Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Student:	Email:
Kanchan Chopde	hq0656@wayne.edu

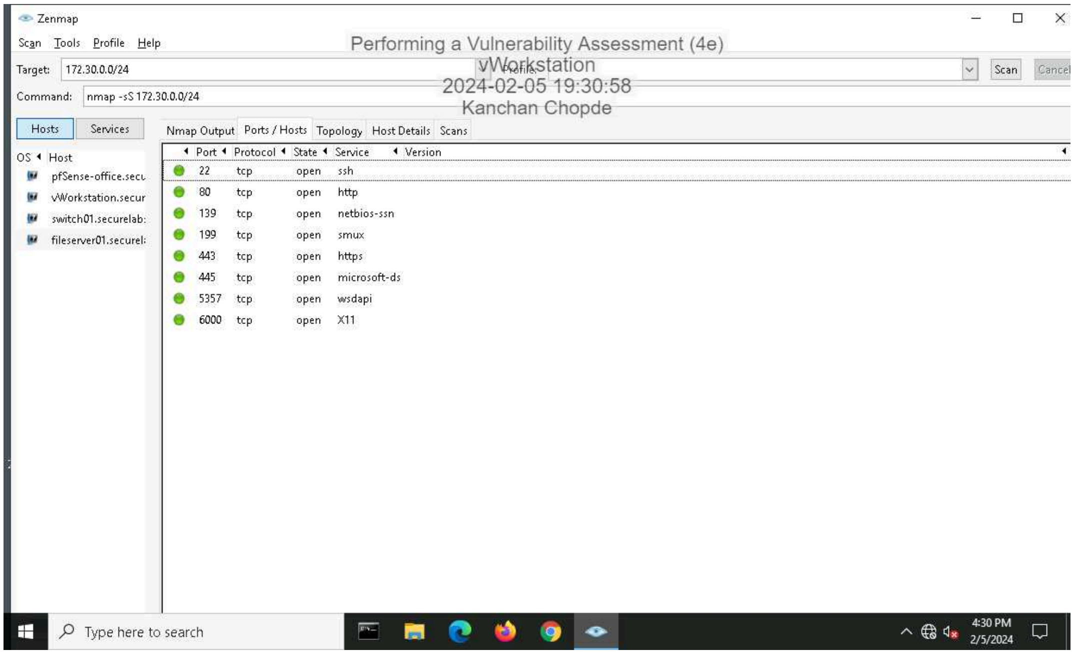
Time on Task:	Progress:
4 hours, 27 minutes	100%

Report Generated: Thursday, February 8, 2024 at 12:22 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
2024-02-05 19:30:58
Kanchan Chopde

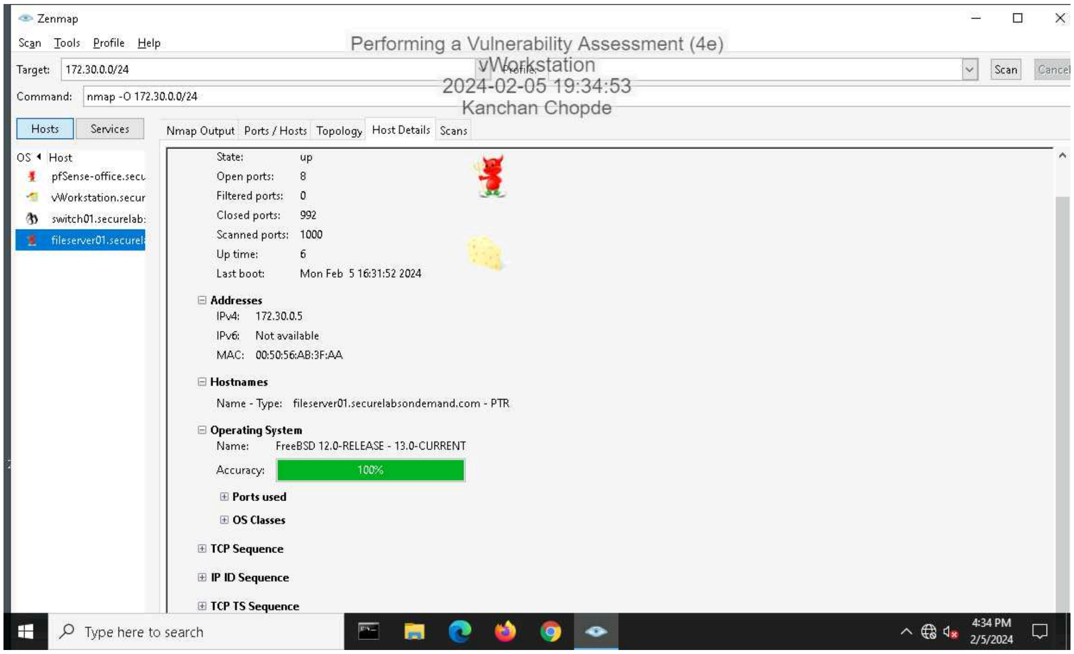
Target: 172.30.0.0/24

Command: nmap -sS 172.30.0.0/24

OS	Host
	pfSense-office.secu
	vWorkstation.secur
	switch01.securelab:
	fileserver01.securel:

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**.



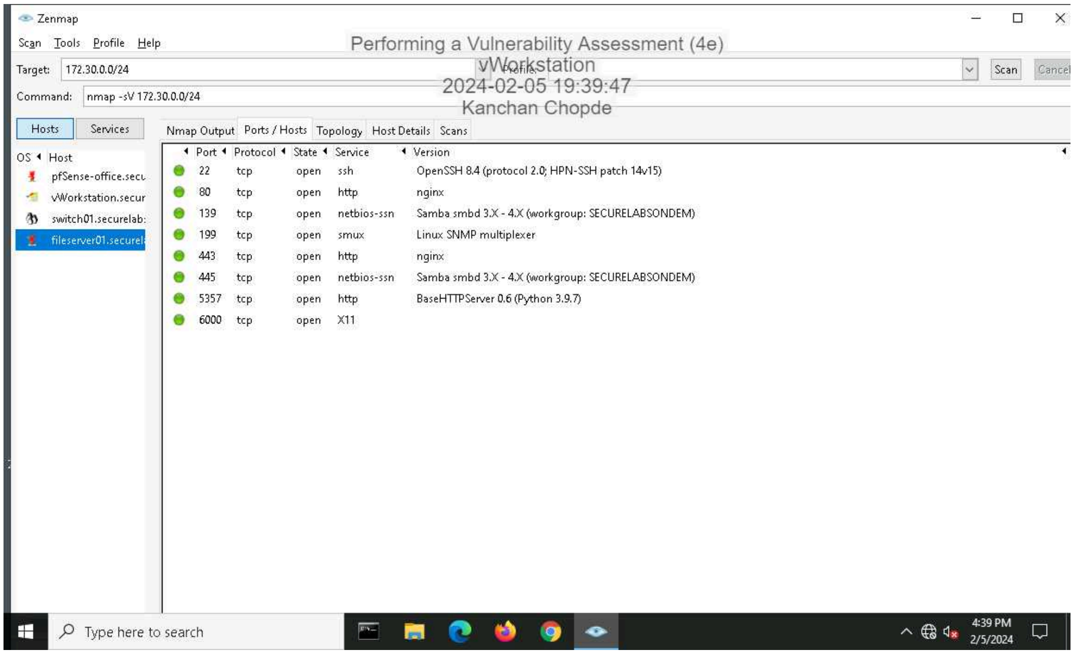
Performing a Vulnerability Assessment (4e)
vWorkstation
2024-02-05 19:34:53
Kanchan Chopde

Target: 172.30.0.0/24

Command: nmap -O 172.30.0.0/24

```
State:          up
Open ports:     8
Filtered ports: 0
Closed ports:   992
Scanned ports:  1000
Up time:        6
Last boot:      Mon Feb  5 16:31:52 2024

⊟ Addresses
    IPv4:  172.30.0.5
    IPv6:  Not available
    MAC:   00:50:56:AB:3F:AA

⊟ 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
```

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
2024-02-05 19:39:47
Kanchan Chopde

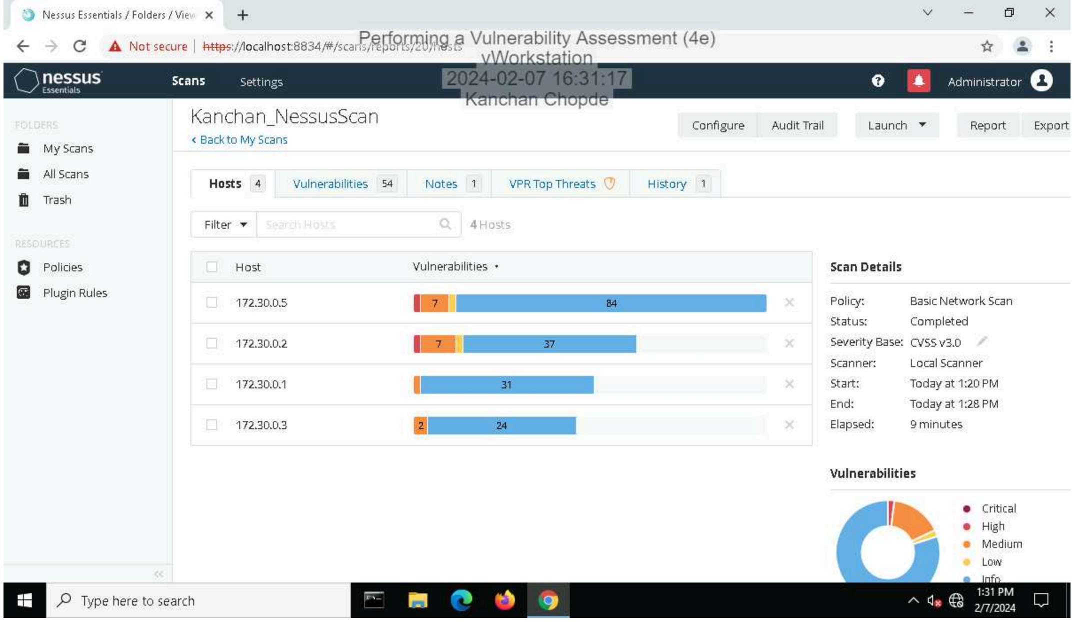
Target: 172.30.0.0/24

Command: nmap -sV 172.30.0.0/24

	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
2024-02-07 16:31:17
Kanchan Chopde

Kanchan_NessusScan
‹ Back to My Scans

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 1:20 PM
End:	Today at 1:28 PM
Elapsed:	9 minutes

Vulnerabilities

Part 3: Evaluate Your Findings

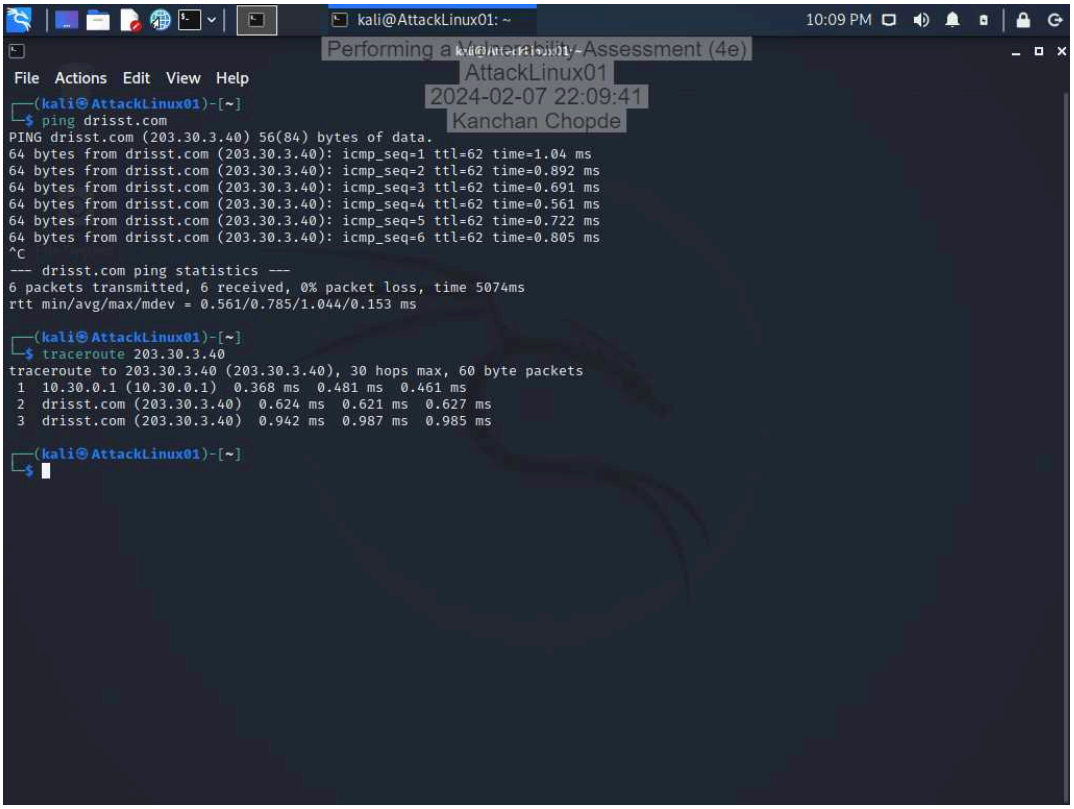
11. **Summarize** the vulnerability you selected, including the CVSS risk score, and **recommend** a mitigation strategy.

Selected vulnerability: Plugin 15901 : SSL Certificate Expiry
It is a medium severity vulnerability which tells that the date of expiry of SSL certificate used by any SSL enabled services on target machine must be expired.
CVSS risk score: 5
Recommended Mitigation Strategy: Can purchase new SSL certificate and replace it with existing one.

Section 2: Applied Learning

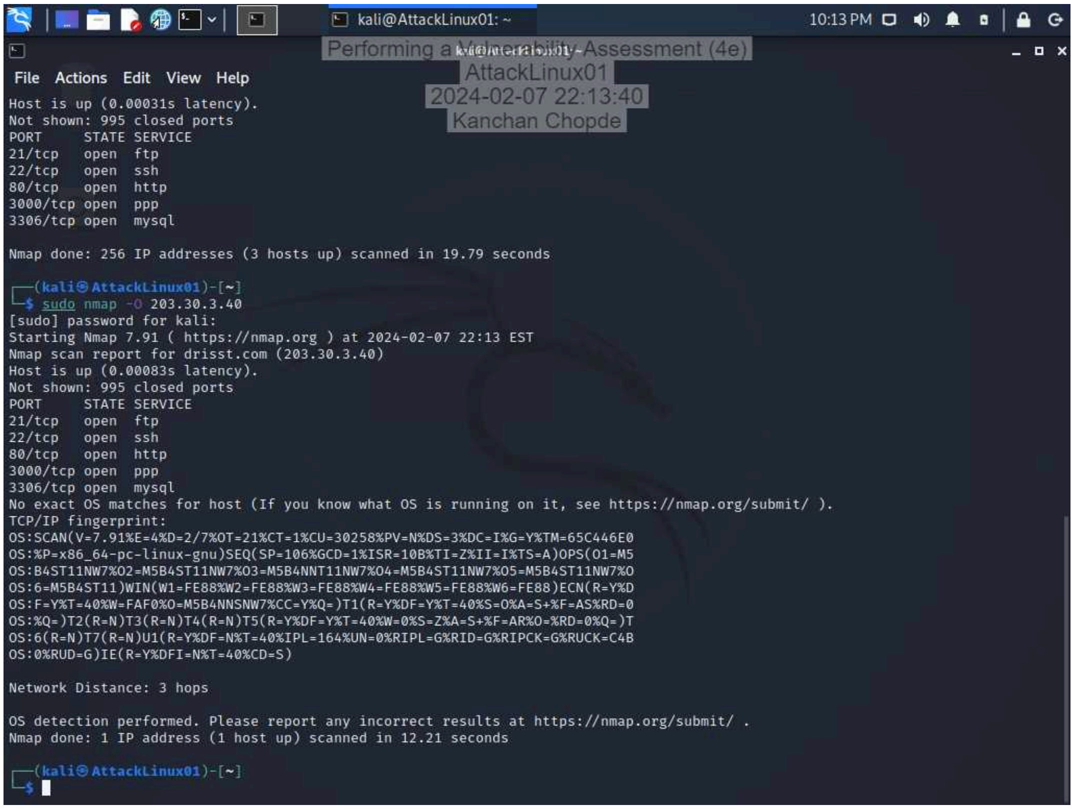
Part 1: Scan the Network with Nmap

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=1.04 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=0.892 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.691 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=0.561 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=0.722 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=6 ttl=62 time=0.805 ms
^C
--- drisst.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5074ms
rtt min/avg/max/mdev = 0.561/0.785/1.044/0.153 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)  0.368 ms  0.481 ms  0.461 ms
 2  drisst.com (203.30.3.40)  0.624 ms  0.621 ms  0.627 ms
 3  drisst.com (203.30.3.40)  0.942 ms  0.987 ms  0.985 ms

┌──(kali㉿AttackLinux01)-[~]
└─$ 
```

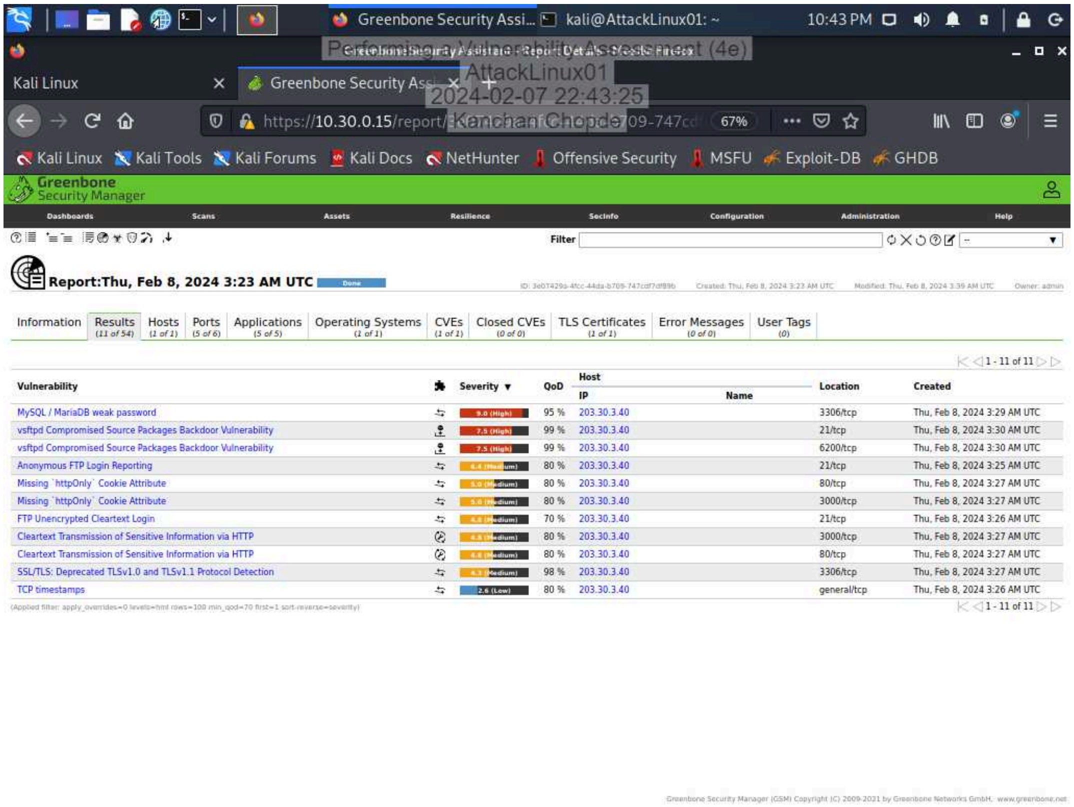
10. **Make a screen capture** showing the **results of the Nmap scan with OS detection activated**.



```
Host is up (0.00031s 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 19.79 seconds

┌──(kali㉿AttackLinux01)-[~]
└─$ sudo nmap -O 203.30.3.40
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-02-07 22:13 EST
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=2/7%OT=21%CT=1%CU=30258%PV=N%DS=3%DC=I%G=Y%TM=65C446E0
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%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=C4B
OS:0%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 12.21 seconds

┌──(kali㉿AttackLinux01)-[~]
└─$ ▮
```

Part 2: Conduct a Vulnerability Scan with OpenVAS

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



Report:Thu, Feb 8, 2024 3:23 AM UTC Done

ID: 3eb7429a-4fcc-44da-b709-747cdf7df89b Created: Thu, Feb 8, 2024 3:23 AM UTC Modified: Thu, Feb 8, 2024 3:39 AM UTC Owner: admin

Information | Results (11 of 54) | Hosts (1 of 1) | Ports (5 of 6) | Applications (5 of 5) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (0 of 0) | TLS Certificates (1 of 1) | Error Messages (0 of 0) | User Tags (0)

1 - 11 of 11

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
MySQL / MariaDB weak password	⇆	9.0 (High)	95 %	203.30.3.40		3306/tcp	Thu, Feb 8, 2024 3:29 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	⤓	7.5 (High)	99 %	203.30.3.40		21/tcp	Thu, Feb 8, 2024 3:30 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	⤓	7.5 (High)	99 %	203.30.3.40		6200/tcp	Thu, Feb 8, 2024 3:30 AM UTC
Anonymous FTP Login Reporting	⇆	6.4 (Medium)	80 %	203.30.3.40		21/tcp	Thu, Feb 8, 2024 3:25 AM UTC
Missing `httpOnly` Cookie Attribute	⇆	5.0 (Medium)	80 %	203.30.3.40		80/tcp	Thu, Feb 8, 2024 3:27 AM UTC
Missing `httpOnly` Cookie Attribute	⇆	5.0 (Medium)	80 %	203.30.3.40		3000/tcp	Thu, Feb 8, 2024 3:27 AM UTC
FTP Unencrypted Cleartext Login	⇆	4.8 (Medium)	70 %	203.30.3.40		21/tcp	Thu, Feb 8, 2024 3:26 AM UTC
Cleartext Transmission of Sensitive Information via HTTP	⟳	4.8 (Medium)	80 %	203.30.3.40		3000/tcp	Thu, Feb 8, 2024 3:27 AM UTC
Cleartext Transmission of Sensitive Information via HTTP	⟳	4.8 (Medium)	80 %	203.30.3.40		80/tcp	Thu, Feb 8, 2024 3:27 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	203.30.3.40		3306/tcp	Thu, Feb 8, 2024 3:27 AM UTC
TCP timestamps	⇆	2.6 (Low)	80 %	203.30.3.40		general/tcp	Thu, Feb 8, 2024 3:26 AM UTC

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

1 - 11 of 11

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.

Research on three high severity vulnerabilities identified by OpenVAS

Completed by

Insert your name here.

Kanchan Chopde

On

Insert current date here.

07-02-2024

Purpose

Identify the purpose of the penetration test.

The main purpose of penetration testing is to find and exploit the vulnerabilities in a computer system to prevent security breaches and protect an organization's security.

Scope

Identify the scope of the penetration test.

The scope of penetration testing is about all the factors or components whether excluded or included decided by the testing team which are required to test the system. It is usually the list of factors that help detect vulnerabilities and is very useful for organizations. It can be thought of as a way the company ensures a clear understanding of its penetration test and what is not going to be included in testing.

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.

Three high severity issues:

1) MySQL/MariaDB weak password at location 3306/tcp
It is rate as 9.0 which is high severity issue.

It suggests that login into remote MYSQL or MariaDB is possible with root using weak credentials such as "password".

Remediation: Immediately change of password, preferably something difficult should be kept, which is not easy to guess.

2)vsftpd compromised Source Packages Backdoor Vulnerability at location 21/tcp
It is rated as 7.5 with high severity.

vsftpd file contains backdoor and attacker can cause the application to open a backdoor on some port by logging into FTP server with username.

Remediation: Repaired packages can be downloaded and should be verified with its signature before using.

3)vsftpd compromised Source Packages Backdoor Vulnerability at location 6200/tcp

It is rated as 7.5 with high severity.

vsftpd file contains backdoor and attacker can cause the application to open a backdoor on some port by logging into FTP server with username.

Remediation: Repaired packages can be downloaded and should be verified with its signature before using.

Conclusion

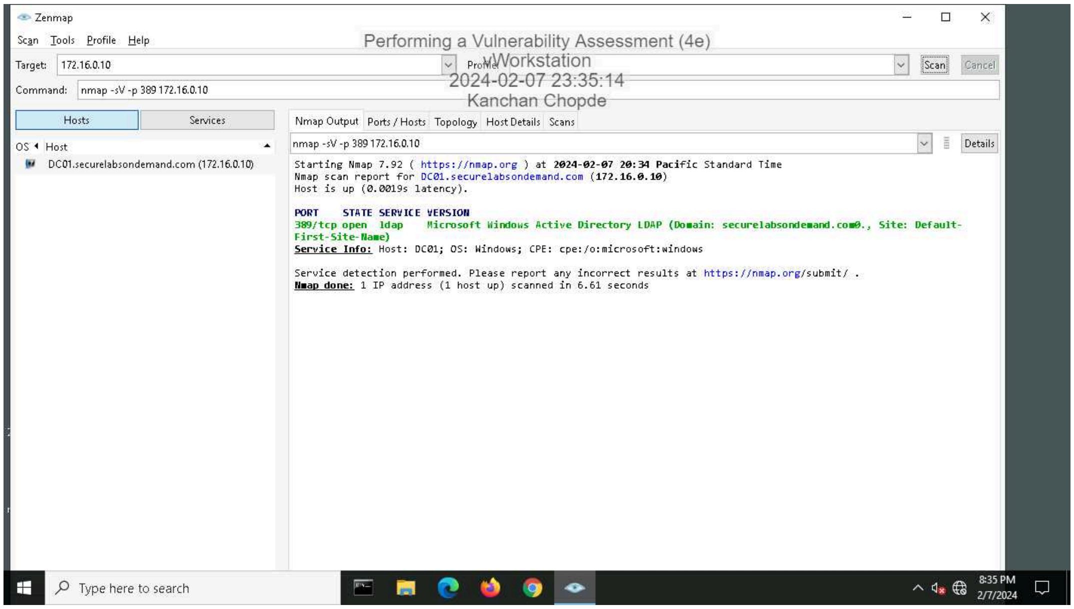
Identify your key findings.

Key findings:
1) Need to immediately take action on high-severity issues as they can cause security breaches.
2) The same vulnerabilities can be found in different locations. Need to carefully track the location and fix them with the provided remediations.
example: 2 and 3 vulnerability described in Summary are same issues but at different locations.

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

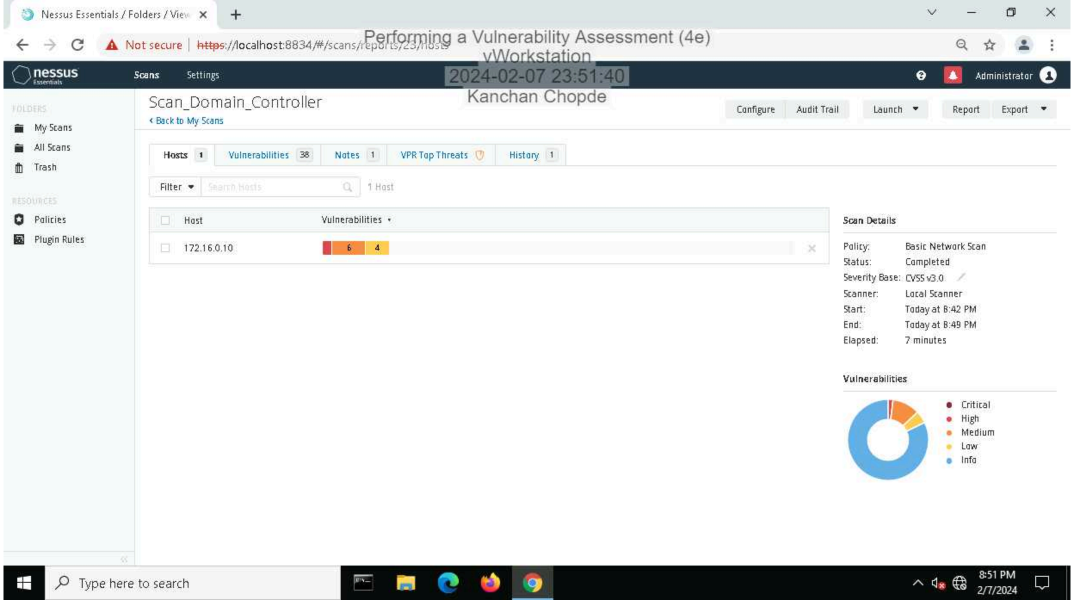
Command: nmap -sV -p 389 172.16.0.10

DC01.securelabsondemand.com (172.16.0.10)

```
nmap -sV -p 389 172.16.0.10
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-07 20:34 Pacific Standard Time
Nmap scan report for DC01.securelabsondemand.com (172.16.0.10)
Host is up (0.0019s latency).

PORT    STATE SERVICE VERSION
389/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 6.61 seconds
```

Part 2: Scan the Domain Controller with Nessus

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



Scan_Domain_Controller

Host	Vulnerabilities
172.16.0.10	6 4

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:42 PM
End:	Today at 8:49 PM
Elapsed:	7 minutes

Vulnerabilities

Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

Research on High vulnerability detected by Nessus scan

Completed by

Insert your name here.

Kanchan Chopde

On

Insert current date here.

07-02-2024

Purpose

Identify the purpose of the penetration test.

The main purpose of penetration testing is to find and exploit the vulnerabilities in a computer system to prevent security breaches and protect an organization's security.

Scope

Identify the scope of the penetration test.

The scope of penetration testing is about all the factors or components whether excluded or included decided by the testing team which are required to test the system. It is usually the list of factors that help detect vulnerabilities and is very useful for organizations. It can be thought of as a way the company ensures a clear understanding of its penetration test and what is not going to be included in testing.

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.

Summary of High Vulnerability found during penetration testing:

SSL Medium Strength Cipher Suites Supported

Severity: High Severity - CVSS v3.0 Base score 7.5

Issue description: The remote host has used SSL cipher which offer medium encryption.
According to Nessus it is stated that medium encryption strength is the on which used key lengths at least 64 bits and less than 112 bits or else that uses the 3DE5 encryption suite.

Remediation: Reconfiguring the affected application in order to avoid medium strength ciphers.

Conclusion

Identify your key findings.

The report displays all vulnerabilities belonging to high, low, medium severity types and shows a complete pie chart with the percentage of severity in each section.

It gives plugin details about each severity with possible remedies/solutions which can be used to avoid these issues.

It lists all details such as the family it belongs to, for example, Misc., General, Windows, Service Detection etc.

It also gives counts of such severities in output section along with locations mentioning port details and host details.