

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Student:

John Monteiro

Email:

jmonteiro48@bristolcc.edu

Time on Task:

8 hours, 36 minutes

Progress:

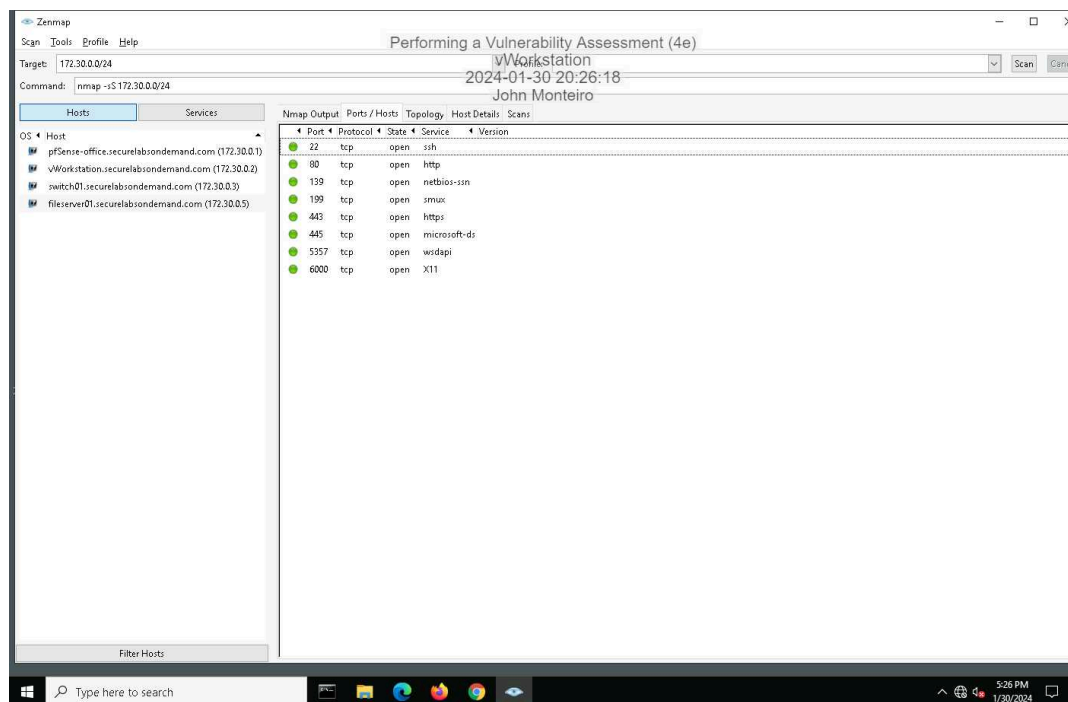
100%

Report Generated: Wednesday, January 31, 2024 at 1:32 PM

Section 1: Hands-On Demonstration

Part 1: Scan the Network with Zenmap

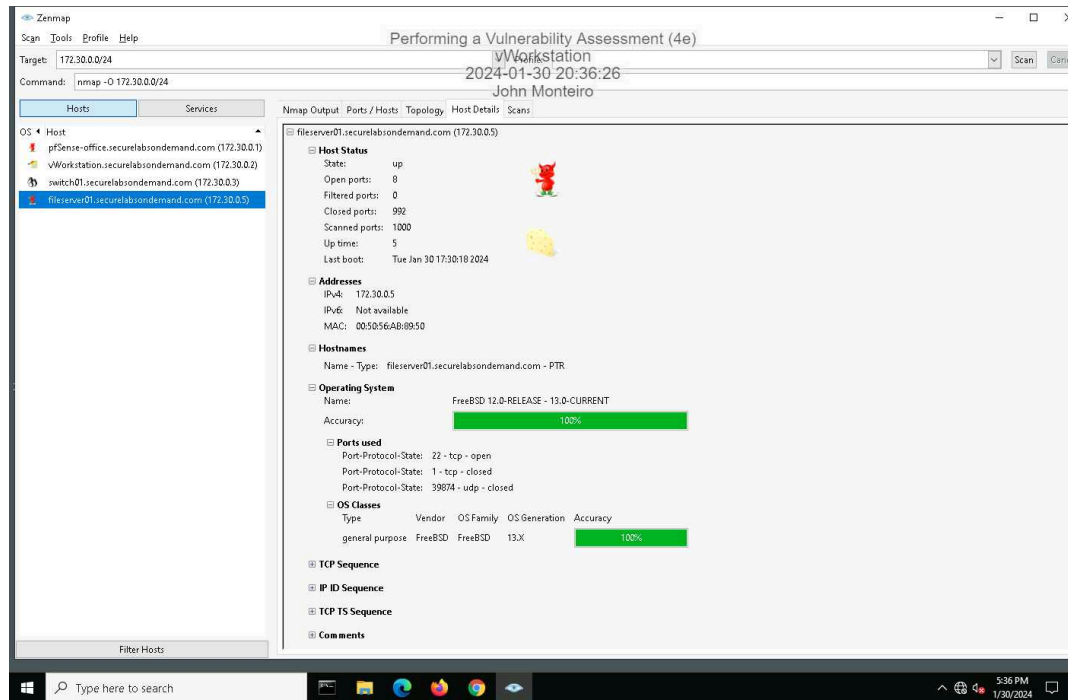
9. **Make a screen capture** showing the contents of the **Ports/Hosts** tab from the **SYN** scan for **fileserver01.securelabsondemand.com**.



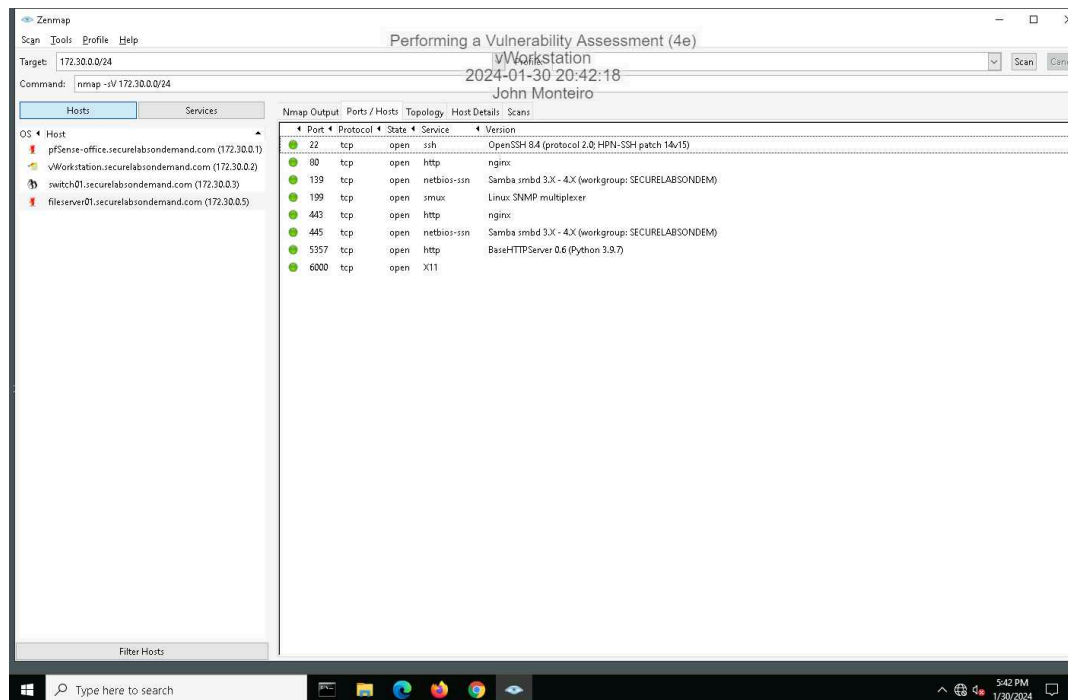
Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

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

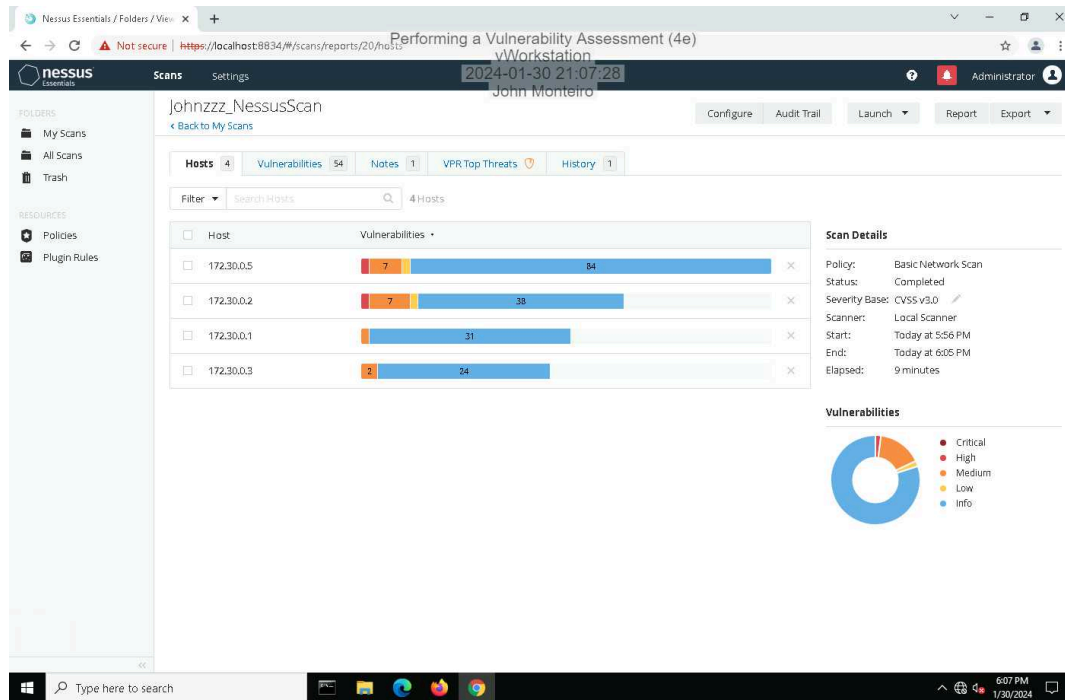


19. Make a screen capture showing the details in the **Ports/Hosts** tab from the **Service** scan for **fileserver01.securelabsondemand.com**.



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.

Plugin ID 51192 SSL Certificate Cannot Be Trusted

Synopsis: The SSL certificate for this service cannot be Trusted

Summary: The servers certificate chain may have three potential issues. Firstly, the top chain might not descend from a recognized public certificate authority, possible due to an unrecognized self-signed certificate or missing intermediate certificates. Secondly, the chain may include a certificate that is not valid at the time of the scan, either because the scan occurs before the certificate's 'notBefore' date or after its 'noAfter' date. Lastly, the chain may contain a signature that doesn't match the certificate's information or cannot be verified, possibly due to the issuer using an unsupported or unrecognized signing algorithm. These issues can compromise the authenticity and identity verification of a public host in production, increasing the risk of man-in-the-middle attacks.

CVSS v2 Base Score: 6.5

CVSS v3 Base Score: 6.5

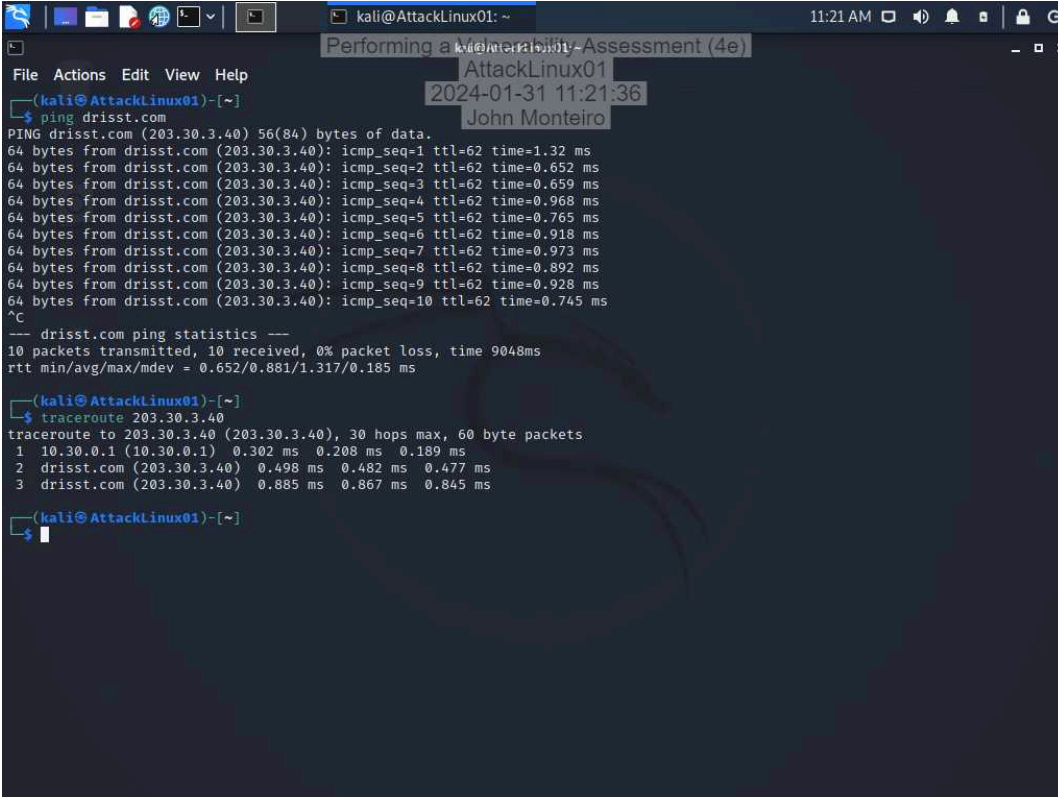
Risk Factor: Medium

Recommended Solution: Purchase or generate a proper SSL certificate for this service

Section 2: Applied Learning

Part 1: Scan the Network with Nmap

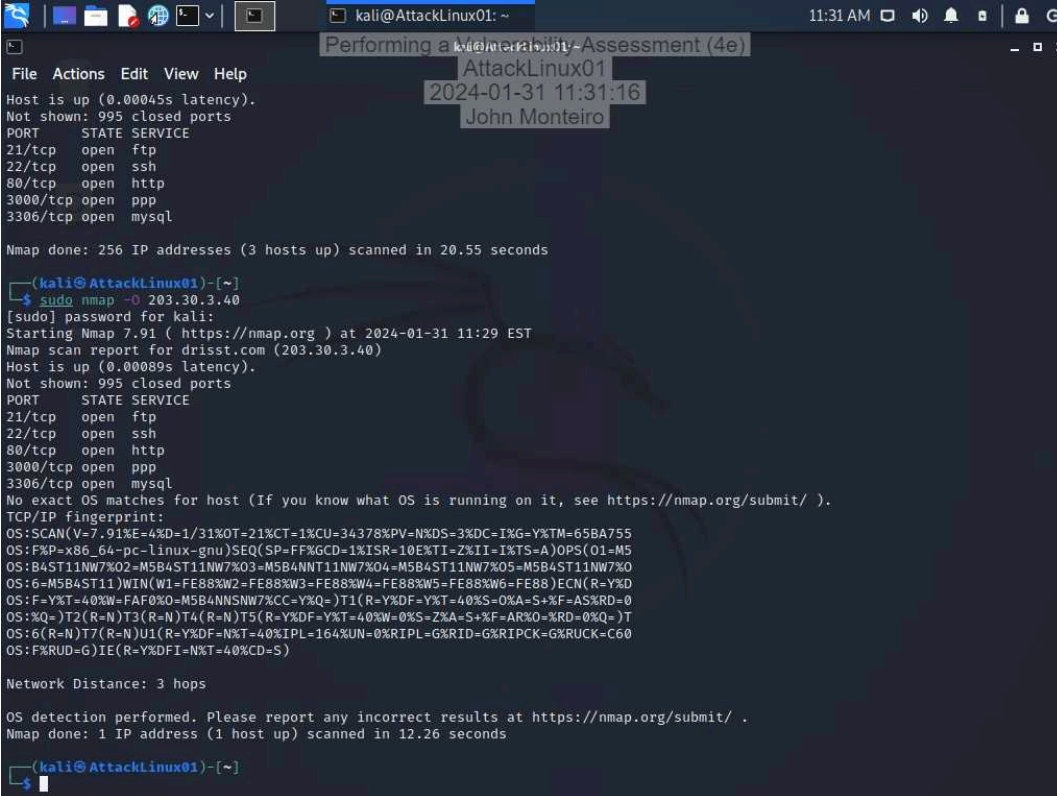
6. Make a screen capture showing the results of the traceroute command.



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

```
kali@AttackLinux01: ~  
File Actions Edit View Help  
--  
(kali@AttackLinux01)-[~]  
$ ping drisst.com  
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=1.32 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=0.652 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.659 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=0.968 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=0.765 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=6 ttl=62 time=0.918 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=7 ttl=62 time=0.973 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=8 ttl=62 time=0.892 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=9 ttl=62 time=0.928 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=10 ttl=62 time=0.745 ms  
^C  
-- drisst.com ping statistics --  
10 packets transmitted, 10 received, 0% packet loss, time 9048ms  
rtt min/avg/max/mdev = 0.652/0.881/1.317/0.185 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) 0.302 ms 0.208 ms 0.189 ms  
2 drisst.com (203.30.3.40) 0.498 ms 0.482 ms 0.477 ms  
3 drisst.com (203.30.3.40) 0.885 ms 0.867 ms 0.845 ms  
  
(kali@AttackLinux01)-[~]  
$
```

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



```
(kali@AttackLinux01)~$ sudo nmap -O 203.30.3.40
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-01-31 11:29 EST
Nmap scan report for drisst.com (203.30.3.40)
Host is up (0.00089s 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 20.55 seconds

(kali@AttackLinux01)~$ sudo nmap -O 203.30.3.40
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-01-31 11:29 EST
Nmap scan report for drisst.com (203.30.3.40)
Host is up (0.00089s 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=1/31%OT=21%CT=1%CU=34378%PV=N%DS=3%DC=I%G=Y%TM=65BA755
OS:F%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10E%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%
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=C60
OS:F%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

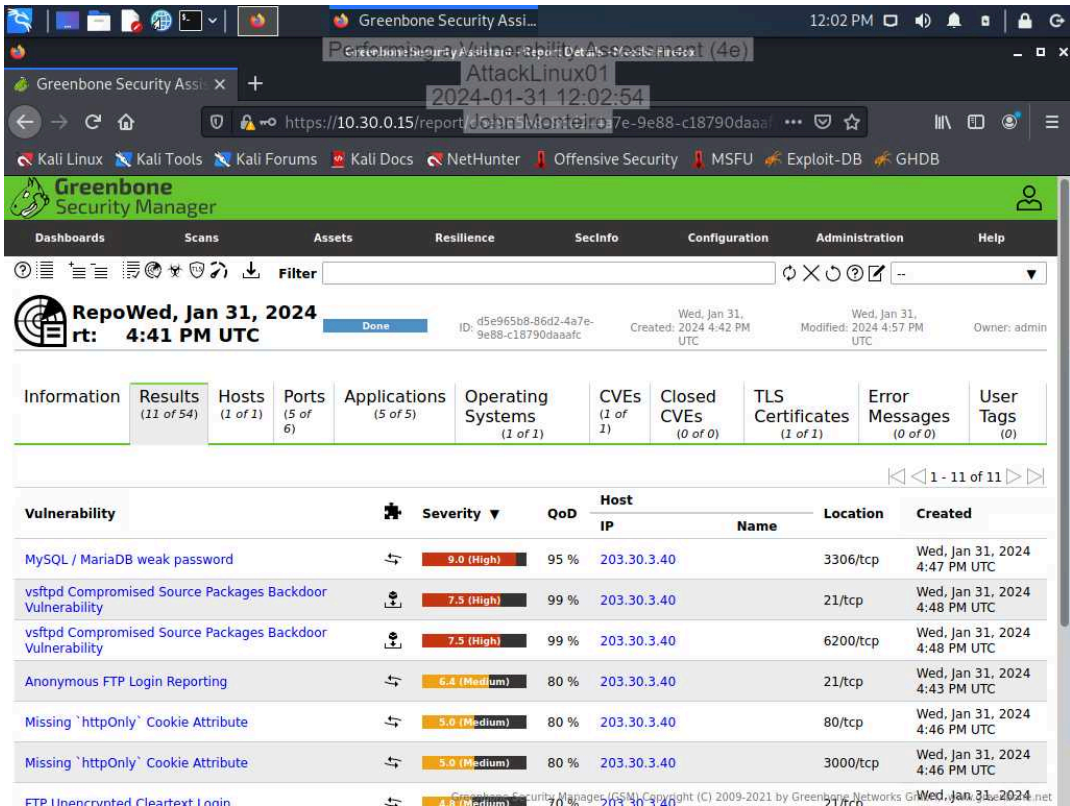
Network Distance: 3 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.26 seconds

(kali@AttackLinux01)~$
```

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.

drisst.com 203.30.3.40

Completed by

Insert your name here.

John Monteiro

On

Insert current date here.

January 31, 2024

Purpose

Identify the purpose of the penetration test.

conducting a vulnerability scan to check for vulnerabilities on drisst.com using obtained web server host ip address of 203.30.3.40

Scope

Identify the scope of the penetration test.

simple vulnerability scan of the drisst.com web server to identify the three highest severity vulnerabilities identified by the OpenVAS scan results

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.

Summary of the three highest severity vulnerabilities found by scan:

MySQL/MariaDB weak Password - Severity (HIGH 9.0), Issue (Possible to login into the remote MySQL as root using weak credentials. I was possible to login using password "password", Solution (Change the password as soon as possible)

vsftpd Compromised Source Packages Backdoor Vulnerability - Severity (HIGH 7.5), Issue (vsftpd is prone to a backdoor vulnerability, it was detected according to the Detection Method), Impact (Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.), Solution (The repaired package can be downloaded from the link "vendorfix". Validate the package with its signature)

vsftpd Compromised Source Packages Backdoor Vulnerability - Severity (HIGH 7.5), Issue (vsftpd prone to a backdoor vulnerability, was detected according to the Detection Method.), Impact (Attackers can use this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.) Solution (The repair package can be downloaded from "vendorfix" validate package with its signature).

Conclusion

Identify your key findings.

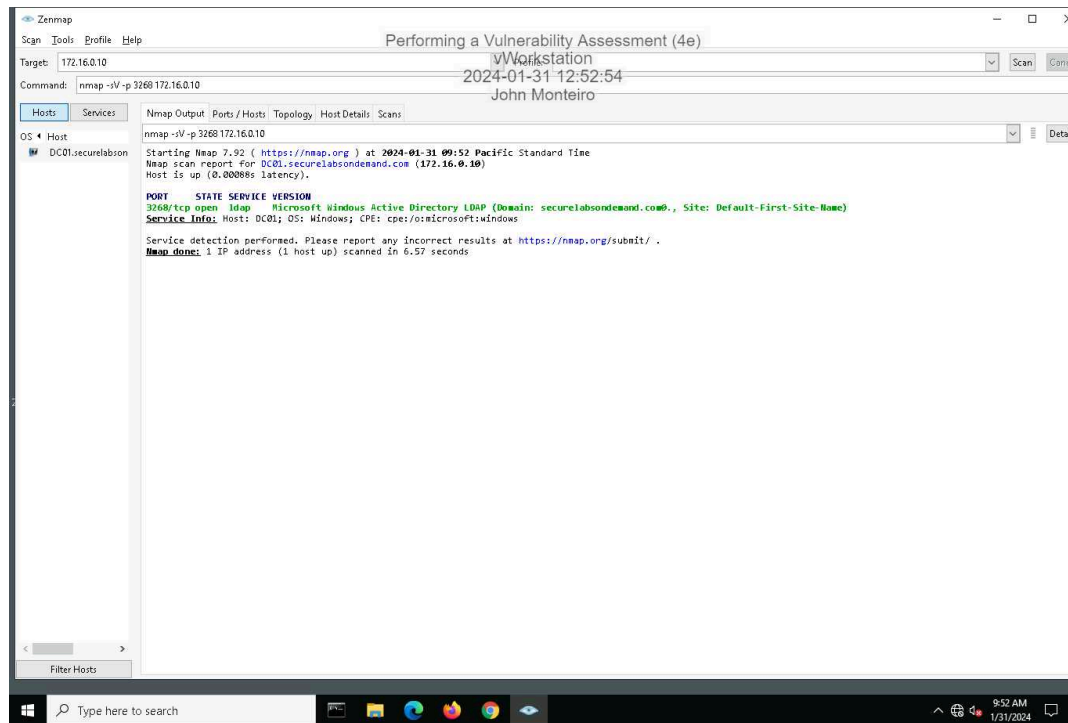
The vulnerability assessment has identified three high severity vulnerabilities:

The overall severity of the findings is high, indicating a significant risk to the confidentiality, integrity, and availability of the system and its data.

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.

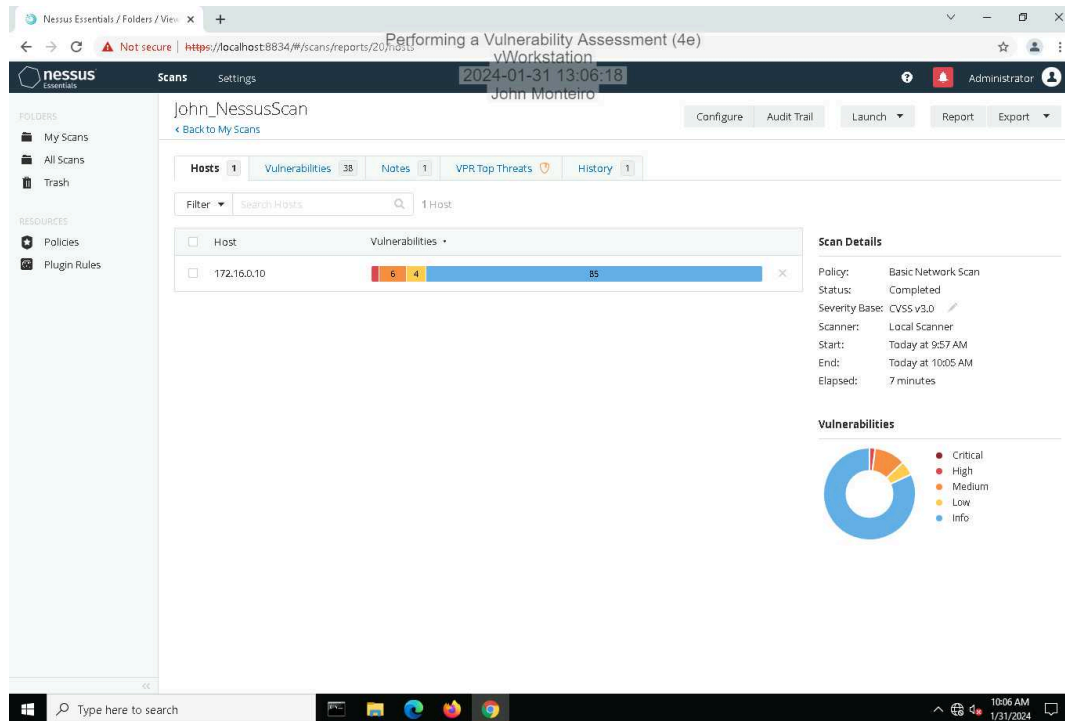


Part 2: Scan the Domain Controller with Nessus

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

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.

Secure Labs on Demand Domain Controller host ip address 172.16.0.10

Completed by

Insert your name here.

John Monteiro

On

Insert current date here.

January 31, 2024

Purpose

Identify the purpose of the penetration test.

conducting a vulnerability scan to check for vulnerabilities on Domain Controller ip 172.16.0.10

Scope

Identify the scope of the penetration test.

penetration vulnerability scan of the Domain controller to identify the highest severity vulnerabilities identified by the Nessus Scan results.

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.

Remote Desktop Protocol Server Man-in-the-Middle Weakness

Severity is *medium*

CVSS v2 Base Score: 5.1

CVSS v3 Base Score: 6.5

It may be possible to gain access to the remote host via vulnerability to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. This type of attack would allow the attacker to obtain sensitive information being transmitted, including authentication credentials.

Remediation Recommendation:

Force the use of SSL as a transport layer for this service if supported and/or

On Microsoft Windows OS select '**Allow connections only from computers running Remote Desktop with Network Level Authentication**' setting if it is available.

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

[illegible]