Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Student:	Email:
Jamal Sherif	jamalsherif2@gmail.com

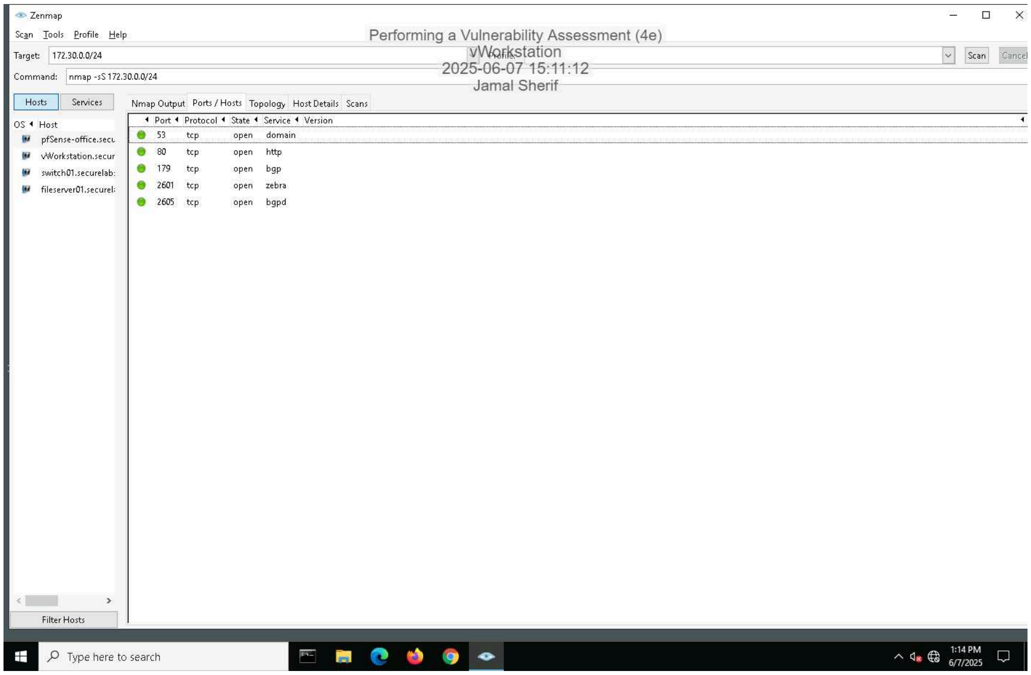
Time on Task:	Progress:
7 hours, 41 minutes	100%

Report Generated: Tuesday, September 30, 2025 at 5:34 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**.



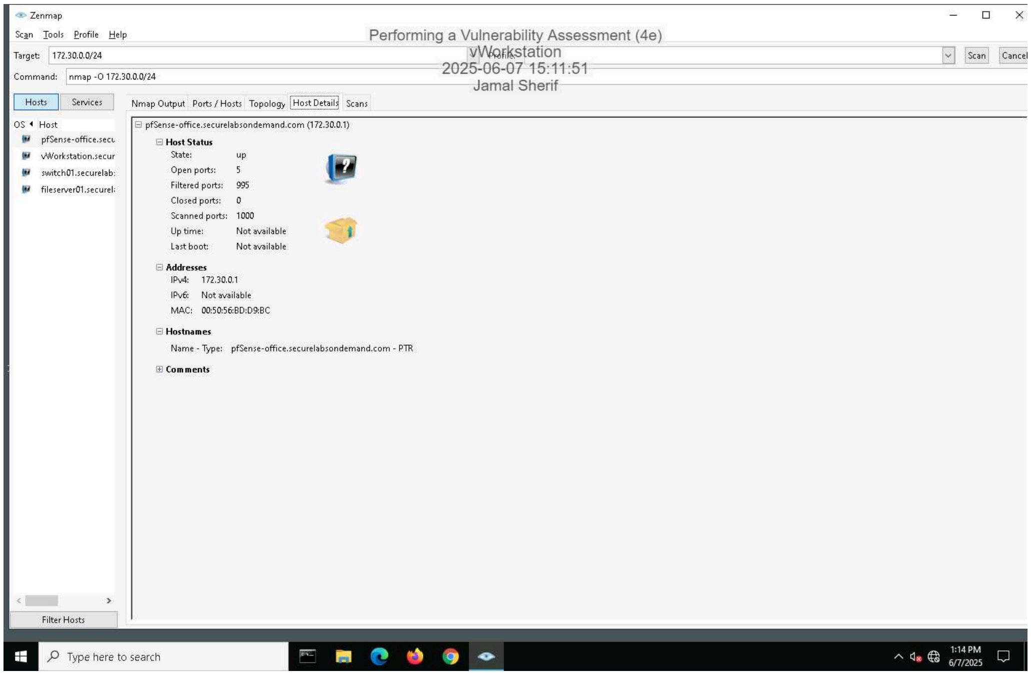
Performing a Vulnerability Assessment (4e)
vWorkstation
2025-06-07 15:11:12
Jamal Sherif

Target: 172.30.0.0/24

Command: nmap -sS 172.30.0.0/24

Port	Protocol	State	Service	Version
53	tcp	open	domain	
80	tcp	open	http	
179	tcp	open	bgp	
2601	tcp	open	zebra	
2605	tcp	open	bgpd	

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



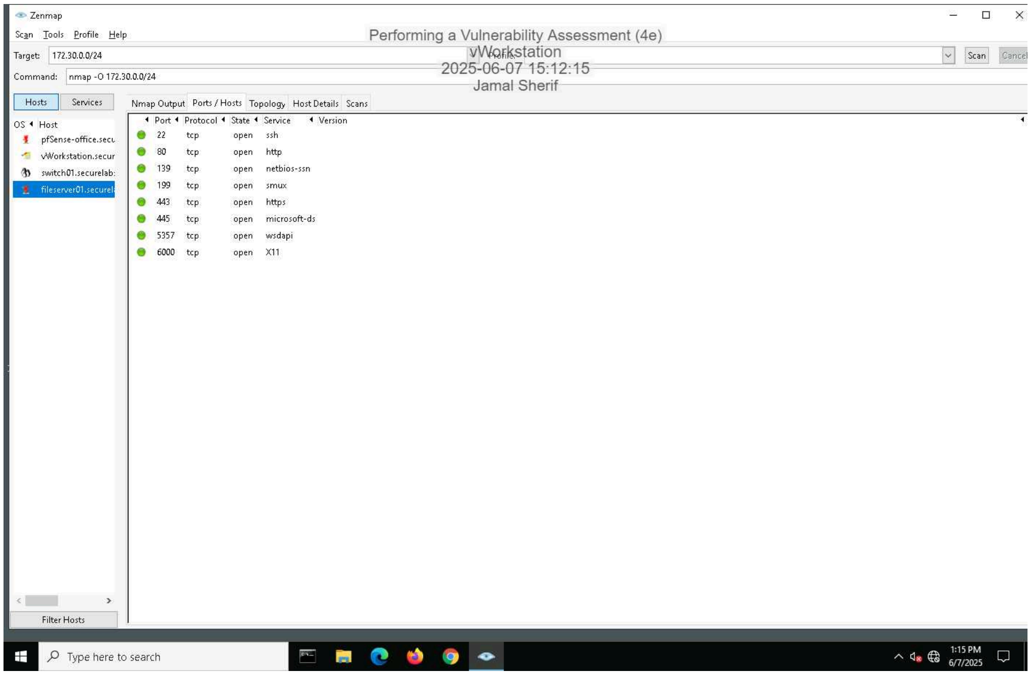
Performing a Vulnerability Assessment (4e)
vWorkstation
2025-06-07 15:11:51
Jamal Sherif

Target: 172.30.0.0/24

Command: nmap -O 172.30.0.0/24

```
⊟ pfSense-office.securelabsondemand.com (172.30.0.1)
    ⊟ Host Status
        State:          up
        Open ports:     5
        Filtered ports: 995
        Closed ports:   0
        Scanned ports:  1000
        Up time:        Not available
        Last boot:      Not available
    ⊟ Addresses
        IPv4:   172.30.0.1
        IPv6:   Not available
        MAC:    00:50:56:BD:D9:BC
    ⊟ Hostnames
        Name - Type:   pfSense-office.securelabsondemand.com - PTR
    ⊞ 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
2025-06-07 15:12:15
Jamal Sherif

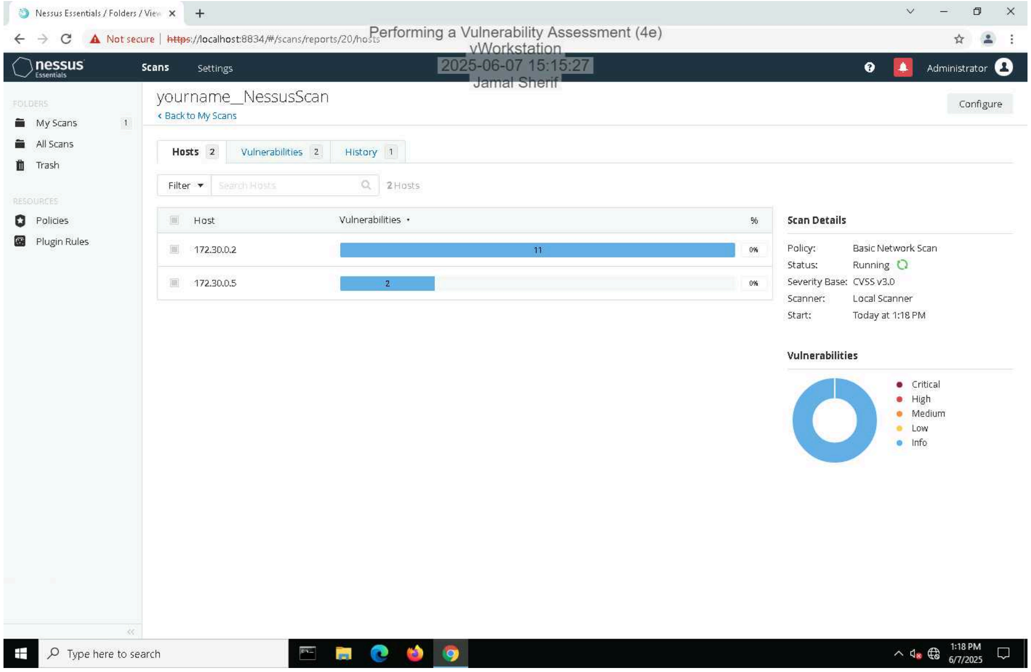
Target: 172.30.0.0/24

Command: nmap -O 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
```

Part 2: Conduct a Vulnerability Scan with Nessus

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



Performing a Vulnerability Assessment (4e)
vWorkstation
2025-06-07 15:15:27
Jamal Sherif

https://localhost:8834/#/scans/reports/20/hosts

yourname__NessusScan

Host	Vulnerabilities	%
172.30.0.2	11	0%
172.30.0.5	2	0%

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:18 PM

Part 3: Evaluate Your Findings

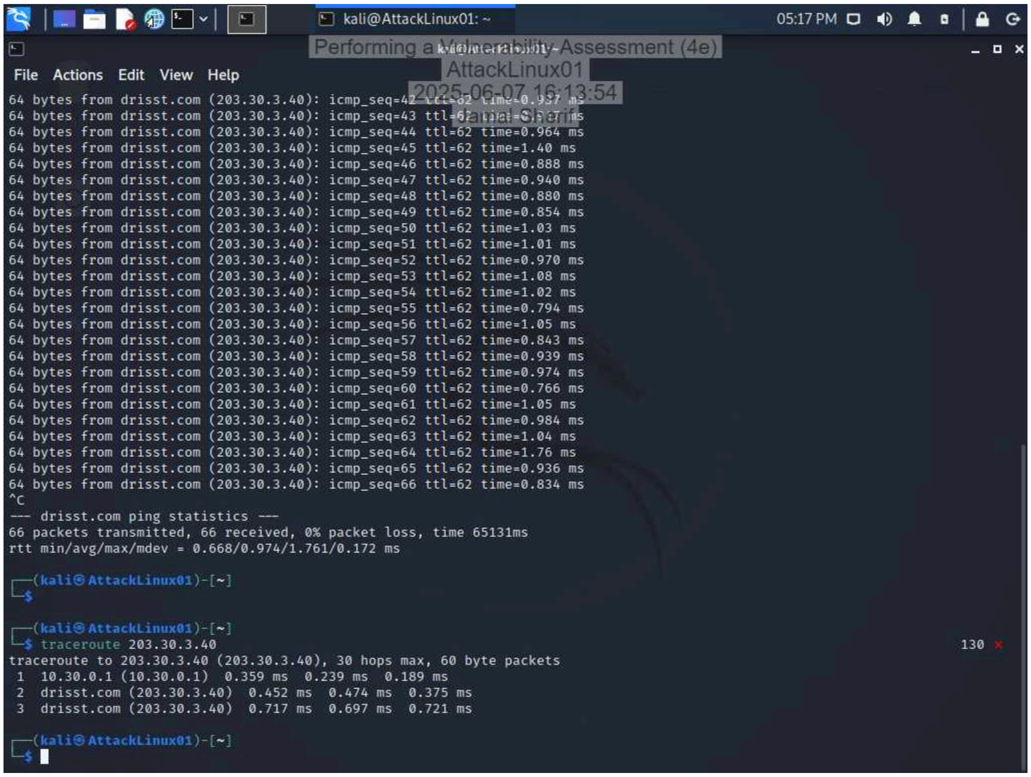
11. **Summarize** the vulnerability you selected, including the CVSS risk score, and **recommend** a mitigation strategy.

cvss risk 10Caused by bad usage of cryptographic routines in Netlogon’s secure channel protocol, enabling attackers to spoof the identity of any computer on the networkMicrosoft releases patches ,two part patch rollout:

Section 2: Applied Learning

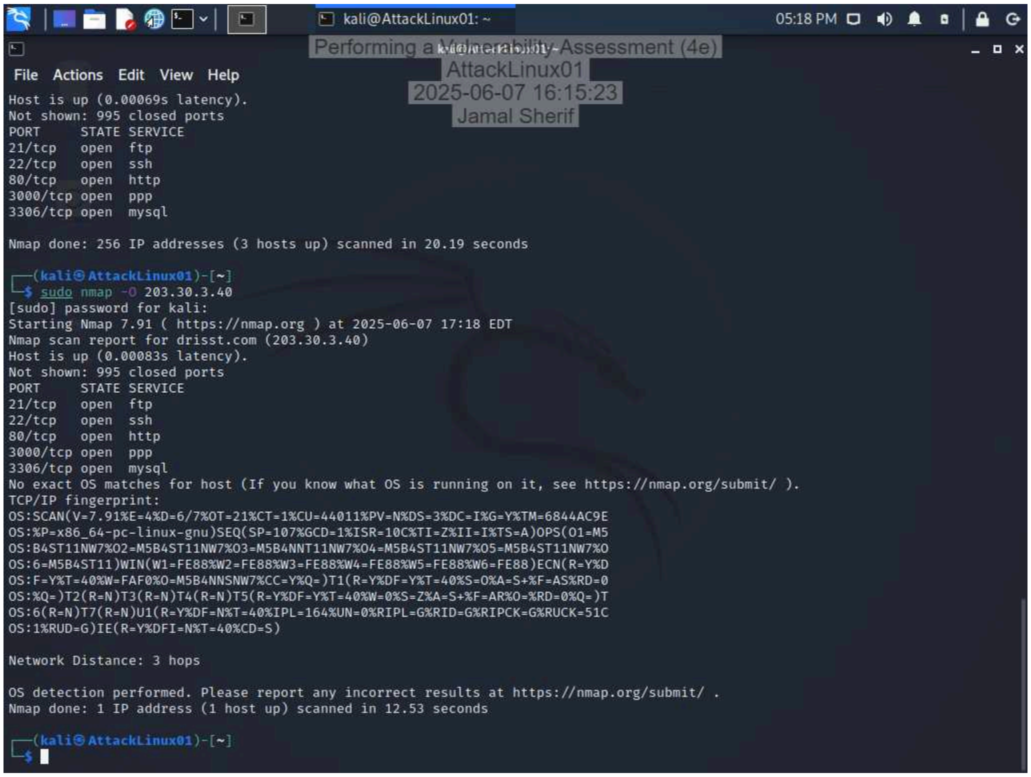
Part 1: Scan the Network with Nmap

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



```
64 bytes from drisst.com (203.30.3.40): icmp_seq=42 ttl=62 time=0.937 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=43 ttl=62 time=[illegible] ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=44 ttl=62 time=0.964 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=45 ttl=62 time=1.40 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=46 ttl=62 time=0.888 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=47 ttl=62 time=0.940 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=48 ttl=62 time=0.880 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=49 ttl=62 time=0.854 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=50 ttl=62 time=1.03 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=51 ttl=62 time=1.01 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=52 ttl=62 time=0.970 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=53 ttl=62 time=1.08 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=54 ttl=62 time=1.02 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=55 ttl=62 time=0.794 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=56 ttl=62 time=1.05 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=57 ttl=62 time=0.843 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=58 ttl=62 time=0.939 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=59 ttl=62 time=0.974 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=60 ttl=62 time=0.766 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=61 ttl=62 time=1.05 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=62 ttl=62 time=0.984 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=63 ttl=62 time=1.04 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=64 ttl=62 time=1.76 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=65 ttl=62 time=0.936 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=66 ttl=62 time=0.834 ms
^C
--- drisst.com ping statistics ---
66 packets transmitted, 66 received, 0% packet loss, time 65131ms
rtt min/avg/max/mdev = 0.668/0.974/1.761/0.172 ms

┌──(kali㉿AttackLinux01)-[~]
└─$

┌──(kali㉿AttackLinux01)-[~]
└─$ traceroute 203.30.3.40                                                   130 ✗
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)  0.359 ms  0.239 ms  0.189 ms
 2  drisst.com (203.30.3.40)  0.452 ms  0.474 ms  0.375 ms
 3  drisst.com (203.30.3.40)  0.717 ms  0.697 ms  0.721 ms

┌──(kali㉿AttackLinux01)-[~]
└─$ 
```

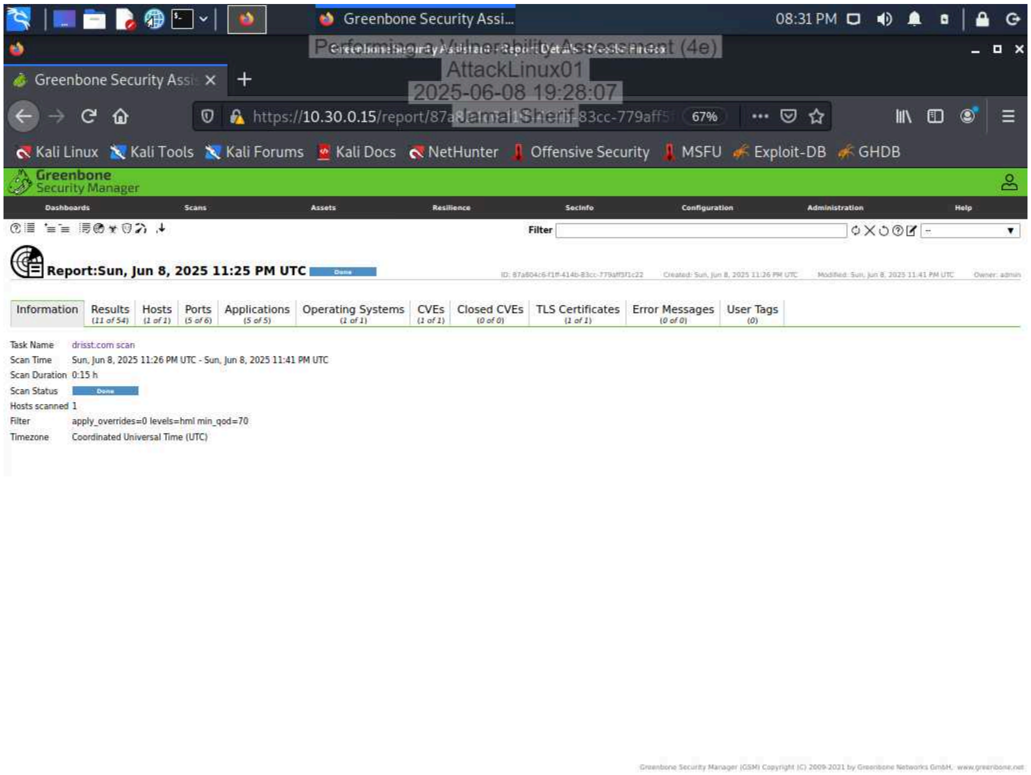
10. **Make a screen capture** showing the **results of the Nmap scan with OS detection activated**.



```
Host is up (0.00069s 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 20.19 seconds

┌──(kali㉿AttackLinux01)-[~]
└─$ sudo nmap -O 203.30.3.40
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2025-06-07 17:18 EDT
Nmap scan report for drisst.com (203.30.3.40)
Host is up (0.00083s 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=6/7%OT=21%CT=1%CU=44011%PV=N%DS=3%DC=I%G=Y%TM=6844AC9E
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10C%TI=Z%II=I%TS=A)OPS(O1=M5
OS:B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O
OS:6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%D
OS:F=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%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=)T
OS:6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=51C
OS:1%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 12.53 seconds

┌──(kali㉿AttackLinux01)-[~]
└─$ 
```

Part 2: Conduct a Vulnerability Scan with OpenVAS

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



Report:Sun, Jun 8, 2025 11:25 PM UTC Done

ID: 87a804c6-f1ff-414b-83cc-779aff3f1c22 Created: Sun, Jun 8, 2025 11:26 PM UTC Modified: Sun, Jun 8, 2025 11:41 PM UTC Owner: admin

Task Name drisst.com scan
Scan Time Sun, Jun 8, 2025 11:26 PM UTC - Sun, Jun 8, 2025 11:41 PM UTC
Scan Duration 0:15 h
Scan Status Done
Hosts scanned 1
Filter apply_overrides=0 levels=hml min_qod=70
Timezone Coordinated Universal Time (UTC)

Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

drisst.com 203.30.3.60

Completed by

Insert your name here.

Jamal Sherif

On

Insert current date here.

6/7/25

Purpose

Identify the purpose of the penetration test.

Goal of this penetration test was to look for serious security weaknesses on the target 203.30.3.60 server. Using OpenVAS to run a vulnerability scan and focused specifically on high severity issues. This test show what kinds of problems might allow an attacker to gain access or control of the system, and what steps should be taken to fix them.

Scope

Identify the scope of the penetration test.

I just used OpenVAS to scan for known issues. The scan covered open services on the server and focused only on the top three high-risk vulnerabilities that could pose a serious threat.

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 9 MySQLSummary: database on the server is using weak username and password
result: the scan was able to login as the user "password"attackers can login with root username and password.
remedy: change the password as soon as possible and with using a strong password.
vsftpd severity 7.5: the ftp server is running a version of vsftpd with a backdoor vulnerability.the scan confirmed that a vulnerable version of that software is installed.attackers could use this as a backdoor to execute commands and infiltrate the system.
remedy: update or replace the software.
severity 7.5: the ftp service allows only anonymous users to loginthe scanner successfully connected using an anonymous login userunauthorized users may access files or directories which would risk data exposure.remedy: disable anonymous login
severity 4.5: the application is missing the httpOnly cookie.scanner found that a cookie thats named cookie.sid was being set without it.without this , cookies are exposed to attacks like XSS and hijack the user.remedy: add the httpOnly attributeseverity 4.5: the web application is sending data that is sensitive over an unencrypted http connectionan attacker can intercept the data being sent back and forth and steal private informationremedy: the data needs to go through an encrypted https
severity 4.5: the remote host is running a ftp service that allows cleartext logins over unencrypted connectionsan attacker can uncover login names and passwords by looking around the ftp serviceremedy: enable ftp or enforce tls connections via auth tls.
severity 4.5: server is still supporting an older version of TLSattackers can exploit or know flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within secured connection.remedy: disable tlsv1.0 and 1.1

Conclusion

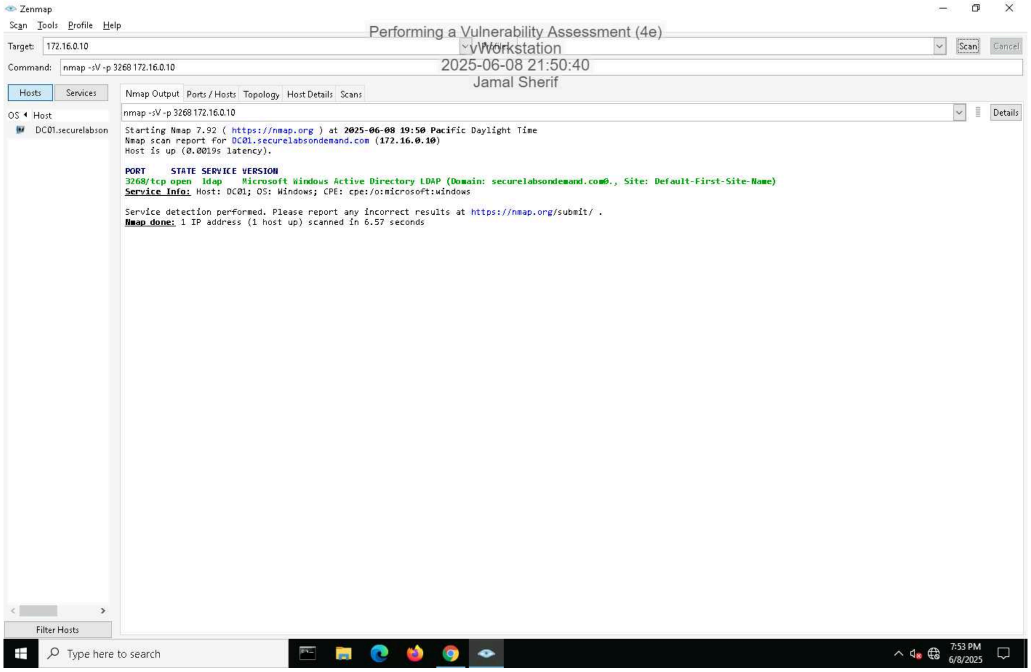
Identify your key findings.

the scan for drisst.com showed me a lot of very serious issues like for example the cleartext transmission. Overrall these issues show that we needed better ways for encryption or changing your root password.

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**.



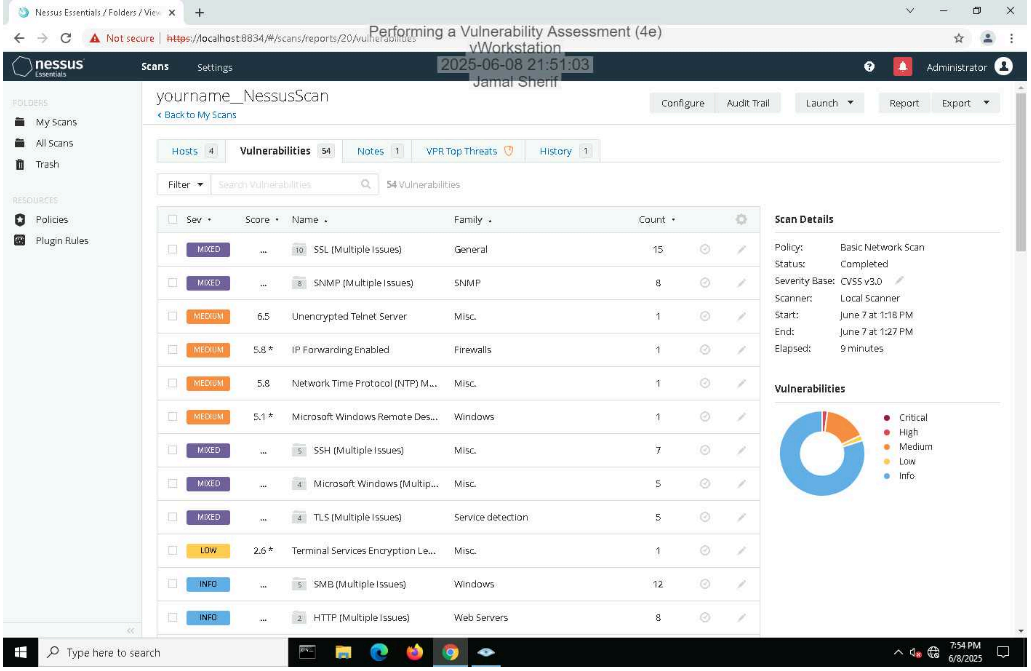
Target: 172.16.0.10

Command: nmap -sV -p 3268 172.16.0.10

```
nmap -sV -p 3268 172.16.0.10
Starting Nmap 7.92 ( https://nmap.org ) at 2025-06-08 19:50 Pacific Daylight Time
Nmap scan report for DC01.securelabsondemand.com (172.16.0.10)
Host is up (0.0019s latency).

PORT     STATE SERVICE VERSION
3268/tcp open  ldap    Microsoft Windows Active Directory LDAP (Domain: securelabsondemand.com0., Site: Default-First-Site-Name)
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.57 seconds
```

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
2025-06-08 21:51:03
Jamal Sherif

yourname__NessusScan
‹ Back to My Scans

54 Vulnerabilities

Sev	Score	Name	Family	Count
MIXED	...	10 SSL (Multiple Issues)	General	15
MIXED	...	8 SNMP (Multiple Issues)	SNMP	8
MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1
MEDIUM	5.8 *	IP Forwarding Enabled	Firewalls	1
MEDIUM	5.8	Network Time Protocol (NTP) M...	Misc.	1
MEDIUM	5.1 *	Microsoft Windows Remote Des...	Windows	1
MIXED	...	5 SSH (Multiple Issues)	Misc.	7
MIXED	...	4 Microsoft Windows (Multip...	Misc.	5
MIXED	...	4 TLS (Multiple Issues)	Service detection	5
LOW	2.6 *	Terminal Services Encryption Le...	Misc.	1
INFO	...	5 SMB (Multiple Issues)	Windows	12
INFO	...	2 HTTP (Multiple Issues)	Web Servers	8

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	June 7 at 1:18 PM
End:	June 7 at 1:27 PM
Elapsed:	9 minutes

Vulnerabilities

Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

172.30.0.2

Completed by

Insert your name here.

Jamal Sherif

On

Insert current date here.

6/8/25

Purpose

Identify the purpose of the penetration test.

to find any security vulnerabilities in the hosts.

Scope

Identify the scope of the penetration test.

find vulnerabilities using the scan in the vWorkstation

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.

server is still supporting old versions of TLSIt supports TLSv1.2, the server also supports TLSv1.0 and TLSv1.1any attacker could exploit known flaws like to break encryption or find sensitive data.

Conclusion

Identify your key findings.

This test was able to find vulnerabilities and expose it so we can find fix it because it gave us solutions to it.