Vulnerability Assessment Report

Vulnerability Assessment on Agricore

Prepared For:

Marc Hayes

Seneca Polytechnic

Prepared By:

Ornan Roberts

Syed Mujahid Hamid Ali

Ramachandra Muralidhara

Yannish Kumar Ballachandher Sreedevi

December 11, 2023

Table of Contents

Executive Summary 3
Scope 3
Assessment Findings 4
Nessus Scans 4
Vulnerabilities Summary Table 6
NMAP Scans 17
Mitigation Strategies 20
Conclusion 23

Executive Summary

The report outlines the key findings on the vulnerabilities discovered within the infrastructure. The infrastructure for Agricore, an ecommerce business was deployed and vulnerability scans were conducted on the network. Through the vulnerability assessment, key insights into the security posture of Agricore's infrastructure were discovered. The report meticulously documents the vulnerabilities discovered, categorizing them based on the severity levels. Nessus is the vulnerability scanning tool that was used to identify and address security vulnerabilities in the systems. Similarly, NMAP scans were also performed to check for weakness in the system. Lastly, we discuss some of the mitigation strategies actions based on the solutions presented by these scanners. We discuss some recommendations that can be added to remediate these weaknesses.

Based on the Nessus scans the following is a brief overview of the vulnerabilities based on the severity levels.

Critical	High	Medium	Low	Info
0	0	16	1	300

Scope

The scope of the assessment is limited to the domain of www.agricore-spr.com to evaluate the security posture. The sole purpose of scanning is to identify and mitigate potential vulnerabilities that could compromise the integrity and of business assets. The scans were conducted using multiple scanners which consisted of Nessus and NMAP. The assets consist of web applications, databases, network architecture, and associated components. Both internal and external-facing systems are within the defined scope on which the scanning was conducted. The assessment will employ a combination of vulnerability scanning tools and analysis of system configurations. The tools are chosen for their ability to detect a diverse range of vulnerabilities and security issues.

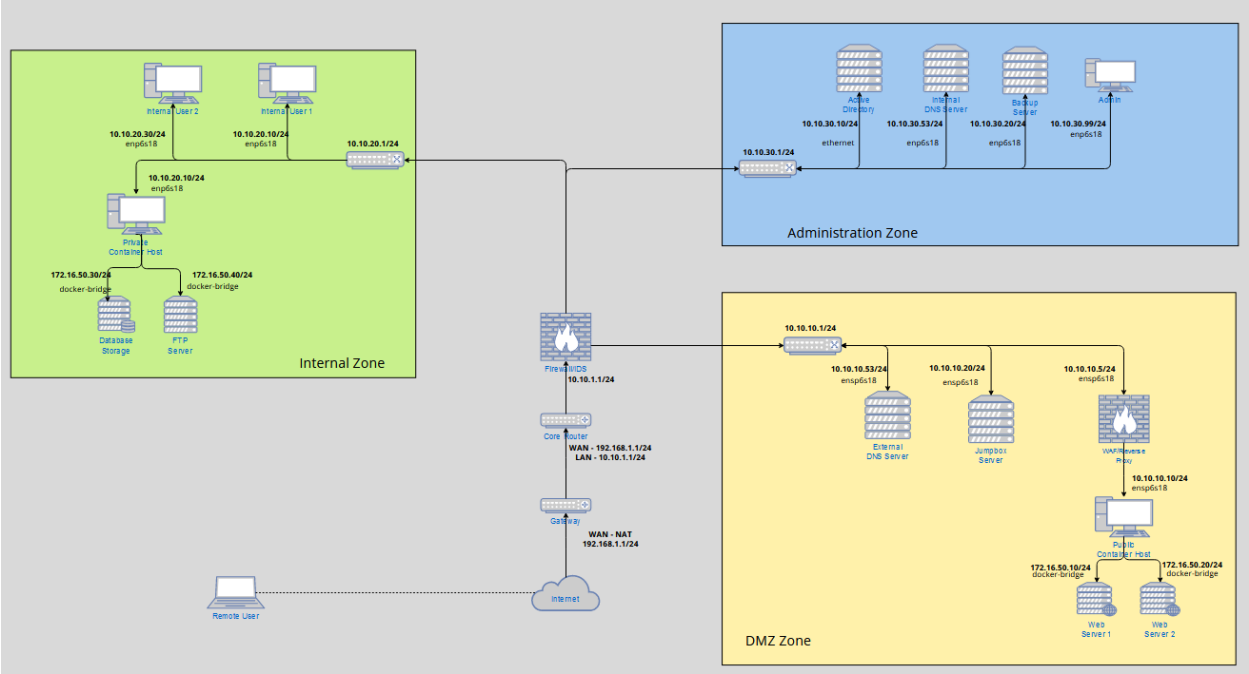


Fig.1 Network Topology

Assessment Findings

Nessus Scans

Based on the scans conducted on the Agricore network the following is the overview of the vulnerabilities discovered using Nessus. As we can see, the majority of the vulnerabilities were informational. The information vulnerabilities are not directly leading to unauthorized access or compromise of a system and may not pose an immediate threat on their own. A few vulnerabilities with medium and low severity levels were discovered on some of the systems within the infrastructure.

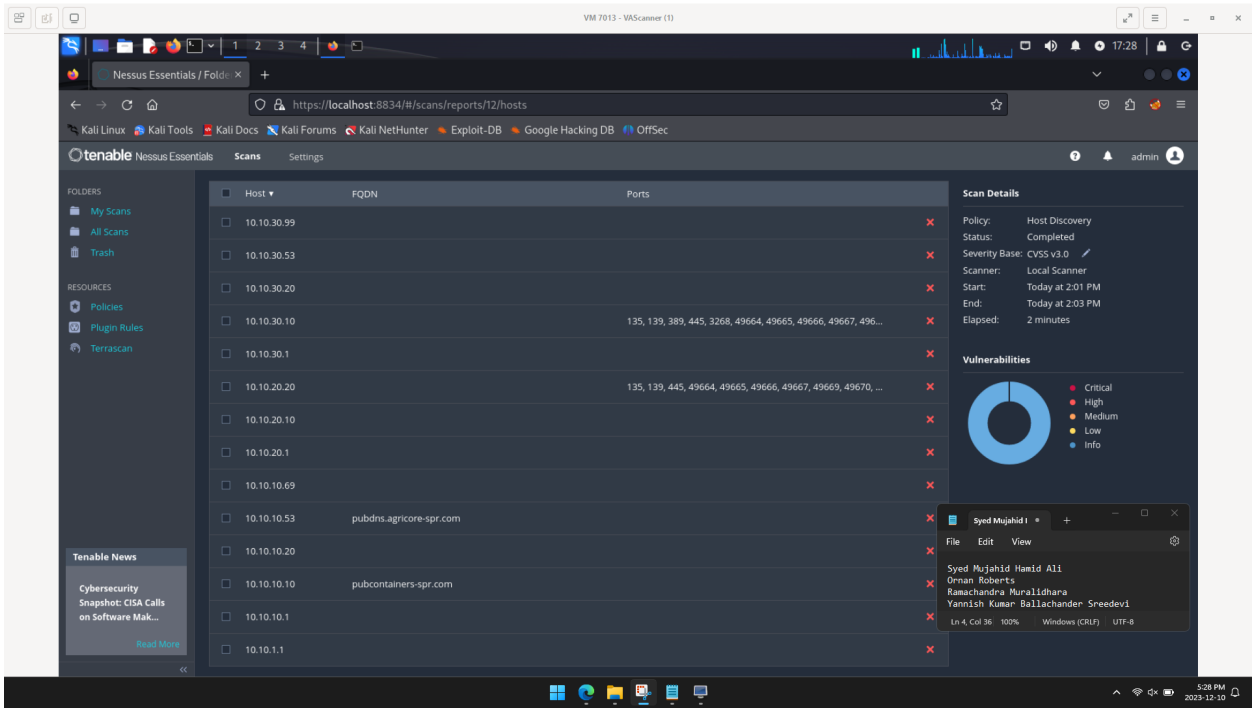


Fig.1 Hosts discovery during the network scan

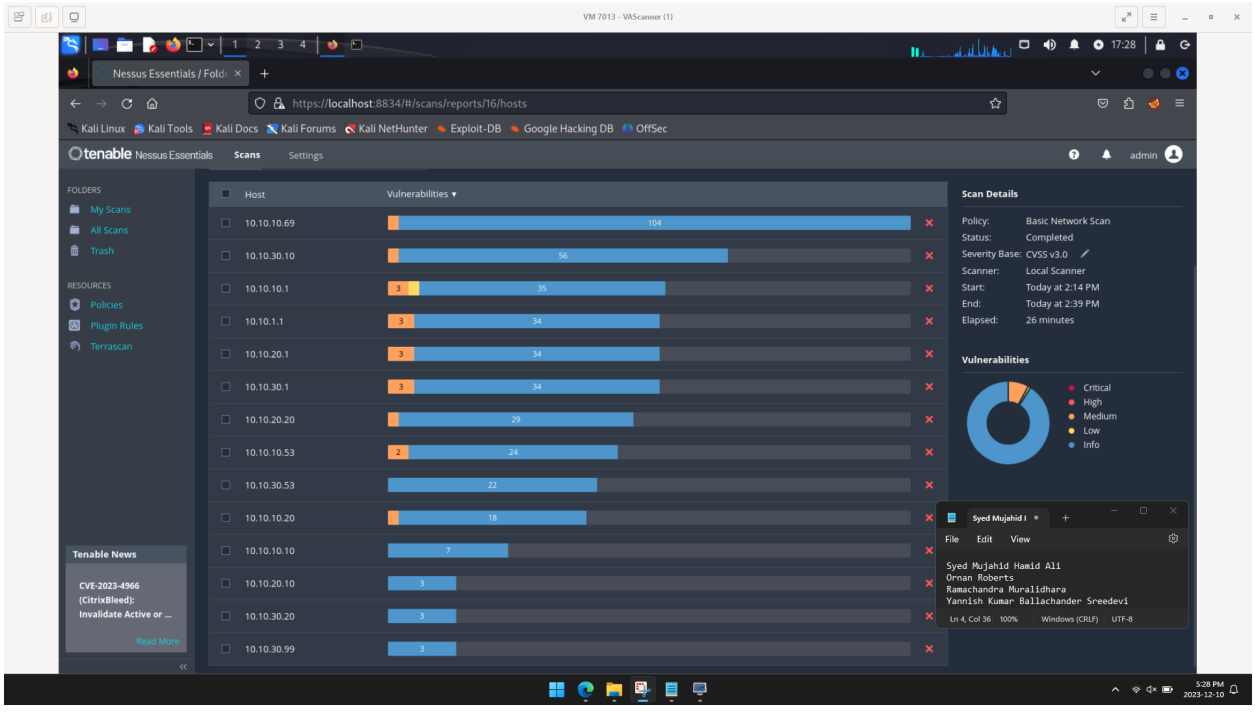


Fig.2 vulnerabilities discovered for network scan

Vulnerabilities Summary Table

The following table shows the summary of vulnerabilities discovered during the scans. Since there is a majority of informational vulnerabilities and some of the medium severity were repeated therefore we will be only discussing the following.

Vulnerability ID	Name	Severity Level
1	Query 1.2 < 3.5.0 Multiple XSS	Medium
2	SSL Certificate Cannot Be Trusted	Medium
3	Microsoft Windows EFSRPC NTLM Reflection	Medium
4	Network Time Protocol (NTP) Mode 6 Scanner	Medium
5	SSL Self-Signed Certificate	Medium
6	SMB Signing not required	Medium
7	DNS Server Cache Snooping Remote Information Disclosure	Medium
8	DNS Server Zone Transfer Information Disclosure (AXFR)	Medium
9	IP Forwarding Enabled	Medium
10	DHCP Server Detection	Low

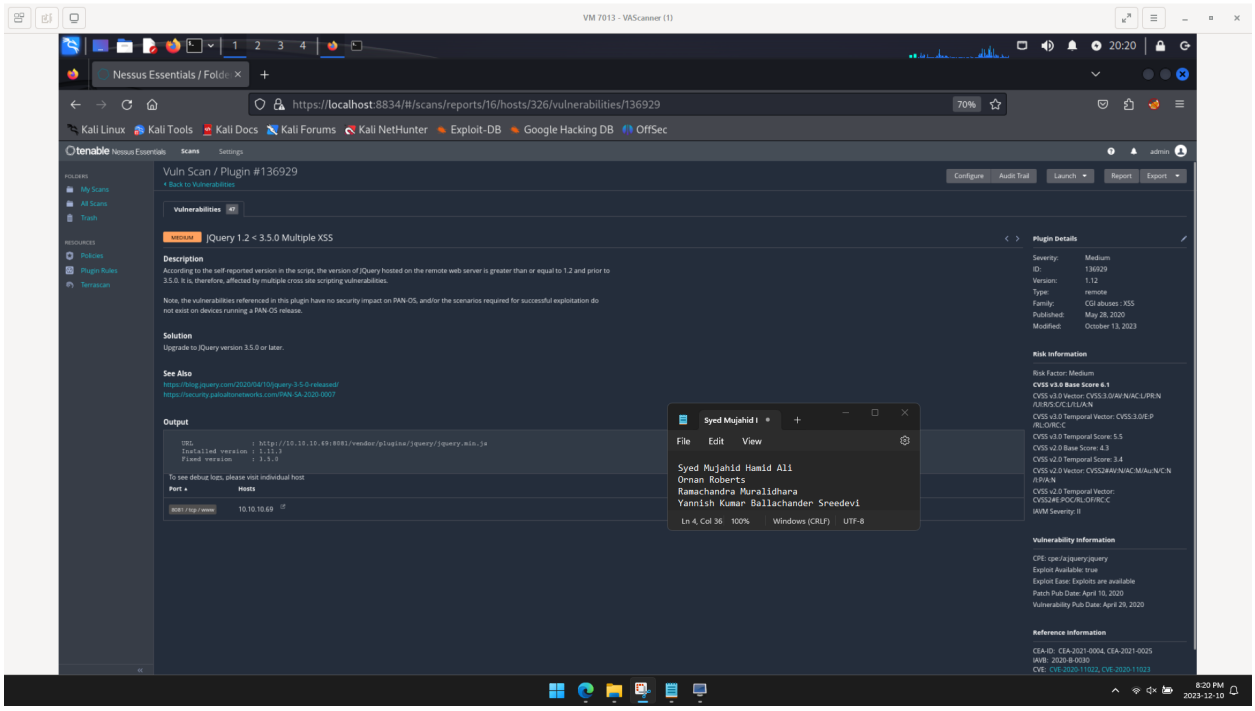
V1 - Query 1.2 < 3.5.0 Multiple XSS

Description: As per the self-disclosed information in the script, the jQuery version present on the external web server is equal to or exceeds 1.2 but is less than 3.5.0. Consequently, it is susceptible to several cross-site scripting vulnerabilities.

Severity: Medium

Affected Scope: 10.10.10.69

Proof of Concept:



Solution: Upgrade to JQuery version 3.5.0 or later.

V2 - SSL Certificate Cannot Be Trusted

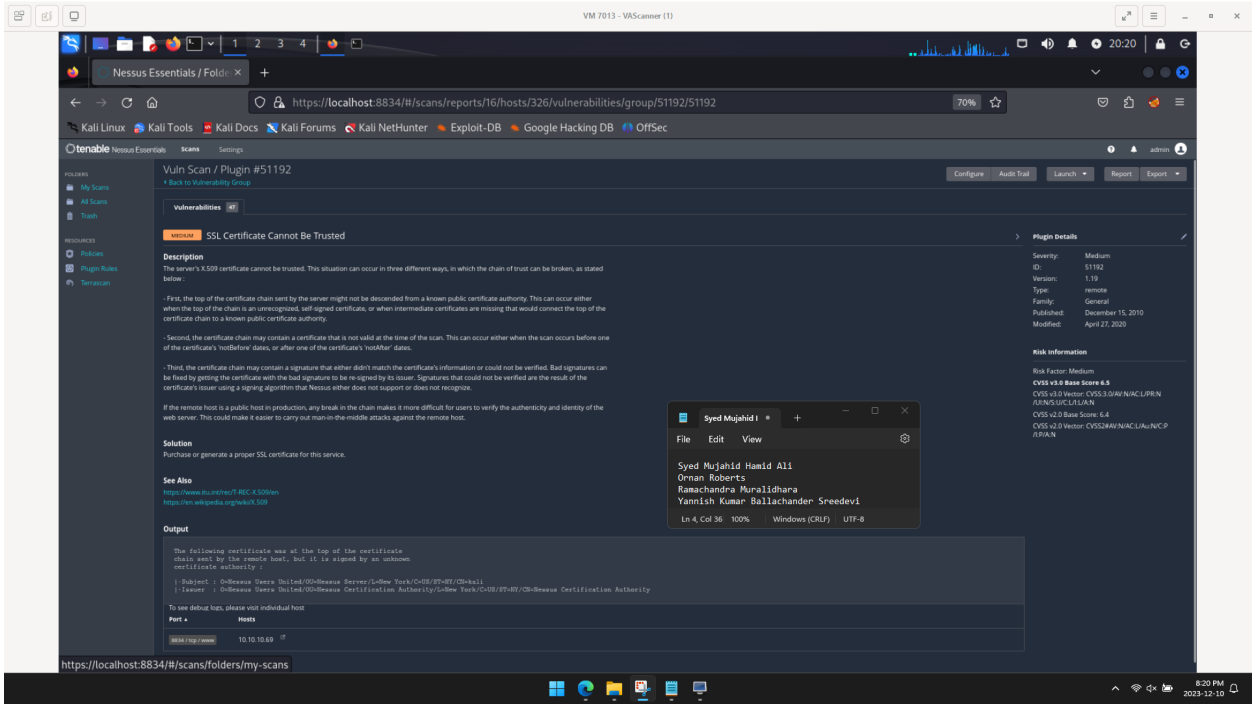
Description: The X.509 certificate of the server cannot be deemed trustworthy, and this situation may manifest in three distinct ways, as outlined below:

1. First, the top of the certificate chain provided by the server might not be derived from a recognized public certificate authority. This occurs when the apex of the chain is an unfamiliar, self-signed certificate, or when intermediate certificates are absent, preventing the linkage of the certificate chain's apex to a known public certificate authority.
2. Second, the certificate chain might include a certificate that is invalid at the time of the scan. This happens when the scan takes place either before one of the certificate's 'notBefore' dates or after one of its 'notAfter' dates.
3. Third, the certificate chain might feature a signature that either does not match the certificate's information or cannot be verified. Resolving bad signatures involves re-signing the certificate with the flawed signature by its issuer. Signatures that cannot be verified result from the certificate's issuer using a signing algorithm that Nessus does not support or recognize.

Severity: Medium

Affected Scope: 10.10.10.69

Proof of Concept:



Solution: Purchase or generate a proper SSL certificate for this service.

V3 - Microsoft Windows EFSRPC NTLM Reflection

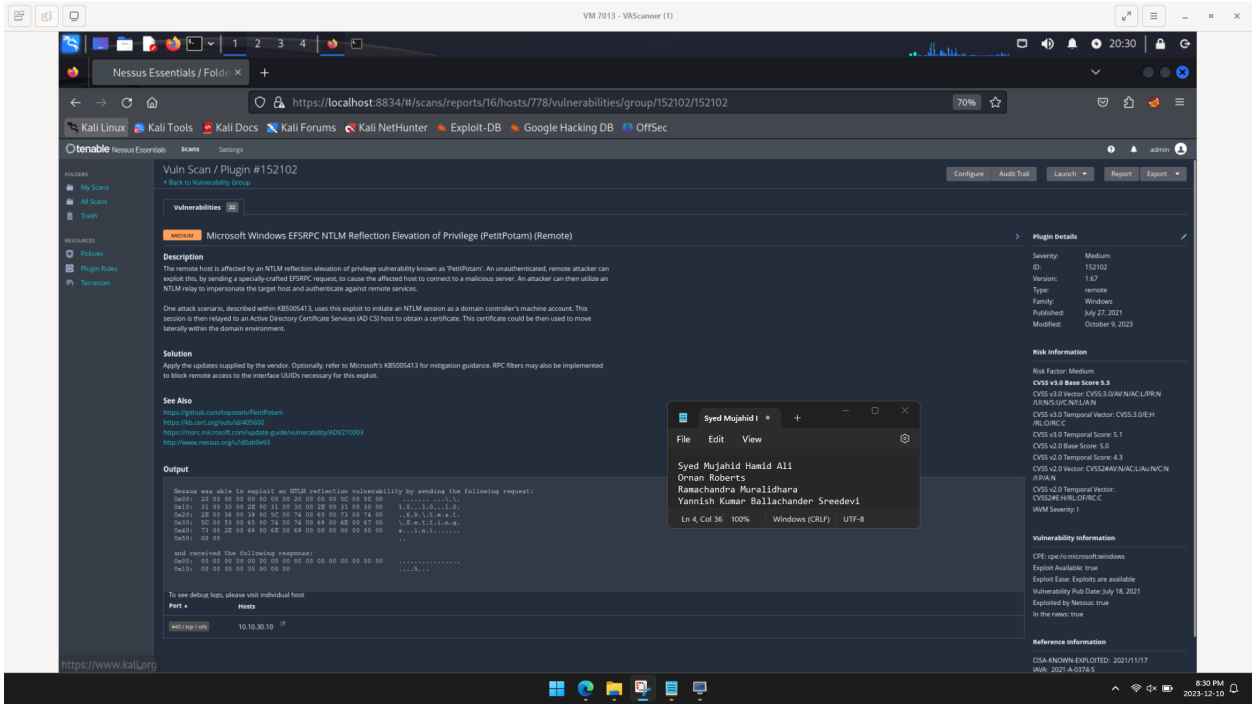
Description: The NTLM reflection elevation of privilege vulnerability known as 'PetitPotam' impacts the remote host. This vulnerability allows an unauthenticated, remote attacker to exploit it by sending a specifically crafted EFSRPC request. This action causes the affected host to connect to a malicious server. Subsequently, the attacker can employ an NTLM relay to impersonate the target host and authenticate against remote services.

One potential attack scenario, outlined in KB5005413, involves leveraging this exploit to initiate an NTLM session using a domain controller's machine account. This established session is then relayed to an Active Directory Certificate Services (AD CS) host to obtain a certificate. This acquired certificate could be utilized to move laterally within the domain environment.

Severity: Medium

Affected Scope: 10.10.30.10

Proof of Concept:



Solution: Apply the updates supplied by the vendor. Optionally, refer to Microsoft's KB5005413 for mitigation guidance. RPC filters may also be implemented to block remote access to the interface UUIDs necessary for this exploit.

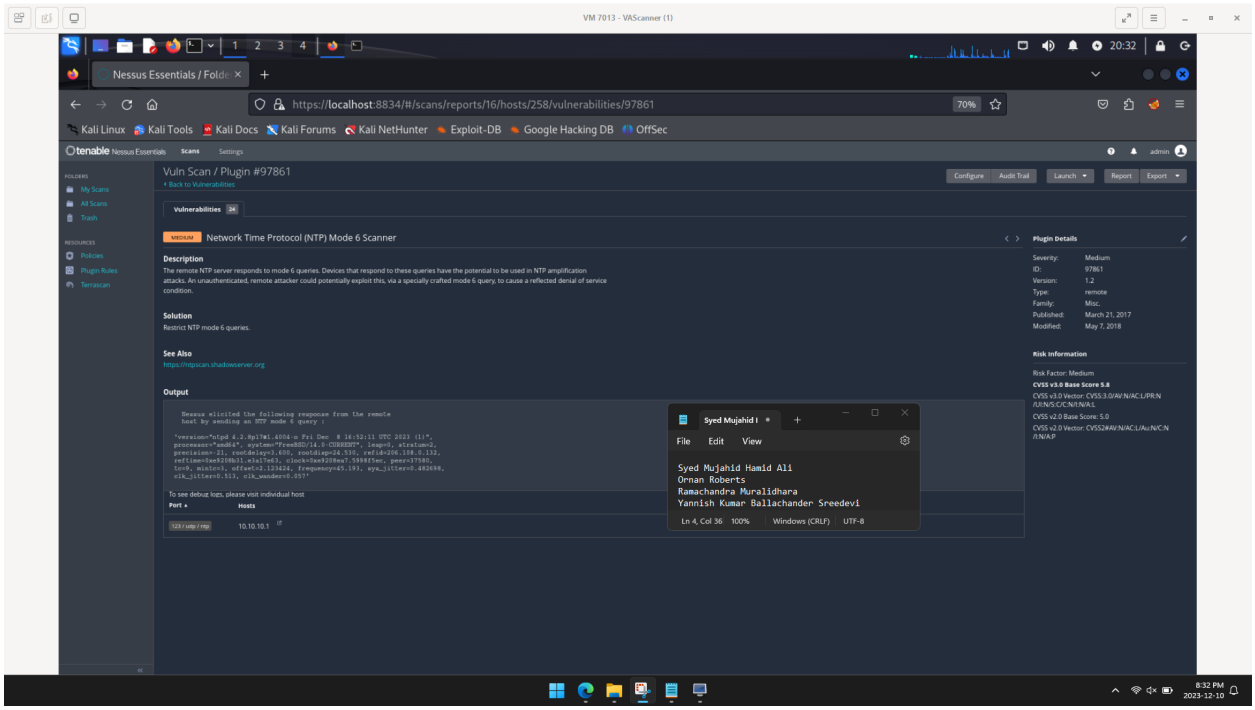
V4 - Network Time Protocol (NTP) Mode 6 Scanner

Description: The remote NTP (Network Time Protocol) server is susceptible to mode 6 queries. Devices that respond to such queries may be exploited in NTP amplification attacks. An unauthenticated, remote attacker could potentially take advantage of this vulnerability by sending a specifically crafted mode 6 query. This action could lead to a reflected denial-of-service condition.

Severity: Medium

Affected Scope: 10.10.10.1

Proof of Concept:



Solution: Restrict NTP mode 6 queries.

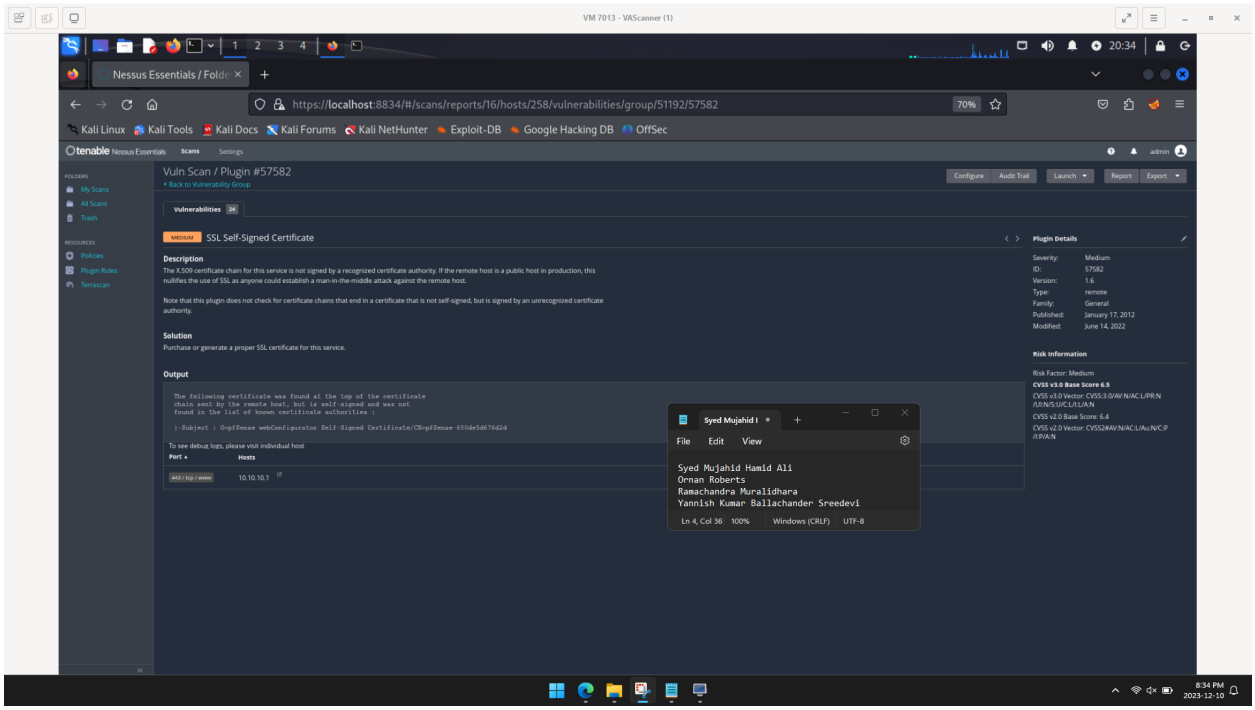
V5 - SSL Self-Signed Certificate

Description: The X.509 certificate chain for this service lacks a signature from a recognized certificate authority. In the case of the remote host being a publicly accessible production host, this undermines the efficacy of SSL (Secure Sockets Layer) as it opens the door for potential man-in-the-middle attacks, allowing unauthorized interception of communication with the remote host.

Severity: Medium

Affected Scope: 10.10.10.1

Proof of Concept:



Solution: Purchase or generate a proper SSL certificate for this service.

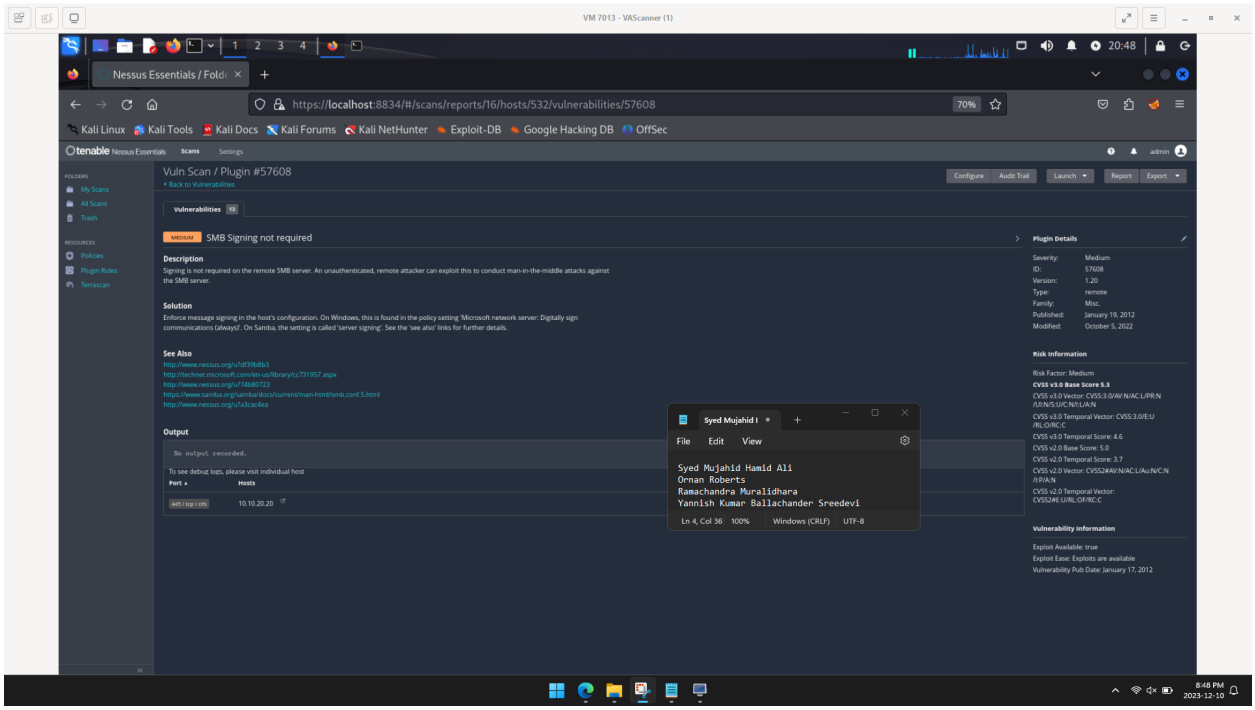
V6 - SMB Signing not required

Description: The remote SMB (Server Message Block) server does not enforce signing. This absence of signing presents an opportunity for an unauthenticated, remote attacker to exploit the vulnerability, enabling them to conduct man-in-the-middle attacks against the SMB server. The lack of signing opens the door for potential interception and manipulation of SMB communications between clients and the server. Enabling signing is recommended to enhance the security of SMB communications and mitigate the risk of unauthorized tampering.

Severity: Medium

Affected Scope: 10.10.20.20

Proof of Concept:



Solution: Enforce message signing in the host's configuration. On Samba, the setting is called 'server signing'.

V7 - DNS Server Cache Snooping Remote Information Disclosure

Description: The remote DNS server responds to queries for third-party domains without the recursion bit set. This behavior creates a potential avenue for a remote attacker to discern which domains have been recently resolved through this name server, revealing information about recently visited hosts.

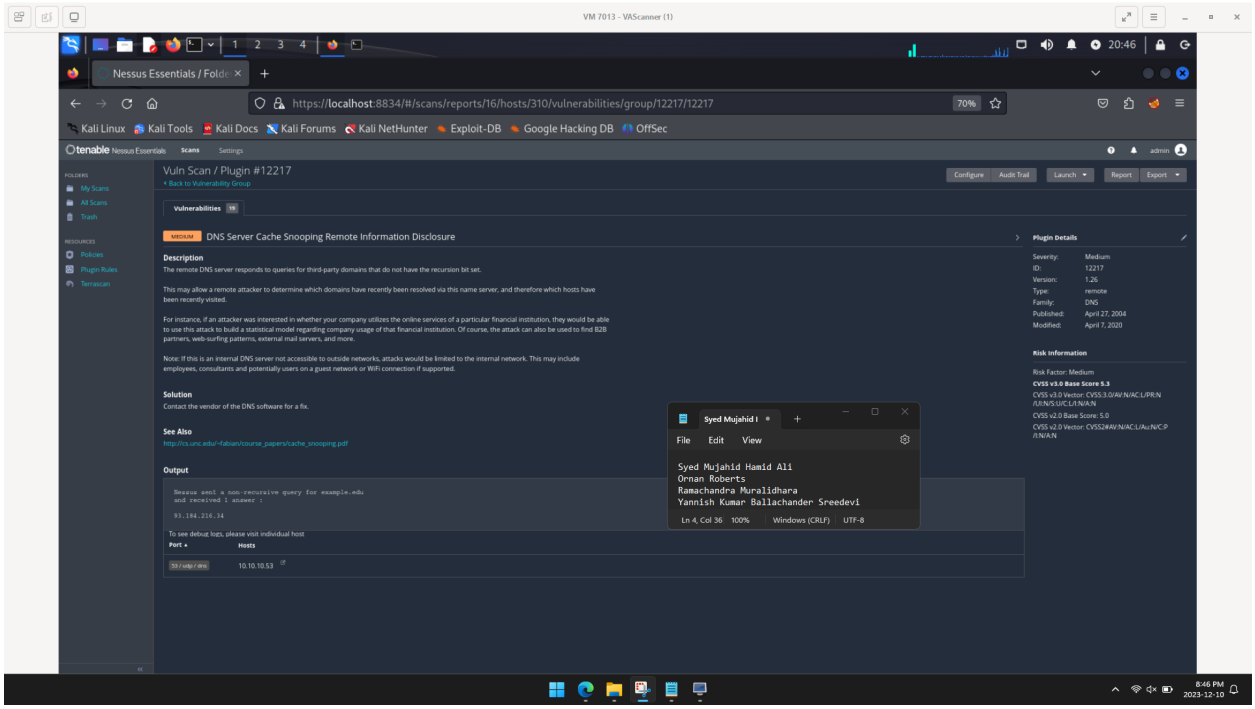
For example, an attacker could use this method to build a statistical model regarding a company's usage of specific online services, such as those provided by a particular financial institution. Beyond financial institutions, the attack could be applied to uncover patterns related to B2B partners, web-surfing habits, external mail servers, and more.

It's crucial to note that if this DNS server is internal and not accessible from external networks, the scope of potential attacks would be limited to the internal network. This could include employees, consultants, and possibly users on a guest network or WiFi connection if supported.

Severity: Medium

Affected Scope: 10.10.10.53

Proof of Concept:



Solution: Contact the vendor of the DNS software for a fix.

V8 - DNS Server Zone Transfer Information Disclosure (AXFR)

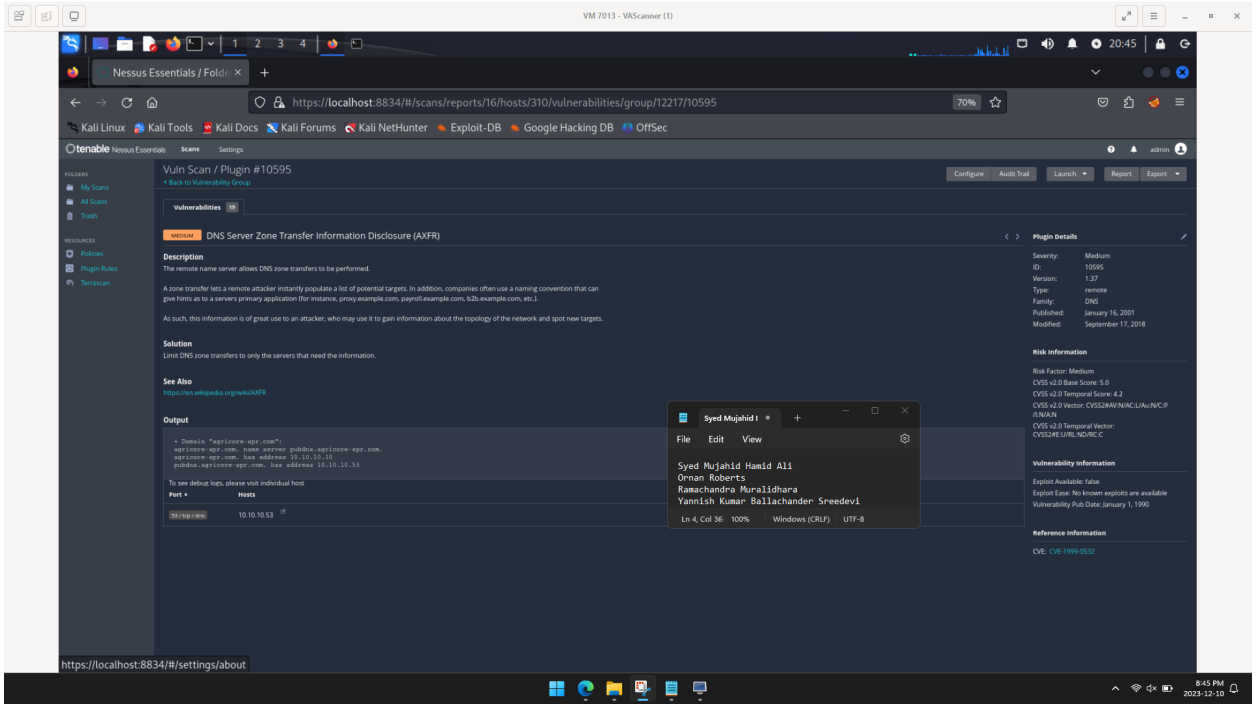
Description: The remote name server permits DNS zone transfers. This functionality enables a potential attacker to swiftly compile a list of potential targets. Additionally, organizations often utilize a naming convention that provides insights into a server's primary application (e.g., proxy.example.com, payroll.example.com, b2b.example.com, etc.).

This information is highly valuable to an attacker, allowing them to gather details about the network topology and identify new potential targets..

Severity: Medium

Affected Scope: 10.10.10.53

Proof of Concept:



Solution: Limit DNS zone transfers to only the servers that need the information.

V9 - IP Forwarding Enabled

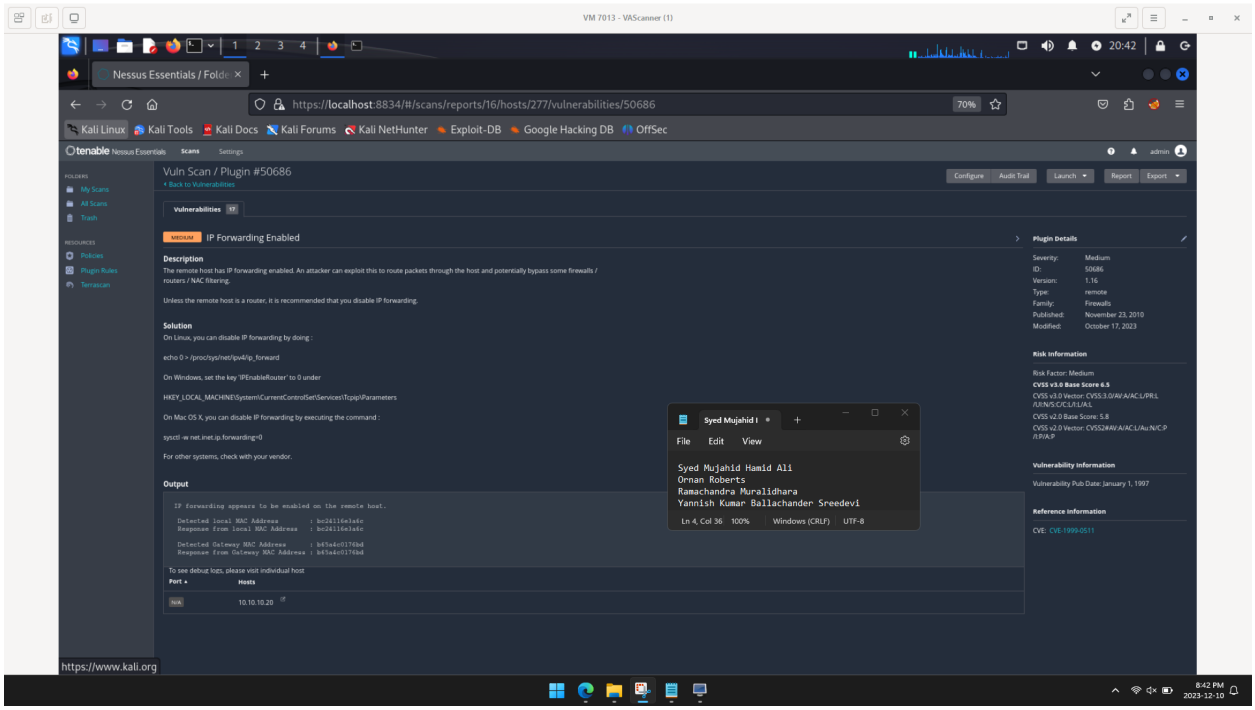
Description: IP forwarding is active on the remote host. This configuration presents an opportunity for an attacker to route packets through the host, potentially circumventing certain firewalls, routers, or NAC (Network Access Control) filtering mechanisms.

Unless the remote host serves as a router, it is advisable to disable IP forwarding to enhance security and mitigate the risk of unauthorized packet routing through the system.

Severity: Medium

Affected Scope: 10.10.10.20

Proof of Concept:



Solution: On Linux, we can disable IP forwarding by doing : echo 0 > /proc/sys/net/ipv4/ip_forward

V10 - DHCP Server Detection

Description: This script communicates with the remote DHCP server, if present, and endeavors to gather details about the network configuration.

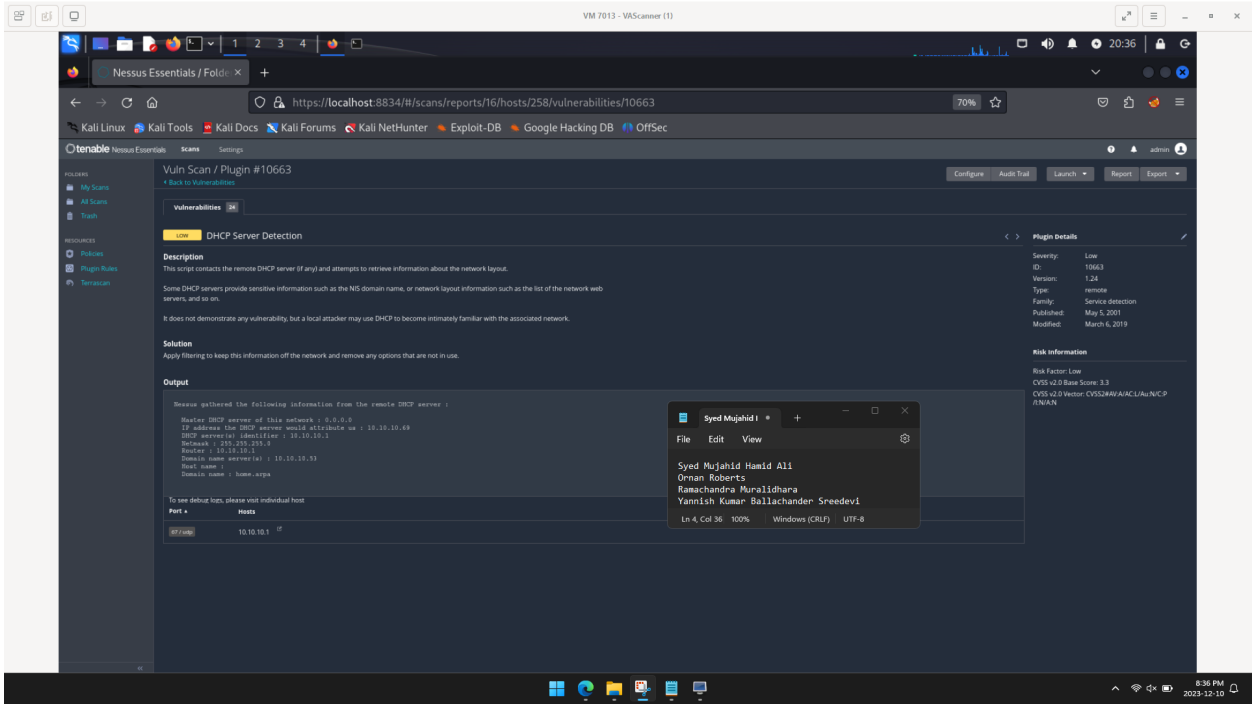
Certain DHCP servers disclose sensitive information, including the NIS domain name or network layout specifics such as the list of network web servers.

While the script itself doesn't showcase any vulnerabilities, it's worth noting that a local attacker could potentially exploit DHCP to gain an in-depth understanding of the connected network.

Severity: Low

Affected Scope: 10.10.10.1

Proof of Concept:



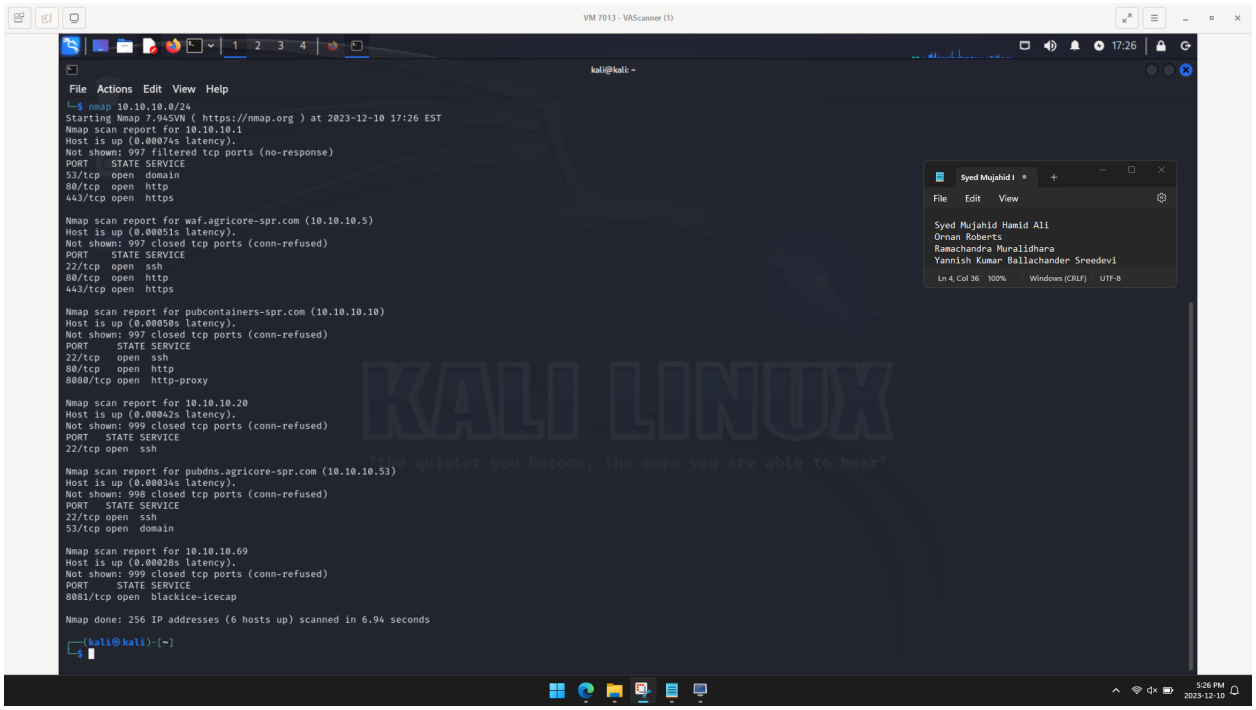
Solution: Apply filtering to keep this information off the network and remove any options that are not in use.

NMAP Scans

The second scanning was performed using NMAP, where we scanned each of the zones within the infrastructure. NMAP is designed to explore networks, detect open ports, discover hosts, and analyze network services running on remote systems. The basic scan was conducted where we found the devices and the services running within each of the zones.

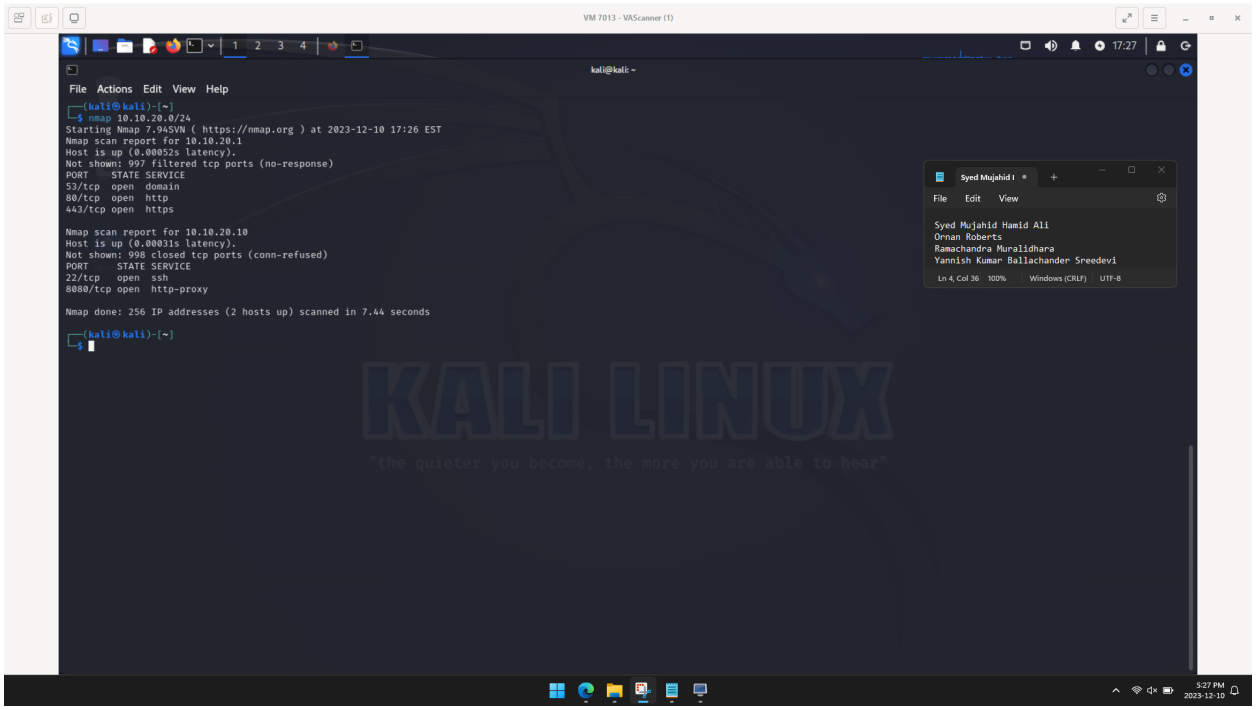
DMZ Zone Scan - 10.10.10.0/24

This subnetwork was assigned to devices which will be used for public facing services which includes the webserver, public host containers etc. Based on the scan we were able to see services such as HTTP, HTTPS, SSH. These are all critical services that were deployed for Agricore public facing infrastructure.



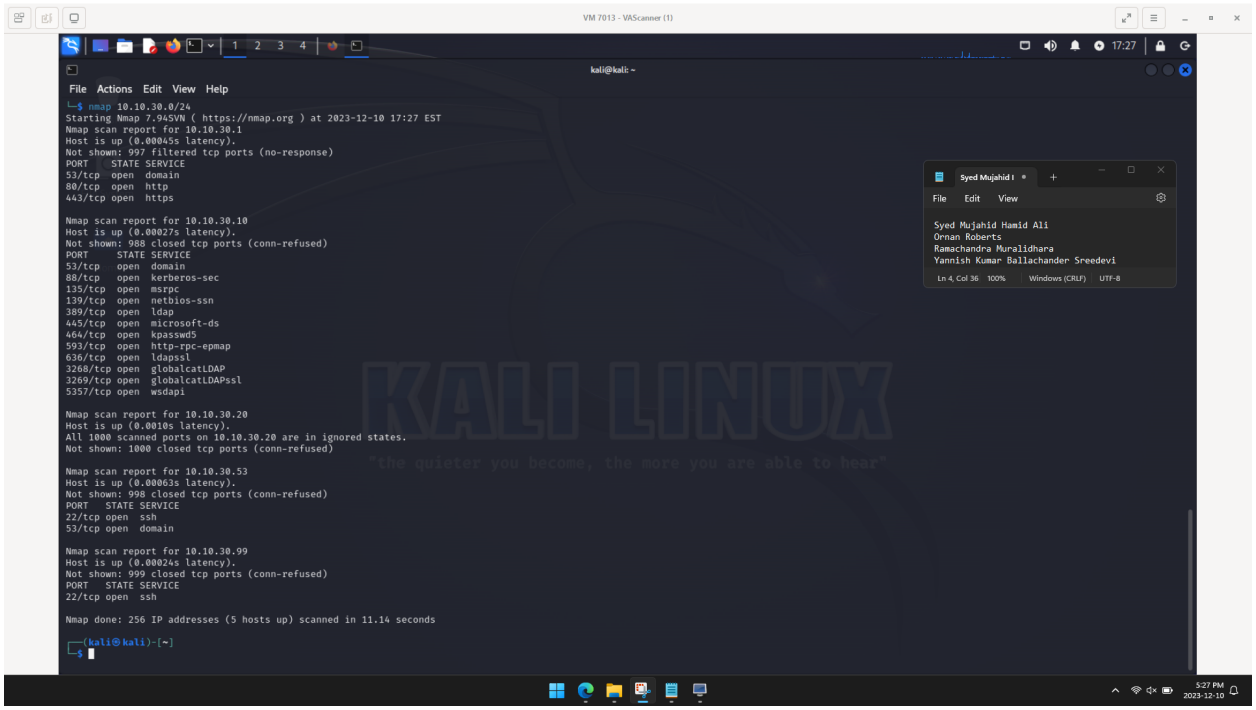
Internal Zone Scan - 10.10.20.0/24

The internal zone where all the infernal devices and resources such as the end user devices, database, private container hosts is located. During scanning this network, we discovered a few services and ports which include HTTP, HTTPS, SSH. Based on this information we can say that the zone is much safer where less resources are vulnerable and not shown to public.



Administrative Zone - 10.10.30.0/24

The administrative zone is where the domain controller and other essential servers are placed supporting the infrastcuture. We scanned this zone as well and discovered open services and ports specifically on domain controllers. These services are important for domains to operate and hence these can be seen through the scans.



Mitigation Strategies

Following are the mitigation strategies and recommendations that can be implemented for each of the above vulnerabilities discussed.

V1 - Query 1.2 < 3.5.0 Multiple XSS

Cross-Site Scripting (XSS) is a type of security vulnerability where an attacker injects malicious scripts into web pages. Perform an upgrade to version 3.5.0 or a more recent release as a preventive measure. Newer versions of jQuery include security patches and bug fixes, providing a more robust and secure framework.

V2 - SSL Certificate Cannot Be Trusted

Take proactive steps to enhance the security of this service by obtaining or generating a suitable SSL certificate. The implementation of a valid SSL certificate is pivotal for establishing a secure and authenticated communication channel. This certificate, issued by a trusted certificate authority, ensures that data exchanged between the client and the server remains confidential and protected against potential eavesdropping or tampering.

By investing in a proper SSL certificate, you not only strengthen the integrity of the communication but also inspire confidence among users by providing a clear indicator of a secure connection. This proactive measure safeguards sensitive information, such as user credentials or personal data, and mitigates the risk of unauthorized access or interception.

V3 - Microsoft Windows EFSRPC NTLM Reflection

Ensure the security of your system by promptly applying the updates provided by the vendor. Consider referring to Microsoft's KB5005413 for additional guidance on mitigating potential risks. As an optional measure, implement RPC filters to block remote access to the interface UUIDs essential for this particular exploit. This comprehensive approach helps fortify your system against vulnerabilities, incorporating both vendor-provided updates and additional protective measures outlined in relevant knowledge base articles. Regularly monitor and manage these security measures to maintain a robust defense against potential threats.

V4 - Network Time Protocol (NTP) Mode 6 Scanner

Enhance the security of your NTP (Network Time Protocol) service by implementing restrictions on mode 6 queries. By limiting or carefully controlling NTP mode 6 queries, you can significantly reduce the risk of potential misuse or exploitation. This can involve configuring the NTP server to only respond to authorized and necessary mode 6 queries, thereby preventing unauthorized access and mitigating the potential for abuse. Regularly review and adjust these restrictions as needed to maintain a balance between operational functionality and security safeguards.

V5 - SSL Self-Signed Certificate

This essential measure ensures a robust and encrypted communication channel between clients and the server. Acquiring a SSL certificate from a trusted certificate authority not only safeguards sensitive data but also instills confidence for users to use the website. Since we are using a self-signed web certificate, therefore we encounter this vulnerability. To mitigate this issue, a trusted party needs to sign the certificate which will completely safeguard the web servers.

V6 - SMB Signing not required

Strengthen the security of the host by mandating message signing in the configuration. Specifically, in Samba, activate the 'server signing' setting. This security measure ensures that messages exchanged between the host and other entities are signed, adding an additional layer of protection against tampering or unauthorized alterations. Enforcing message signing enhances the overall integrity and authenticity of communication, contributing to a more resilient defense against potential security threats. Regularly review and manage these configurations to sustain a robust security posture over time.

V7 - DNS Server Cache Snooping Remote Information Disclosure

Initiate communication with the DNS software vendor to obtain a solution. Promptly reaching out to the vendor is crucial for addressing and remedying any identified issues or vulnerabilities in the DNS software. Collaborating with the vendor ensures that you receive the latest updates, patches, or fixes necessary to enhance the security and functionality of the DNS software. Additionally, staying in contact with the vendor allows for ongoing support and guidance in maintaining a secure and reliable DNS environment.

V8 - DNS Server Zone Transfer Information Disclosure (AXFR)

Enhance the security of your DNS infrastructure by implementing restrictions on zone transfers. Specifically, limit DNS zone transfers to only the servers that genuinely require the information. This targeted approach minimizes the potential attack surface and reduces the risk of unauthorized access or data exposure. By carefully controlling which servers are permitted to perform zone transfers, you effectively mitigate the likelihood of information leakage and unauthorized reconnaissance attempts. Regularly review and update these access controls to align with your network's evolving requirements and maintain a proactive security posture.

V9 - IP Forwarding Enabled

To disable IP forwarding on Linux, execute the following command:

echo 0 > /proc/sys/net/ipv4/ip_forward

This command updates the value of the ip_forward parameter in the /proc/sys/net/ipv4/ directory to 0, effectively turning off IP forwarding. This configuration change helps enhance security by preventing the system from forwarding IP packets between network interfaces, unless explicitly configured otherwise. Additionally, consider making this change persistent across reboots by updating the corresponding configuration file or using system-specific methods.

V10 - DHCP Server Detection

Implement filtering mechanisms to prevent the dissemination of this information on the network. Additionally, eliminate any unnecessary options that are not actively in use. By applying effective filtering, you can control the flow of information, enhance security, and reduce the exposure of potentially sensitive data. Regularly review and update the filtering rules to align with the current network requirements and ensure a streamlined, secure, and efficient network configuration. This proactive approach contributes to a more robust defense against potential security threats.

Conclusion

In conclusion, the vulnerability assessment conducted on Agricore's infrastructure has provided valuable insights into the security posture of the network. The findings were discovered using both Nessus and NMAP scanning tools to identify vulnerabilities. The vulnerabilities encompass various aspects such as related to SSL, DNS and other various services involved in the domain. The identified vulnerabilities pose potential risks to the confidentiality, integrity, and availability of Agricore's systems. The explained mitigation strategies provided offer concrete steps and configuration adjustments that could be implemented to enhance the overall security posture of Agricore's infrastructure.