Student:	Email:
Matias Kun	rvh4zx@virginia.edu

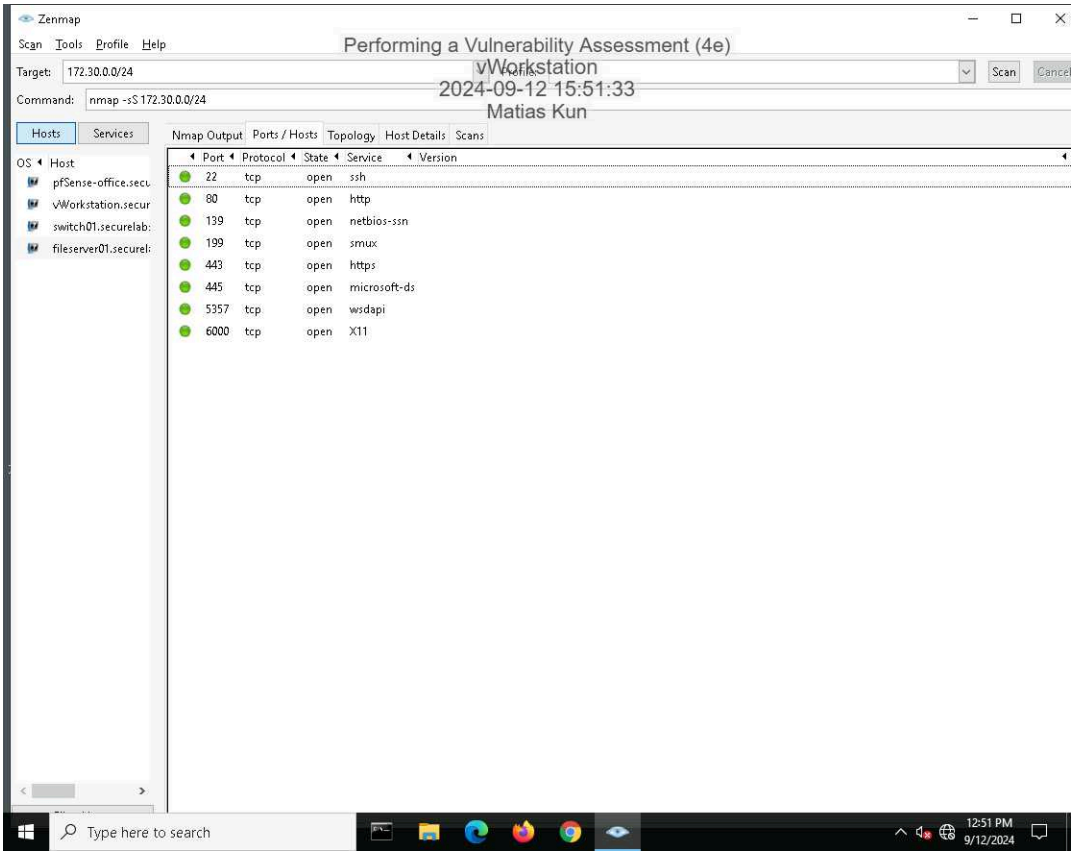
Time on Task:	Progress:
8 hours, 16 minutes	100%

Report Generated: Thursday, September 12, 2024 at 7:50 PM

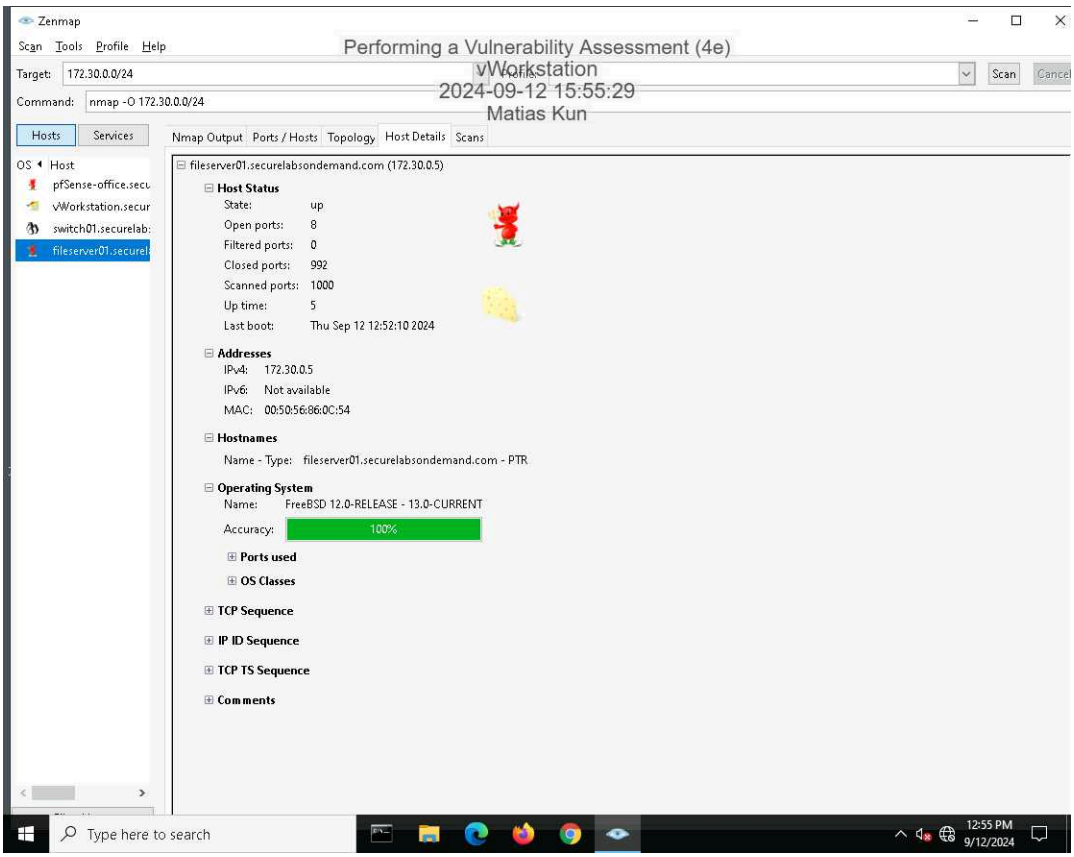
Section 1: Hands-On Demonstration

Part 1: Scan the Network with Zenmap

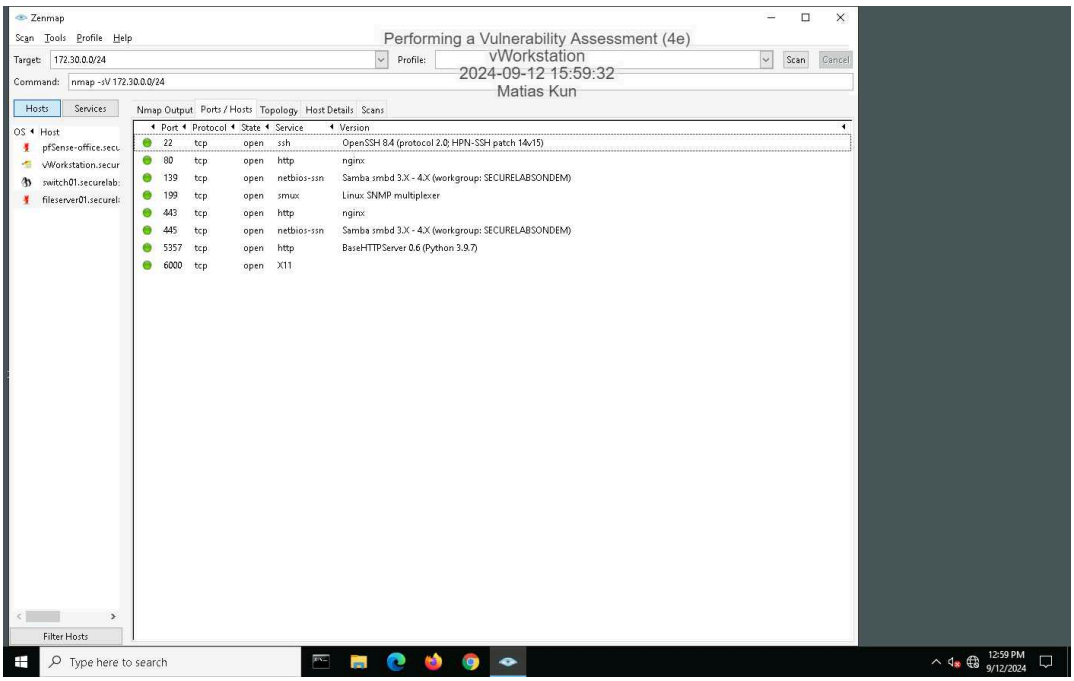
9. **Make a screen capture** showing the contents of the **Ports/Hosts tab from the SYN scan for fileserver01.securelabsondemand.com**.



15. **Make a screen capture** showing the contents of the **Host Details tab from the OS scan for fileserver01.securelabsondemand.com**.

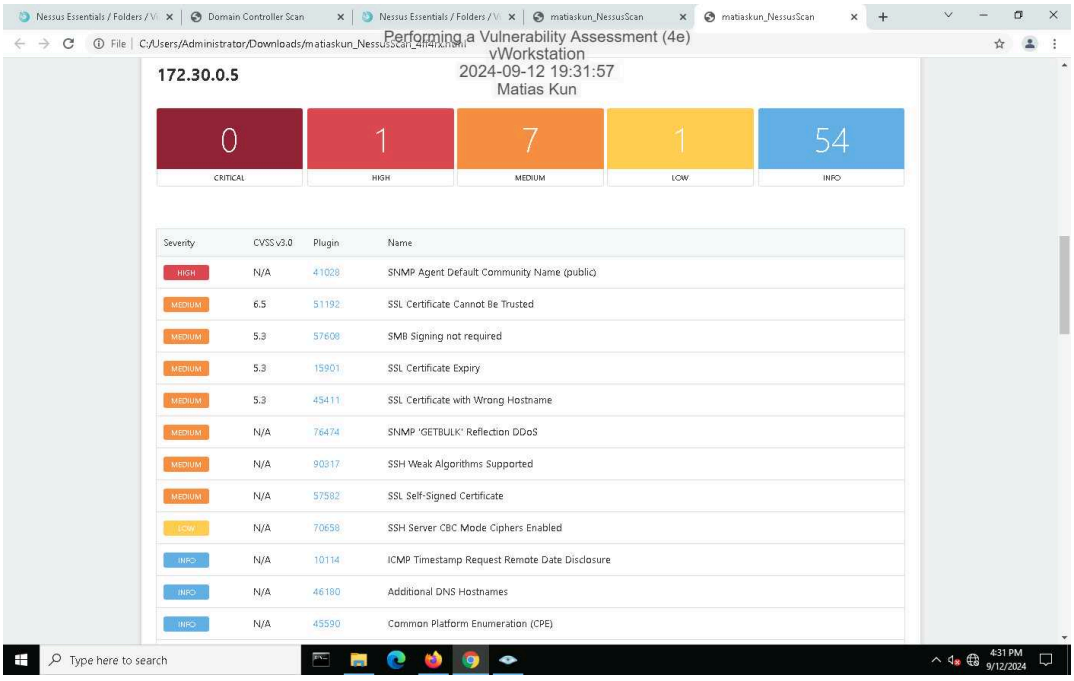


19. **Make a screen capture** showing the details in the **Ports/Hosts tab from the Service scan for fileserver01.securelabsondemand.com.**



Part 2: Conduct a Vulnerability Scan with Nessus

14. **Make a screen capture** showing the **Nessus report summary**.



Part 3: Evaluate Your Findings

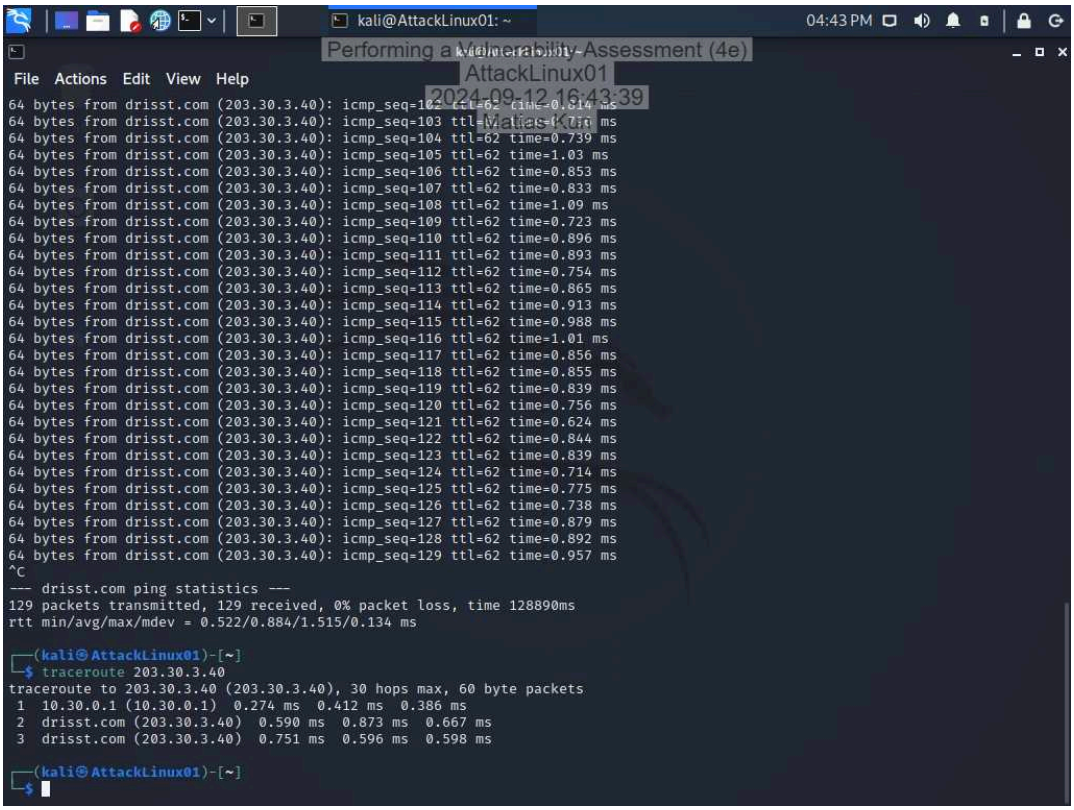
11. **Summarize** the vulnerability you selected, including the CVSS risk score, and **recommend** a mitigation strategy.

The medium vulnerability I have selected, I have selected plugin ID 15901. Plugin ID 15901 is when the SSL Certificate has expired. The CVSS risk score is 5.3 in v3 (equivalent to 5 in v2). The recommended solution or mitigation strategy is to either purchase or generate a new SSL certificate to replace the already expired one. Along with that, a policy implementation for when to replace SSL certificates when expiration is ahead.

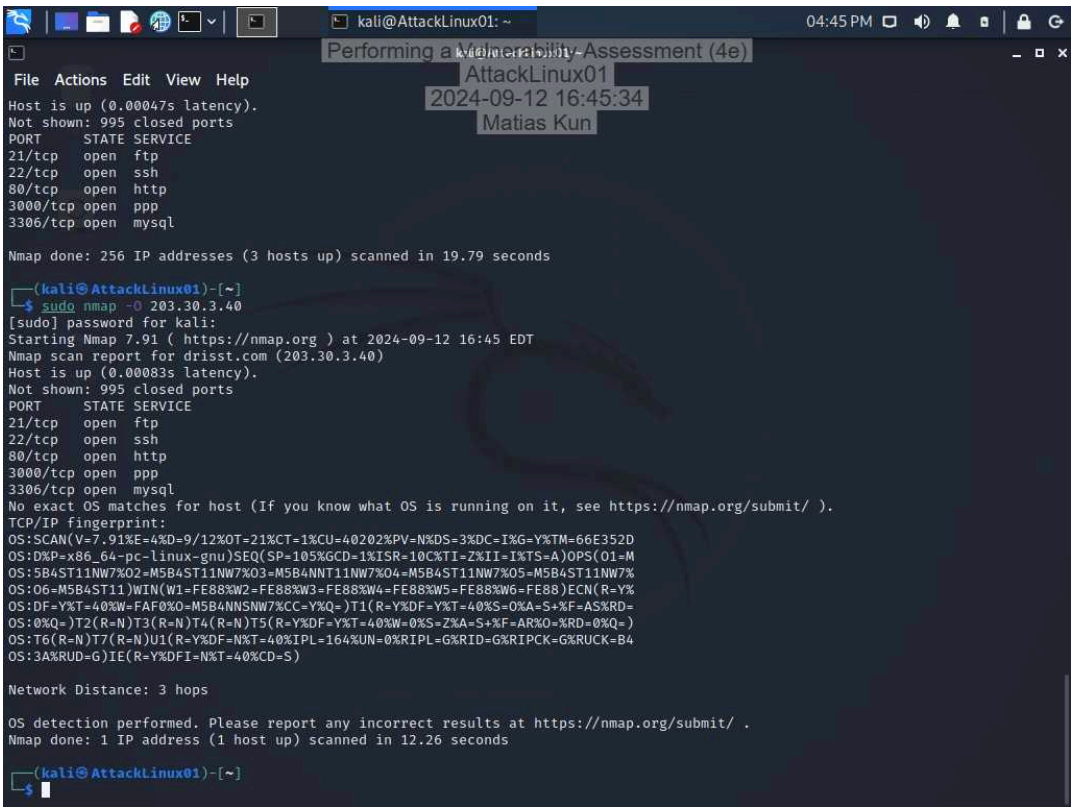
Section 2: Applied Learning

Part 1: Scan the Network with Nmap

6. **Make a screen capture** showing the **results of the traceroute command**.

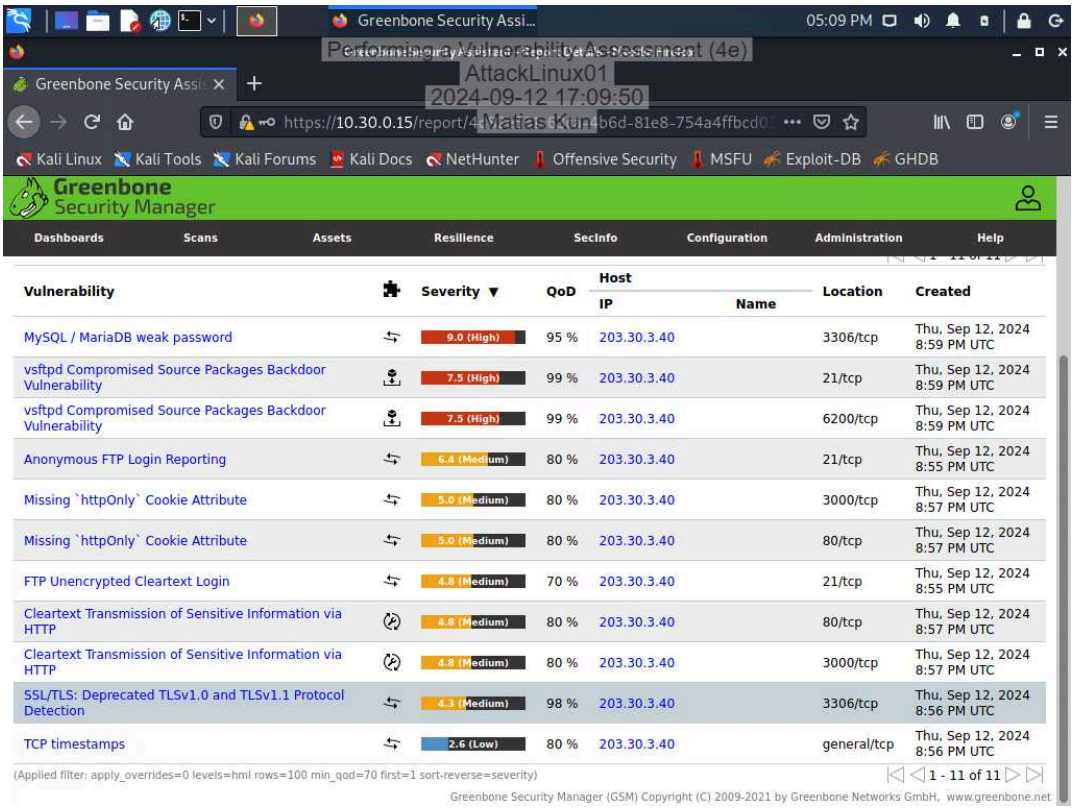


10. **Make a screen capture** showing the **results of the Nmap scan with OS detection activated**.



Part 2: Conduct a Vulnerability Scan with OpenVAS

13. **Make a screen capture** showing the **detailed OpenVAS scan results**.



Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

The target for this scan is drisst.com (IP address: 203.30.3.40).

Completed by

Insert your name here.

Matias Laszlo Kun

On

Insert current date here.

September 12, 2024

Purpose

Identify the purpose of the penetration test.

Purpose of this lab is targeting exploitation from an unknown source.

Scope

Identify the scope of the penetration test.

The scope is to identify weak and compromised passwords attackers used. In addition, the source packages could potentially have hidden entrances to bypass basic security functionality. Finally, scanning vulnerability in the internal employee network and determining whether one of the servers are targeted by a malicious actor or hacktivist group.

Summary of Findings

Identify and summarize each of the three high-severity vulnerabilities identified during your penetration test. For each vulnerability, identify the severity, describe the issue, and recommend a remediation.

For the first severe vulnerability (Severity level 9.0), the possibility of logging in high by using a remote MySQL for using weak credentials, like in this case, using "password" as the password. The simplicity of the password makes unauthorized accessing more effective. The password must be promptly and quickly change or else this mitigation solution will be ineffective, as well as Multifactor Authentication (MFA) to secure the MySQL instance.
Another thing to point out the daemon or software program vsftpd being prone to this backdoor attack (Severity level for both vsftpd compromissions: 7.5). Vsftpd 2.3.4 source package was affected. The solution is to download and install the patched package from the referenced link, as well as verifying the package signature's validity. All the compromised vsftpd packages must be to the updated, secure version ensuring application stability.
Please ensure password policies with MFA is implemented as well as installing secure, updated vsftpd packages.

Conclusion

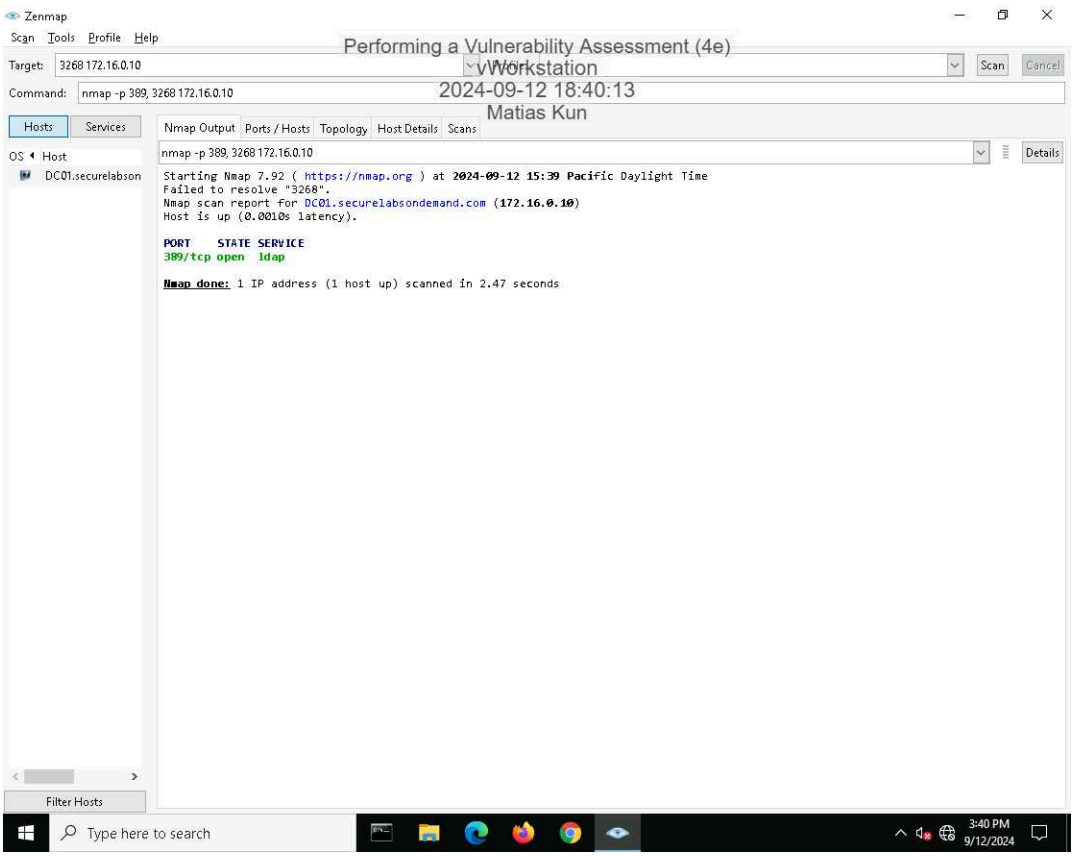
Identify your key findings.

The weak credentials were the primary factor for the attack and should be changed and further heighten its security, like MFA implementation alongside the password or PIN, not just how strong it is. The compromised vsftpd packages were a secondary source for the compromised network and both verifying the signature along with installing the secure, patched version should resolve this vulnerability. There are potential risks of installing beta files that could possibly have unresolved vulnerabilities.
Anonymous remote access to the FTP service, though not as severe as the severe issues listed above, were used in this attack too. Ensuring the employees understand whom they grant access to sensitive files will significantly reduce the likelihood of access to sensitive data. The cookie used Javascript, which is commonly known for session hijackings, as opposed to httpOnly which is more secure. An FTP Encryption could have prevented the sensitive data from transiting through compromised login credentials through unencrypted FTP. Protocol TLSv1.0 was used in the attack. Companies will need to adhere supported protocols to ensure safety and security.

Section 3: Challenge and Analysis

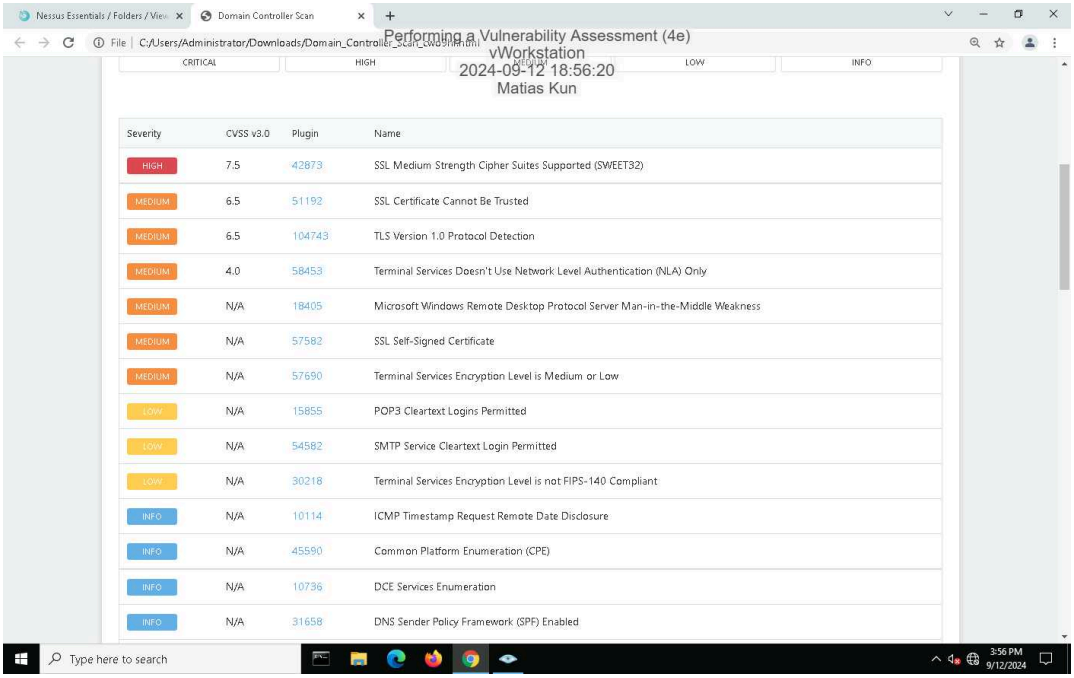
Part 1: Scan the Domain Controller with Nmap

Make screen capture showing the **results of your targeted port scan on the domain controller**.



Part 2: Scan the Domain Controller with Nessus

Make a screen capture showing the **Nessus report summary for the domain controller**.



Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

Domain Control (172.16.0.10)

Completed by

Insert your name here.

Matias Laszlo Kun

On

Insert current date here.

September 12, 2024

Purpose

Identify the purpose of the penetration test.

Secure network test and analysis per Secure Labs on Demand's request.

Scope

Identify the scope of the penetration test.

The scope of the penetration test focused on assets within the internal network, including identifying and addressing vulnerabilities, implementing remediation measures, and considering network segmentation.

Summary of Findings

Identify and summarize each vulnerability identified during your penetration test. For each vulnerability, identify the severity, describe the issue, and recommend a remediation.

The highest vulnerability (CVSS: 7.5) is the SSL Medium Strength Cipher Suites Supported issue. This level encryption is easy for hackers on the same network to bypass and potentially attack. Therefore, the best solution is to reconfigure affected applications and refrain the use of medium strength ciphers if possible. The second highest vulnerability, though on the medium level (CVSS: 6.5), is an untrusted SSL Certificate. Please ensure to purchase and generate a proper SSL certificate. Another medium level issue with the same CVSS score as the second issue is the TLS 1.0 protocol. Ensure to enable support for TLS 1.2+ and disable TLS 1.0 support. Terminal Services Encryption Level is Medium or Low (CVSS v3 severity and score: Medium and 4.0). Medium or Low Terminal Services Encryption eases access for malicious actors to eavesdrop on communications. Ensure to change the level to High and comply with FIPS.

Conclusion

Identify your key findings.

Since SSL Medium Strength Ciphers are easy to bypass on the same network as the hacker, the best course of action from this finding is to disable medium strength Ciphers and enable stronger encryption levels. An unreliable SSL Certificate was discovered. It is crucial to verify and validate the integrity of a purchased or generated SSL Certificate as invalid SSL Certificates can increase vulnerability. As TLS 1.0 is unsupported, it increases the risk of exploitation. TLS 1.2 and above should decrease the risk of exploitation. Since the Terminal Services has used medium or low levels of authentication, adding more authenticity to the Terminal Services and ensuring FIPS compliance should make Terminal Services more secure.