

Student: Andrew Sweeney

Email: asweene8@depaul.edu

Time on Task: 5 hours, 34 minutes

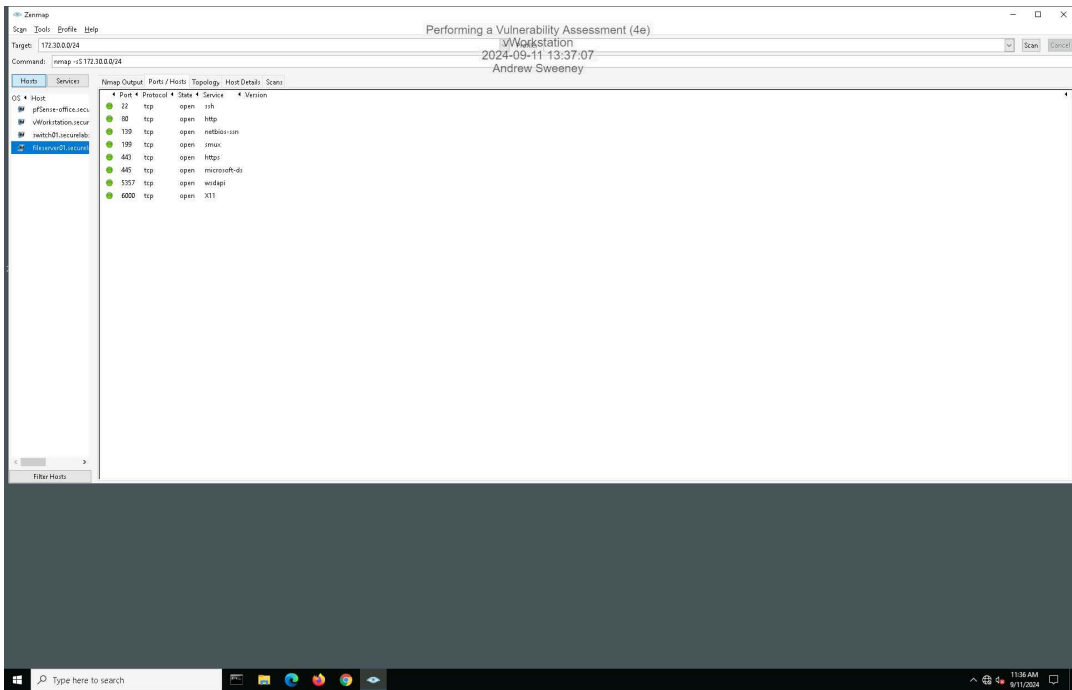
Progress: 100%

Report Generated: Monday, September 16, 2024 at 11:19 PM

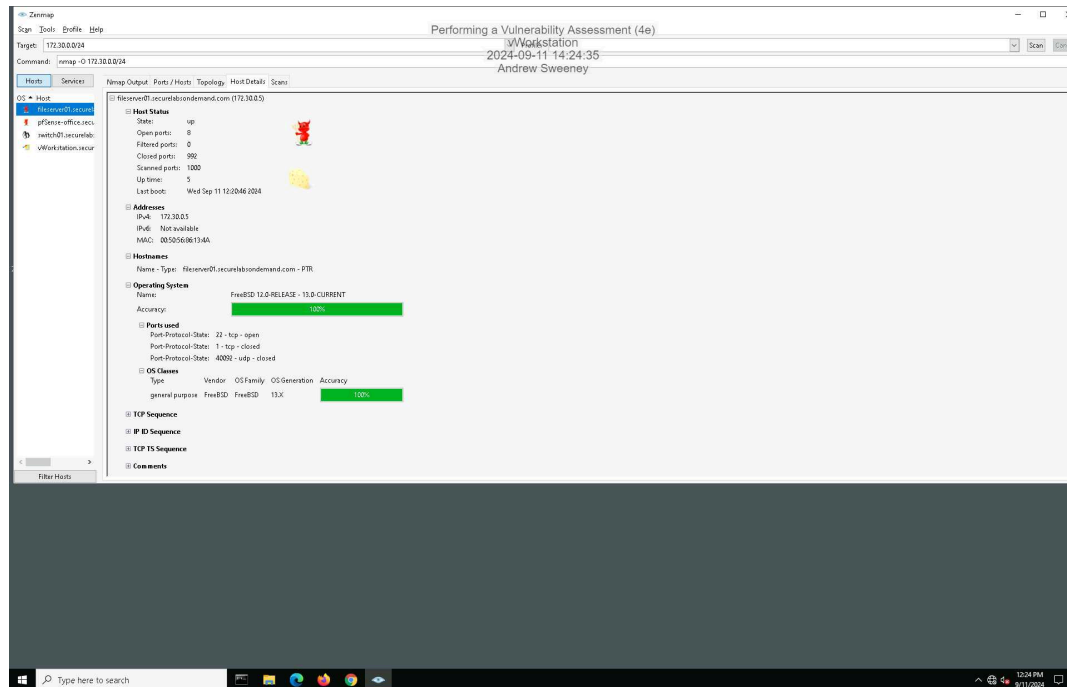
Section 1: Hands-On Demonstration

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**.

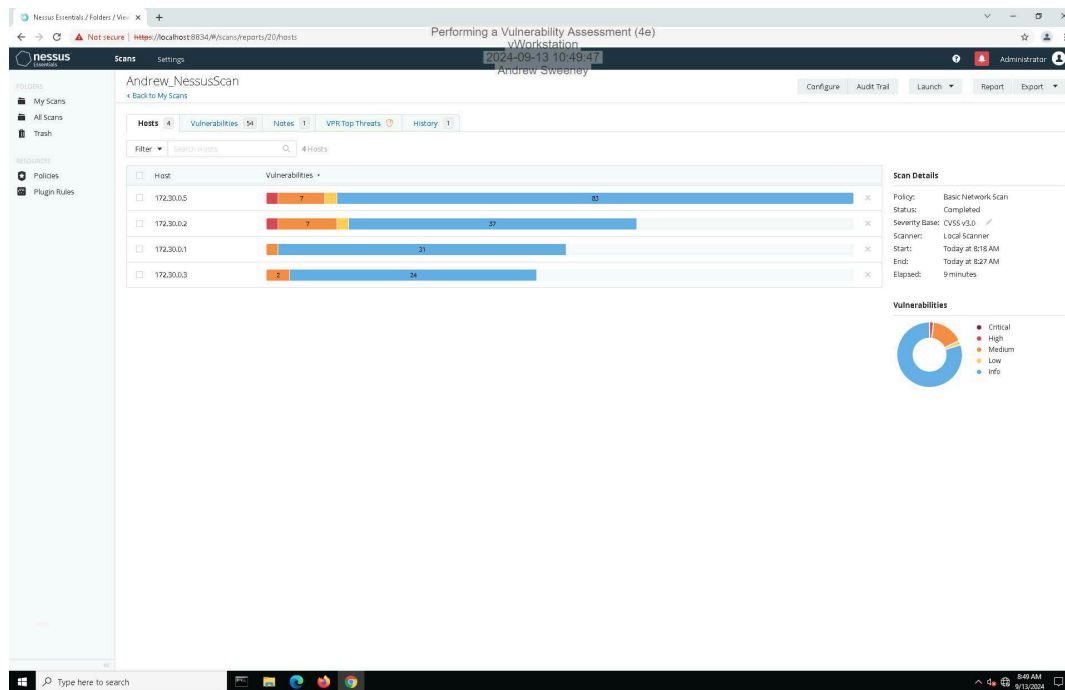


19. Make a screen capture showing the details in the **Ports/Hosts** tab from the **Service** scan for **fileserver01.securelabsondemand.com**.



Part 2: Conduct a Vulnerability Scan with Nessus

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



Part 3: Evaluate Your Findings

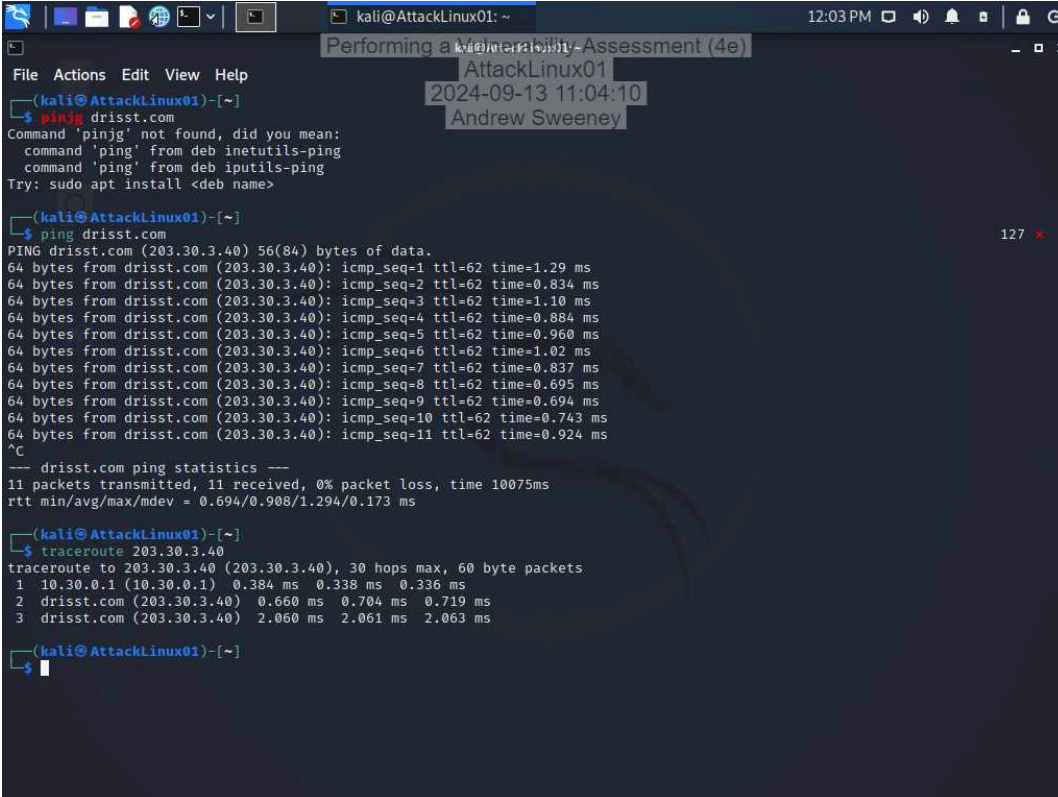
11. **Summarize** the vulnerability you selected, including the CVSS risk score, and **recommend** a mitigation strategy.

Vulnerability 51192 SSL Cert cannot be Trusted. CVSS score 6.5. To fix this issue a new SSL cert that is valid needs to be purchased. Make sure that the domain name is correct on the cert and is correctly configured for your use.

Section 2: Applied Learning

Part 1: Scan the Network with Nmap

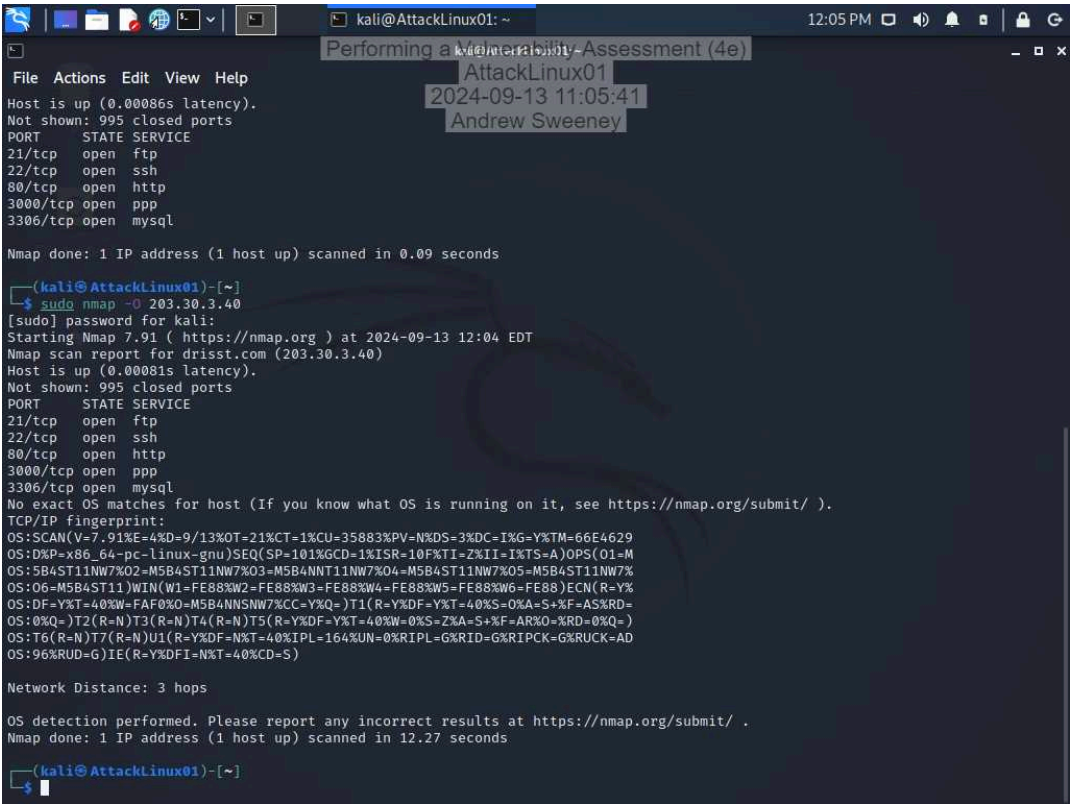
6. Make a screen capture showing the results of the traceroute command.



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

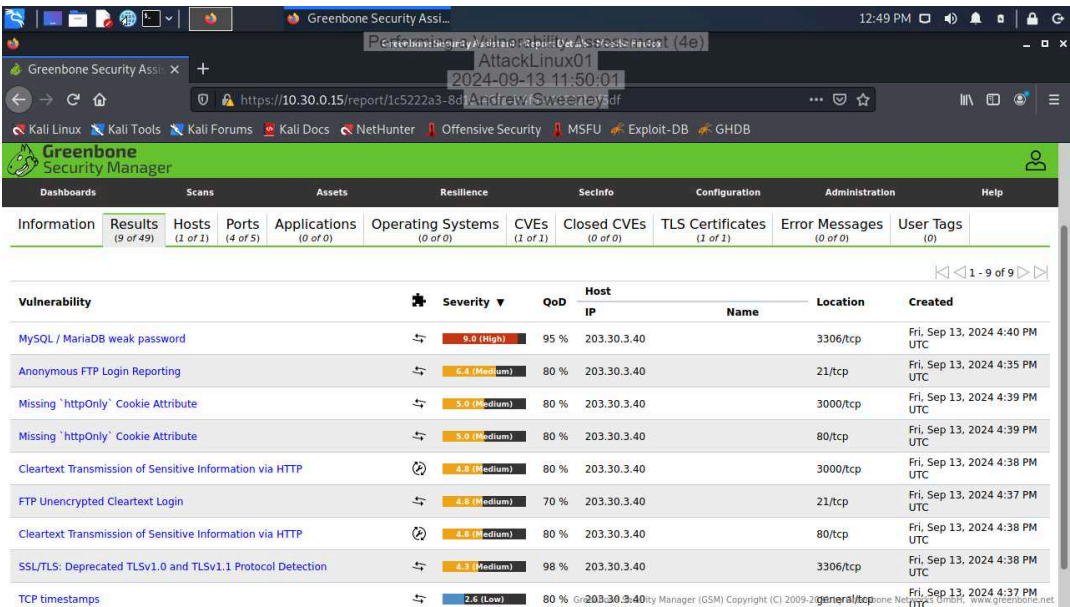
```
kali@AttackLinux01: ~  
File Actions Edit View Help  
-(kali@AttackLinux01)-[~]  
$ ping drisst.com  
Command 'ping' not found, did you mean:  
command 'ping' from deb inetutils-ping  
command 'ping' from deb iputils-ping  
Try: sudo apt install <deb name>  
  
-(kali@AttackLinux01)-[~]  
$ ping 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=1.29 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=0.834 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=1.10 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=0.884 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=0.960 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=6 ttl=62 time=1.02 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=7 ttl=62 time=0.837 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=8 ttl=62 time=0.695 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=9 ttl=62 time=0.694 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=10 ttl=62 time=0.743 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=11 ttl=62 time=0.924 ms  
^C  
-- drisst.com ping statistics --  
11 packets transmitted, 11 received, 0% packet loss, time 10075ms  
rtt min/avg/max/mdev = 0.694/0.908/1.294/0.173 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) 0.384 ms 0.338 ms 0.336 ms  
2 drisst.com (203.30.3.40) 0.660 ms 0.704 ms 0.719 ms  
3 drisst.com (203.30.3.40) 2.060 ms 2.061 ms 2.063 ms  
  
-(kali@AttackLinux01)-[~]  
$
```

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.

CVE-2023-33456

Corporate Web Application

Completed by

Insert your name here.

Andrew Sweeney

On

Insert current date here.

09/16/2024

Purpose

Identify the purpose of the penetration test.

The purpose was to test the web application to ensure that it was secure and identify any weak points. Then use any found weak points to make adjustments and remediate.

Scope

Identify the scope of the penetration test.

The web app. Its background services, and supporting network infrastructure.

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.

Severity: high:

Description: A SQL injection attack was found in the login form allowing outside unauthorized person to execute SQL commands to retrieve or modify sensitive data.

Remediation: Remove bad scripts, and use new Content Security Policy headers

Conclusion

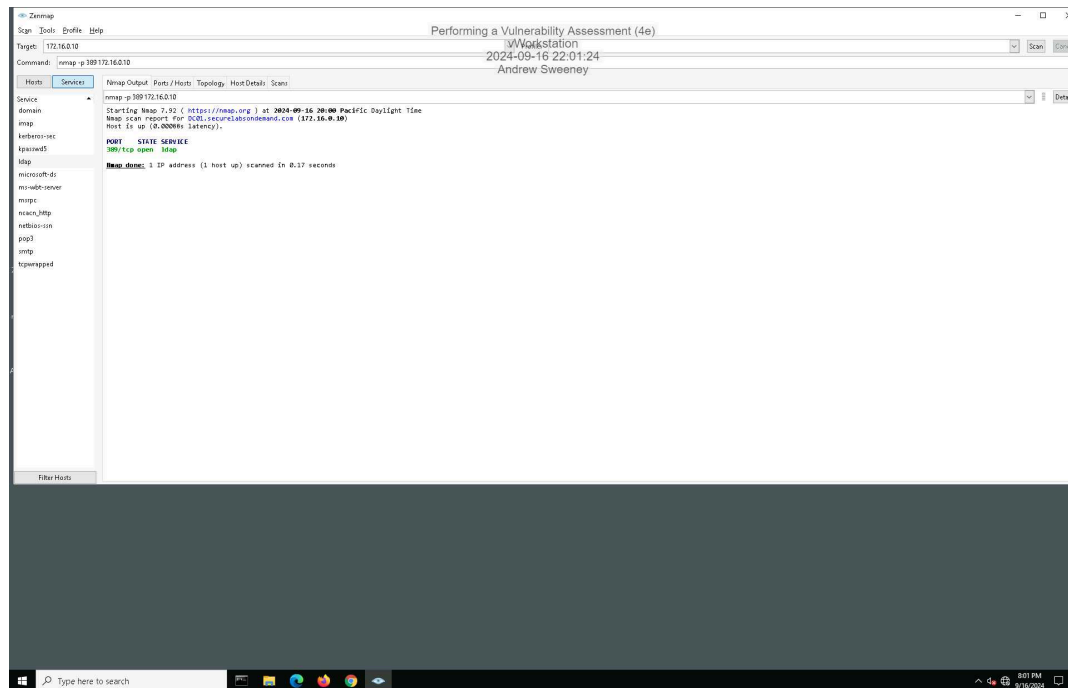
Identify your key findings.

Serious vulnerabilities were found during the penetration test: privilege escalation, stored cross-site scripting (XSS), and SQL injection. It is advised to apply security headers, enforce more stringent role-based access control restrictions, and provide input validation in order to address these. The overall security posture of the application should be maintained with regular security evaluations and updates.

Section 3: Challenge and Analysis

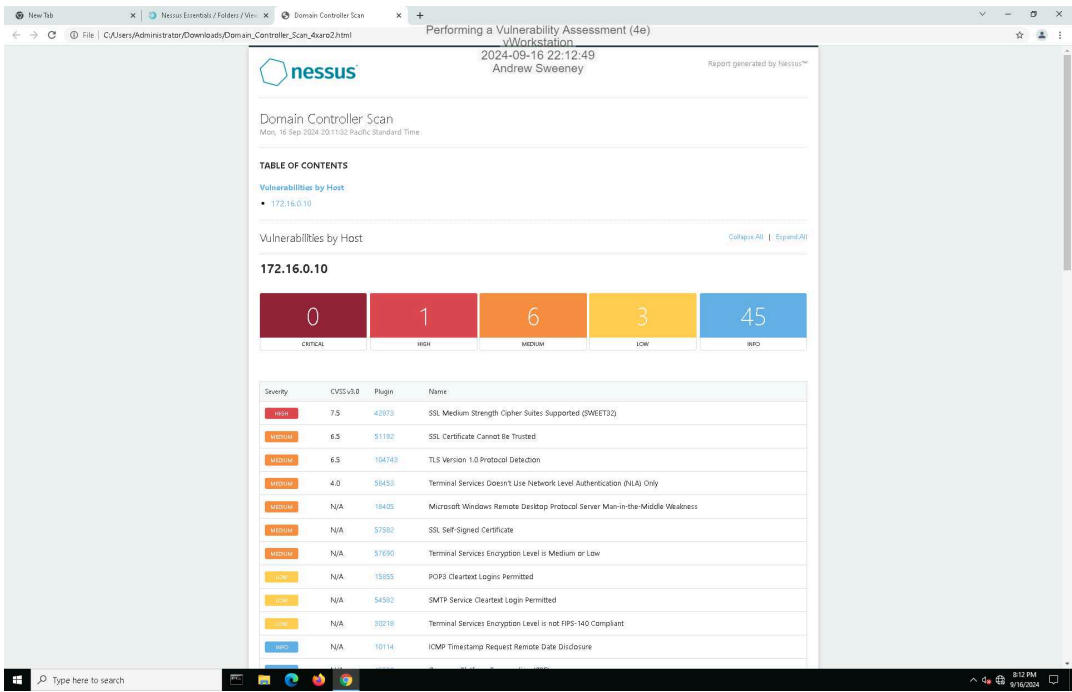
Part 1: Scan the Domain Controller with Nmap

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.

Corporate Domain Controller (172.160.0.2)

Completed by

Insert your name here.

Andrew Sweeney

On

Insert current date here.

09/16/2024

Purpose

Identify the purpose of the penetration test.

The obj of this pen test was to evaluate the security of the corporate domain controller, with a focus on identifying and mitigating vulnerabilities relates to ssl/tls encryption protocols. The goal was to enhance security measures protecting sensitive data.

Scope

Identify the scope of the penetration test.

The penetration test focused on the SSL/TLS configurations of the corporate domain controller server hosted at 172.160.0.2. The test included the evaluation of encryption protocols, cipher suites, and server responses to various types of SSL-based attacks.

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.

Severity: high

Score: 7.2

Description: The server supports 64-bit block cipher suites, which are vulnerable to the SWEET32 attack

Remediation: Disable 3DES and other 64-bit block ciphers on the server. It's recommended to use cipher suites that support AES with key sizes of at least 128 bits.

Conclusion

Identify your key findings.

The penetration test revealed that the corporate domain server is vulnerable to the SWEET32 attack due to the support of medium strength cipher suites. Immediate action is required to update the SSL/TLS configurations by disabling all 64-bit block cipher suites and prioritizing the use of stronger algorithms like AES.