

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Student:

Mustafa Shah

Email:

ho3168@wayne.edu

Time on Task:

3 hours, 29 minutes

Progress:

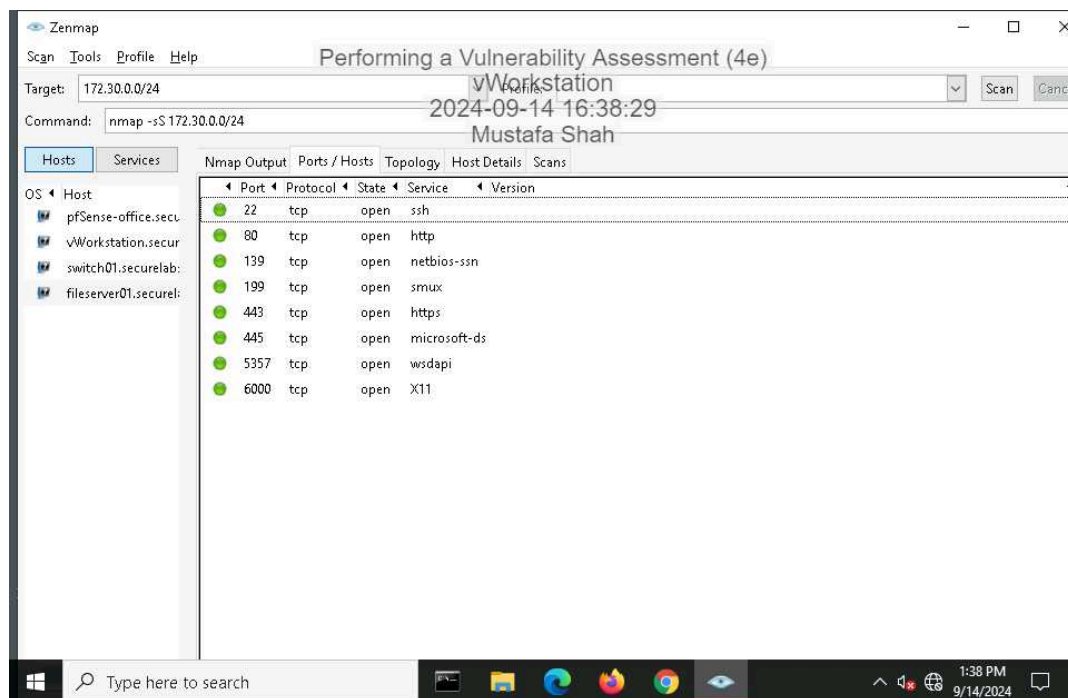
100%

Report Generated: Sunday, September 15, 2024 at 11:48 AM

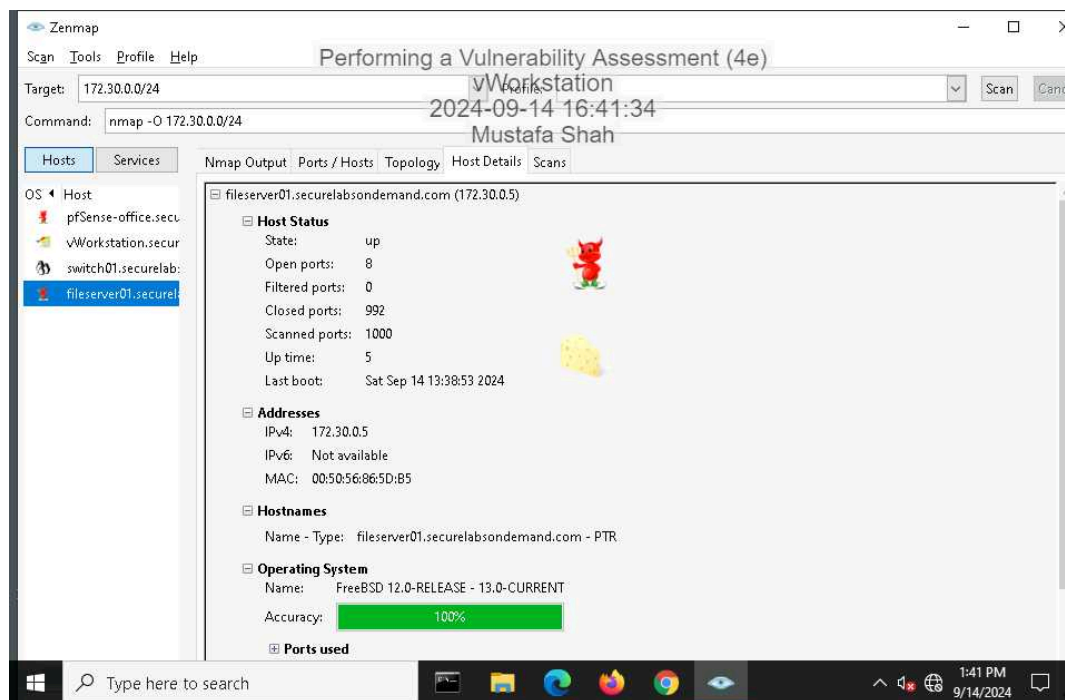
Section 1: Hands-On Demonstration

Part 1: Scan the Network with Zenmap

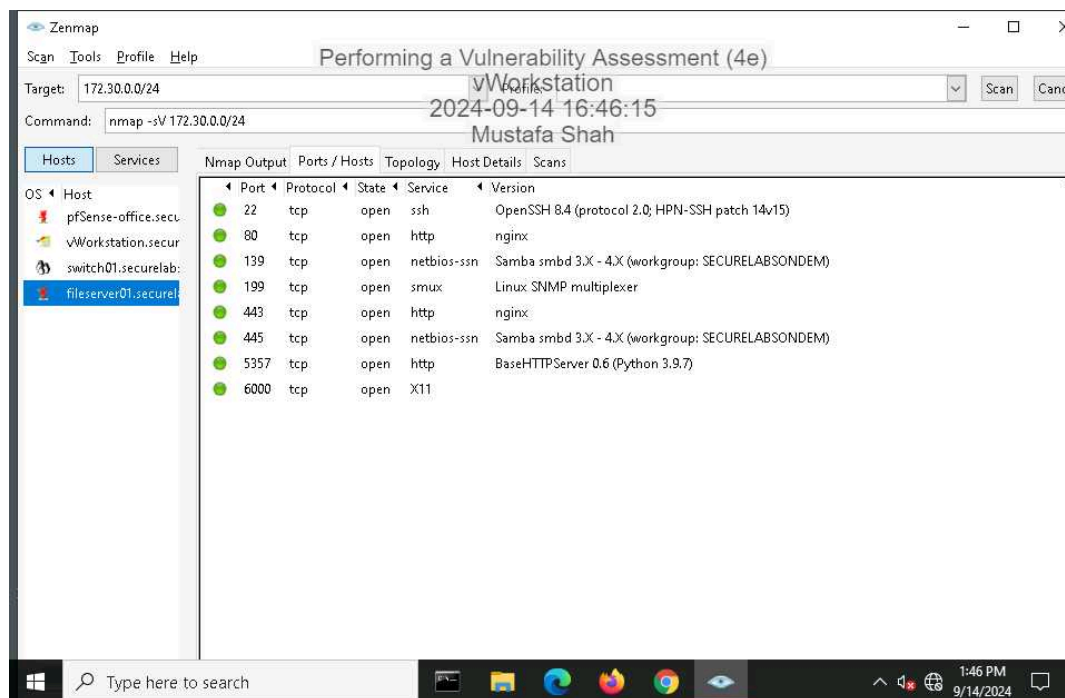
9. **Make a screen capture** showing the contents of the **Ports/Hosts** tab from the **SYN** scan for **fileserver01.securelabsondemand.com**.



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

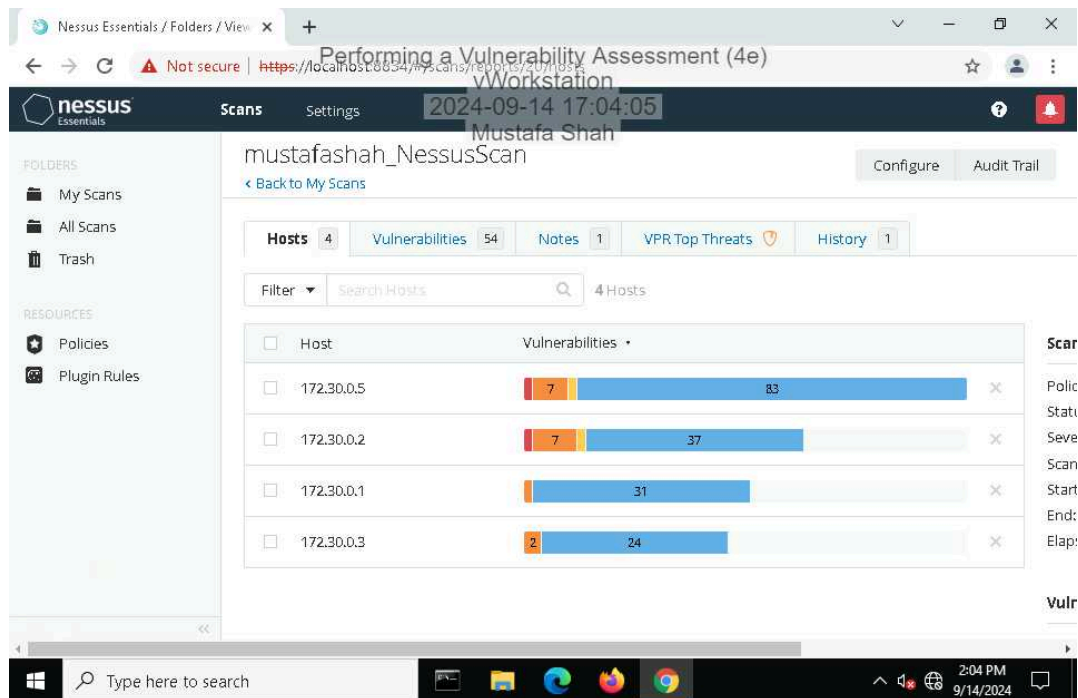


19. Make a screen capture showing the details in the **Ports/Hosts** tab from the **Service** scan for **fileserver01.securelabsondemand.com**.



Part 2: Conduct a Vulnerability Scan with Nessus

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



Part 3: Evaluate Your Findings

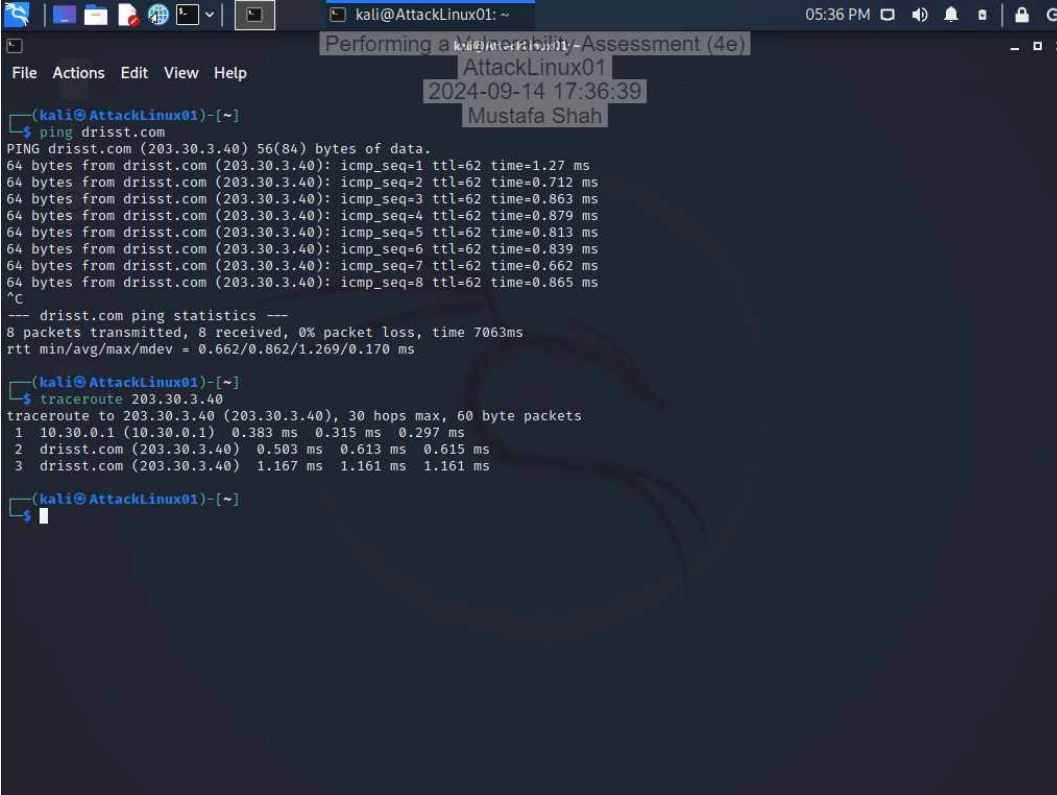
11. Summarize the vulnerability you selected, including the CVSS risk score, and recommend a mitigation strategy.

The vulnerability identified by Nessus plugin ID 57608 refers to the issue where SMB (Server Message Block) signing is not required on a remote server. This can allow an unauthenticated, remote attacker to exploit the lack of message signing to perform a man-in-the-middle attack, intercepting and manipulating communication between the SMB server and its clients. The CVSS (Common Vulnerability Scoring System) score for this issue is classified as medium risk, as it can expose sensitive data to potential interception but requires specific network conditions to exploit. To mitigate, enforce message signing in the host's configuration.

Section 2: Applied Learning

Part 1: Scan the Network with Nmap

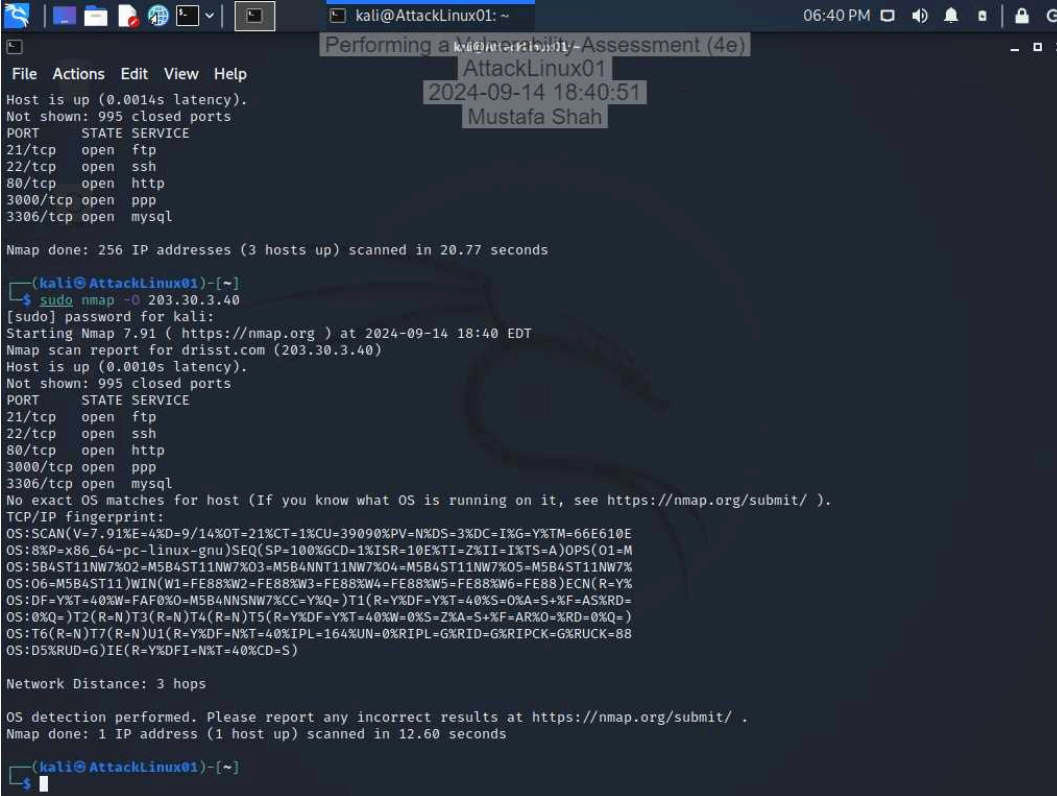
6. Make a screen capture showing the results of the traceroute command.



The screenshot shows a Kali Linux terminal window with the following content:

```
kali@AttackLinux01: ~  
File Actions Edit View Help  
(kali@AttackLinux01)-[~]  
$ ping drisst.com  
PING drisst.com (203.30.3.40) 56(84) bytes of data.  
64 bytes from drisst.com (203.30.3.40): icmp_seq=1 ttl=62 time=1.27 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=0.712 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.863 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=0.879 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=0.813 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=6 ttl=62 time=0.839 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=7 ttl=62 time=0.662 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=8 ttl=62 time=0.865 ms  
^C  
--- drisst.com ping statistics ---  
8 packets transmitted, 8 received, 0% packet loss, time 7063ms  
rtt min/avg/max/mdev = 0.662/0.862/1.269/0.170 ms  
  
(kali@AttackLinux01)-[~]  
$ traceroute 203.30.3.40  
traceroute to 203.30.3.40 (203.30.3.40), 30 hops max, 60 byte packets  
 1 10.30.0.1 (10.30.0.1) 0.383 ms 0.315 ms 0.297 ms  
 2 drisst.com (203.30.3.40) 0.503 ms 0.613 ms 0.615 ms  
 3 drisst.com (203.30.3.40) 1.167 ms 1.161 ms 1.161 ms  
  
(kali@AttackLinux01)-[~]  
$
```

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



```
(kali@AttackLinux01: ~)
File Actions Edit View Help
Host is up (0.0014s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
3000/tcp  open  ppp
3306/tcp  open  mysql

Nmap done: 256 IP addresses (3 hosts up) scanned in 20.77 seconds

(kali@AttackLinux01: ~)
$ sudo nmap -O 203.30.3.40
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-09-14 18:40 EDT
Nmap scan report for drisst.com (203.30.3.40)
Host is up (0.0010s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
3000/tcp  open  ppp
3306/tcp  open  mysql
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=9/14%OT=21%CT=1%CU=39090%PV=N%DS=3%DC=I%G=Y%TM=66E610E
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10E%TI=Z%II=I%TS=A)OPS(O1=M
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%
OS:O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%
OS:DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=88
OS:D5%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

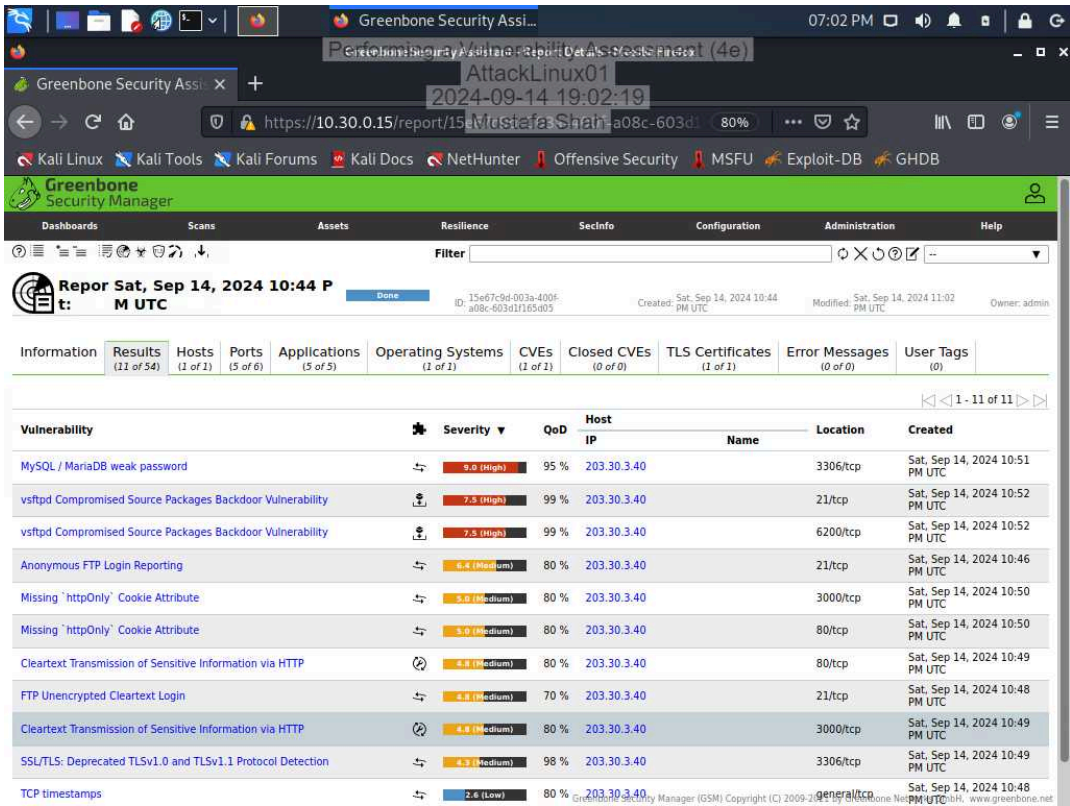
Network Distance: 3 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.60 seconds

(kali@AttackLinux01: ~)
$
```

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.

drisst.com (203.30.3.4)

Completed by

Insert your name here.

Mustafa Shah

On

Insert current date here.

9/14/2024

Purpose

Identify the purpose of the penetration test.

The purpose of this penetration test is to identify, assess, and verify the presence of three high-severity vulnerabilities within the target environment: weak MariaDB/SQL passwords, and vsftpd backdoor vulnerabilities on both the default and custom ports (21 and 6200). The testing will focus on discovering misconfigurations, vulnerabilities related to access controls, and potential backdoors that could allow unauthorized access or privilege escalation.

Scope

Identify the scope of the penetration test.

In-Scope Systems: Database Systems: MariaDB or MySQL servers hosting critical data.FTP

Servers: Systems running the vsftpd service

Testing:Databases

- Conduct brute force password attacks- Test password strength policies- Verify access controls and configurations for password policiesVSFTPD- Check version of VSFTPD- Analyze traffic on ports- Attempt exploit on VSFTPD

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.

Weak MariaDB/SQL PasswordsSeverity: High**Issue:** This vulnerability arises when MariaDB or MySQL databases use weak or default passwords, making them susceptible to brute-force attacks. Attackers can exploit weak credentials to gain unauthorized access to the database, leading to data theft or modification.**Remediation:** Implement strong passwords for all database accounts and enforce password policies

vsftpd Compromised Source Packages Backdoor Vulnerability (Port 21)Severity: High**Issue:** The vsftpd (Very Secure FTP Daemon) vulnerability stems from a backdoor in certain versions of the vsftpd package. This vulnerability allows attackers to gain root access to the system by connecting to the FTP service. Once exploited, attackers can remotely execute arbitrary commands as root, leading to a full system compromise.**Remediation:** Update vsftpd to the latest secure version as soon as possible, check the integrity of installed packages and ensure they are from trusted sources, and disable FTP if it is not required, or switch to more secure file transfer protocols like SFTP.

vsftpd Compromised Source Packages Backdoor Vulnerability on Custom Port (Port 6200)Severity: High**Issue:** Also being an issue with vsftpd, the backdoor vulnerability lies on a custom port, which again can compromise the entire system.**Remediation:** As with the previous vsftpd vulnerability, immediately upgrade to a secure version of vsftpd and close unnecessary ports (e.g., 6200) and restrict access to only required ports.

Conclusion

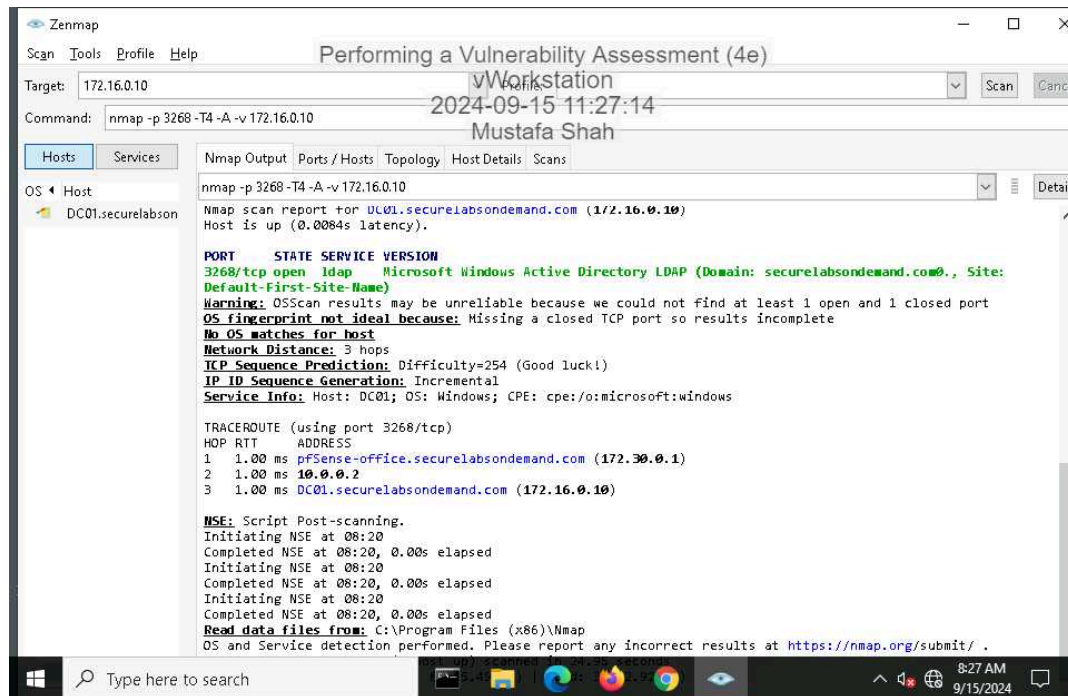
Identify your key findings.

With the following findings, it is imperative that the database passwords are changed immediately, and for preventative measure password policies should be implemented in order to enforce strong passwords. In regards to vsftpd, the latest version should be installed, all package sources should be verified, and any custom ports should be shut down if not in use.

Section 3: Challenge and Analysis

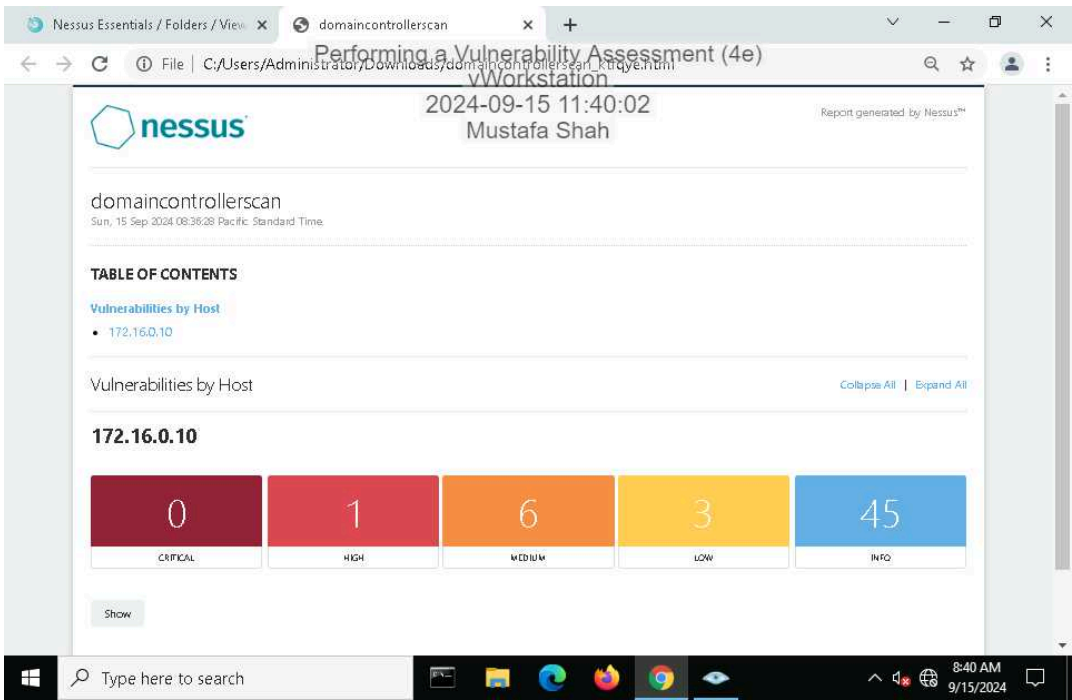
Part 1: Scan the Domain Controller with Nmap

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 Controller (172.16.0.10)

Completed by

Insert your name here.

Mustafa Shah

On

Insert current date here.

9/15/2024

Purpose

Identify the purpose of the penetration test.

The objective of this penetration test is to assess and identify potential weaknesses in the SSL/TLS configuration of the target system. Specifically, the focus is on detecting whether the server supports medium-strength cipher suites, which are vulnerable to the SWEET32 attack, a known security flaw in 64-bit block ciphers.

Scope

Identify the scope of the penetration test.

Target IP: 172.16.0.10 **Tested Port:** SSL-enabled services on standard HTTPS port 443. **Focus:** Identifying the use of medium-strength cipher suites vulnerable to the SWEET32 attack. **Exclusions:** Non-SSL services, unrelated ports, and network segments not supporting SSL/TLS protocols are out of scope for this test.

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.

SSL Medium Strength Cipher Suites Supported (SWEET32) Severity: High

Issue: The server was found to support SSL/TLS cipher suites that use 64-bit block ciphers (e.g., 3DES). These ciphers are susceptible to the SWEET32 attack, where large amounts of data encrypted with the same key can potentially be decrypted, compromising data integrity and confidentiality. **Remediation:** Disable support for 3DES cipher suites, reconfigure the server to use stronger cipher suites such as AES-based ciphers, and test SSL/TLS configurations using online services or tools like SSL Labs to verify the removal of vulnerable ciphers.

Conclusion

Identify your key findings.

The SWEET32 vulnerability was identified on the target system due to the support of medium-strength cipher suites using 64-bit block ciphers. To mitigate this risk, it is recommended to disable the use of these vulnerable cipher suites and configure the server to use stronger, modern cipher suites, such as those based on AES-GCM. Ensuring that SSL/TLS configurations adhere to the latest security standards will help protect against potential exploitation of these weaknesses.