

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Student:

Udo Udo Williams

Email:

raggg12@gmail.com

Time on Task:

12 hours, 42 minutes

Progress:

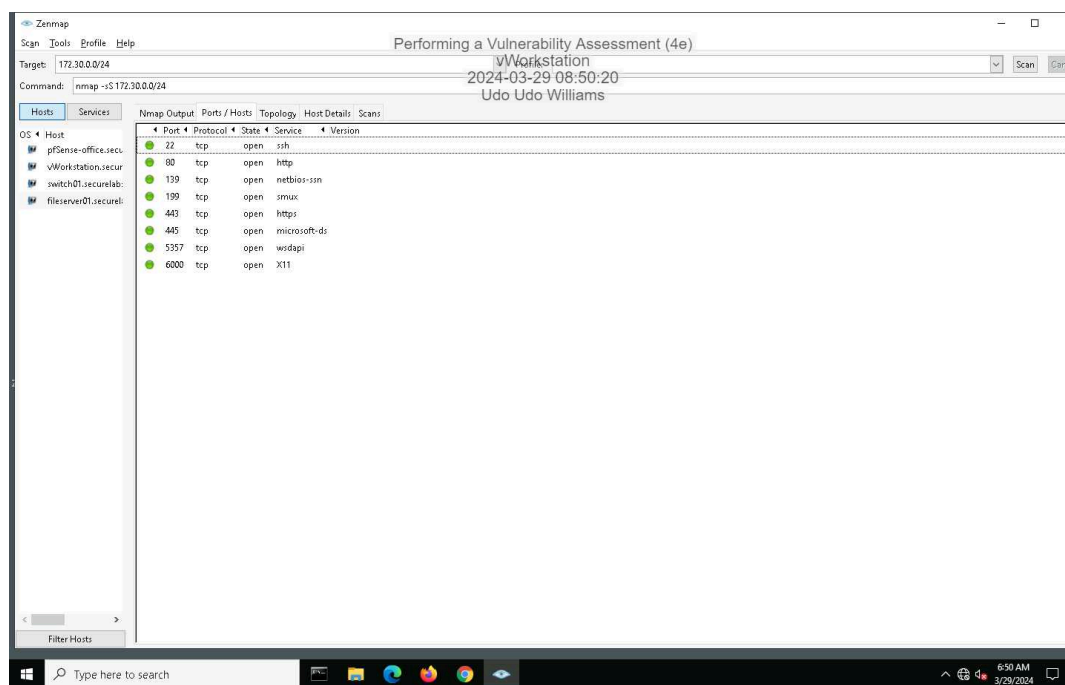
100%

Report Generated: Friday, March 29, 2024 at 1:48 PM

Section 1: Hands-On Demonstration

Part 1: Scan the Network with Zenmap

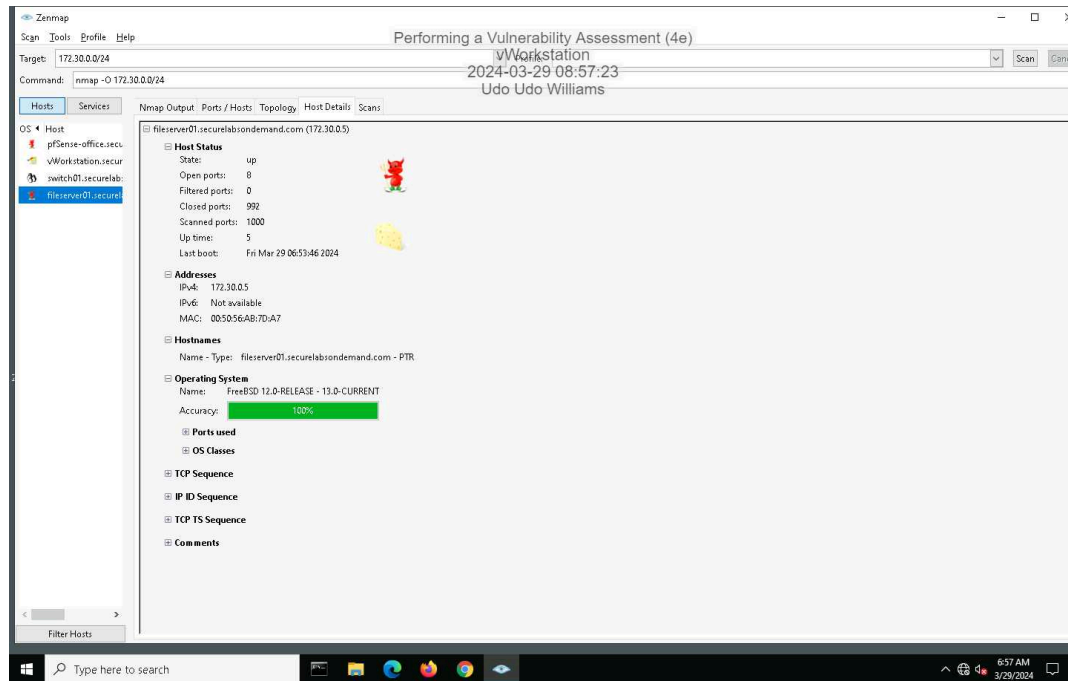
9. **Make a screen capture** showing the contents of the **Ports/Hosts** tab from the **SYN** scan for **fileserver01.securelabsondemand.com**.



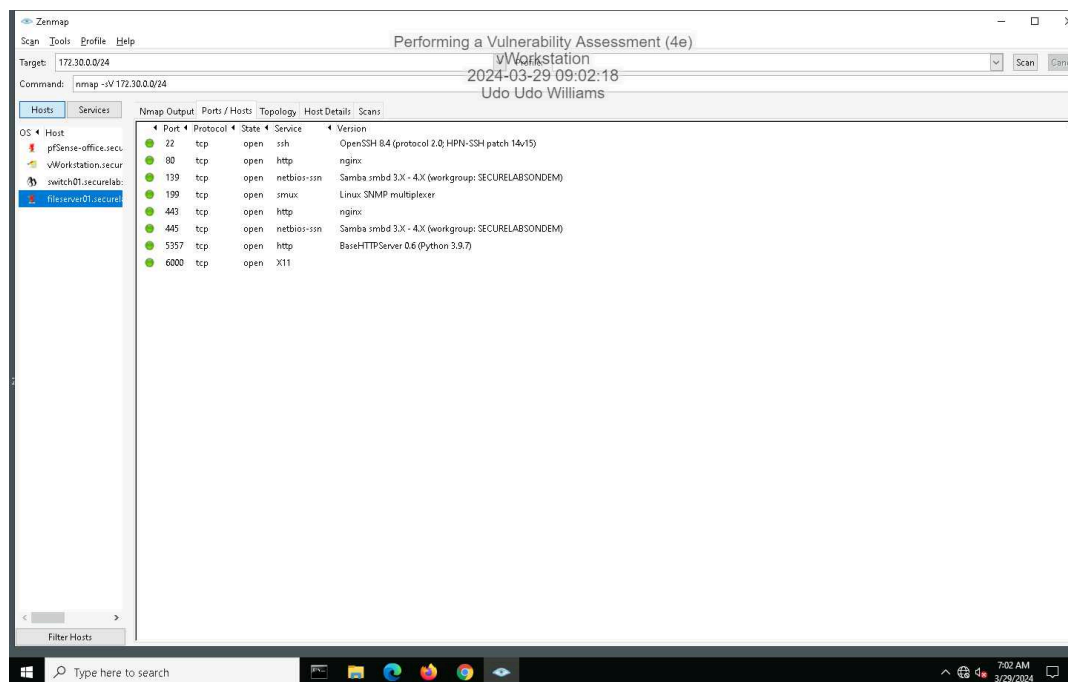
Performing a Vulnerability Assessment (4e)

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**.

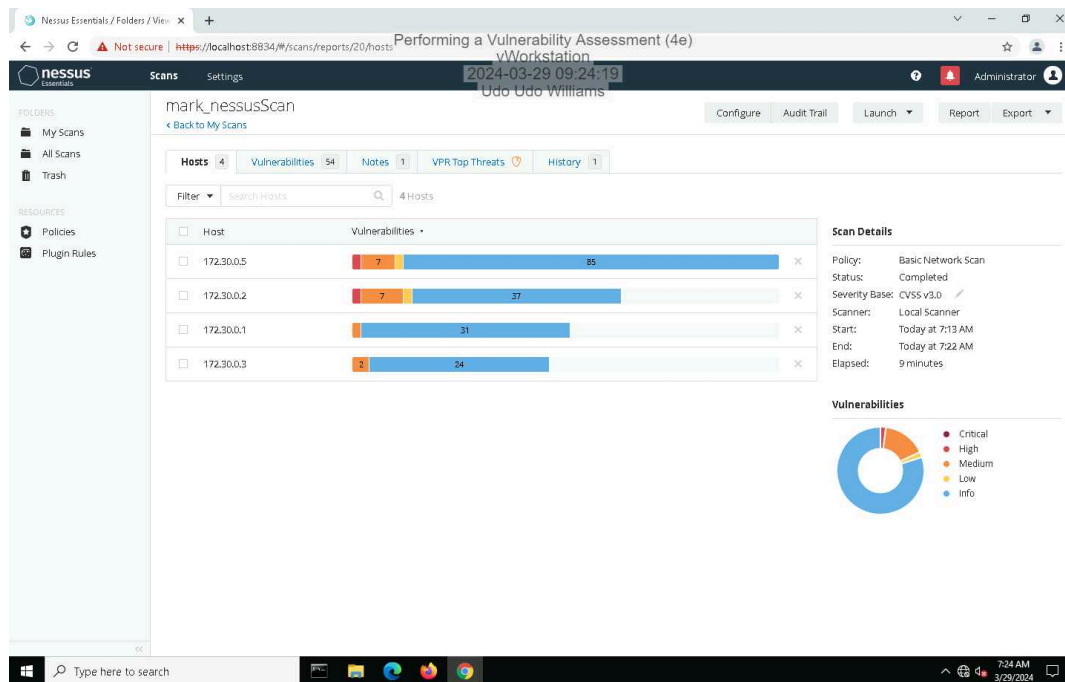


19. Make a screen capture showing the details in the **Ports/Hosts** tab from the **Service** scan for **fileserver01.securelabsondemand.com**.



Part 2: Conduct a Vulnerability Scan with Nessus

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



Part 3: Evaluate Your Findings

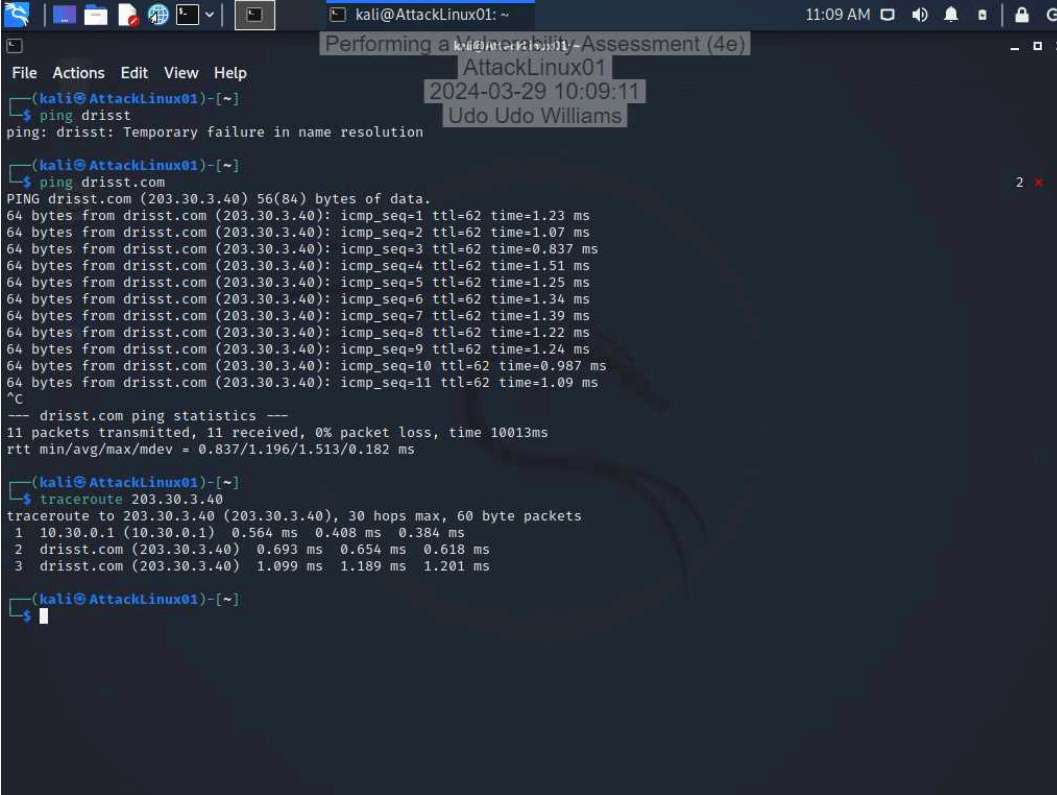
11. Summarize the vulnerability you selected, including the CVSS risk score, and recommend a mitigation strategy.

CVSS v2 Risk Factor: Medium Base Score: 5 Temporal Score: 3.7 agent/snmp_agent.c in snmpd in net-snmp 5.0.9 in Red Hat Enterprise Linux (RHEL) 3 allows remote attackers to cause a denial of service (daemon crash) via a crafted SNMP GETBULK request that triggers a divide-by-zero error. this vulnerability exists because of an incorrect fix for CVE-2008-4309. look for and update the correct fix for cve-2008-4309

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: ~
Performing a Vulnerability Assessment (4e)
AttackLinux01
2024-03-29 10:09:11
Udo Udo Williams

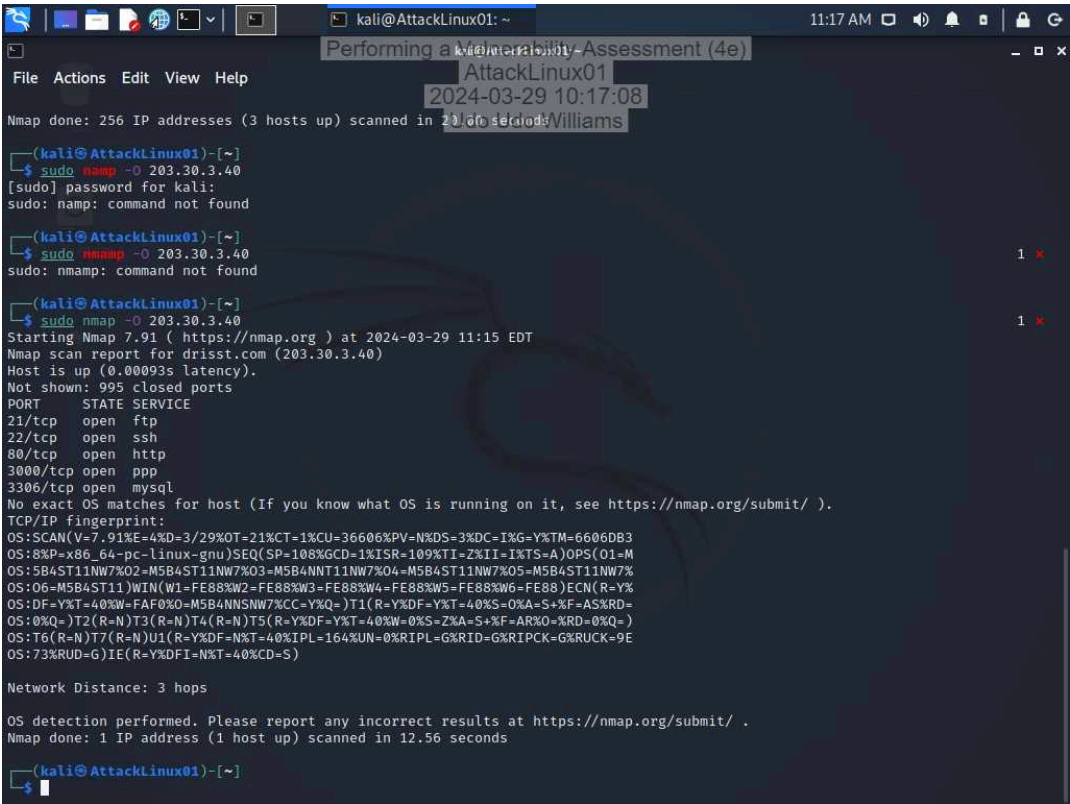
File Actions Edit View Help
(kali@AttackLinux01)-[~]
$ ping drisst
ping: drisst: Temporary failure in name resolution

(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=1.23 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=1.07 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.837 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=1.51 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=1.25 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=6 ttl=62 time=1.34 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=7 ttl=62 time=1.39 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=8 ttl=62 time=1.22 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=9 ttl=62 time=1.24 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=10 ttl=62 time=0.987 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=11 ttl=62 time=1.09 ms
^C
--- drisst.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10013ms
rtt min/avg/max/mdev = 0.837/1.196/1.513/0.182 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)  0.564 ms  0.408 ms  0.384 ms
 2  drisst.com (203.30.3.40)  0.693 ms  0.654 ms  0.618 ms
 3  drisst.com (203.30.3.40)  1.099 ms  1.189 ms  1.201 ms

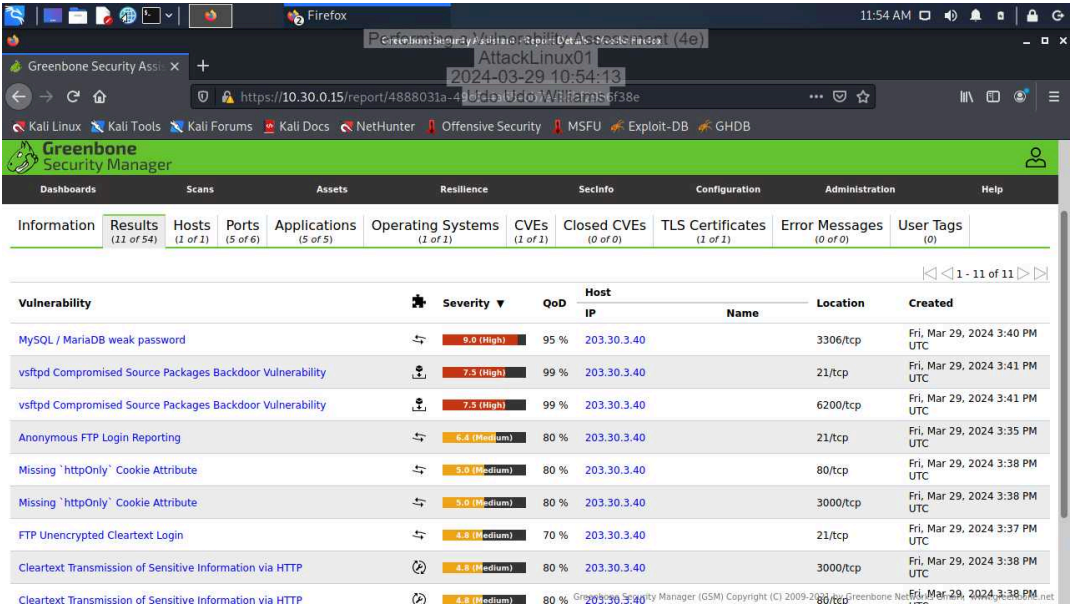
(kali@AttackLinux01)-[~]
$
```

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



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.

scan of web server drisst.com at 203.30.3.40

Completed by

Insert your name here.

Udo Williams

On

Insert current date here.

03/24/2024

Purpose

Identify the purpose of the penetration test.

The purpose of the penetration test on the web server drisst.com 203.30.3.40 is to identify and assess potential vulnerabilities and security weaknesses in the server's configuration, software, and infrastructure.

Scope

Identify the scope of the penetration test.

The scope of a simple penetration test on a web server drisst.com typically includes identifying vulnerabilities in the server's configuration, software, and infrastructure. it is limited to the three highest severity scores

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.

Vulnerability: MySQL/MariaDB weak password Severity: HIGH 9.0 Location: 3306/tcp Summary: It was possible to log in to the remote MySQL as root using weak credentials. It was possible to log in with the password in the password field. Remediation: Change the password as soon as possible.

Vulnerability: vsftpd compromised source packages backdoor vulnerability Severity: HIGH 7.5 Location: 21/tcp Summary: vsftpd is prone to a backdoor vulnerability. This vulnerability allowed attackers to gain unauthorized access to systems running vsftpd. Remediation: The solution to the vsftpd backdoor vulnerability involves applying a patch or update provided by the software vendor.

Vulnerability: vsftpd compromised source packages backdoor vulnerability Severity: HIGH 7.5 Location: 6200/tcp Summary: vsftpd is prone to a backdoor vulnerability. This vulnerability allowed attackers to gain unauthorized access to systems running vsftpd. Remediation: The solution to the vsftpd backdoor vulnerability involves applying a patch or update provided by the software vendor.

Conclusion

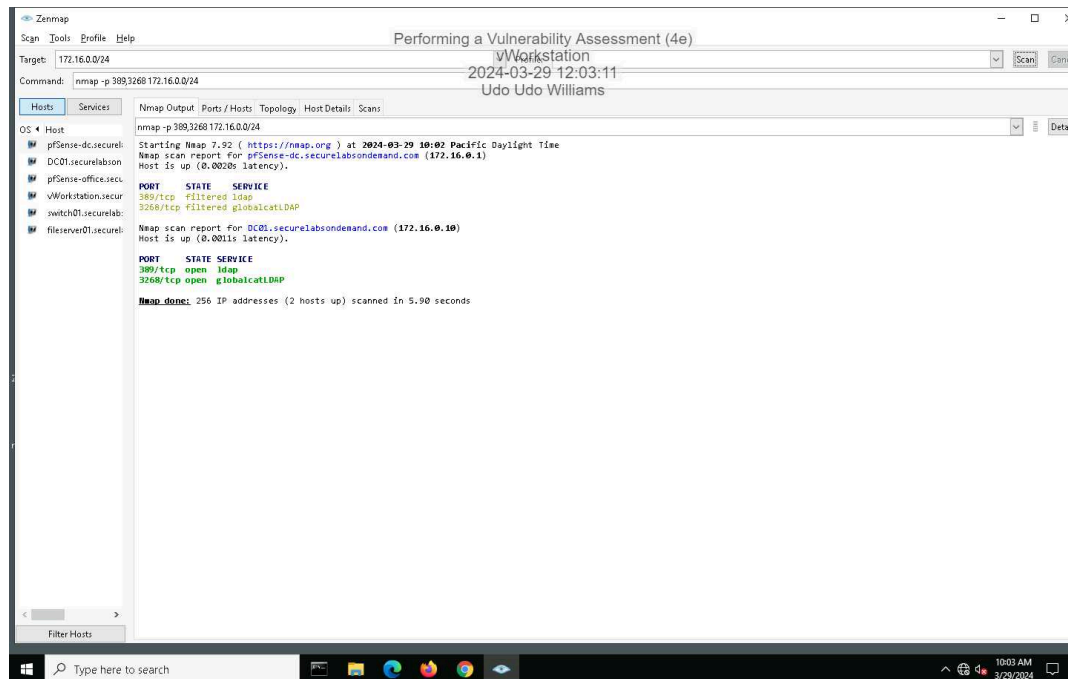
Identify your key findings.

The key finding in this vulnerability assessment is the presence of critical vulnerabilities in both MySQL/MariaDB and vsftpd services. These vulnerabilities pose a significant risk to the security of the systems as they allow unauthorized access, potentially leading to data breaches or system compromise.

Section 3: Challenge and Analysis

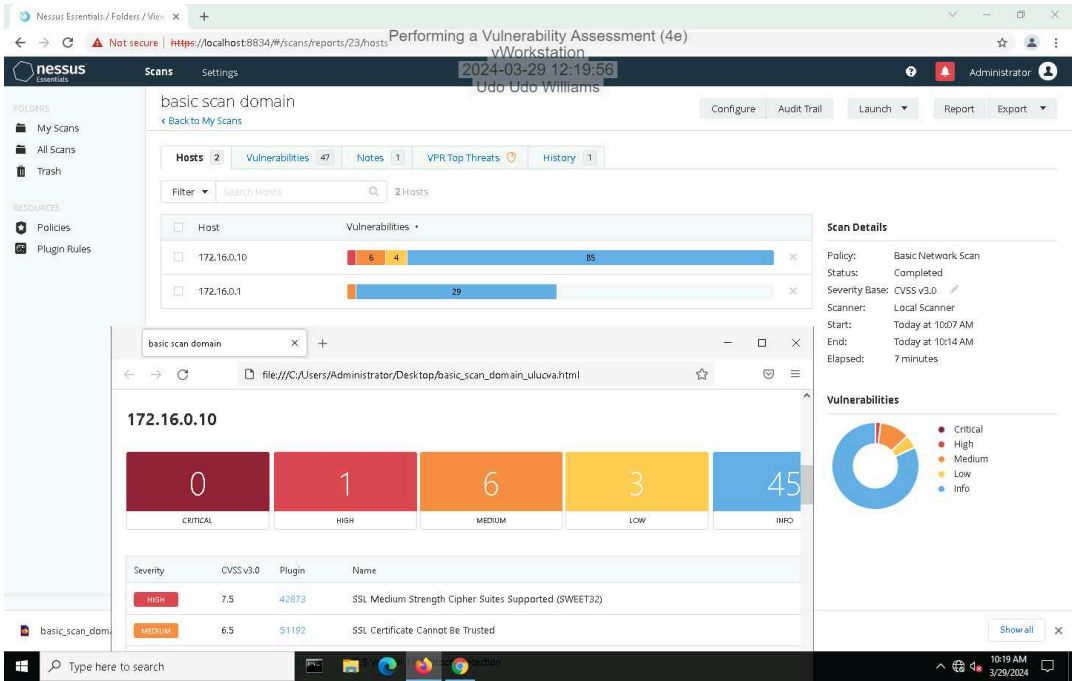
Part 1: Scan the Domain Controller with Nmap

Make screen capture showing the results of your targeted port scan on the domain controller.



Part 2: Scan the Domain Controller with Nessus

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.

domain controller

Completed by

Insert your name here.

Udo Williams

On

Insert current date here.

3/29/2024

Purpose

Identify the purpose of the penetration test.

The purpose of a penetration test on the domain controller is to identify and assess potential vulnerabilities and security weaknesses in the domain controllers configuration, software, and infrastructure

Scope

Identify the scope of the penetration test.

The scope of the penetration test on a domain controller will involve assessing the security of the domain controller itself, as well as its associated network infrastructure and services but will be limited to just one of the highest severity scores

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.

Vulnerability :SSI medium strength cipher suites supported (SWEET32) Severity : HIGH 7.5 Summary :This vulnerability affects encryption protocols like TLS, SSH, and IPSec when using DES or Triple DES ciphers. These ciphers have a limitation known as the "birthday bound," which makes them vulnerable to a specific type of attack called a "birthday attack." Remediation : Reconfigure the affected application if possible to avoid use of medium strength ciphers. Configure the affected systems (such as web servers, VPNs, etc.) to use modern encryption protocols (such as TLS 1.2 or higher) and stronger cipher suites

Conclusion

Identify your key findings.

The key finding is the susceptibility of systems using DES and Triple DES encryption ciphers to "Sweet32" attacks. These attacks leverage the birthday bound of approximately four billion blocks associated with these ciphers, making it feasible for remote attackers to conduct successful attacks against long-duration encrypted sessions.