Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Student:	Email:
Zachary Marabeas	gx4993@wayne.edu

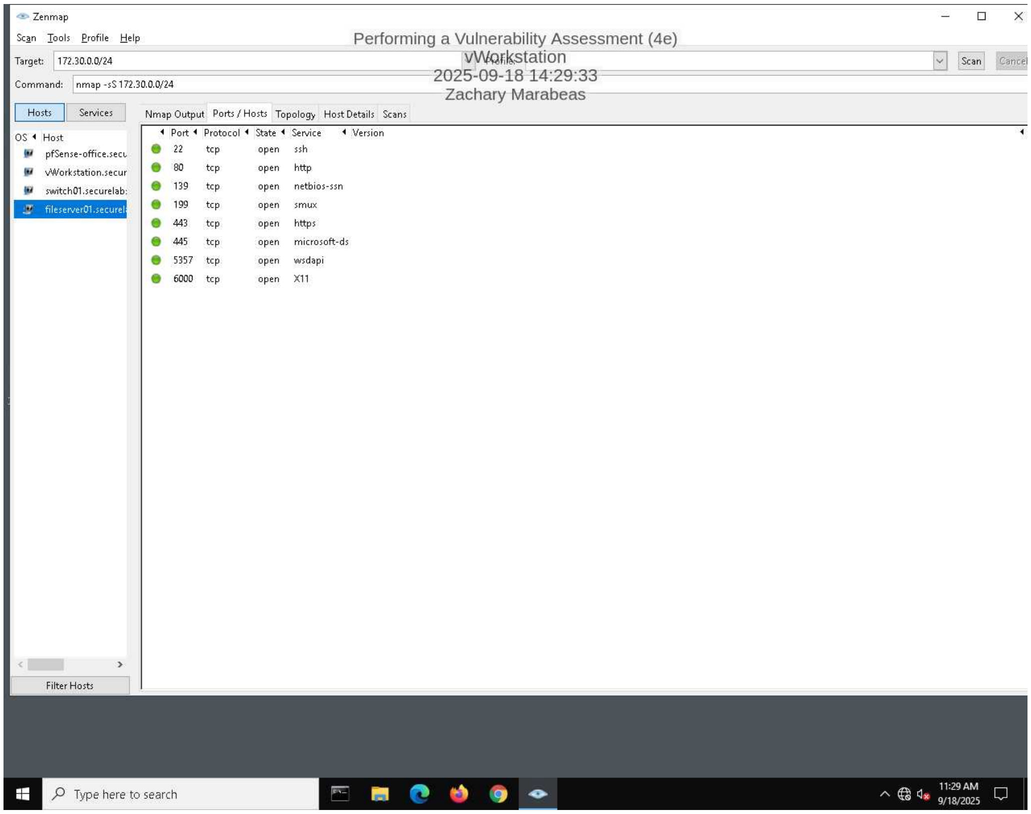
Time on Task:	Progress:
2 hours, 55 minutes	100%

Report Generated: Friday, September 19, 2025 at 12:12 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**.



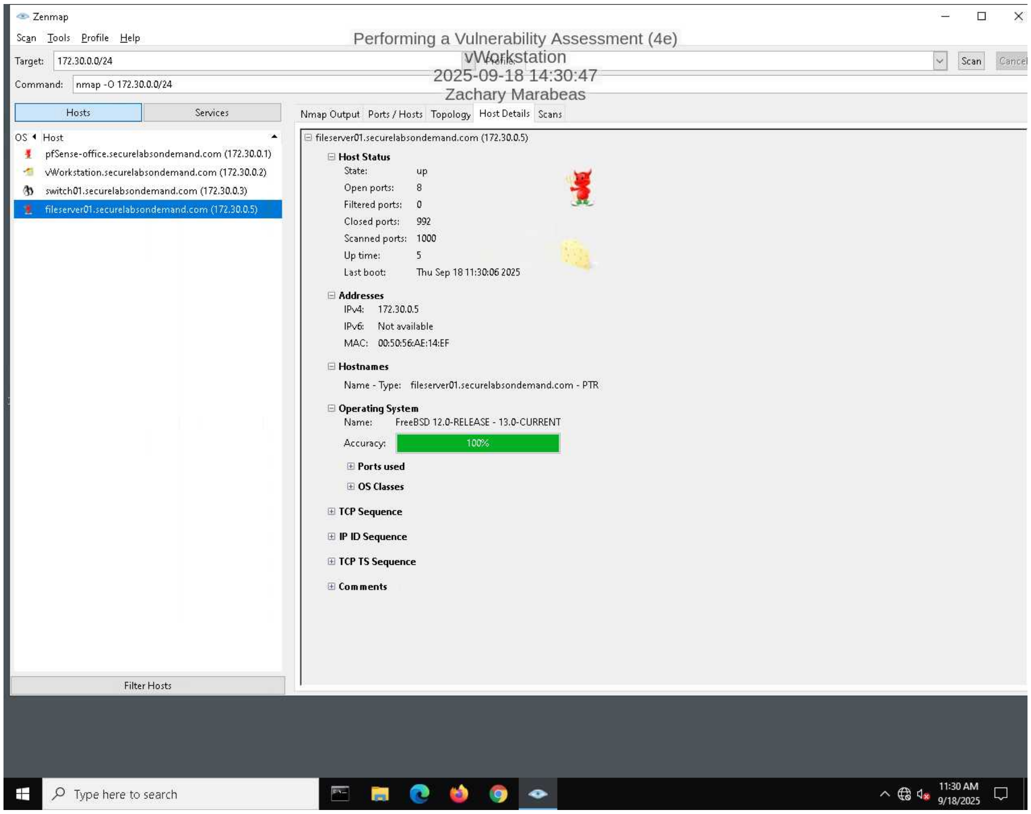
Performing a Vulnerability Assessment (4e)
vWorkstation
2025-09-18 14:29:33
Zachary Marabeas

Target: 172.30.0.0/24

Command: nmap -sS 172.30.0.0/24

Port	Protocol	State	Service	Version
22	tcp	open	ssh	
80	tcp	open	http	
139	tcp	open	netbios-ssn	
199	tcp	open	smux	
443	tcp	open	https	
445	tcp	open	microsoft-ds	
5357	tcp	open	wsdapi	
6000	tcp	open	X11	

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



Performing a Vulnerability Assessment (4e)
vWorkstation
2025-09-18 14:30:47
Zachary Marabeas

Target: 172.30.0.0/24

Command: nmap -O 172.30.0.0/24

pfSense-office.securelabsondemand.com (172.30.0.1)
vWorkstation.securelabsondemand.com (172.30.0.2)
switch01.securelabsondemand.com (172.30.0.3)
fileserver01.securelabsondemand.com (172.30.0.5)

⊟ fileserver01.securelabsondemand.com (172.30.0.5)

⊟ **Host Status**

State:	up
Open ports:	8
Filtered ports:	0
Closed ports:	992
Scanned ports:	1000
Up time:	5
Last boot:	Thu Sep 18 11:30:06 2025

⊟ **Addresses**

IPv4:	172.30.0.5
IPv6:	Not available
MAC:	00:50:56:AE:14:EF

⊟ **Hostnames**

Name - Type: fileserver01.securelabsondemand.com - PTR

⊟ **Operating System**

Name: FreeBSD 12.0-RELEASE - 13.0-CURRENT

Accuracy: 100%

⊞ **Ports used**

⊞ **OS Classes**

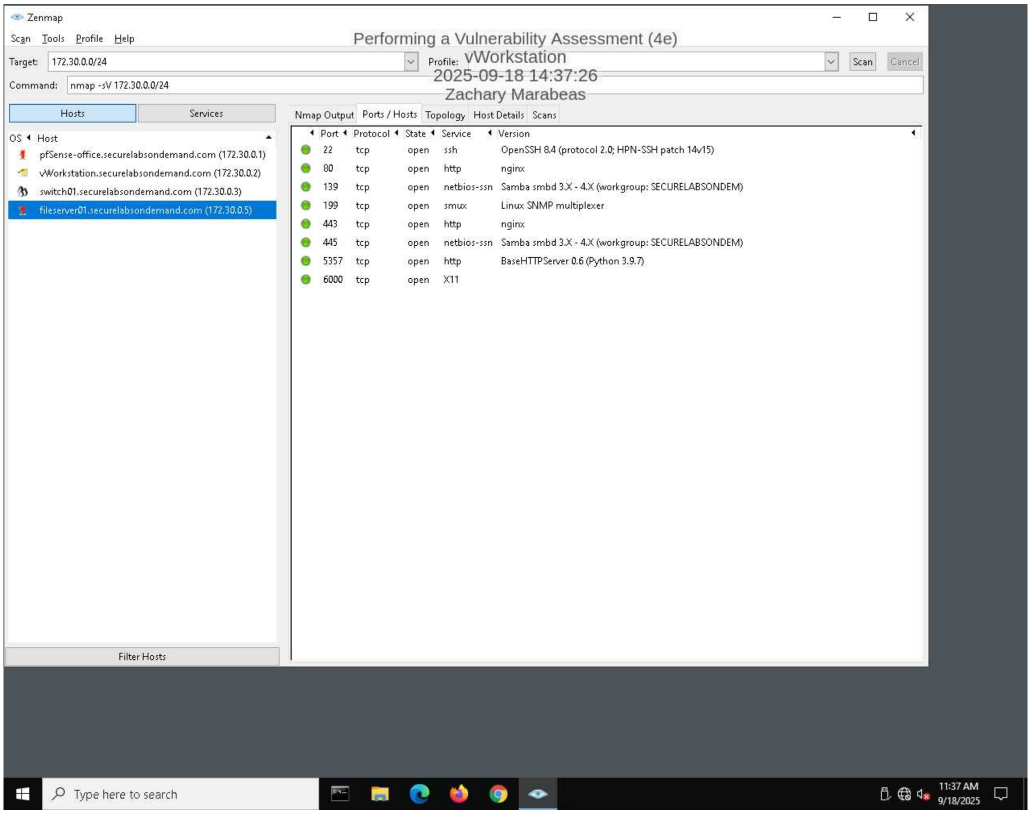
⊞ **TCP Sequence**

⊞ **IP ID Sequence**

⊞ **TCP TS Sequence**

⊞ **Comments**

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



Performing a Vulnerability Assessment (4e)
vWorkstation
2025-09-18 14:37:26
Zachary Marabeas

Target: 172.30.0.0/24

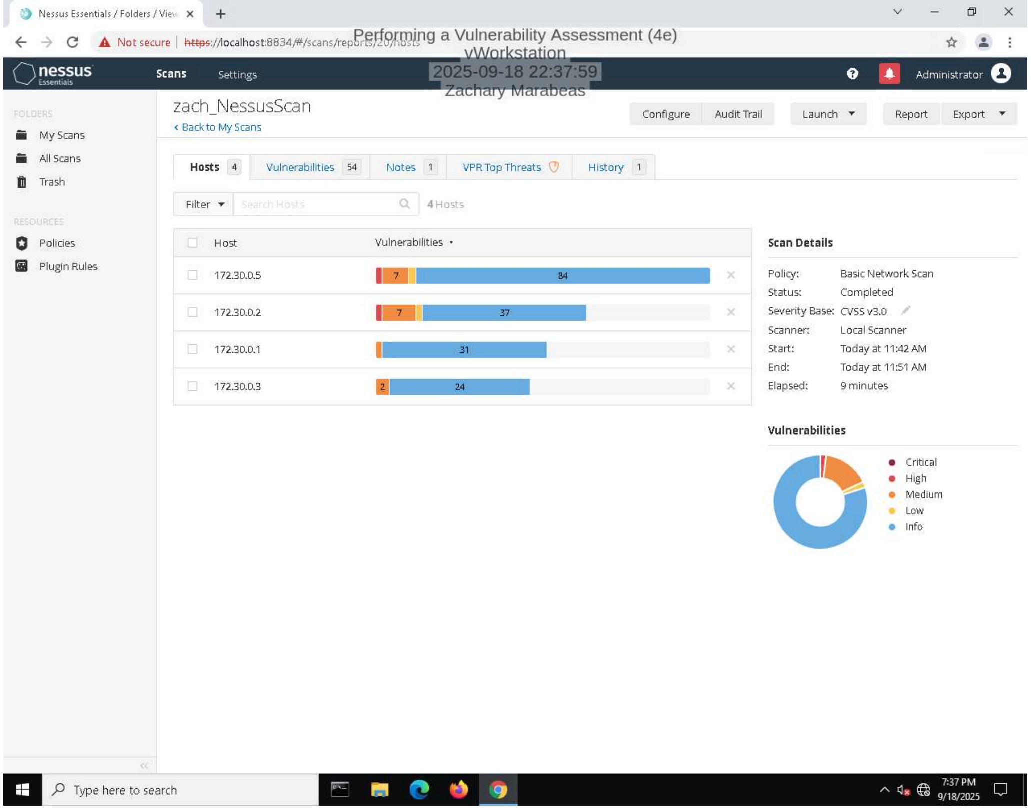
Command: nmap -sV 172.30.0.0/24

OS	Host
	pfSense-office.securelabsondemand.com (172.30.0.1)
	vWorkstation.securelabsondemand.com (172.30.0.2)
	switch01.securelabsondemand.com (172.30.0.3)
	fileserver01.securelabsondemand.com (172.30.0.5)

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 8.4 (protocol 2.0; HPN-SSH patch 14v15)
●	80	tcp	open	http	nginx
●	139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: SECURELABSONDEM)
●	199	tcp	open	smux	Linux SNMP multiplexer
●	443	tcp	open	http	nginx
●	445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: SECURELABSONDEM)
●	5357	tcp	open	http	BaseHTTPServer 0.6 (Python 3.9.7)
●	6000	tcp	open	X11	

Part 2: Conduct a Vulnerability Scan with Nessus

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



Performing a Vulnerability Assessment (4e)
vWorkstation
2025-09-18 22:37:59
Zachary Marabeas

zach_NessusScan

Host	Vulnerabilities
172.30.0.5	7 84
172.30.0.2	7 37
172.30.0.1	31
172.30.0.3	2 24

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 11:42 AM
End:	Today at 11:51 AM
Elapsed:	9 minutes

Part 3: Evaluate Your Findings

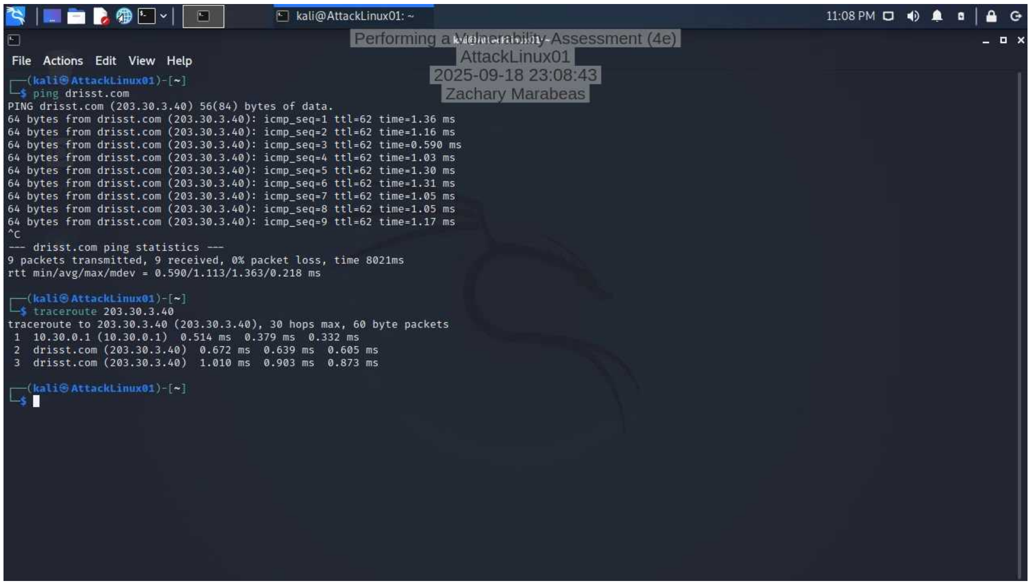
11. **Summarize** the vulnerability you selected, including the CVSS risk score, and **recommend** a mitigation strategy.

CVE-2008-4309 is an integer overflow vulnerability in Net-SNMP agent with a CVSS score of 5.0 (Medium). The issue allows remote attackers to cause denial of service via integer overflow in the netsnmp_create_subtree_cache function, affecting Net-SNMP versions 5.2-5.4. Fix by upgrading to patched versions 5.4.2.1+, 5.3.2.3+, or 5.2.5.1+.

Section 2: Applied Learning

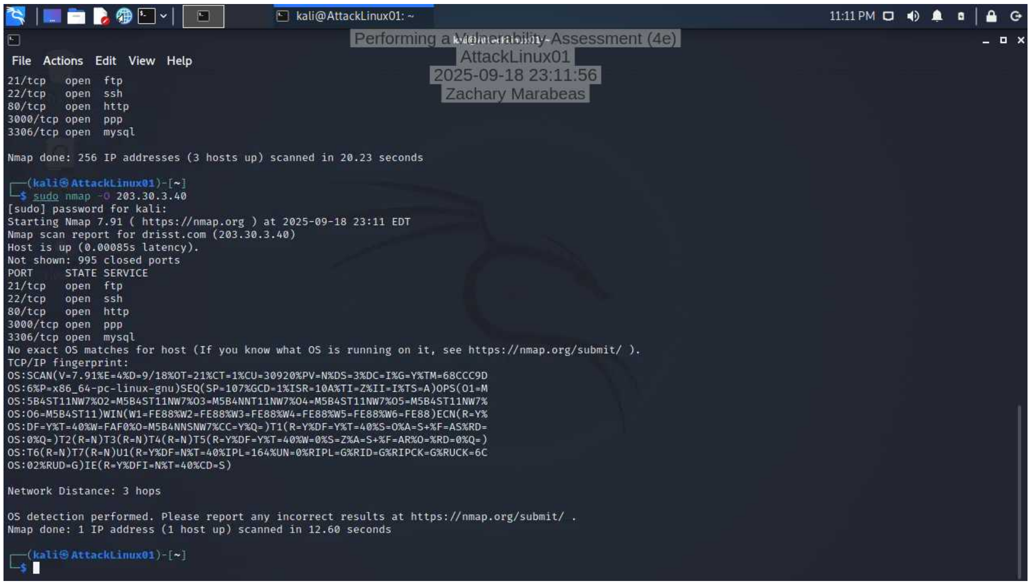
Part 1: Scan the Network with Nmap

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



```
┌──(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=1.36 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=1.16 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.590 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=1.03 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=1.30 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=6 ttl=62 time=1.31 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=7 ttl=62 time=1.05 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=8 ttl=62 time=1.05 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=9 ttl=62 time=1.17 ms
^C
--- drisst.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8021ms
rtt min/avg/max/mdev = 0.590/1.113/1.363/0.218 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)  0.514 ms  0.379 ms  0.332 ms
 2  drisst.com (203.30.3.40)  0.672 ms  0.639 ms  0.605 ms
 3  drisst.com (203.30.3.40)  1.010 ms  0.903 ms  0.873 ms

┌──(kali㉿AttackLinux01)-[~]
└─$ 
```

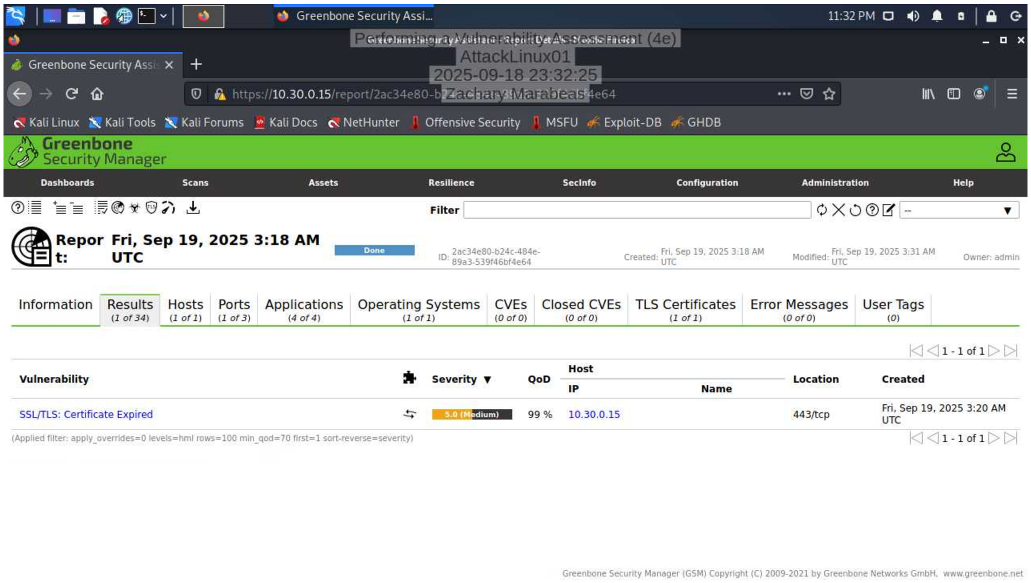
10. **Make a screen capture** showing the **results of the Nmap scan with OS detection activated**.



```
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 20.23 seconds

┌──(kali㉿AttackLinux01)-[~]
└─$ sudo nmap -O 203.30.3.40
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2025-09-18 23:11 EDT
Nmap scan report for drisst.com (203.30.3.40)
Host is up (0.00085s 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=9/18%OT=21%CT=1%CU=30920%PV=N%DS=3%DC=I%G=Y%TM=68CCC9D
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10A%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=%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=6C
OS:02%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**.



Performing a Vulnerability Assessment (4e)
AttackLinux01
2025-09-18 23:32:25
Zachary Marabeas

Report: Fri, Sep 19, 2025 3:18 AM UTC   Done   ID: 2ac34e80-b24c-484e-89a3-539f46bf4e64   Created: Fri, Sep 19, 2025 3:18 AM UTC   Modified: Fri, Sep 19, 2025 3:31 AM UTC   Owner: admin

Information | Results (1 of 34) | Hosts (1 of 1) | Ports (1 of 3) | Applications (4 of 4) | Operating Systems (1 of 1) | CVEs (0 of 0) | Closed CVEs (0 of 0) | TLS Certificates (1 of 1) | Error Messages (0 of 0) | User Tags (0)

1 - 1 of 1

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
SSL/TLS: Certificate Expired	⇆	5.0 (Medium)	99 %	10.30.0.15		443/tcp	Fri, Sep 19, 2025 3:20 AM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 1 of 1

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

Web Applications and Network Infrastructure

Completed by

Insert your name here.

Zachary Marabeas

On

Insert current date here.

9/18/25

Purpose

Identify the purpose of the penetration test.

Identify high-severity vulnerabilities in web servers, SSL/TLS implementations, and network services that could be exploited for ddos attacks or man-in-the-middle attacks

Scope

Identify the scope of the penetration test.

HTTP/2 enabled web services, OpenSSL implementations

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.

1. CVE-2023-44487 - HTTP/2 Rapid Reset Attack
  Severity: High (CVSS 7.5)
  Issue: HTTP/2 protocol vulnerability allowing massive DDoS attacks through stream multiplexing abuse. Attackers send numerous requests followed by immediate RST_STREAM frames, causing substantial server-side resource consumption. This vulnerability enabled record-breaking DDoS attacks exceeding 398 million requests per second.
  Remediation: Apply HTTP/2 patches from vendors, implement rate limiting on stream creation, consider disabling HTTP/2 if not required, and deploy DDoS protection services.

2. CVE-2024-12797 - OpenSSL Raw Public Keys Vulnerability
  Severity: High
  Issue: TLS/DTLS connections using RFC7250 raw public keys fail to properly authenticate servers, enabling man-in-the-middle attacks. Affects OpenSSL 3.2, 3.3, and 3.4 versions where attackers can intercept and manipulate encrypted communications.
  Remediation: Upgrade to OpenSSL versions 3.2.4, 3.3.2, or 3.4.1. Disable raw public key usage if not required and implement certificate pinning for critical connections.

3. CVE-2024-40766 - SonicWall SSL VPN Access Control Bypass
  Severity: Critical (CVSS 9.3)
  Issue: Access control bypass vulnerability in SonicWall SSL VPN allowing unauthorized access and potential firewall crashes leading to network outages. Actively exploited in the wild with confirmed attacks.
  Remediation: Apply SonicWall security patches immediately, implement network segmentation, enable additional authentication factors, and monitor VPN access logs for suspicious activity.

Conclusion

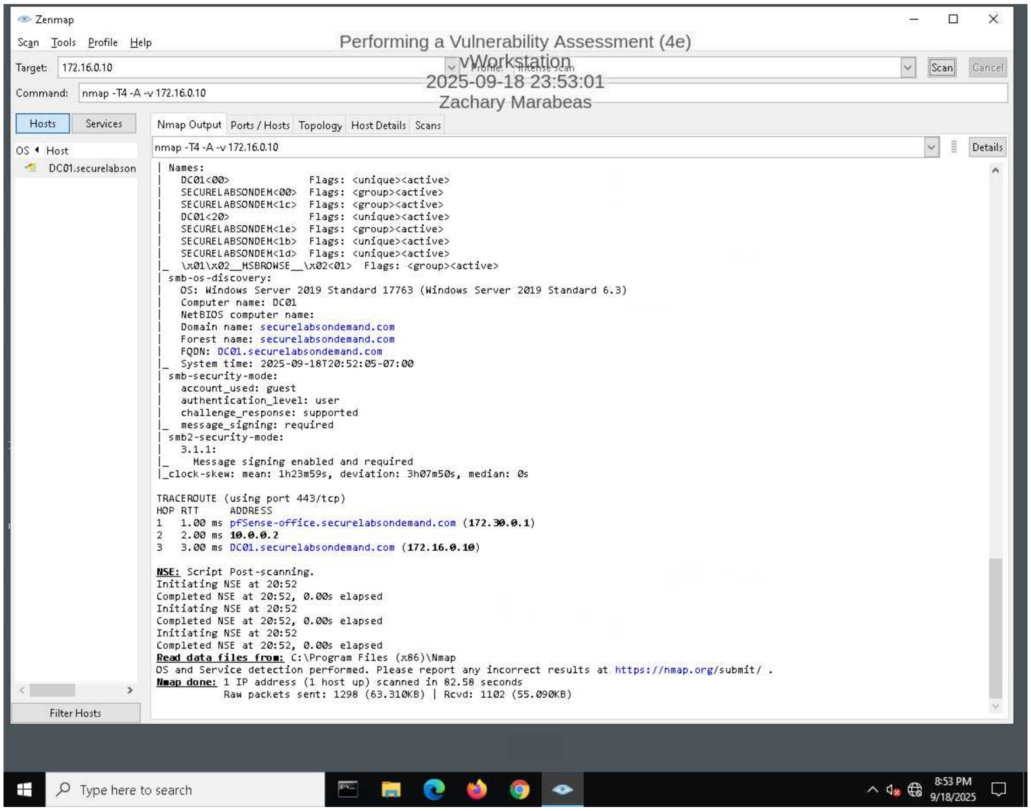
Identify your key findings.

All three vulnerabilities present significant risks to organizational security infrastructure. The HTTP/2 Rapid Reset vulnerability enables unprecedented DDoS attacks, while the OpenSSL and SonicWall vulnerabilities compromise encrypted communications and network access controls. Immediate patching and configuration hardening are critical to prevent exploitation. Organizations should prioritize these remediations based on their exposure to HTTP/2 services, OpenSSL usage, and SonicWall VPN deployments.

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**.



Performing a Vulnerability Assessment (4e)
vWorkstation
2025-09-18 23:53:01
Zachary Marabeas

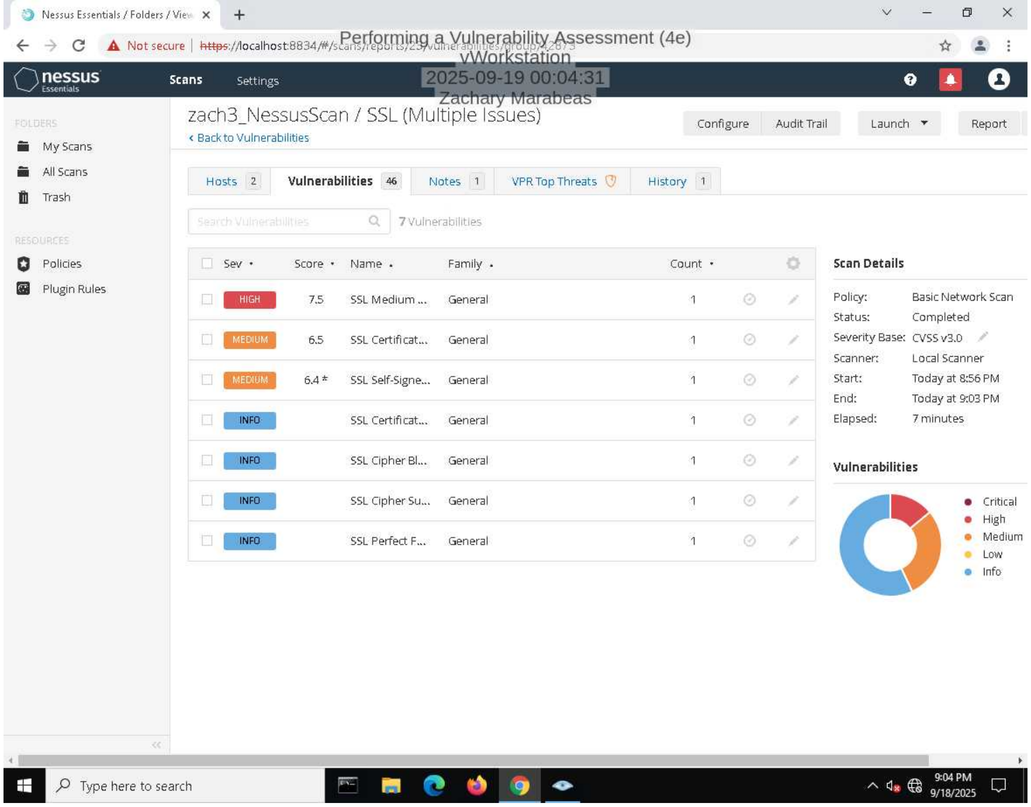
Target: 172.16.0.10

Command: nmap -T4 -A -v 172.16.0.10

```
| Names:
|   DC01<00>             Flags: <unique><active>
|   SECURELABSONDEM<00>  Flags: <group><active>
|   SECURELABSONDEM<1c>  Flags: <group><active>
|   DC01<20>             Flags: <unique><active>
|   SECURELABSONDEM<1e>  Flags: <group><active>
|   SECURELABSONDEM<1b>  Flags: <unique><active>
|   SECURELABSONDEM<1d>  Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)
|   Computer name: DC01
|   NetBIOS computer name:
|   Domain name: securelabsondemand.com
|   Forest name: securelabsondemand.com
|   FQDN: DC01.securelabsondemand.com
|_  System time: 2025-09-18T20:52:05-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
|_clock-skew: mean: 1h23m59s, deviation: 3h07m50s, median: 0s

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   1.00 ms pfSense-office.securelabsondemand.com (172.30.0.1)
2   2.00 ms 10.0.0.2
3   3.00 ms DC01.securelabsondemand.com (172.16.0.10)

NSE: Script Post-scanning.
Initiating NSE at 20:52
Completed NSE at 20:52, 0.00s elapsed
Initiating NSE at 20:52
Completed NSE at 20:52, 0.00s elapsed
Initiating NSE at 20:52
Completed NSE at 20:52, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.58 seconds
           Raw packets sent: 1298 (63.310KB) | Rcvd: 1102 (55.090KB)
```

Part 2: Scan the Domain Controller with Nessus

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



Performing a Vulnerability Assessment (4e)
vWorkstation
2025-09-19 00:04:31
Zachary Marabeas

zach3_NessusScan / SSL (Multiple Issues)

‹ Back to Vulnerabilities

Hosts 2 | Vulnerabilities 46 | Notes 1 | VPR Top Threats | History 1

7 Vulnerabilities

Sev	Score	Name	Family	Count
HIGH	7.5	SSL Medium ...	General	1
MEDIUM	6.5	SSL Certificat...	General	1
MEDIUM	6.4 *	SSL Self-Signe...	General	1
INFO		SSL Certificat...	General	1
INFO		SSL Cipher Bl...	General	1
INFO		SSL Cipher Su...	General	1
INFO		SSL Perfect F...	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:56 PM
End:	Today at 9:03 PM
Elapsed:	7 minutes

Vulnerabilities

Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

172.16.0.10

Completed by

Insert your name here.

Zach Marabeas

On

Insert current date here.

9/19/25

Purpose

Identify the purpose of the penetration test.

Identify cryptographic vulnerabilities in SSL/TLS implementations using weak cipher suites

Scope

Identify the scope of the penetration test.

SSL/TLS services

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.

1. CVE-2016-2183 - SSL Medium Strength Cipher Suites Supported (SWEET32)
  Severity: High (CVSS 7.5)
  Issue: 3DES cipher suites vulnerable to birthday attacks enabling plaintext recovery. Attackers capture 32GB encrypted traffic from long-lived TLS sessions to recover authentication tokens within 40 hours. Affects systems using DES-CBC3-SHA cipher.
  Remediation: Disable 3DES cipher suites. Configure "SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4:!3DES" for Apache or run "Disable-TlsCipherSuite -Name 'TLS_RSA_WITH_3DES_EDE_CBC_SHA'" for Windows. Use AES-based ciphers only.

Conclusion

Identify your key findings.

3DES cipher support enables practical cryptanalytic attacks against encrypted communications. The SWEET32 vulnerability allows authentication token recovery from captured traffic. Immediate cipher suite reconfiguration required to eliminate this attack vector.