Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

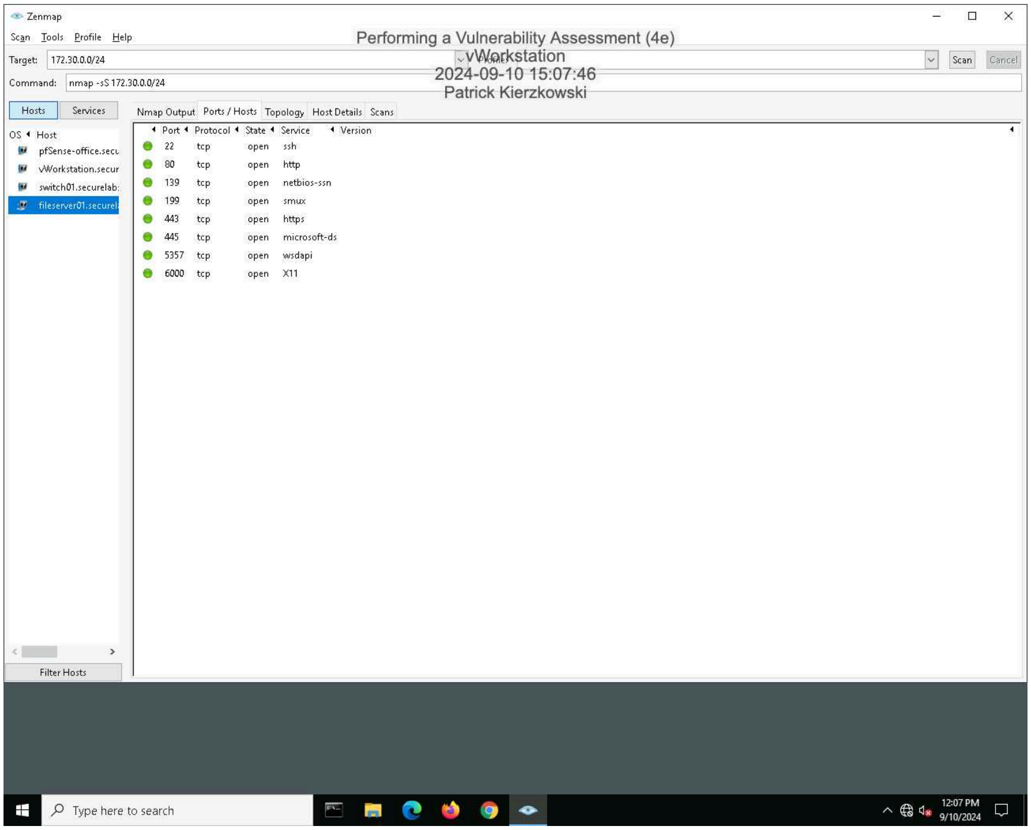
Student: Patrick Kierzkowski	Email: pxk405@francis.edu
Time on Task: 16 hours, 3 minutes	Progress: 100%

Report Generated: Monday, July 7, 2025 at 9:49 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**.



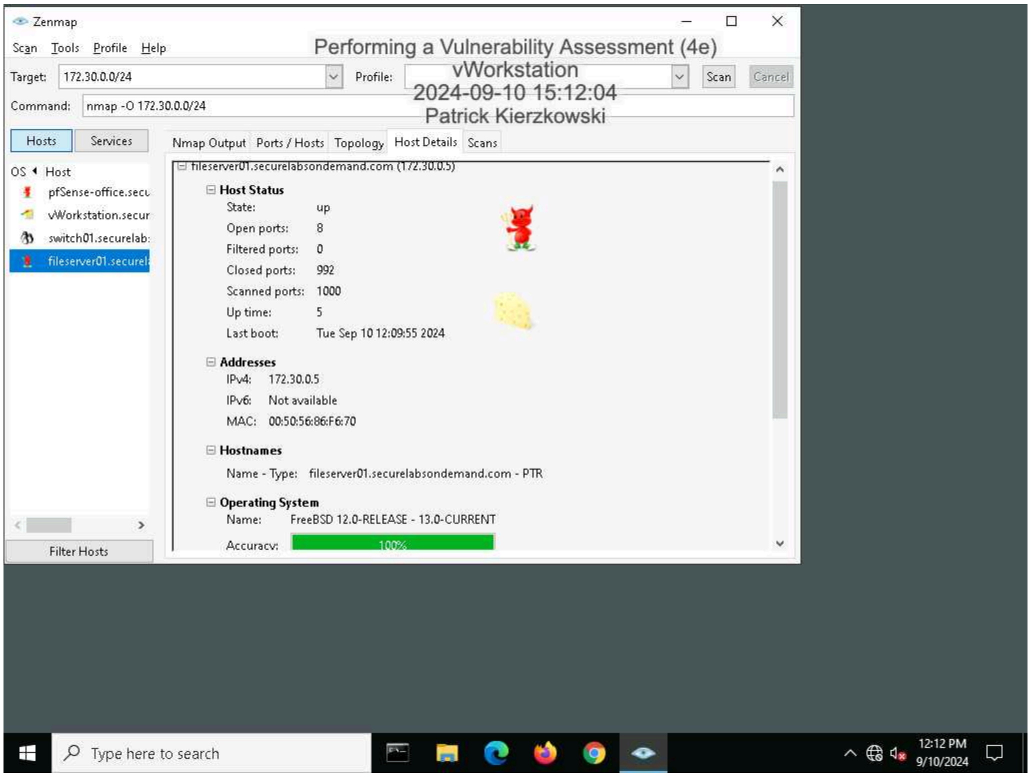
Performing a Vulnerability Assessment (4e)
vWorkstation
2024-09-10 15:07:46
Patrick Kierzkowski

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**.

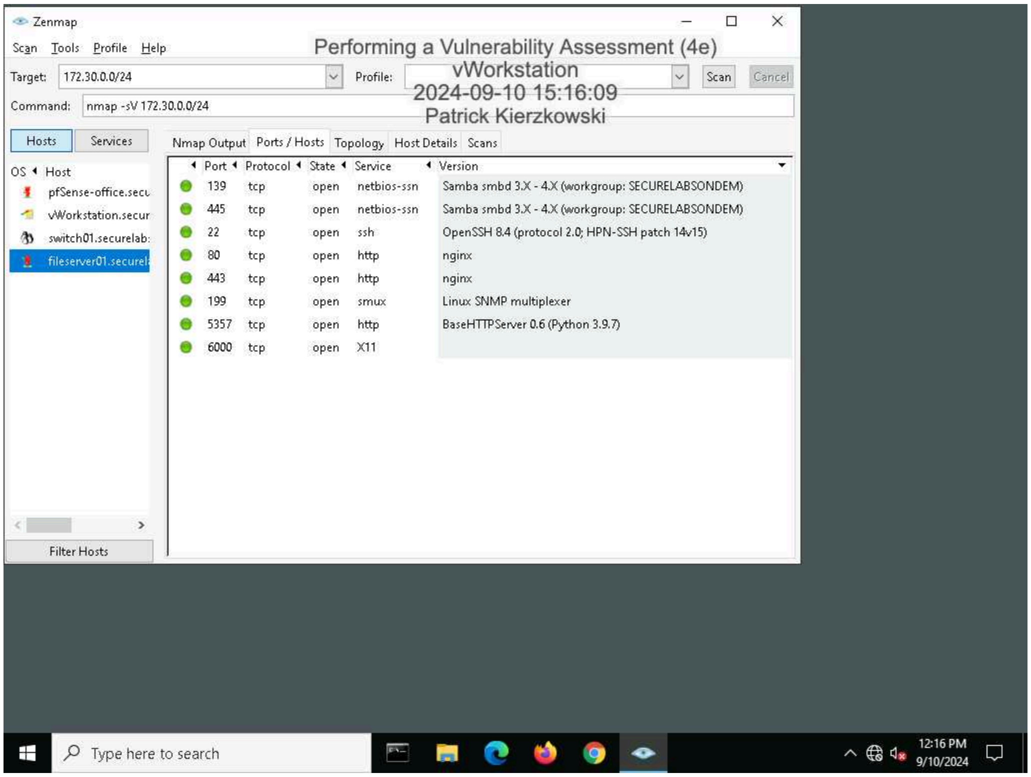


Performing a Vulnerability Assessment (4e)
vWorkstation
2024-09-10 15:12:04
Patrick Kierzkowski

Target: 172.30.0.0/24
Profile:
Command: nmap -O 172.30.0.0/24

```
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:      Tue Sep 10 12:09:55 2024
  Addresses
    IPv4:  172.30.0.5
    IPv6:  Not available
    MAC:   00:50:56:86:F6:70
  Hostnames
    Name - Type:  fileserver01.securelabsondemand.com - PTR
  Operating System
    Name:     FreeBSD 12.0-RELEASE - 13.0-CURRENT
    Accuracy: 100%
```

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



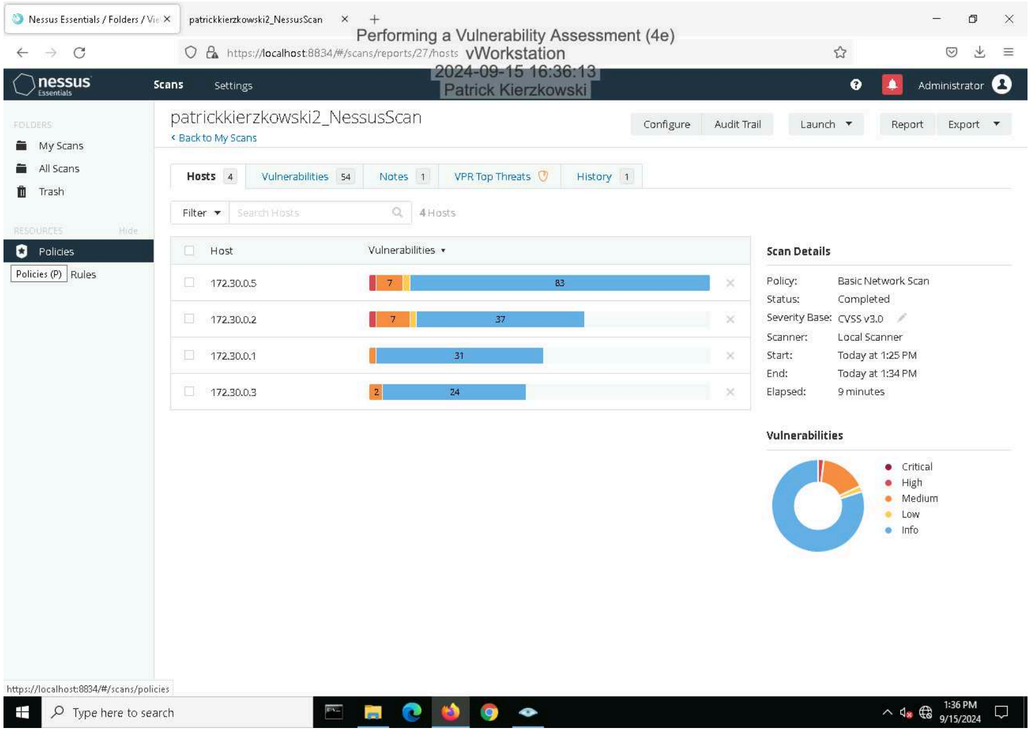
Performing a Vulnerability Assessment (4e)
vWorkstation
2024-09-10 15:16:09
Patrick Kierzkowski

Target: 172.30.0.0/24
Profile:
Command: nmap -sV 172.30.0.0/24

	Port	Protocol	State	Service	Version
●	139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: SECURELABSONDEM)
●	445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: SECURELABSONDEM)
●	22	tcp	open	ssh	OpenSSH 8.4 (protocol 2.0; HPN-SSH patch 14v15)
●	80	tcp	open	http	nginx
●	443	tcp	open	http	nginx
●	199	tcp	open	smux	Linux SNMP multiplexer
●	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
2024-09-15 16:36:13
Patrick Kierzkowski

https://localhost:8834/#/scans/reports/27/hosts

patrickkierzkowski2_NessusScan

Host	Vulnerabilities
172.30.0.5	7 83
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 1:25 PM
End: Today at 1:34 PM
Elapsed: 9 minutes

Part 3: Evaluate Your Findings

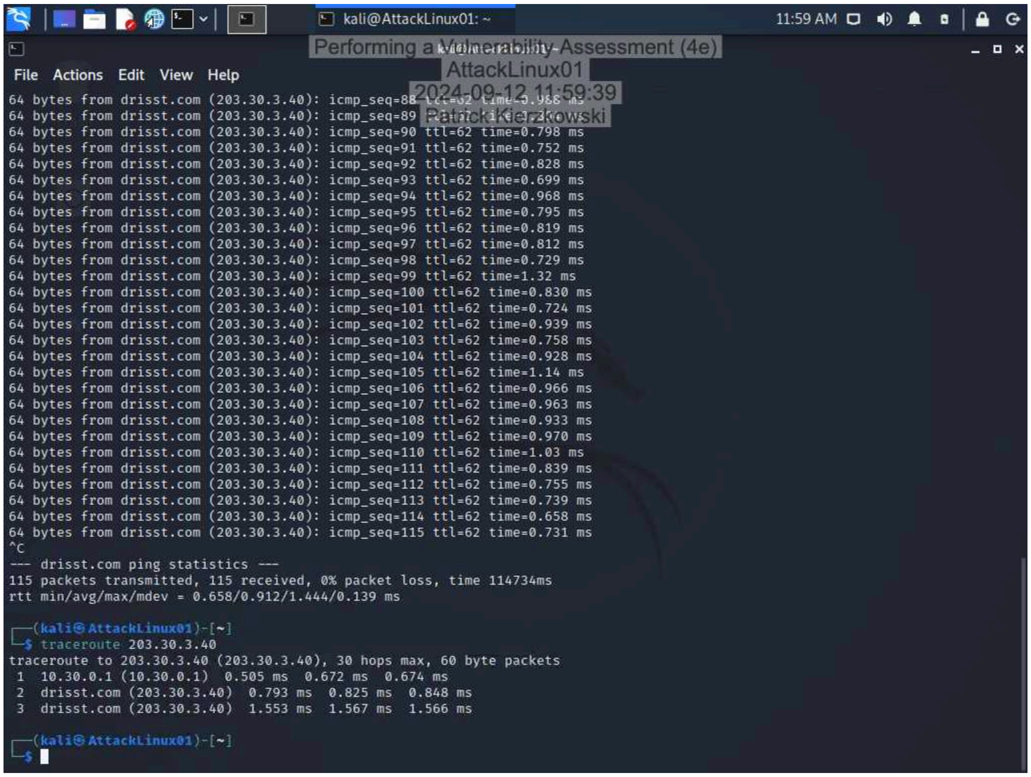
11. **Summarize** the vulnerability you selected, including the CVSS risk score, and **recommend** a mitigation strategy.

The vulnerability I selected was "SNMP Protocol Version Detection." There was no CVSS risk score, and a mitigation strategy would be to disable the SNMP service on the remote host if you don't use it, or filter incoming UDP packets going to this port.

Section 2: Applied Learning

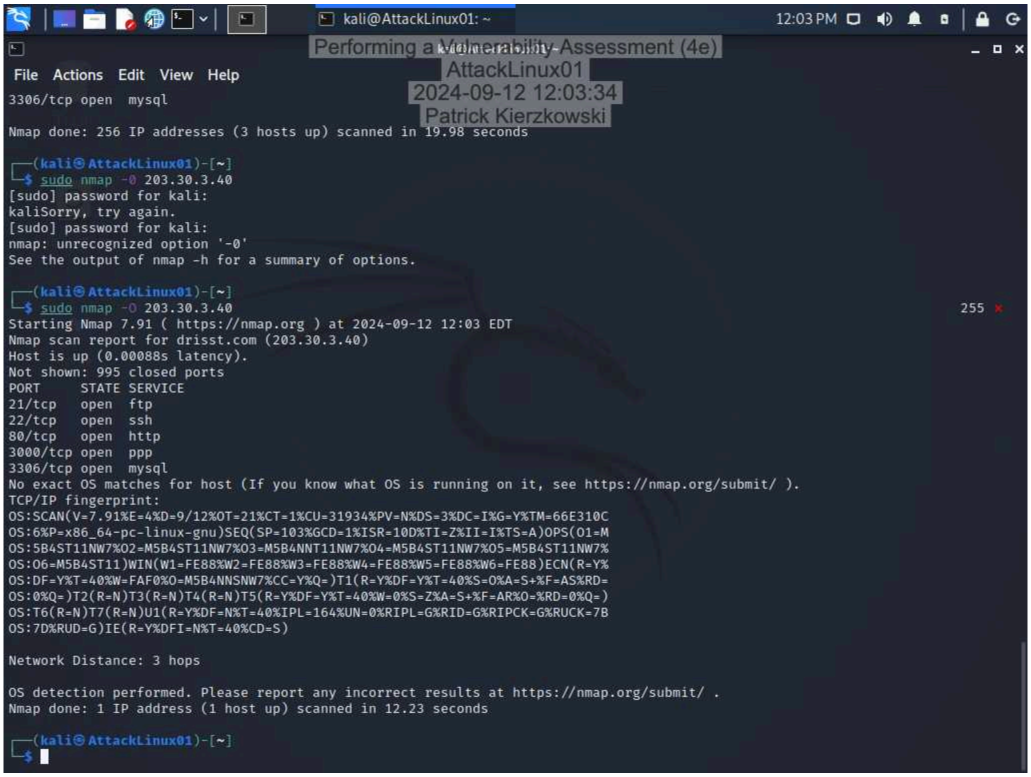
Part 1: Scan the Network with Nmap

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



```
64 bytes from drisst.com (203.30.3.40): icmp_seq=88 ttl=62 time=0.988 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=89 [illegible]
64 bytes from drisst.com (203.30.3.40): icmp_seq=90 ttl=62 time=0.798 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=91 ttl=62 time=0.752 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=92 ttl=62 time=0.828 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=93 ttl=62 time=0.699 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=94 ttl=62 time=0.968 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=95 ttl=62 time=0.795 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=96 ttl=62 time=0.819 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=97 ttl=62 time=0.812 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=98 ttl=62 time=0.729 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=99 ttl=62 time=1.32 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=100 ttl=62 time=0.830 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=101 ttl=62 time=0.724 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=102 ttl=62 time=0.939 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=103 ttl=62 time=0.758 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=104 ttl=62 time=0.928 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=105 ttl=62 time=1.14 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=106 ttl=62 time=0.966 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=107 ttl=62 time=0.963 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=108 ttl=62 time=0.933 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=109 ttl=62 time=0.970 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=110 ttl=62 time=1.03 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=111 ttl=62 time=0.839 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=112 ttl=62 time=0.755 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=113 ttl=62 time=0.739 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=114 ttl=62 time=0.658 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=115 ttl=62 time=0.731 ms
^C
--- drisst.com ping statistics ---
115 packets transmitted, 115 received, 0% packet loss, time 114734ms
rtt min/avg/max/mdev = 0.658/0.912/1.444/0.139 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)  0.505 ms  0.672 ms  0.674 ms
 2  drisst.com (203.30.3.40)  0.793 ms  0.825 ms  0.848 ms
 3  drisst.com (203.30.3.40)  1.553 ms  1.567 ms  1.566 ms

┌──(kali㉿AttackLinux01)-[~]
└─$ 
```

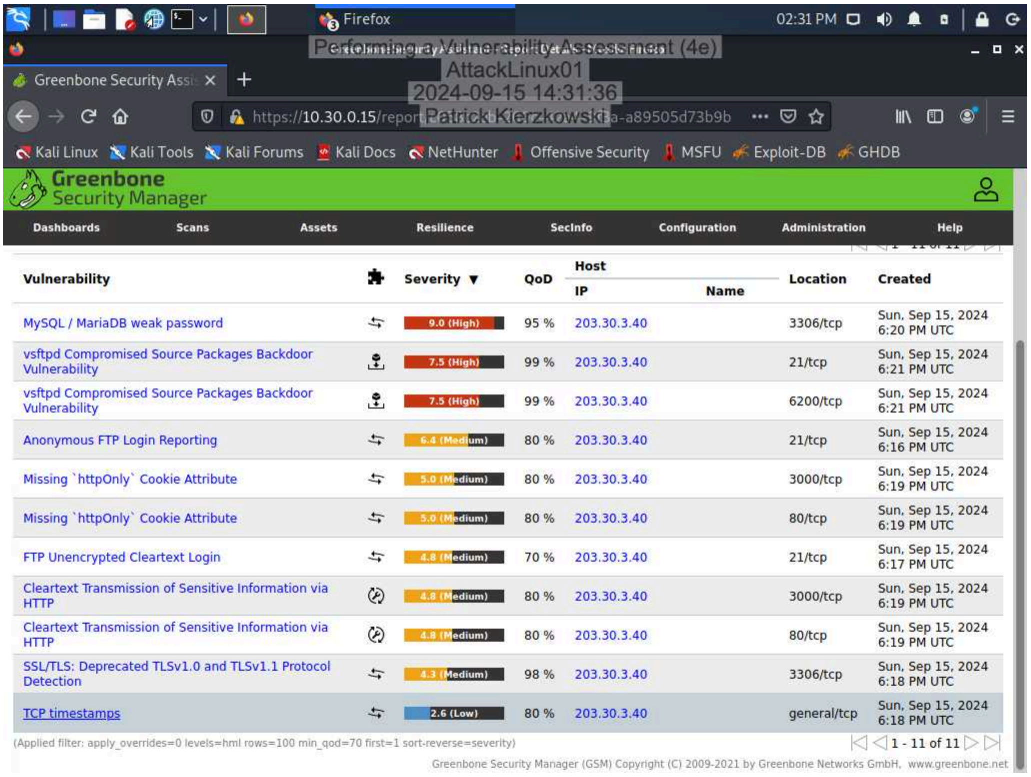
10. **Make a screen capture** showing the **results of the Nmap scan with OS detection activated**.



```
3306/tcp open  mysql

Nmap done: 256 IP addresses (3 hosts up) scanned in 19.98 seconds

┌──(kali㉿AttackLinux01)-[~]
└─$ sudo nmap -0 203.30.3.40
[sudo] password for kali:
kaliSorry, try again.
[sudo] password for kali:
nmap: unrecognized option '-0'
See the output of nmap -h for a summary of options.

┌──(kali㉿AttackLinux01)-[~]
└─$ sudo nmap -O 203.30.3.40                                                                    255 ✗
Starting Nmap 7.91 ( https://nmap.org ) at 2024-09-12 12:03 EDT
Nmap scan report for drisst.com (203.30.3.40)
Host is up (0.00088s 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=9/12%OT=21%CT=1%CU=31934%PV=N%DS=3%DC=I%G=Y%TM=66E310C
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10D%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=7B
OS:7D%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 12.23 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
2024-09-15 14:31:36
Patrick Kierzkowski

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
MySQL / MariaDB weak password	⇆	9.0 (High)	95 %	203.30.3.40		3306/tcp	Sun, Sep 15, 2024 6:20 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	⤓	7.5 (High)	99 %	203.30.3.40		21/tcp	Sun, Sep 15, 2024 6:21 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	⤓	7.5 (High)	99 %	203.30.3.40		6200/tcp	Sun, Sep 15, 2024 6:21 PM UTC
Anonymous FTP Login Reporting	⇆	6.4 (Medium)	80 %	203.30.3.40		21/tcp	Sun, Sep 15, 2024 6:16 PM UTC
Missing `httpOnly` Cookie Attribute	⇆	5.0 (Medium)	80 %	203.30.3.40		3000/tcp	Sun, Sep 15, 2024 6:19 PM UTC
Missing `httpOnly` Cookie Attribute	⇆	5.0 (Medium)	80 %	203.30.3.40		80/tcp	Sun, Sep 15, 2024 6:19 PM UTC
FTP Unencrypted Cleartext Login	⇆	4.8 (Medium)	70 %	203.30.3.40		21/tcp	Sun, Sep 15, 2024 6:17 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	⊘	4.8 (Medium)	80 %	203.30.3.40		3000/tcp	Sun, Sep 15, 2024 6:19 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	⊘	4.8 (Medium)	80 %	203.30.3.40		80/tcp	Sun, Sep 15, 2024 6:19 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	203.30.3.40		3306/tcp	Sun, Sep 15, 2024 6:18 PM UTC
TCP timestamps	⇆	2.6 (Low)	80 %	203.30.3.40		general/tcp	Sun, Sep 15, 2024 6:18 PM 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.

drisst.com

Completed by

Insert your name here.

Patrick Kierzkowski

On

Insert current date here.

9/15/2024

Purpose

Identify the purpose of the penetration test.

The penetration test is used to identify vulnerabilities in the drisst.com server, which in return can be used to make it more secure by telling us which areas are weak.

Scope

Identify the scope of the penetration test.

The scope would be the drisst.com server and whats available on it such as Nmap and CVEs.

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.

MySQL / MariaDB weak password was possible to login into the remote MySQL as; root using weak credentials. It has a severity of 9.0 (high), a good remediation would be to change the password as soon as possible. vsftpd Compromised Source Packages Backdoor Vulnerability has a severity of 7.5 (high). The issue is that vsftpd is prone to a backdoor vulnerability. Attackers can exploit this issue to execute arbitrary commands in the context of the application, meaning successful attacks will compromise the affected application (vsftpd 2.3.4 package is affected) . The solution would be to that the repaired package can be downloaded from the referenced link. Vsftpd Compromised Source Packages Backdoor Vulnerability had a severity of 7.5 (high). The vsftpd uses source packages that have been compromised, which keeps the backdoor vulnerability. A remediation of vsftpd would be to update to the most recent version is advised in order to close the backdoor vulnerability.

Conclusion

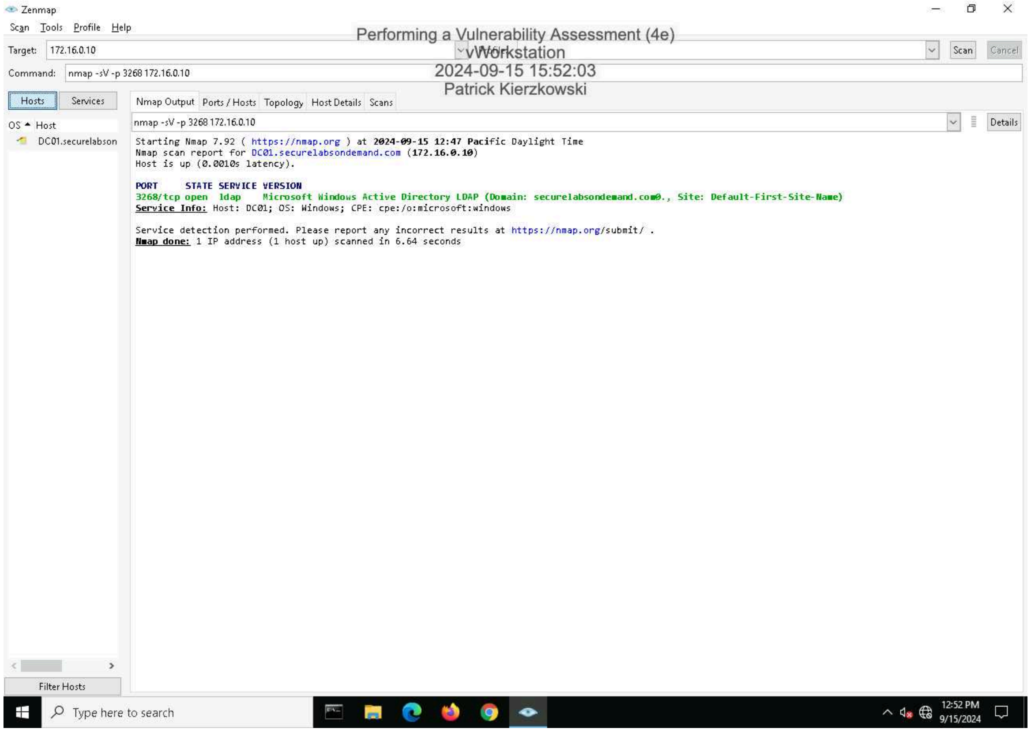
Identify your key findings.

The key findings of this penetration test were that there are 3 high vulnerabilities in the drisst.com server. These 3 include MySQL / MariaDB weak password, vsftpd Compromised Source Packages Backdoor Vulnerability, and vsftpd Compromised Source Packages Backdoor Vulnerability. These 3 vulnerabilities need to be dealt with so attackers can't gain access.

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
2024-09-15 15:52:03
Patrick Kierzkowski

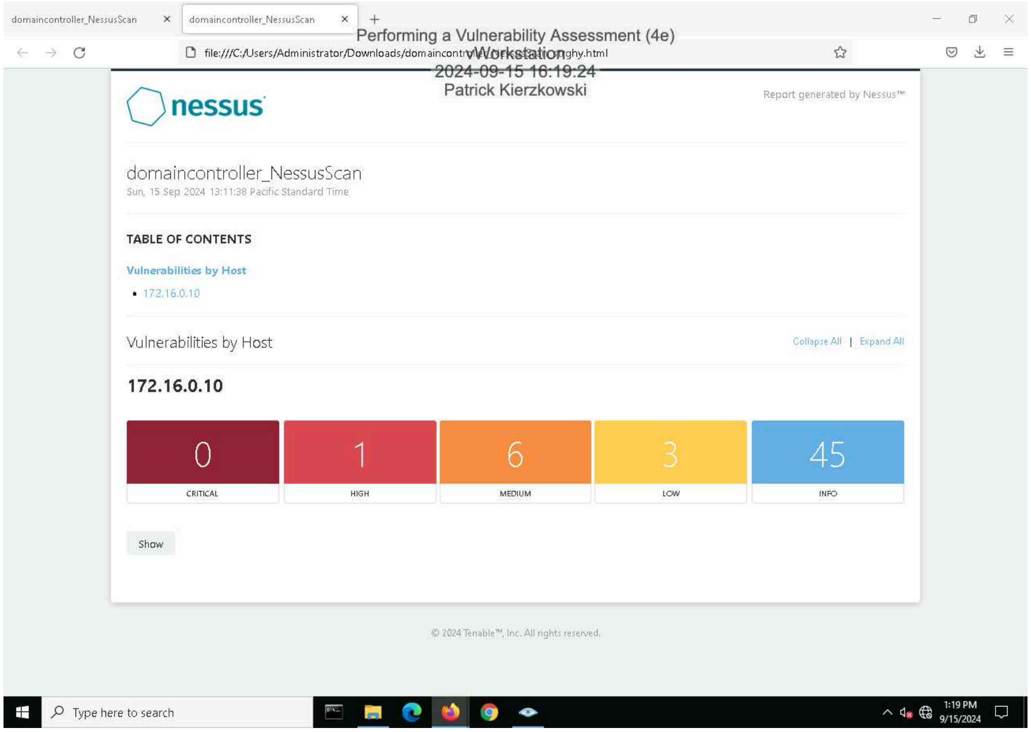
Target: 172.16.0.10

Command: nmap -sV -p 3268 172.16.0.10

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-09-15 12:47 Pacific Daylight Time
Nmap scan report for DC01.securelabsondemand.com (172.16.0.10)
Host is up (0.0010s 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 6.64 seconds
```

Part 2: Scan the Domain Controller with Nessus

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



domaincontroller_NessusScan
domaincontroller_NessusScan
file:///C:/Users/Administrator/Downloads/domaincontr…ghy.html

Performing a Vulnerability Assessment (4e)
vWorkstation
2024-09-15 16:19:24
Patrick Kierzkowski

nessus
Report generated by Nessus™

domaincontroller_NessusScan
Sun, 15 Sep 2024 13:11:38 Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 172.16.0.10

Vulnerabilities by Host

172.16.0.10

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	1	6	3	45

Collapse All | Expand All
Show
© 2024 Tenable™, Inc. All rights reserved.
Type here to search
1:19 PM
9/15/2024

Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

Domain Controller located in Secure Labs on Demand

Completed by

Insert your name here.

Patrick Kierzkowski

On

Insert current date here.

9/15/24

Purpose

Identify the purpose of the penetration test.

The penetration test is used to identify vulnerabilities in the Domain Controller, which in return can be used to make it more secure by telling us which areas are weak.

Scope

Identify the scope of the penetration test.

The scope would be the Domain Controller and whats available through it such as Nmap, CVEs, and the Nessus report

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.

For the vulnerability : SSL Medium Strength Cipher Suites Supported (SWEET32), the severity was 7.5 (high). The issue is that the SSL ciphers provided offer medium strength encryption, which is considered unsuitable by today's security standards. As a remediation, if possible you should reconfigure the affected application to prevent the use of medium strength ciphers.

Conclusion

Identify your key findings.

The key finding I got is that in the Domain Controller located in Secure Labs on Demand has one high vulnerability, which is the SSL Medium Strength Cipher Suites Supported (SWEET32). This vulnerability needs to be dealt with in case of an attack, where an attacker can exploit the cipher and gain access to data