Vulnerability and Threat Analysis

RIS430 NAA

Group Project

Patching Report

Prepared By Group 10,

Khondoker Ishmum Muhammad (155895212)

Aryan Santosh Saindane (136235215)

Ananthu Krishna Vadakkeppatt (154290217)

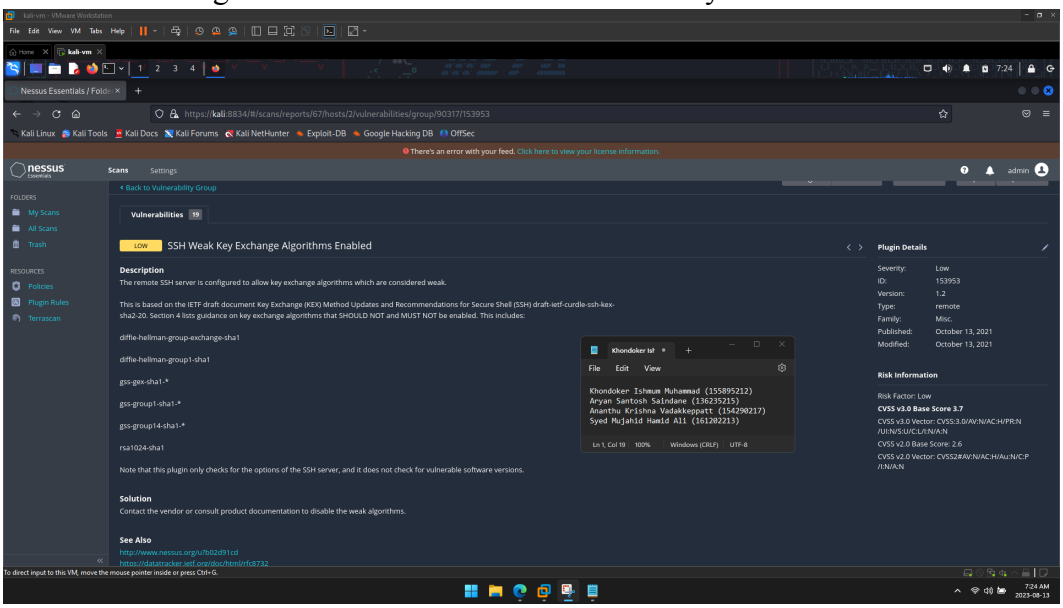
Syed Mujahid Hamid Ali (161202213)

Overview

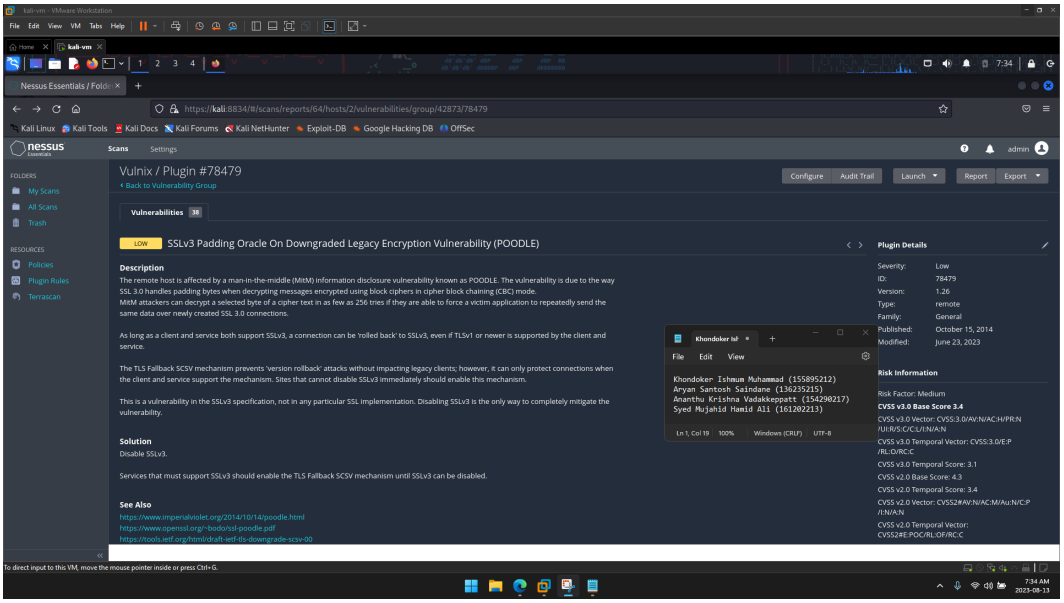
This is the patching report for the assignment. In this patching report we will talk about the patches of the vulnerabilities that we implemented into our devices. These patches are meant to not just mitigate the vulnerabilities within a system but also harden the system from potential malicious attacks in the future.

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	Critical

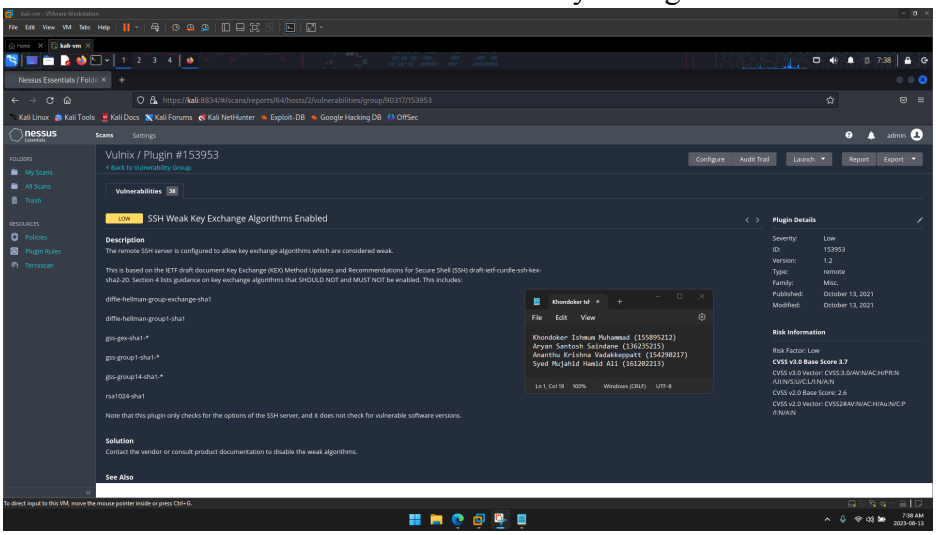
		Disclosure	
V19	DC-1 VM	Unix Operating System Unsupported Version Detection	Critical
V20	DC-1 VM	PHP Unsupported Version Detection	Critical

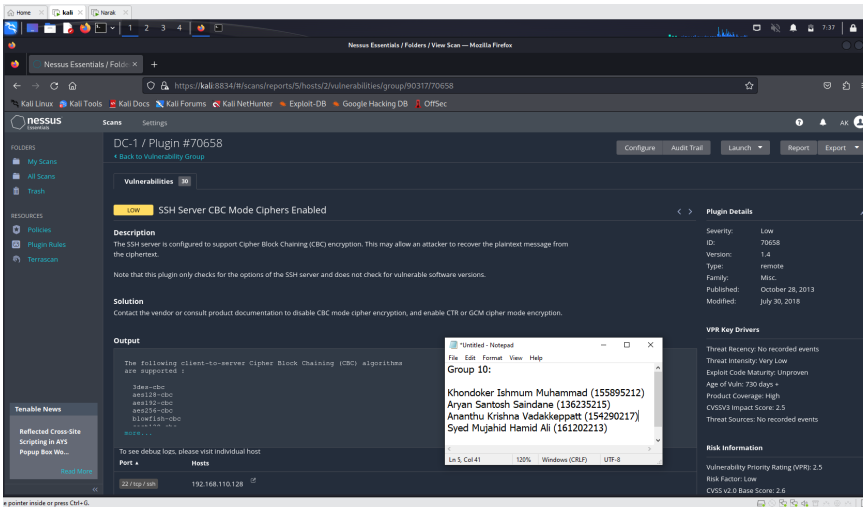
VulnVoIP VM			
Low	V1 - SSH Weak Key Exchange Algorithms Enabled		
Risk Assessment	Impact: Low		Likelihood: Low
Description	The remote SSH server allows weak key exchange algorithms as mentioned in the IETF draft document "Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)." 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. 		
Patching	The patch addresses a security vulnerability in a remote SSH server by disallowing the use of weak key exchange algorithms. The vulnerability is highlighted in an IETF draft document titled "Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)." The patch follows the document's guidelines and identifies specific key exchange algorithms that should not be permitted for use. These algorithms include Diffie-hellman-group-exchange-sha1, Diffie-hellman-group1-sha1, gss-gex-sha1-,		

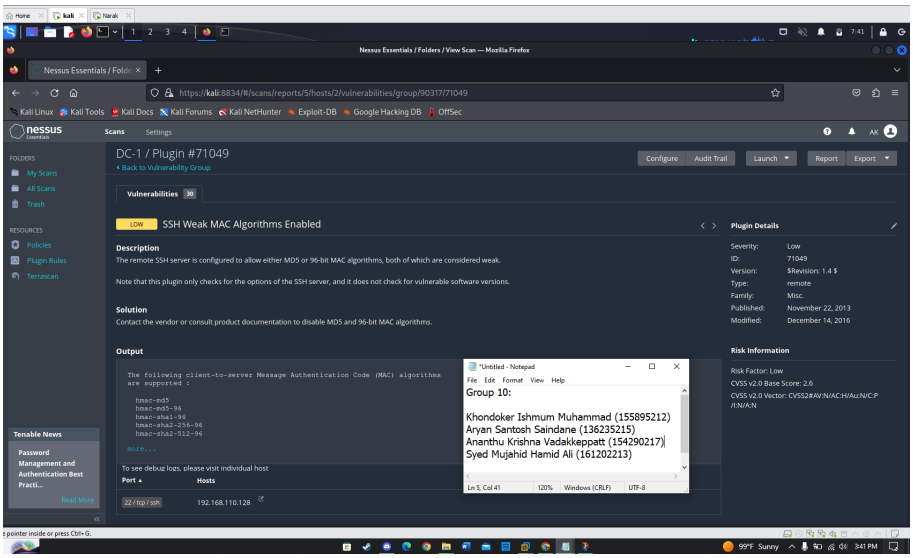
	gss-group1-sha1-, gss-group14-sha1-*, and rsa1024-sha1. The patch ensures that these vulnerable algorithms are no longer enabled in order to enhance the security of the SSH server.
Reference	https://www.tenable.com/plugins/nessus/153953

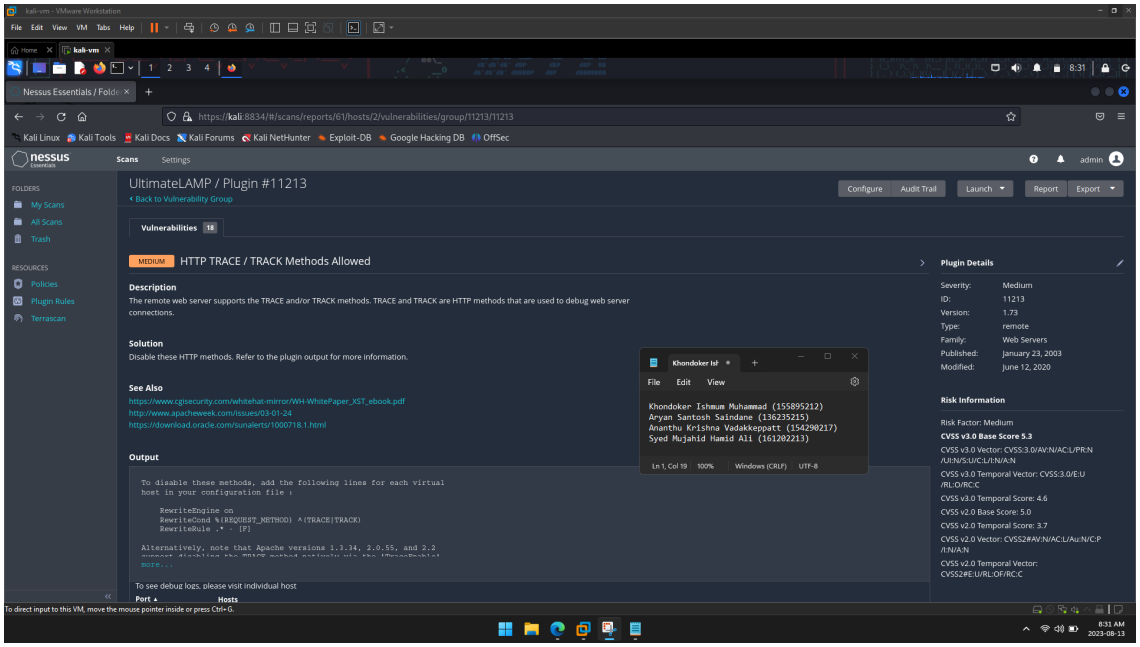
Vulnix VM		
Low	V2 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	
Risk Assessment	Impact: Low	Likelihood: Medium
Description	The remote host has a vulnerability called POODLE, which is a man-in-the-middle information disclosure issue. This vulnerability exists in SSL 3.0 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. 	
Patching	The provided patch addresses a vulnerability known as POODLE, which involves a man-in-the-middle information disclosure issue. The vulnerability affects SSL 3.0 and is related to the way padding is handled during message decryption using block ciphers in cipher block chaining (CBC) mode. Attackers could exploit this	

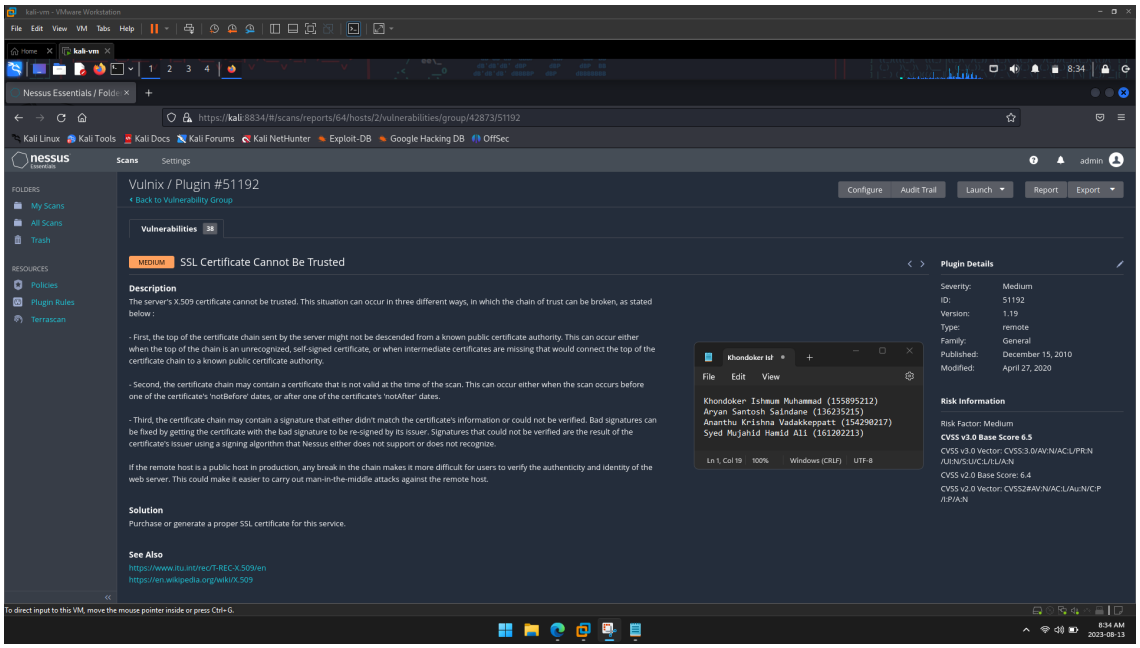
	vulnerability to decrypt a specific byte of cipher text with around 256 attempts. This would require the victim application to repeatedly send the same data over new SSL 3.0 connections. The patch addresses the issue where even if both the client and the service support newer TLS versions, a connection could still be downgraded to SSL 3.0. The patch introduces the TLS Fallback SCSV mechanism, which helps prevent version rollback attacks. However, for this mechanism to work, both the client and the service need to support it. To enhance security, websites that are still using SSLv3 are advised to enable the TLS Fallback SCSV mechanism. It's important to note that this vulnerability is inherent to the SSLv3 specification itself and is not specific to any particular SSL implementation. To fully eliminate this vulnerability, it's recommended to disable SSLv3 altogether.
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. 	
Patching	The provided patch addresses the issue of weak key exchange algorithms on the remote SSH server. These algorithms, outlined in Section 4 of the IETF draft document "Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)," are considered insecure and are not recommended for use. The listed algorithms, such as diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, gss-gex-sha1, gss-group1-sha1, gss-group14-sha1, and rsa1024-sha1, have been flagged as vulnerable and lacking in security. The patch involves disabling these algorithms to enhance the overall security of the SSH server.	
Reference	https://www.tenable.com/plugins/nessus/153953	

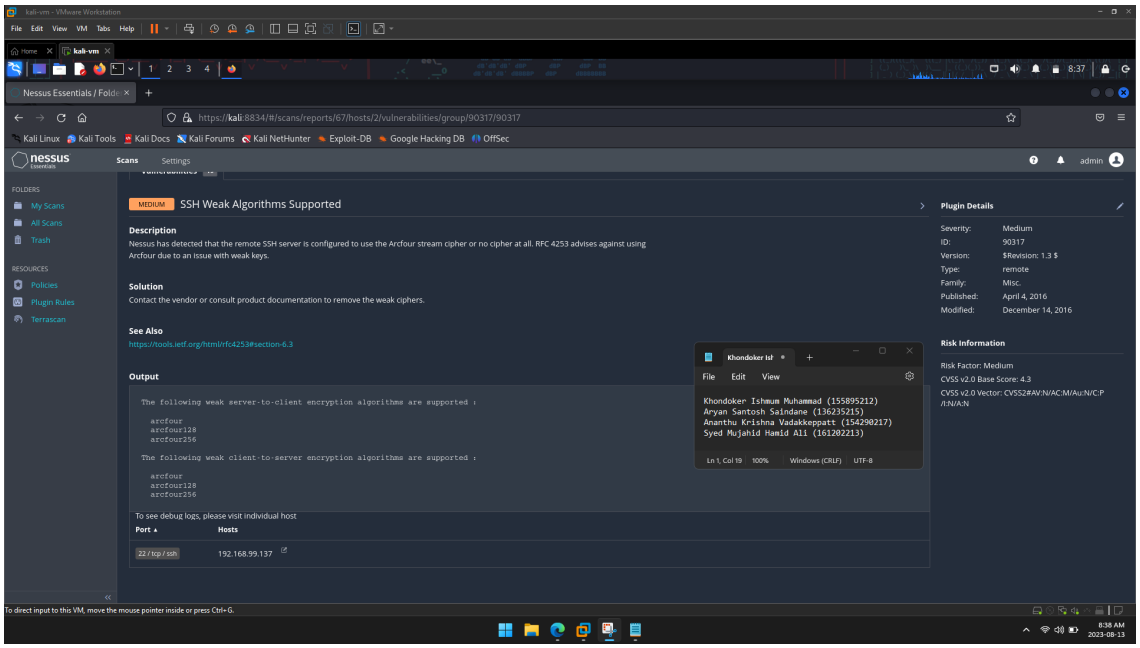
DC-1 VM		
Low	V4 - SSH Server CBC Mode Ciphers Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	The SSH server in question has been set up to use Cipher Block Chaining (CBC) encryption. CBC is a method of encryption that can be susceptible to certain types of attacks, potentially allowing 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		
Patching	The patch addresses a security concern in the SSH server setup, which utilizes Cipher Block Chaining (CBC) encryption. CBC encryption is vulnerable to specific attack methods that could enable an attacker to recover the original plaintext message from the encrypted data. It's important to emphasize that this warning pertains to the encryption configuration and not to the presence of software vulnerabilities. Consequently, employing CBC encryption in this SSH server configuration could pose a potential risk. The patch aims to enhance the server's security by likely recommending a more secure encryption method or configuration.	
Reference	https://www.tenable.com/plugins/nessus/70658	

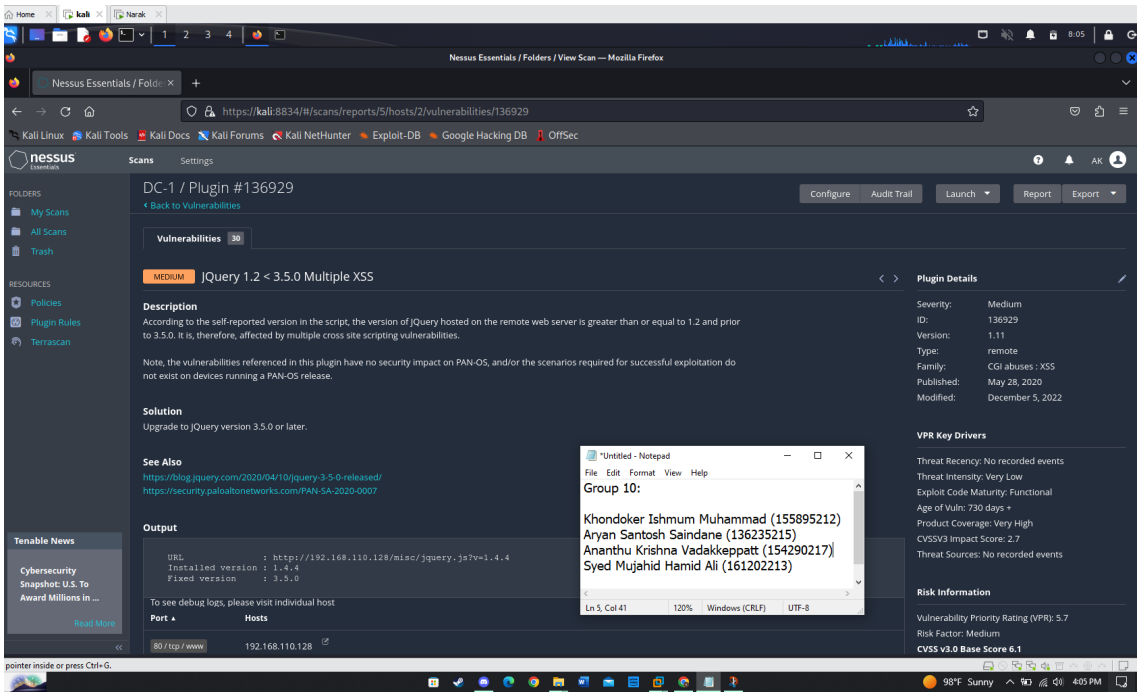
DC-1 VM		
Low	V5 - SSH Weak MAC Algorithms Enabled	
Risk Assessment	Impact: Low	Likelihood: Low
Description	The remote SSH server is set up to permit the use of either MD5 or 96-bit MAC (Message Authentication Code) algorithms. Both of these options are considered weak from a security standpoint. This 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. 	
Patching	The patch addresses the security concern of the remote SSH server allowing the use of weak MD5 and 96-bit MAC algorithms. These options pose risks due to the vulnerabilities of MD5 and the short MAC lengths, potentially exposing SSH communication to attacks. It's important to note that the patch only deals with the server's configuration choices and doesn't assess vulnerabilities arising from software versions.	
Reference	https://www.tenable.com/plugins/nessus/71049	

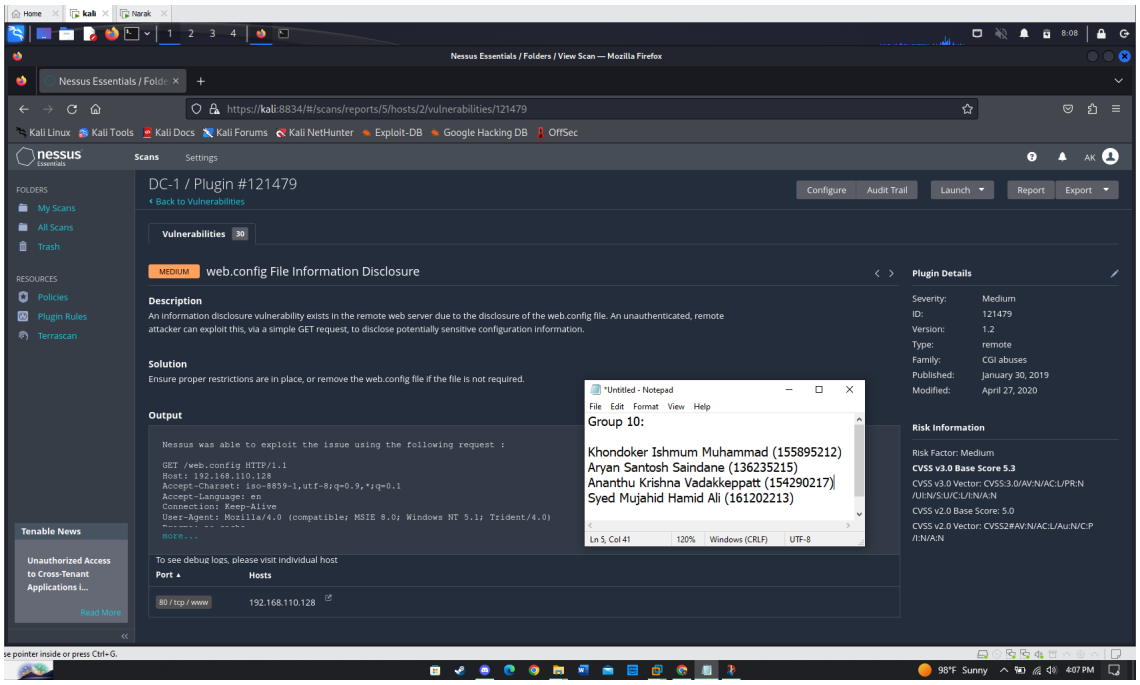
UltimateLAMP VM		
Medium	V6 - HTTP TRACE / TRACK Methods Allowed	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	The remote web server allows the use of the TRACE and/or TRACK methods, which are HTTP methods used for debugging web server connections.	
CVSS Score	5.3	
Affected Scope	192.168.99.135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

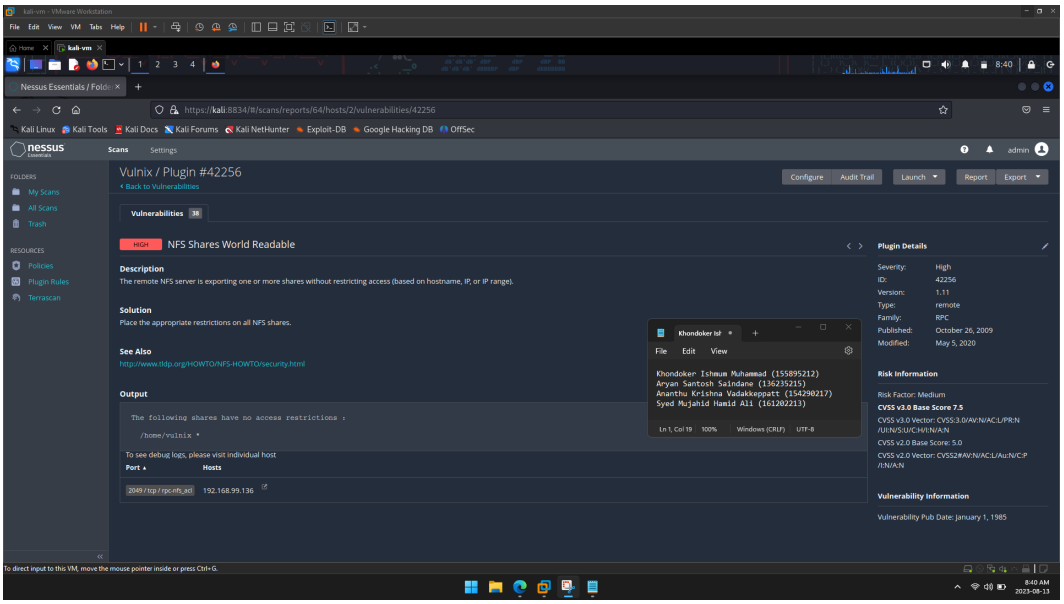
Vulnix VM		
Medium	V7 - SSL Certificate Cannot Be Trusted	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	The server's X.509 certificate trust issues can arise in three ways: 1. The certificate chain's top might not be linked to a recognized public certificate authority. This could be 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		
Patching	The patch addresses X.509 certificate trust issues on the server, which can occur in three ways: 1. The certificate chain's top might not be connected to a recognized public certificate authority, which could be due to a missing intermediate certificate or an unknown self-signed top certificate. 2. The chain might contain a certificate that's invalid during scanning, either before	

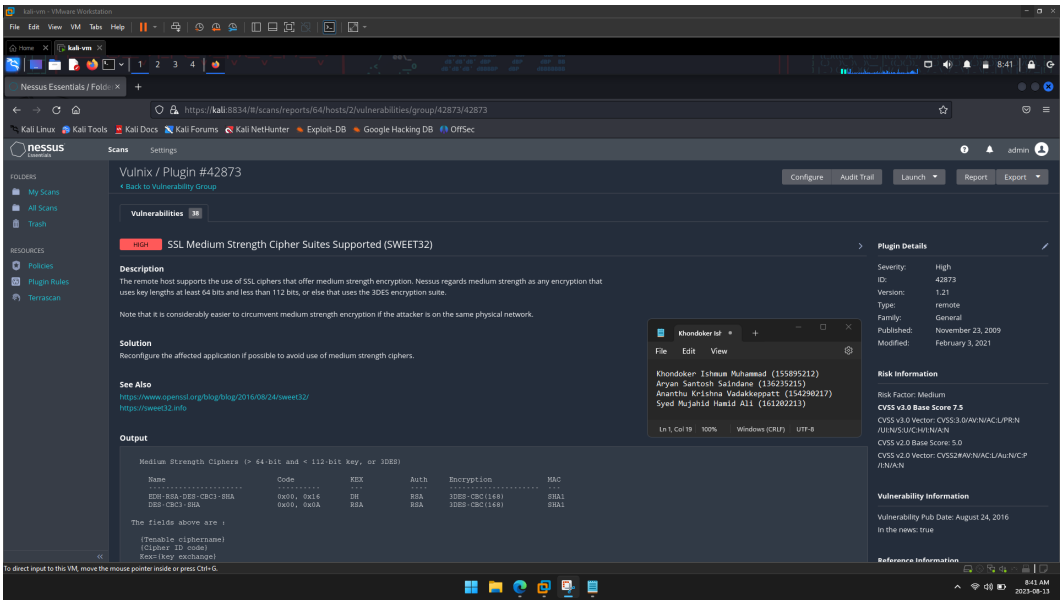
	its 'notBefore' date or after its 'notAfter' date. 3. The chain might have an unverifiable or mismatched signature, possibly due to unsupported signing algorithms by Nessus. If the certificate chain is compromised, it could potentially undermine users' ability to verify the authenticity of the web server, leading to vulnerabilities such as man-in-the-middle attacks. The patch aims to fix these issues for public production hosts.
Reference	https://www.tenable.com/plugins/nessus/51192

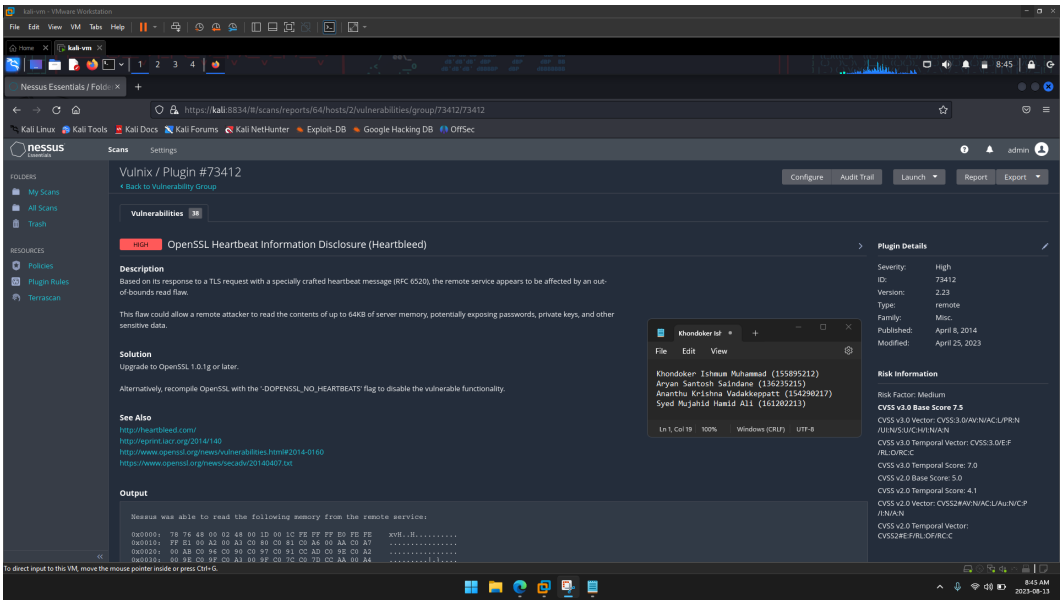
VulnVoIP VM		
Medium	V8 - SSH Weak Algorithms Supported	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	Nessus has identified an issue with the remote SSH server's configuration. It is either using the insecure Arcfour stream cipher or no cipher at all, which goes against the recommendations 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	
Patching	The remote SSH server's configuration has been flagged by Nessus due to either using the insecure Arcfour stream cipher or not using any cipher at all. This contradicts the guidelines outlined in RFC 4253. This is a concern because the Arcfour cipher has a vulnerability associated with weak keys. The issue needs to be addressed to ensure the security of the SSH server.	
Reference	https://www.tenable.com/plugins/nessus/90317	

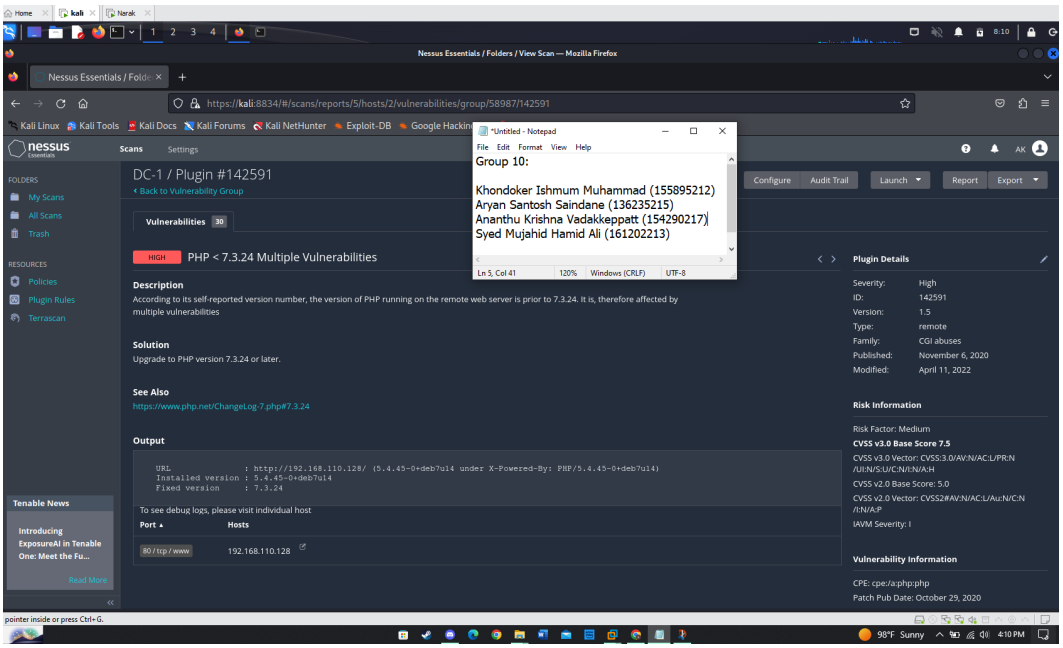
DC-1 VM		
Medium	V9 - JQuery 1.2 < 3.5.0 Multiple XSS	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	Based on the version reported in the script, the remote web server is using a version of jQuery that falls between 1.2 and 3.5.0. This version range is known to be impacted by multiple 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		
Patching	The patch addresses a vulnerability in the remote web server's jQuery version, which lies between 1.2 and 3.5.0. This range is known to have several cross-site scripting (XSS) vulnerabilities. Exploiting these vulnerabilities could enable attackers to insert harmful code into users' web pages, potentially causing security compromises. The patch aims to fix these issues and enhance the server's security.	
Reference	https://www.tenable.com/plugins/nessus/136929	

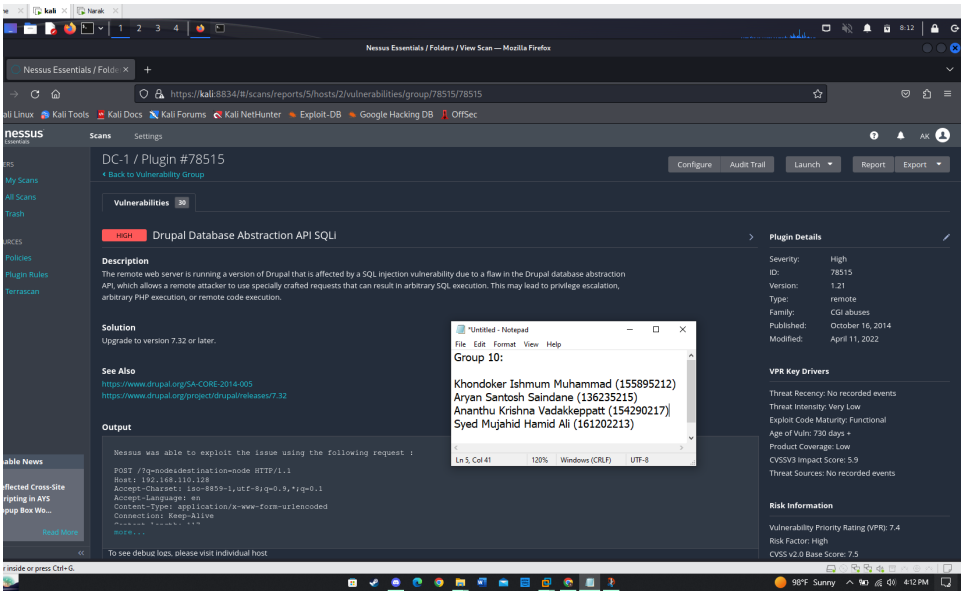
DC-1 VM		
Medium	V10 - web.config File Information Disclosure	
Risk Assessment	Impact: Medium	Likelihood: Medium
Description	An information disclosure vulnerability has been identified in the remote web server. This vulnerability arises from the inadvertent exposure of the "web.config" file. An attacker 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		
Patching	The patch addresses an information disclosure vulnerability found in the remote web server. This vulnerability stems from the accidental exposure of the "web.config" file. Attackers without authentication can take advantage of this by sending a simple GET request to the server. This could result in the unauthorized disclosure of sensitive configuration information. The patch rectifies this issue and prevents such unauthorized access.	
Reference	https://www.tenable.com/plugins/nessus/121479	

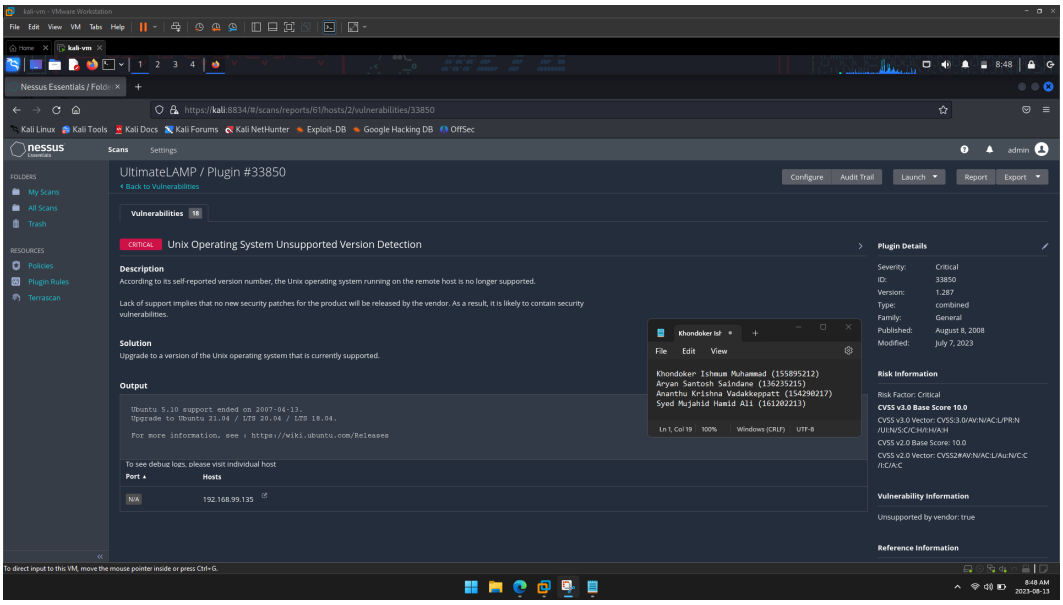
Vulnix VM		
High	V11 - NFS Shares World Readable	
Risk Assessment	Impact: Critical	Likelihood: Medium
Description	The NFS server is allowing access to one or more shares without any restrictions based on hostname, IP address, or IP range.	
CVSS Score	9.3	
Affected Scope	192.168.99.136	
Proof of Concept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

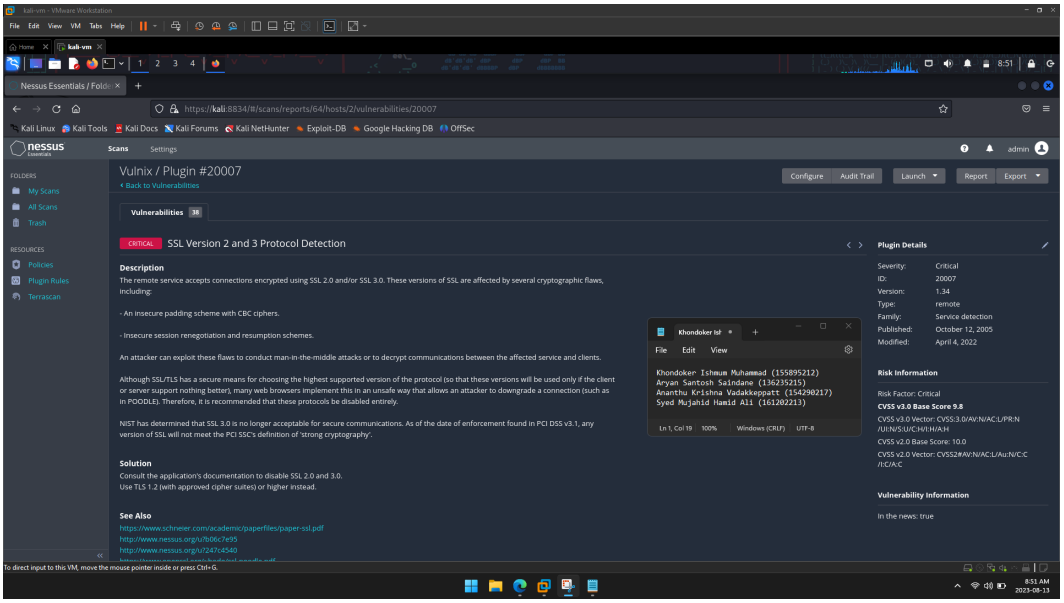
Vulnix VM		
High	V12 - SSL Medium Strength Cipher Suites Supported (SWEET32)	
Risk Assessment	Impact: High	Likelihood: Medium
Description	The remote host allows the use of SSL ciphers with medium strength encryption, defined as encryption with key lengths between 64 and 112 bits, or the use of the 3DES 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		
Patching	The patch addresses a vulnerability in the remote host's SSL ciphers, which currently permit the use of encryption with key lengths ranging from 64 to 112 bits or the 3DES encryption suite. This medium-strength encryption can be compromised more easily if an attacker shares the same physical network. The patch aims to strengthen the security by mitigating this vulnerability and preventing potential network-based attacks.	
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		
Patching	The patch addresses a vulnerability in a remote service where an attacker could exploit an out-of-bounds read flaw through a manipulated heartbeat message in a TLS request. This flaw could lead to unauthorized access to approximately 64KB of server memory, potentially exposing sensitive data such as passwords and private keys. The patch aims to prevent this security risk and protect the server from potential attacks.	
Reference	https://www.tenable.com/plugins/nessus/73412	

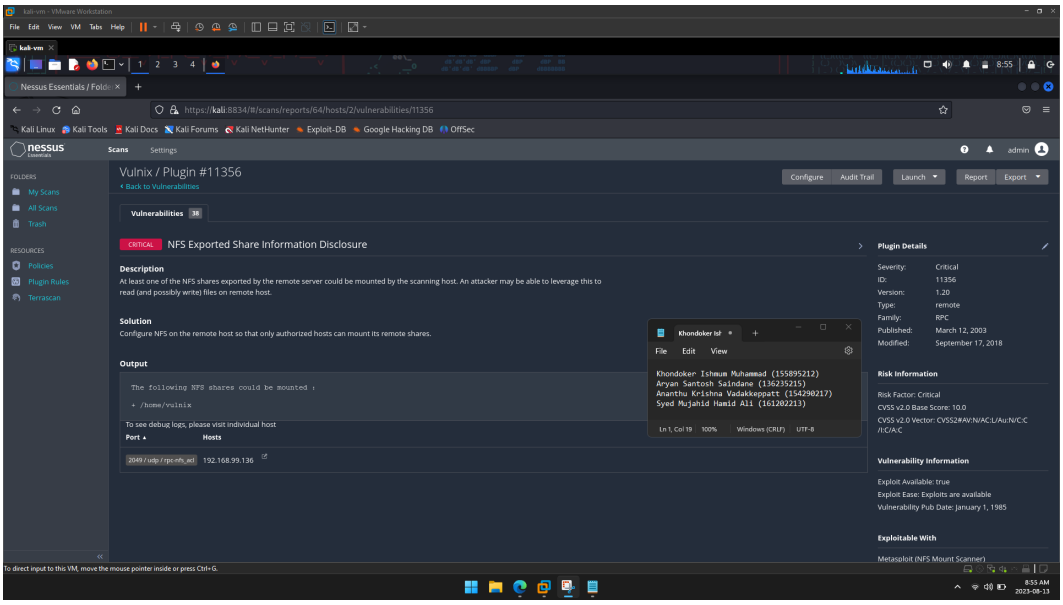
DC-1 VM		
High	V14 - PHP < 7.3.24 Multiple Vulnerabilities	
Risk Assessment	Impact: Critical	Likelihood: High
Description	The PHP version on the remote web server is reported to be older than 7.3.24. This version is known to be affected by several vulnerabilities. Without specifying the exact vulnerabilities, 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		
Patching	The remote web server has an outdated PHP version (older than 7.3.24), which is susceptible to multiple vulnerabilities. Although the specific vulnerabilities aren't mentioned, it's crucial to understand that using an outdated PHP version exposes the server to security risks. Older versions often contain known security flaws that attackers can exploit. To mitigate these risks, updating to a newer PHP version is recommended.	
Reference	https://www.tenable.com/plugins/nessus/142591	

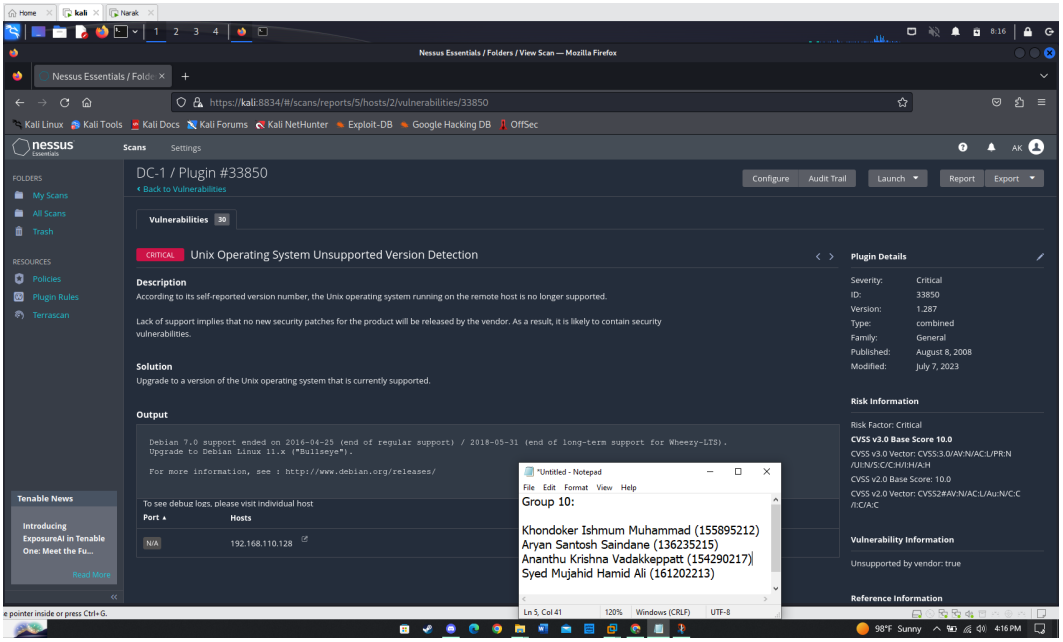
DC-1 VM		
High	V15 - Drupal Database Abstraction API SQLi	
Risk Assessment	Impact: Critical	Likelihood: High
Description	The version of Drupal installed on the remote web server is susceptible to a SQL injection vulnerability. This vulnerability stems from a flaw in the Drupal database abstraction API. 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		
Patching	The patch addresses a SQL injection vulnerability in the installed version of Drupal on a remote web server. The vulnerability originates from a weakness in the Drupal database abstraction API. By sending carefully crafted requests, attackers can exploit this vulnerability to execute unauthorized SQL commands. This can lead to serious consequences including privilege escalation, executing PHP code, and potentially even remote code execution on the compromised system. The patch aims to fix this vulnerability and prevent such malicious activities.	
Reference	https://www.tenable.com/plugins/nessus/78515	

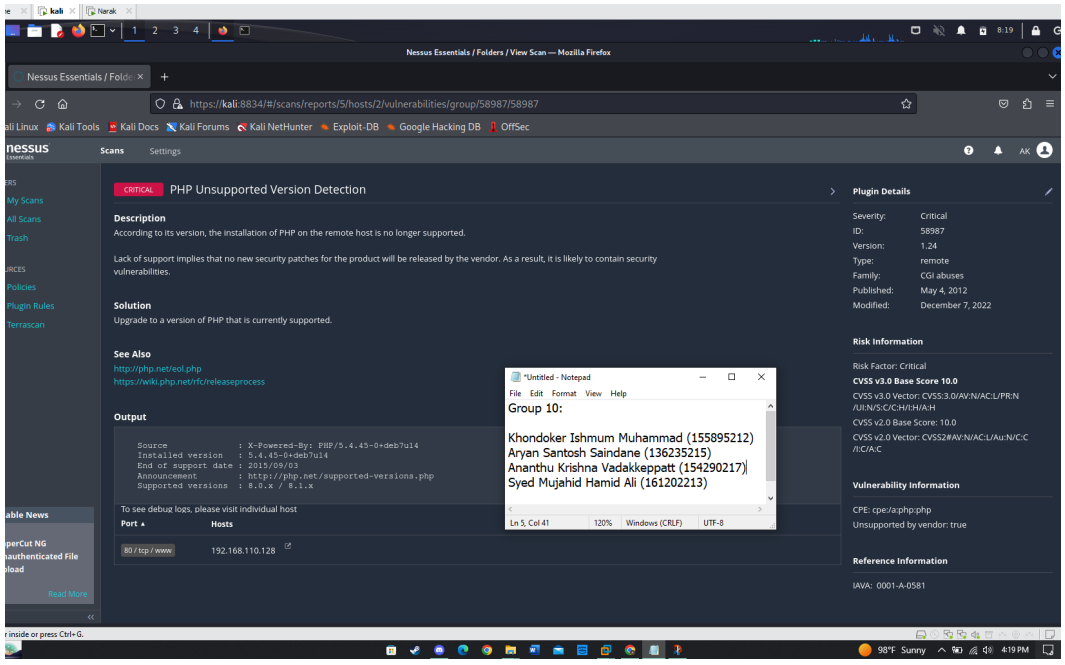
UltimateLAMP VM		
Critical	V16 - Unix Operating System Unsupported Version Detection	
Risk Assessment	Impact: Critical	Likelihood: Critical
Description	The remote host is running an unsupported version of the Unix operating system, which means it won't receive any new security patches from the vendor. This makes it susceptible to security vulnerabilities.	
CVSS Score	10	
Affected Scope	192.168.99.135	
Proof of Concept		
Patching	The system is running an outdated and unsupported version of the Unix operating system. As a result, it won't receive any further security updates from the vendor, leaving it vulnerable to potential security threats.	
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. 	
Patching	The patch addresses a security vulnerability in a remote service that currently allows connections encrypted using insecure versions of SSL (SSL 2.0 and SSL 3.0). These versions have cryptographic weaknesses such as insecure padding schemes and session renegotiation problems. Exploiting these flaws could lead to	

	man-in-the-middle attacks and the decryption of communication between the service and clients. Some web browsers also have unsafe implementations that enable attackers to downgrade connections. To mitigate these risks, it is advised to disable SSL 2.0 and SSL 3.0 protocols entirely. The National Institute of Standards and Technology (NIST) has labeled SSL 3.0 as insecure, and any version of SSL is considered inadequate according to strong cryptography standards defined by PCI SSC, effective after the enforcement date in PCI DSS v3.1.
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. 	
Patching	The provided patch addresses a vulnerability where a scanning host can connect to an NFS share on a remote server. This flaw could enable an attacker to gain unauthorized access to the remote host and manipulate its files. The patch aims to prevent this potential security breach by implementing necessary safeguards.	
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. 	
Patching	The remote host's Unix operating system is no longer supported by the vendor, leaving it without new security patches or updates. This increases the risk of security vulnerabilities, making the system susceptible to exploitation by attackers who could take advantage of these weaknesses due to the lack of new patches.	
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		
Patching	The remote host's PHP installation is no longer supported by the vendor, which means it won't receive any new security patches or updates. This makes the installation vulnerable to security risks and potential exploits. The lack of new patches increases the risk of malicious actors taking advantage of vulnerabilities in the PHP version to compromise the system.	
Reference	https://www.tenable.com/plugins/nessus/156255	

Conclusion

In conclusion, we have detailed our patches that we have implemented to mitigate and harden our software and hardware inventory. From Windows machines to Ubuntu machines, the software, webservices, general services, we carried out a number of patches. With these patches we are making sure that our systems, software, and services are able to fight off future potential malicious attacks by threat actors.