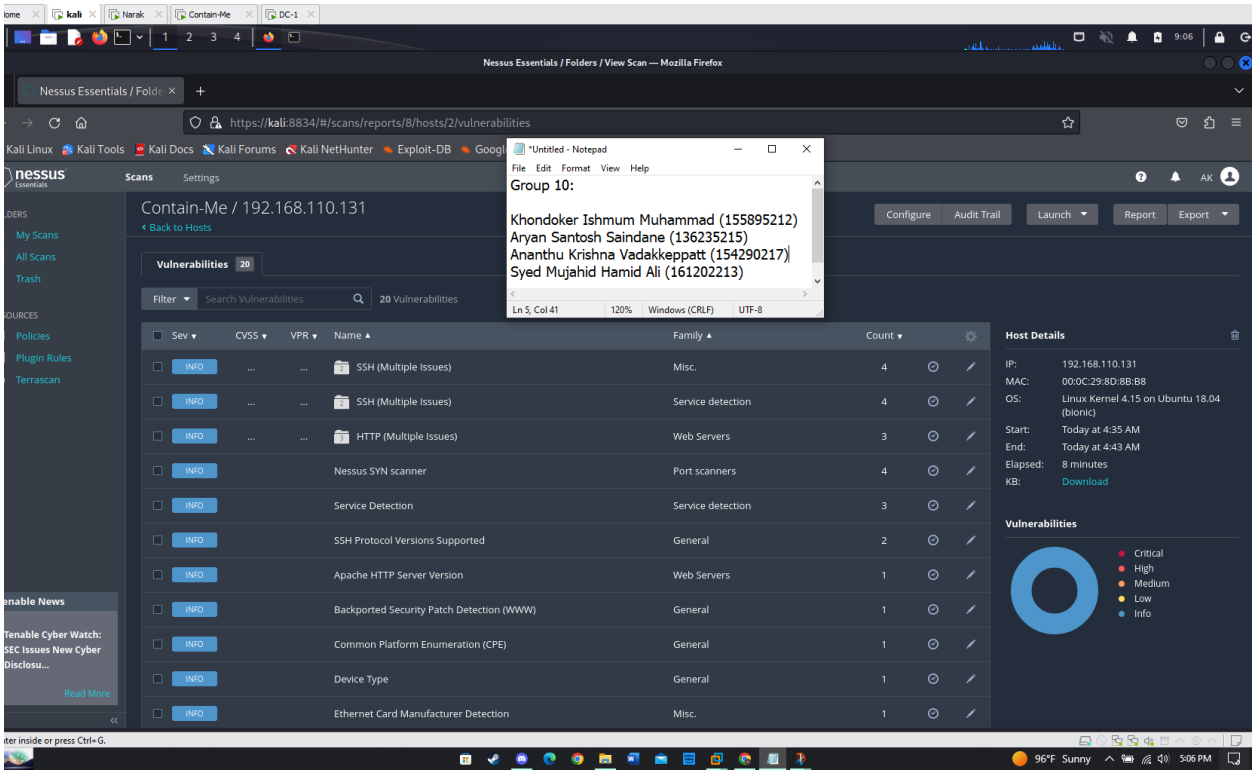
Nessus Scans

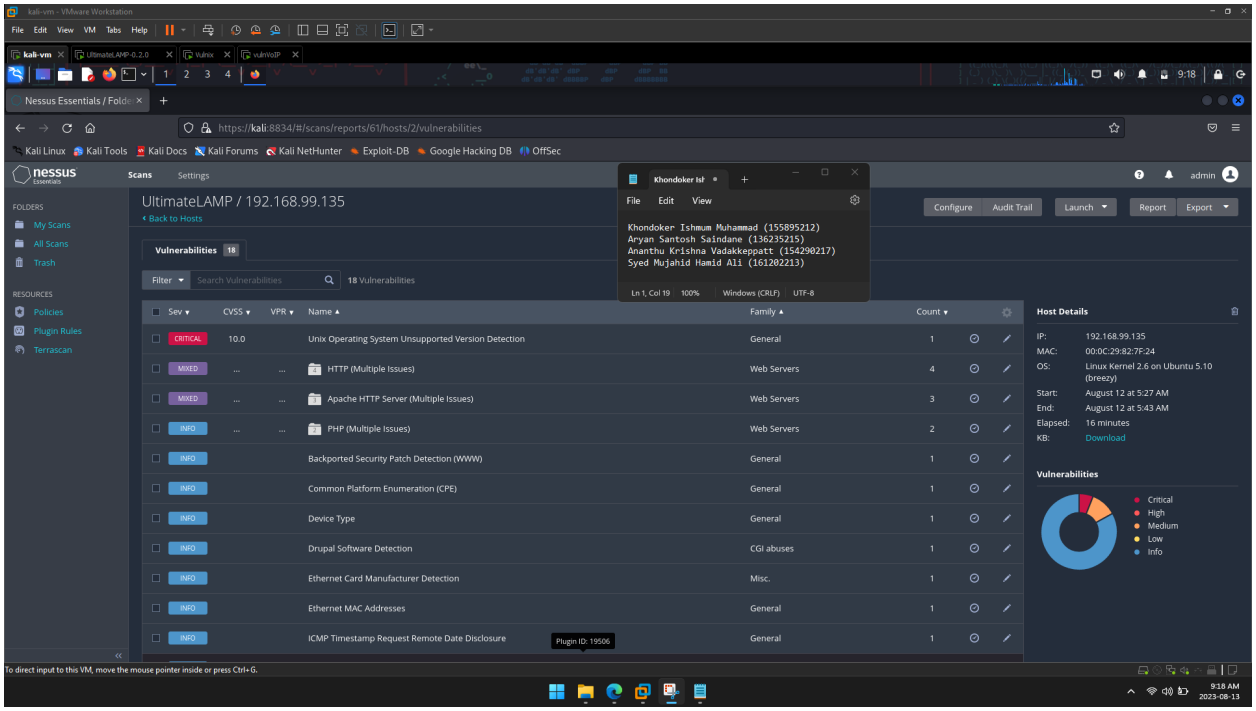


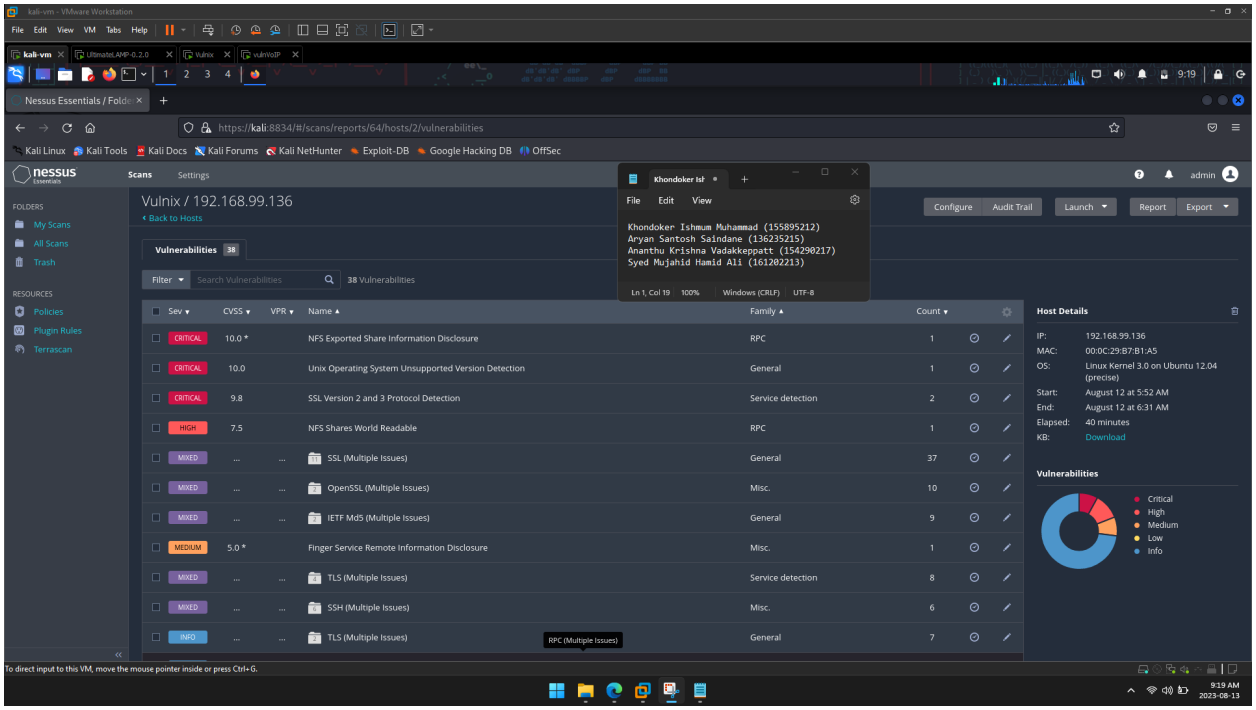


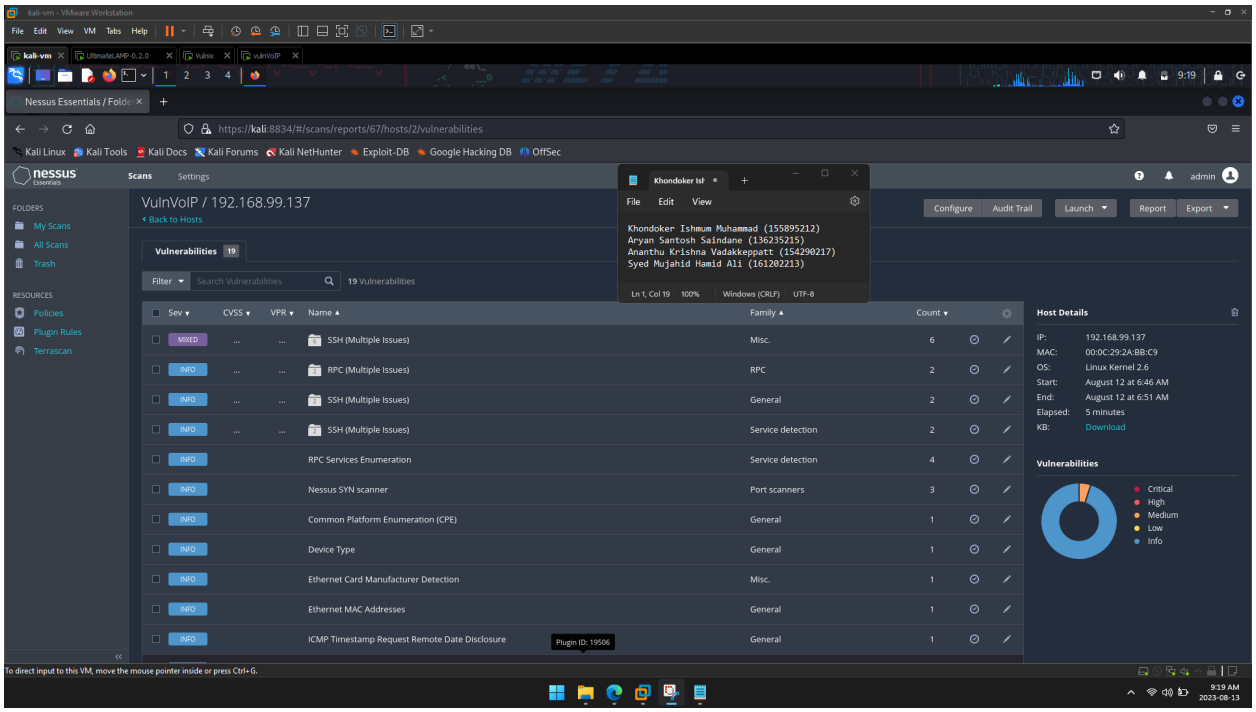

Nessus Essentials / Folders / View Scan — Mozilla Firefox
https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities
*Untitled - Notepad
File Edit Format View Help
Group 10:
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
Ln 5, Col 41 120% Windows (CRLF) UTF-8
DC-1 / 192.168.110.128
Back to Hosts
Configure Audit Trail Launch Report Export
Vulnerabilities 30
Filter Search Vulnerabilities 30 Vulnerabilities
Sev 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
Critical
High
Medium
Low
Info
Tenable News
Microsoft's August 2023 Patch Tuesday Addresses 73...
Read More


Nessus Essentials / Folders / View Scan — Mozilla Firefox
https://kali:8834/#/scans/reports/11/hosts/2/vulnerabilities
*Untitled - Notepad
File Edit Format View Help
Group 10:
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
Ln 5, Col 41 120% Windows (CRLF) UTF-8
Narak / 192.168.110.132
Back to Hosts
Configure Audit Trail Launch Report Export
Vulnerabilities 20
Filter Search Vulnerabilities 20 Vulnerabilities
Sev 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
Critical
High
Medium
Low
Info
Password Management and Authentication Best Practi...
Read More


Nessus Essentials / Folders / View Scan — Mozilla Firefox
https://kali:8834/#/scans/reports/8/hosts/2/vulnerabilities
Untitled - Notepad
Group 10:
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
Contain-Me / 192.168.110.131
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 20
Filter
Search Vulnerabilities
20 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
SSH (Multiple Issues) Misc. 4
SSH (Multiple Issues) Service detection 4
HTTP (Multiple Issues) Web Servers 3
Nessus SYN scanner Port scanners 4
Service Detection Service detection 3
SSH Protocol Versions Supported General 2
Apache HTTP Server Version Web Servers 1
Backported Security Patch Detection (WWW) General 1
Common Platform Enumeration (CPE) General 1
Device Type General 1
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
Critical
High
Medium
Low
Info
96°F Sunny
5:06 PM


kali-vm - VMware Workstation
Nessus Essentials / Folders / View Scan
https://kali:8834/#/scans/reports/61/hosts/2/vulnerabilities
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
UltimateLAMP / 192.168.99.135
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 18
Filter
Search Vulnerabilities
18 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
Unix Operating System Unsupported Version Detection General 1
HTTP (Multiple Issues) Web Servers 4
Apache HTTP Server (Multiple Issues) Web Servers 3
PHP (Multiple Issues) Web Servers 2
Backported Security Patch Detection (WWW) General 1
Common Platform Enumeration (CPE) General 1
Device Type General 1
Drupal Software Detection CGI abuses 1
Ethernet Card Manufacturer Detection Misc. 1
Ethernet MAC Addresses General 1
ICMP Timestamp Request Remote Date Disclosure General 1
Plugin ID: 19506
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
Critical
High
Medium
Low
Info
9:18 AM
2023-08-13


Vulnix / 192.168.99.136
Back to Hosts
Vulnerabilities 38
Filter
Search Vulnerabilities
38 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
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
RPC (Multiple Issues)
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
Critical
High
Medium
Low
Info
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)


VulnVoIP / 192.168.99.137
Back to Hosts
Vulnerabilities 19
Filter
Search Vulnerabilities
19 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
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
Plugin ID: 19506
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
Critical
High
Medium
Low
Info
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

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.

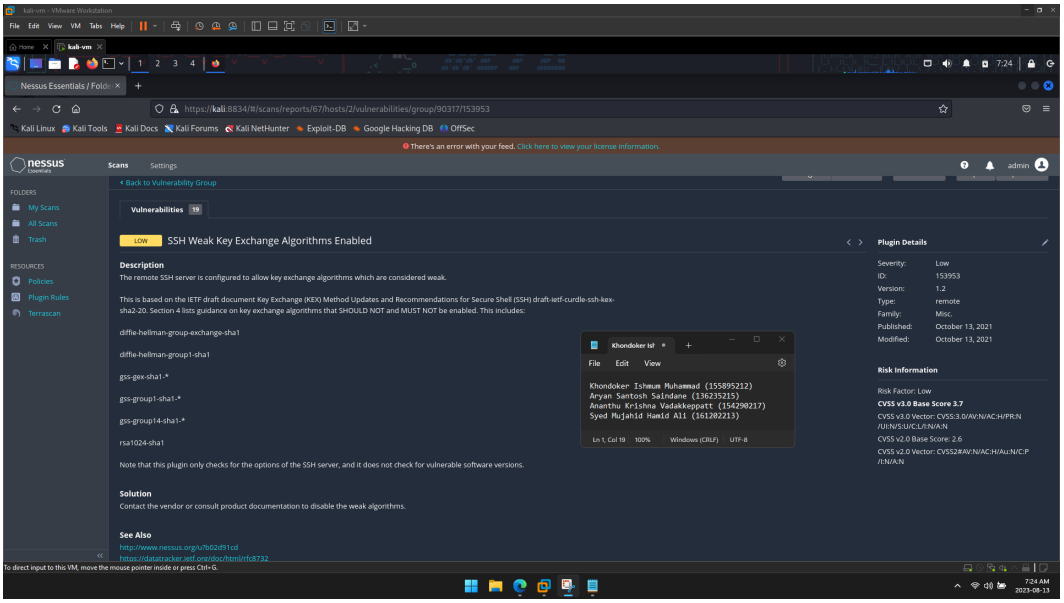
Likelihood	Info	Low	Medium	High	Critical
Critical	Info	Low	Medium	High	Critical
High	Info	Low	Medium	High	Critical
Medium	Info	Low	Medium	Medium	High
Low	Info	Low	Low	Low	Medium
Info	Info	Info	Info	Low	Low

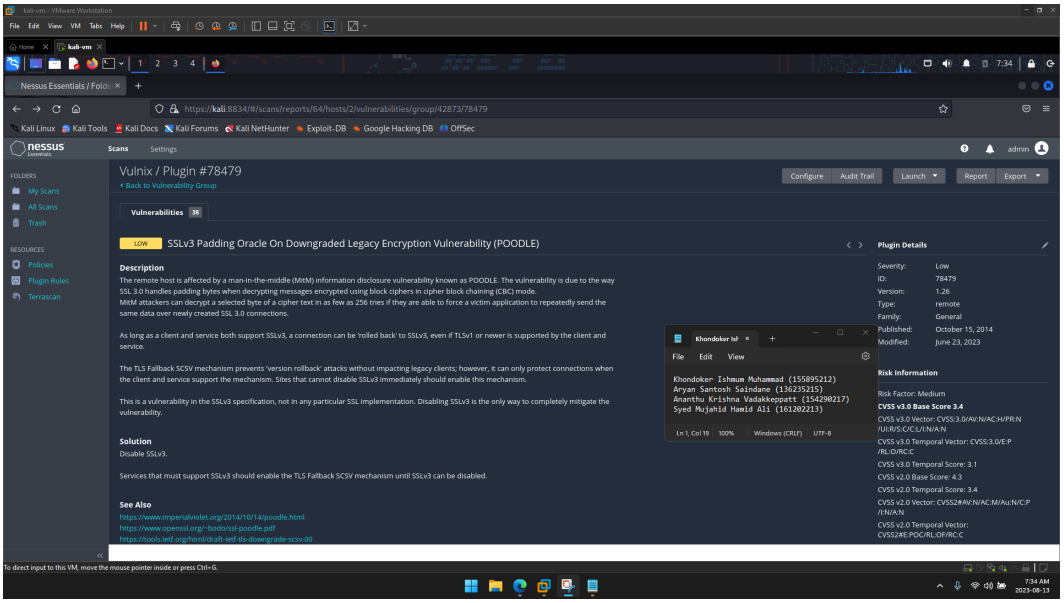
Vulnerability Assessment And Patching Report

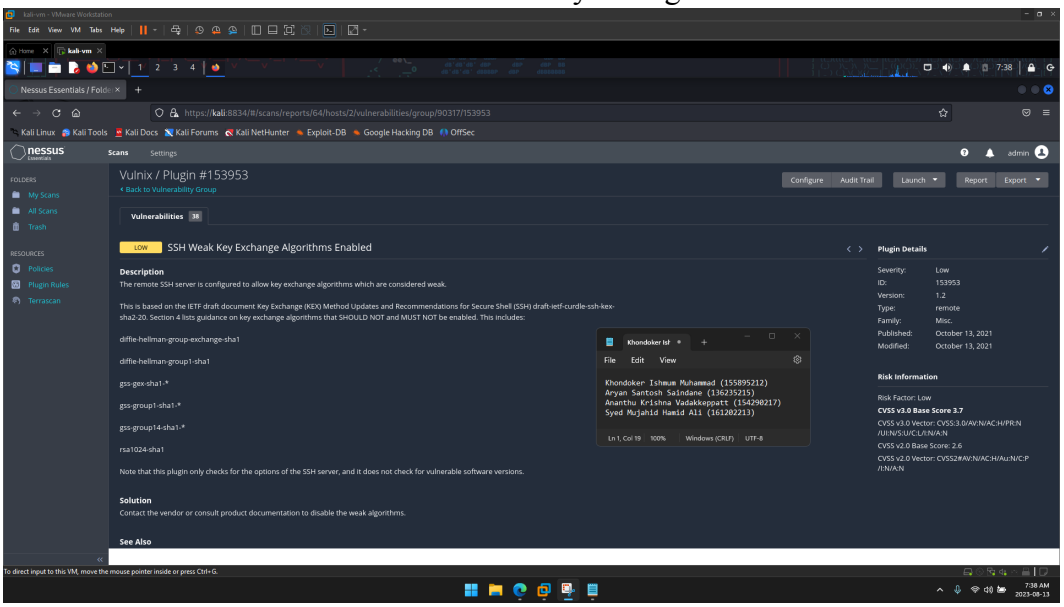
The following is the list of vulnerabilities that we were able to find on all of the operating systems across this assignment:

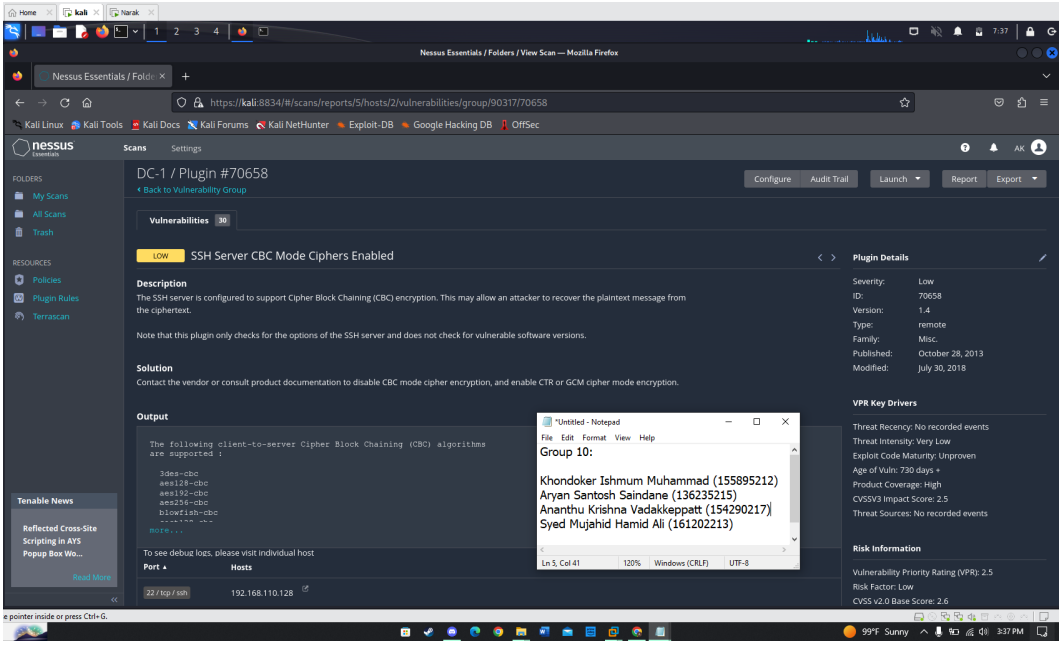
Vulnerabilities			
Vulnerability ID	**Machine**	**Vulnerability Name**	**Risk Level**
V1	VulnVoIP VM	SSH Weak Key Exchange Algorithms Enabled	Low
V2	Vulnix VM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Low
V3	Vulnix VM	SSH Weak Key Exchange Algorithms Enabled	Low
V4	DC-1 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

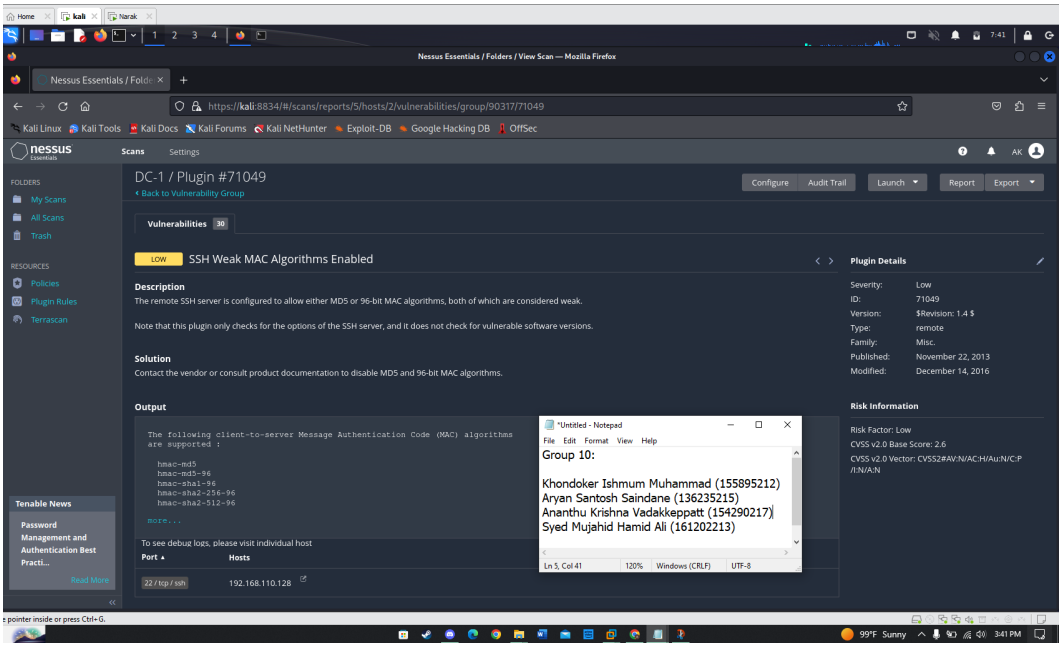
V15	DC-1	Drupal Database Abstraction API SQLi	High
V16	UltimateLAMP VM	Unix Operating System Unsupported Version Detection	Critical
V17	Vulnix VM	SSL Version 2 and 3 Protocol Detection	Critical
V18	Vulnix VM	NFS Exported Share Information Disclosure	Critical
V19	DC-1 VM	Unix Operating System Unsupported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

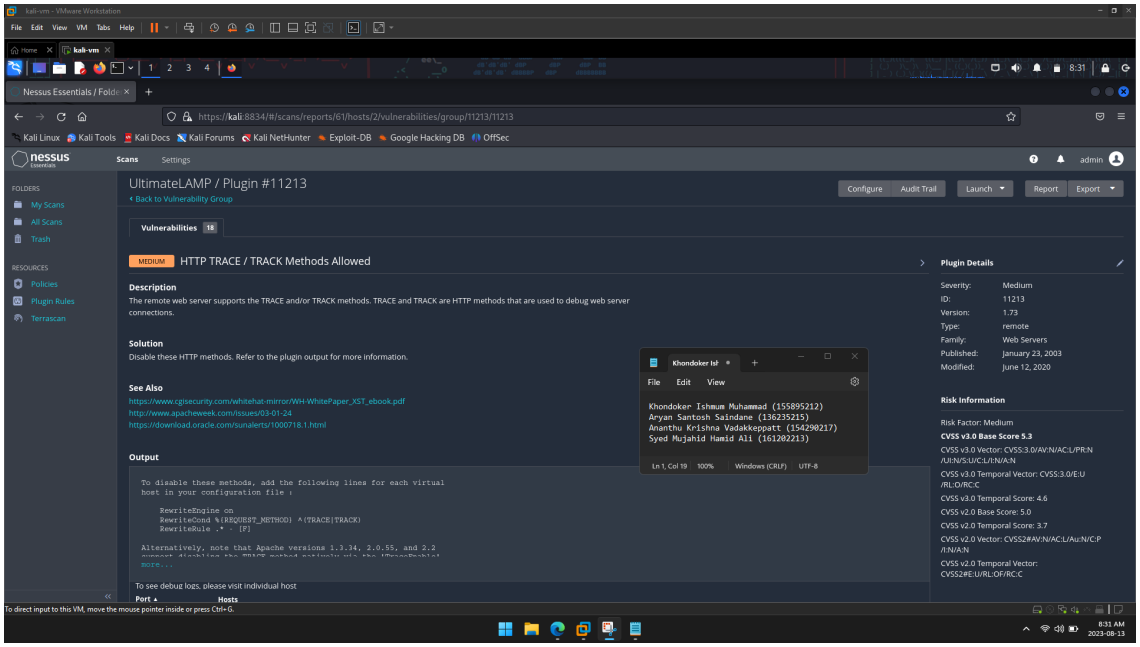
VulnVoIP VM		
Low	V1 - SSH Weak Key Exchange Algorithms Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	The remote SSH server allows weak key exchange algorithms as mentioned in the IETF draft document "Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)." The document provides guidance on which key exchange algorithms should not be enabled. The algorithms listed in Section 4 that should not be used include: • 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	We were able to get information about this Vulnerability from a Nessus scan on the host. 	
Reference	https://www.tenable.com/plugins/nessus/153953	

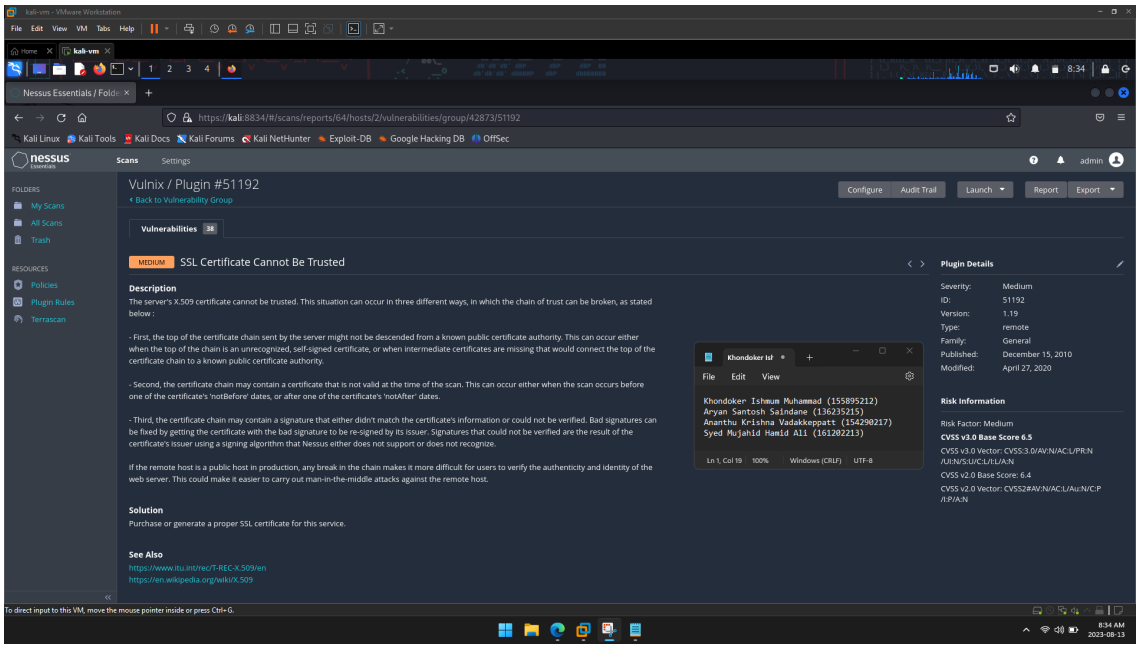
Vulnix VM		
Low	V2 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	
Risk Assessment	Impact: Low	Likelihood: Medium
Description	The remote host has a vulnerability called POODLE, which is a man-in-the-middle information disclosure issue. This vulnerability exists in SSL 3.0 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. 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.	
CVSS Score	3.4	
Affected Scope	192.168.99.136	
Proof of Concept	We were able to know about this vulnerability through a Nessus scan on the host. 	
Reference	https://www.tenable.com/plugins/nessus/78479	

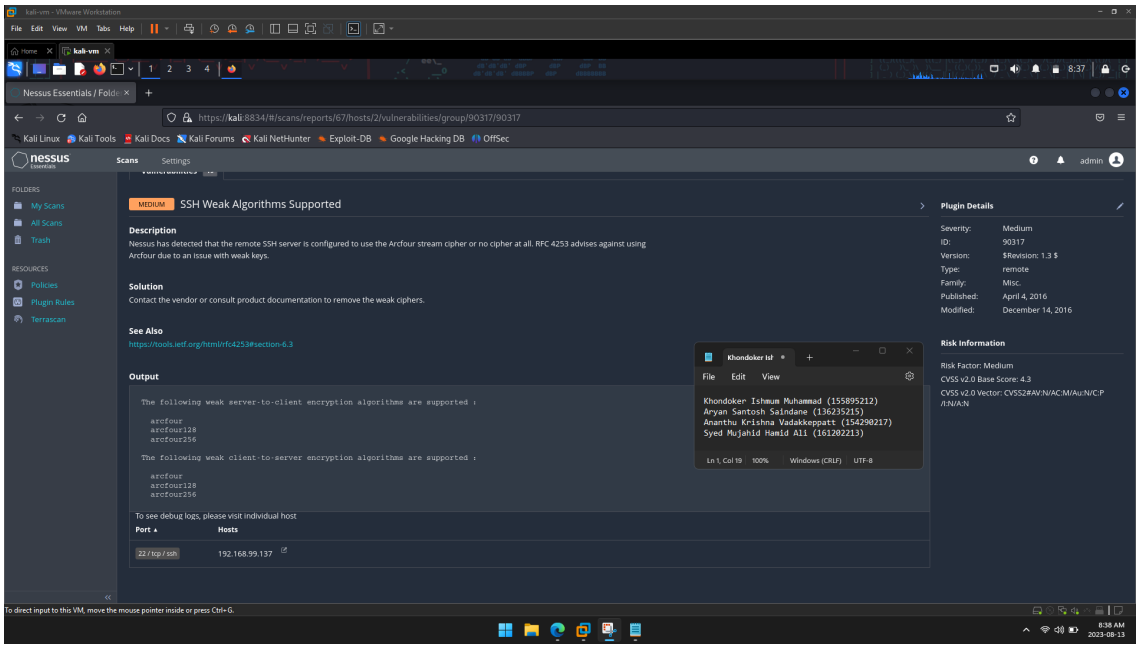
Vulnix VM		
Low	V3 - SSH Weak Key Exchange Algorithms Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	The remote SSH server has been set up with key exchange algorithms that are considered weak according to the IETF draft document "Key Exchange (KEX) Method Updates and Recommendations 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.	
CVSS Score	3.7	
Affected Scope	192.168.99.136	
Proof of Concept	We were able to know about this vulnerability through a Nessus scan. 	
Reference	https://www.tenable.com/plugins/nessus/153953	

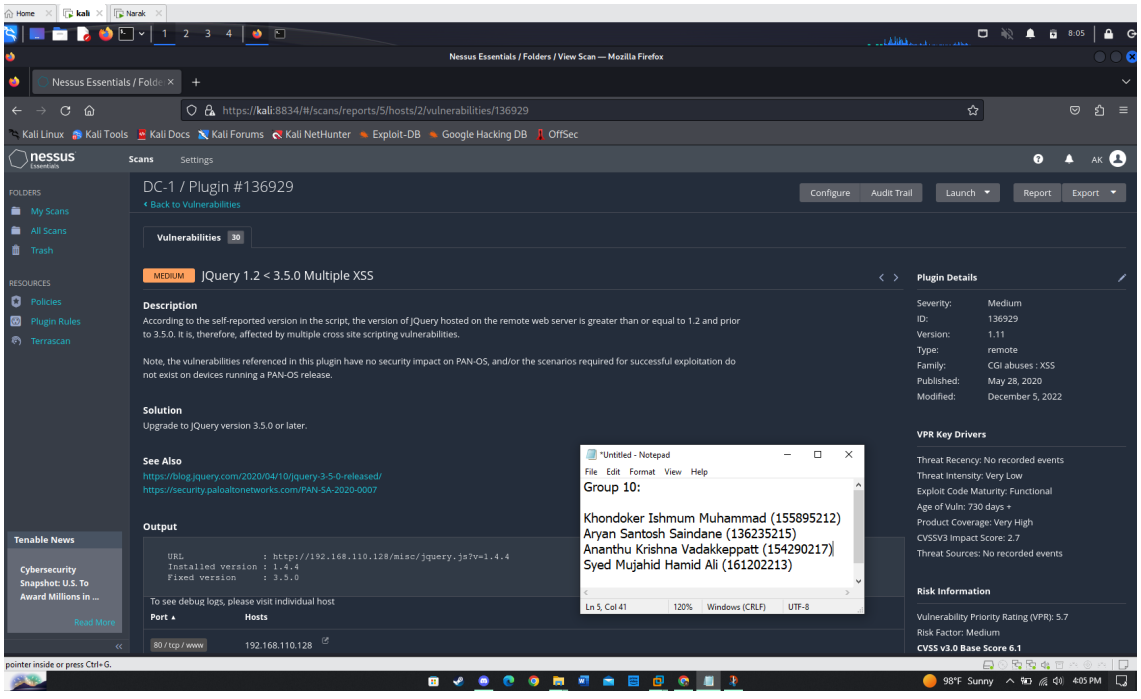
DC-1 VM		
Low	V4 - SSH Server CBC Mode Ciphers Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	The SSH server in question has been set up to use Cipher Block Chaining (CBC) encryption. CBC is a method of encryption that can be susceptible to certain types of attacks, potentially allowing 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.	
CVSS Score	2.6	
Affected Scope	192.168.110.	
Proof of Concept		
Reference	https://www.tenable.com/plugins/nessus/70658	

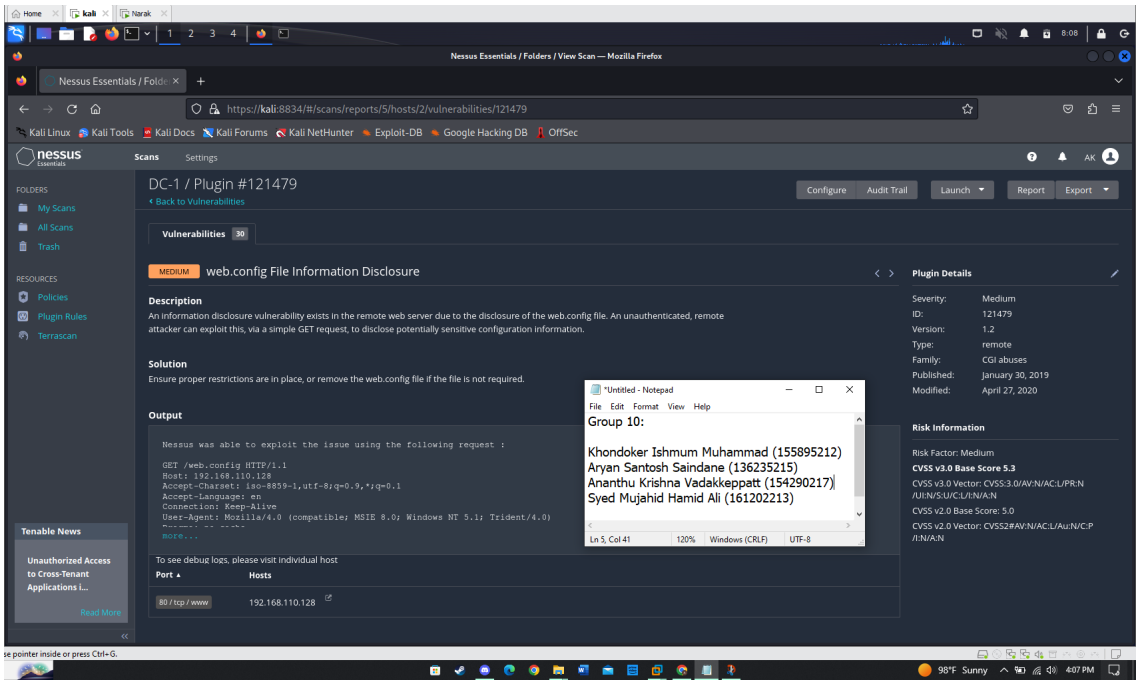
DC-1 VM		
Low	V5 - SSH Weak MAC Algorithms Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	The remote SSH server is set up to permit the use of either MD5 or 96-bit MAC (Message Authentication Code) algorithms. Both of these options are considered weak from a security standpoint. This 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.	
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	

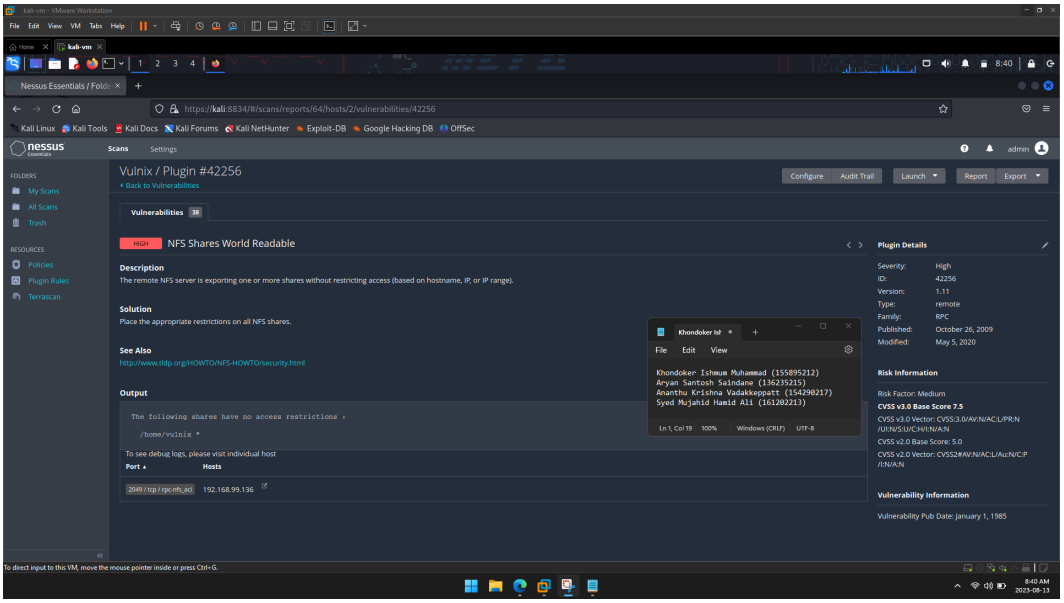
UltimateLAMP VM		
Medium	V6 - HTTP TRACE / TRACK Methods Allowed	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	The remote web server allows the use of the TRACE and/or TRACK methods, which are HTTP methods used for debugging web server connections.	
CVSS Score	5.3	
Affected Scope	192.168.99.135	
Proof of Concept		
Reference	https://www.tenable.com/plugins/nessus/11213	

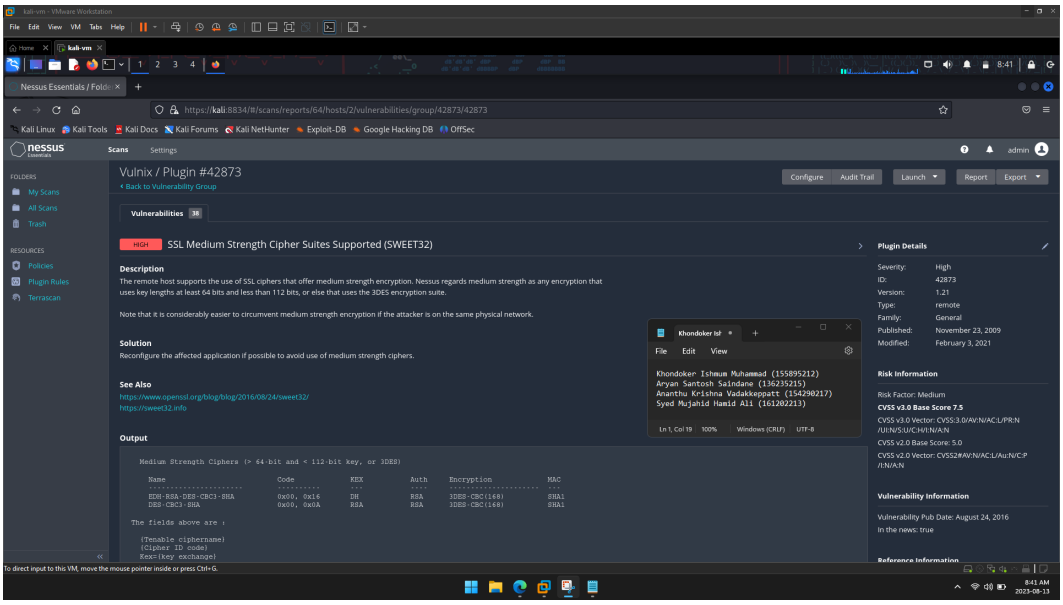
Vulnix VM		
Medium	V7 - SSL Certificate Cannot Be Trusted	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	The server's X.509 certificate trust issues can arise in three ways: 1. The certificate chain's top might not be linked to a recognized public certificate authority. This could be 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. 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.	
CVSS Score	6.5	
Affected Scope	192.168.99.136	
Proof of Concept		
Reference	https://www.tenable.com/plugins/nessus/51192	

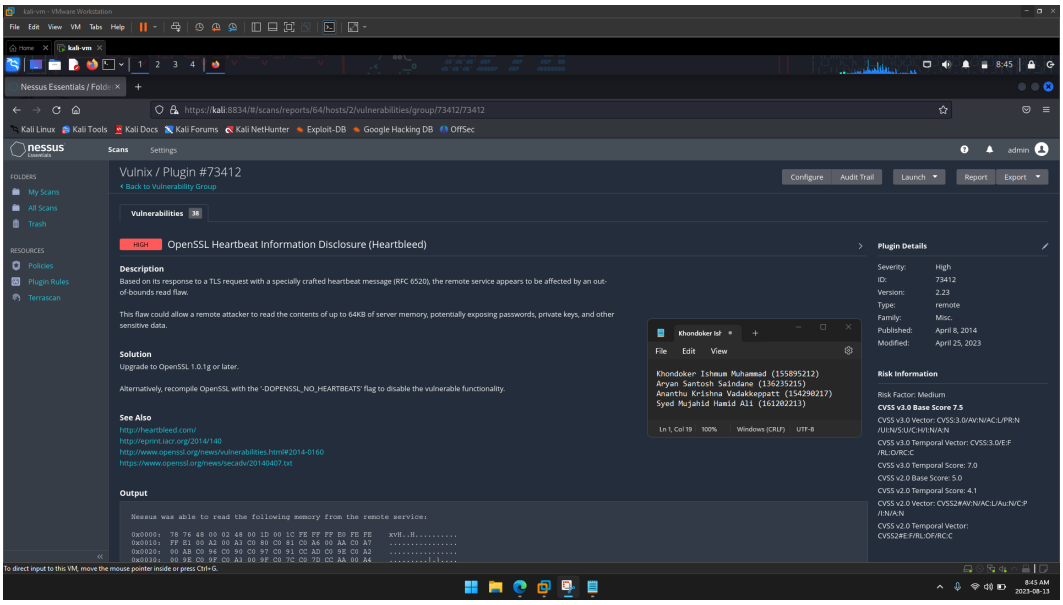
VulnVoIP VM		
Medium	V8 - SSH Weak Algorithms Supported	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	Nessus has identified an issue with the remote SSH server's configuration. It is either using the insecure Arcfour stream cipher or no cipher at all, which goes against the recommendations 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	

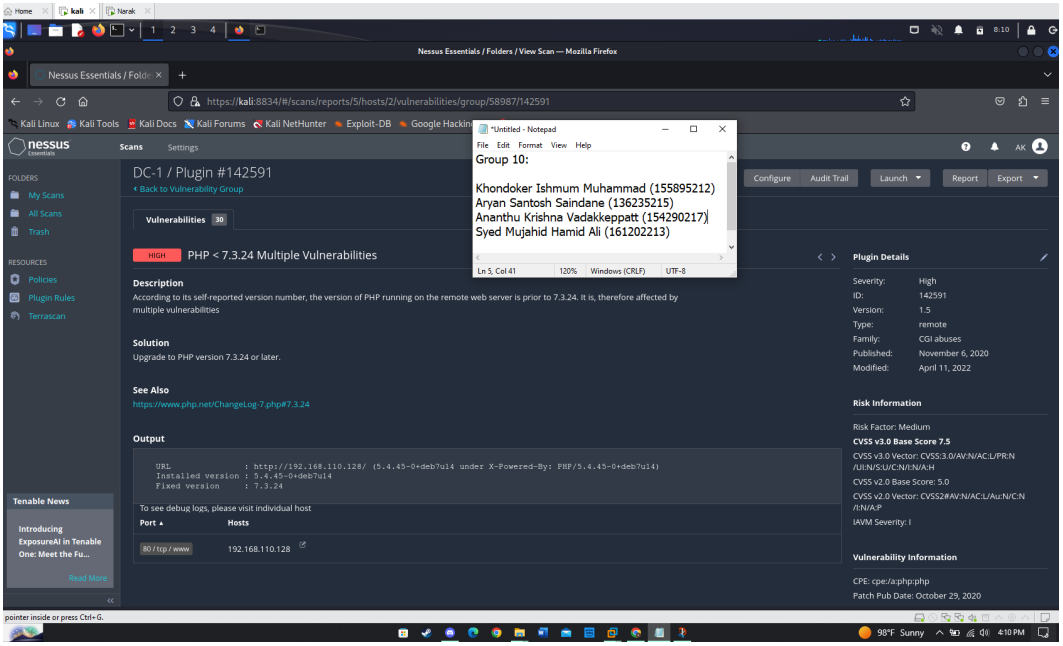
DC-1 VM		
Medium	V9 - JQuery 1.2 < 3.5.0 Multiple XSS	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	Based on the version reported in the script, the remote web server is using a version of jQuery that falls between 1.2 and 3.5.0. This version range is known to be impacted by multiple 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	

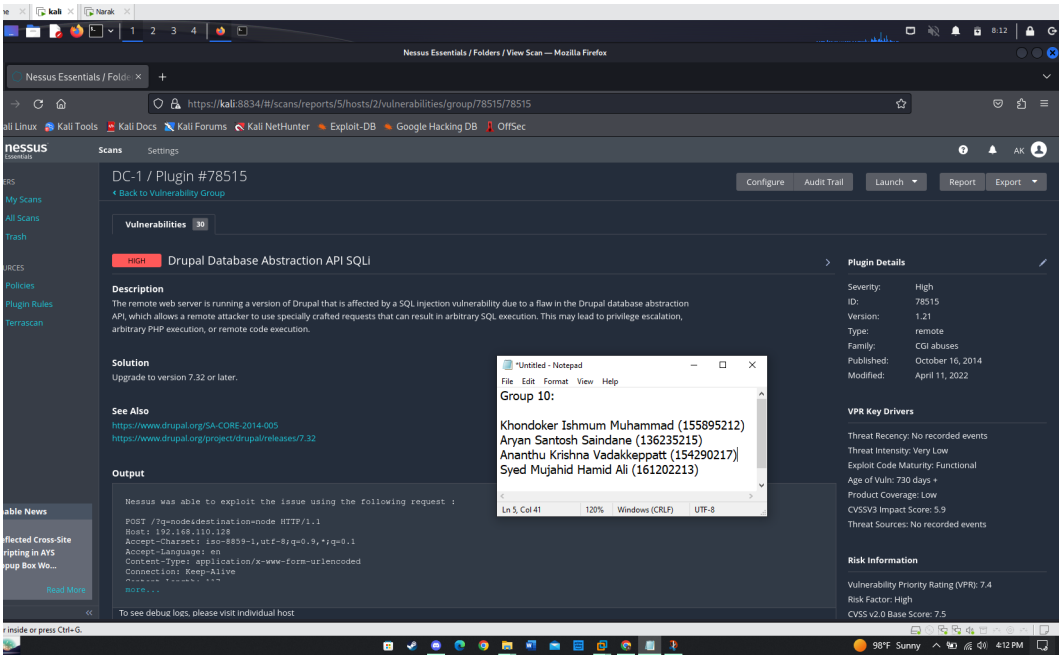
DC-1 VM		
Medium	V10 - web.config File Information Disclosure	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	An information disclosure vulnerability has been identified in the remote web server. This vulnerability arises from the inadvertent exposure of the "web.config" file. An attacker 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		
Reference	https://www.tenable.com/plugins/nessus/121479	

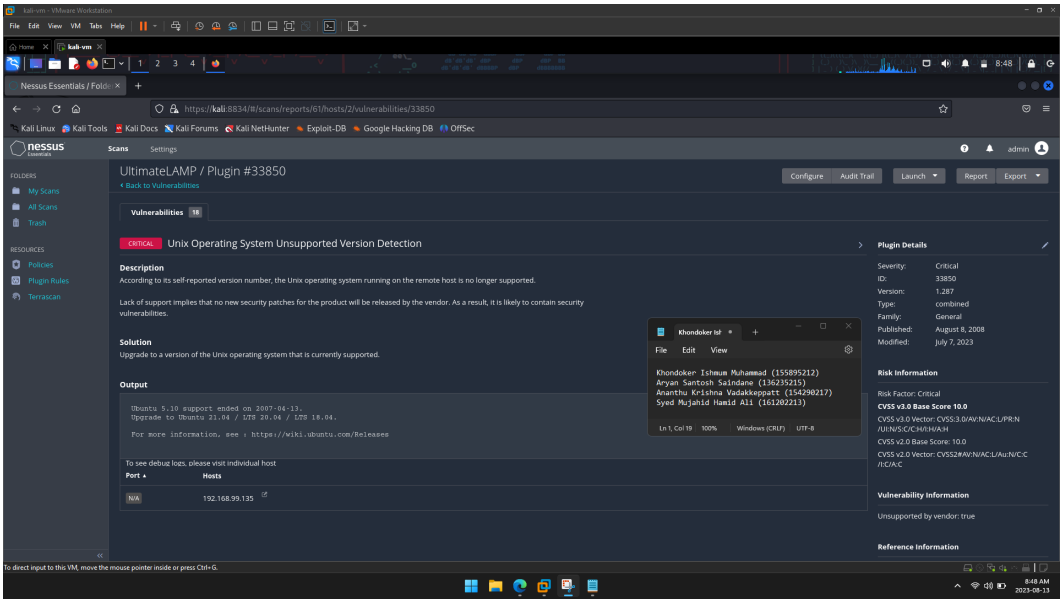
Vulnix VM		
High	V11 - NFS Shares World Readable	
Risk Assessment	Impact: Critical	Likelihood: Medium
Description	The NFS server is allowing access to one or more shares without any restrictions based on hostname, IP address, or IP range.	
CVSS Score	9.3	
Affected Scope	192.168.99.136	
Proof of Concept		
Reference	https://www.tenable.com/plugins/nessus/42256	

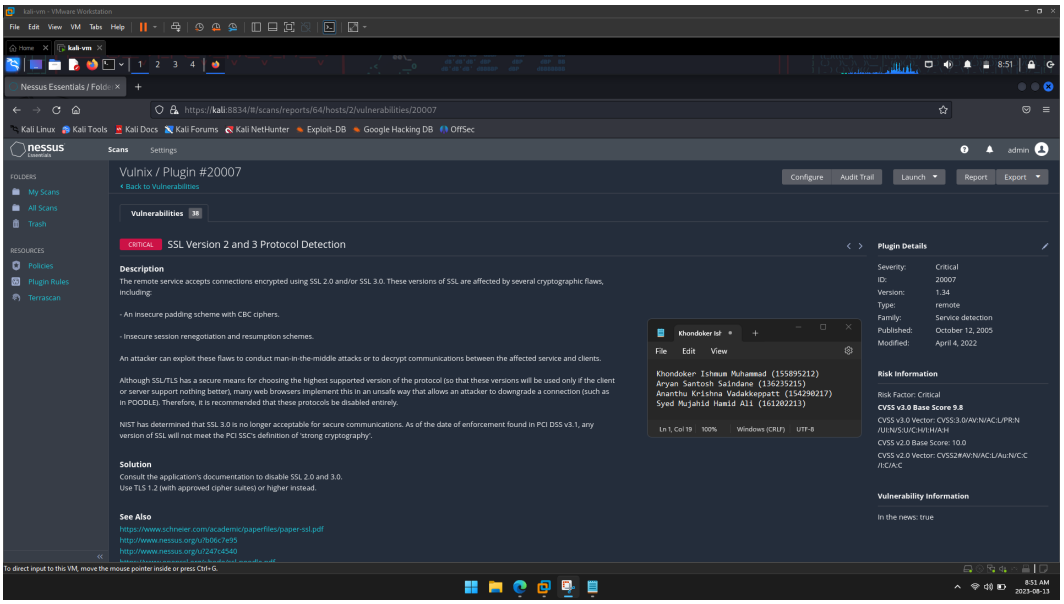
Vulnix VM		
High	V12 - SSL Medium Strength Cipher Suites Supported (SWEET32)	
Risk Assessment	Impact: High	Likelihood: Medium
Description	The remote host allows the use of SSL ciphers with medium strength encryption, defined as encryption with key lengths between 64 and 112 bits, or the use of the 3DES 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		
Reference	https://www.tenable.com/plugins/nessus/42873	

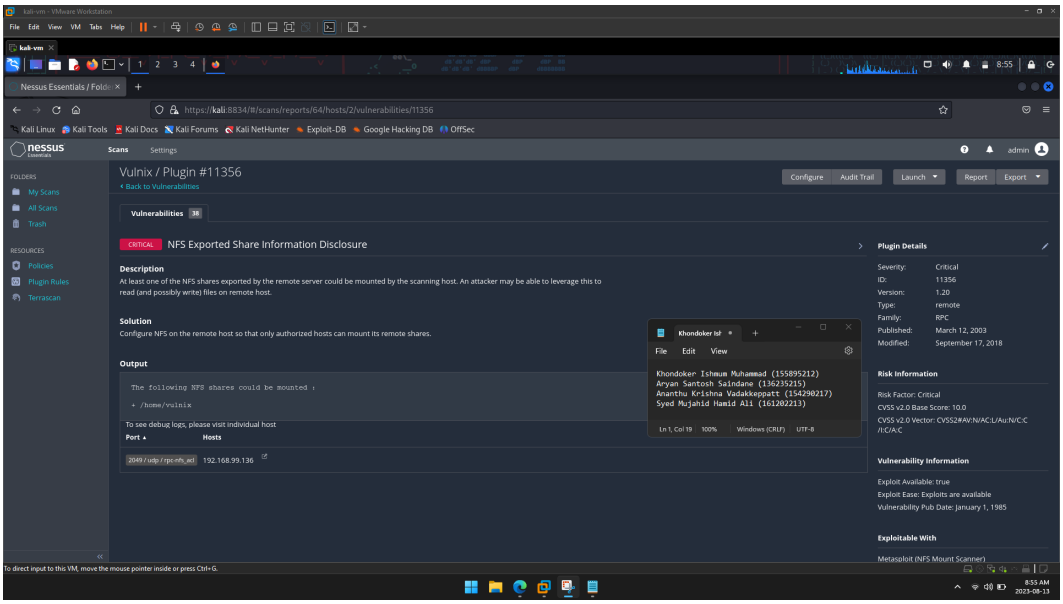
Vulnix VM		
High	V13 - OpenSSL Heartbeat Information Disclosure (Heartbleed)	
Risk Assessment	Impact: High	Likelihood: Medium
Description	The remote service is vulnerable to an out-of-bounds read flaw triggered by a specially crafted heartbeat message in a TLS request (RFC 6520). This flaw could be exploited 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		
Reference	https://www.tenable.com/plugins/nessus/73412	

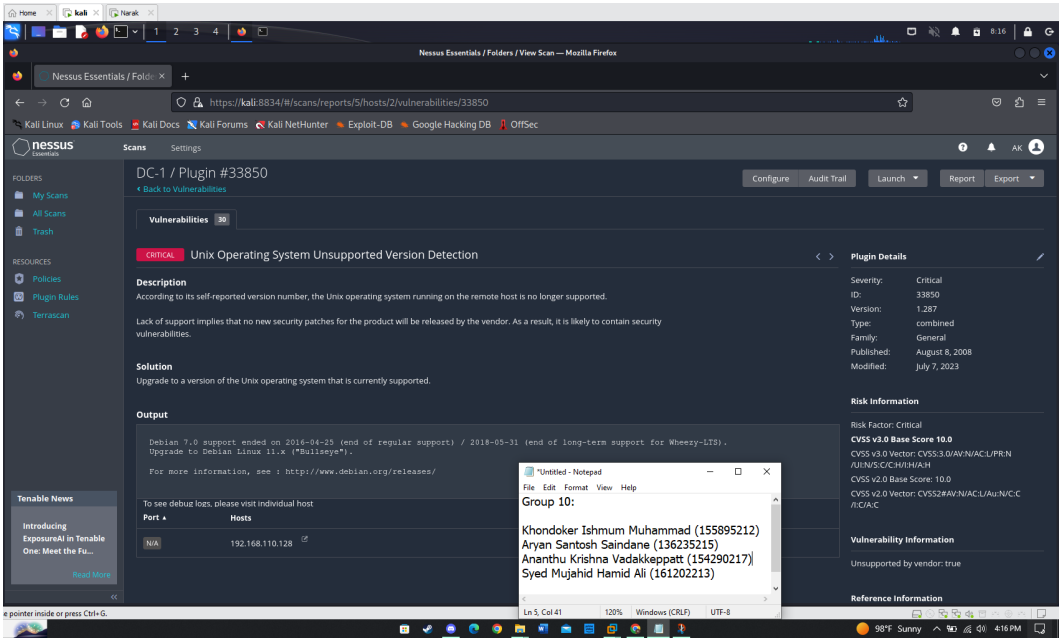
DC-1 VM		
High	V14 - PHP < 7.3.24 Multiple Vulnerabilities	
Risk Assessment	Impact: Critical	Likelihood: High
Description	The PHP version on the remote web server is reported to be older than 7.3.24. This version is known to be affected by several vulnerabilities. Without specifying the exact vulnerabilities, 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		
Reference	https://www.tenable.com/plugins/nessus/142591	

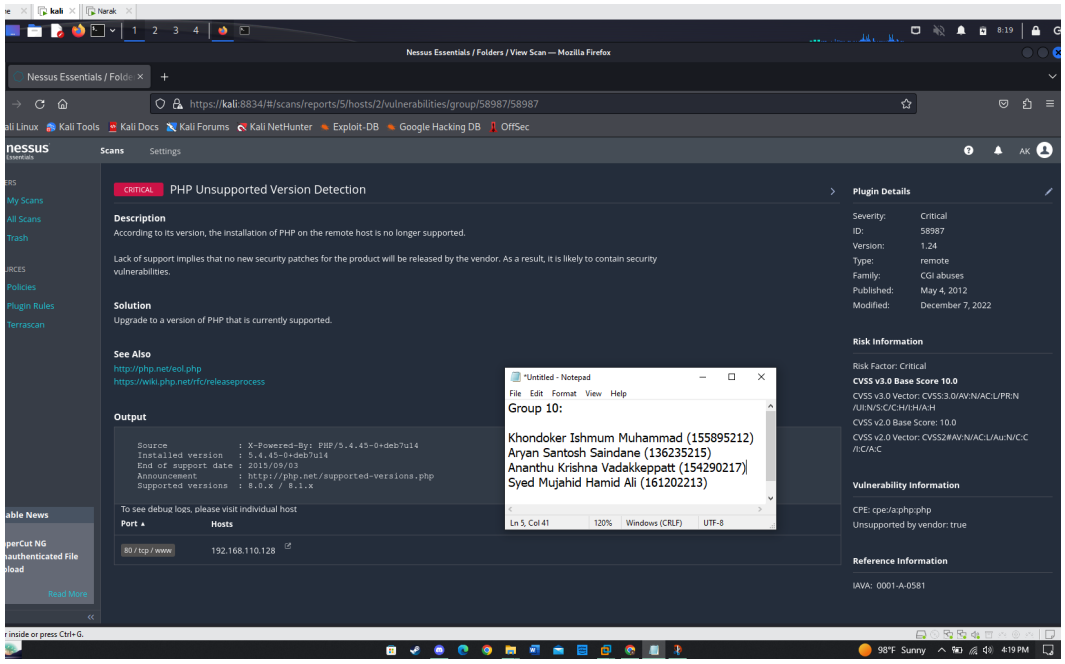
DC-1 VM		
High	V15 - Drupal Database Abstraction API SQLi	
Risk Assessment	Impact: Critical	Likelihood: High
Description	The version of Drupal installed on the remote web server is susceptible to a SQL injection vulnerability. This vulnerability stems from a flaw in the Drupal database abstraction API. 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		
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	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.	
CVSS Score	9.8	
Affected Scope	192.168.99.136	
Proof of Concept	We were able to find this vulnerability from the advanced scans conducted by Nessus. 	
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	We were able to find this vulnerability from the advanced scans conducted by Nessus. 	
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	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.	
CVSS Score	10	
Affected Scope	192.168.110.128	
Proof of Concept	We were able to find this vulnerability from the advanced scans conducted by Nessus. 	
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.