

# Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Student:  
Fernando Parra

Email:  
fparra1@msudenve.edu

Time on Task:  
7 hours, 26 minutes

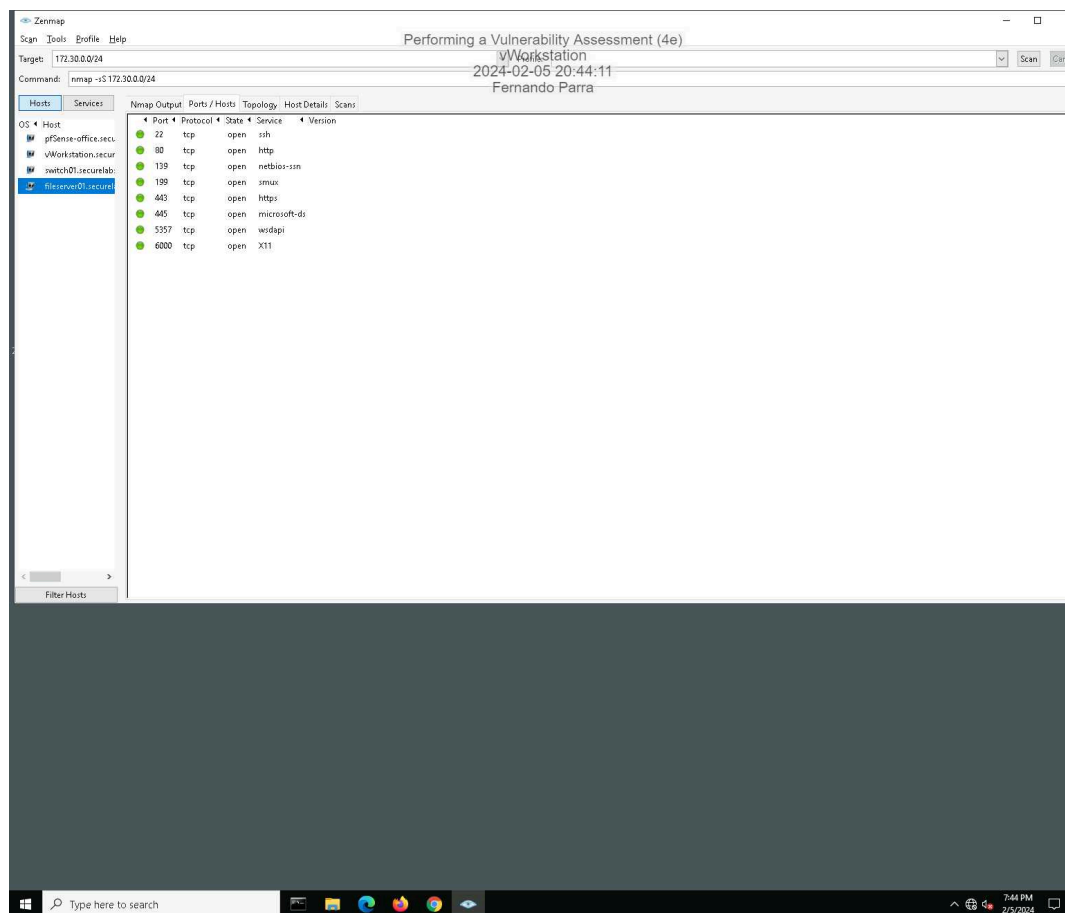
Progress:  
100%

Report Generated: Saturday, February 10, 2024 at 7:04 PM

## Section 1: Hands-On Demonstration

### Part 1: Scan the Network with Zenmap

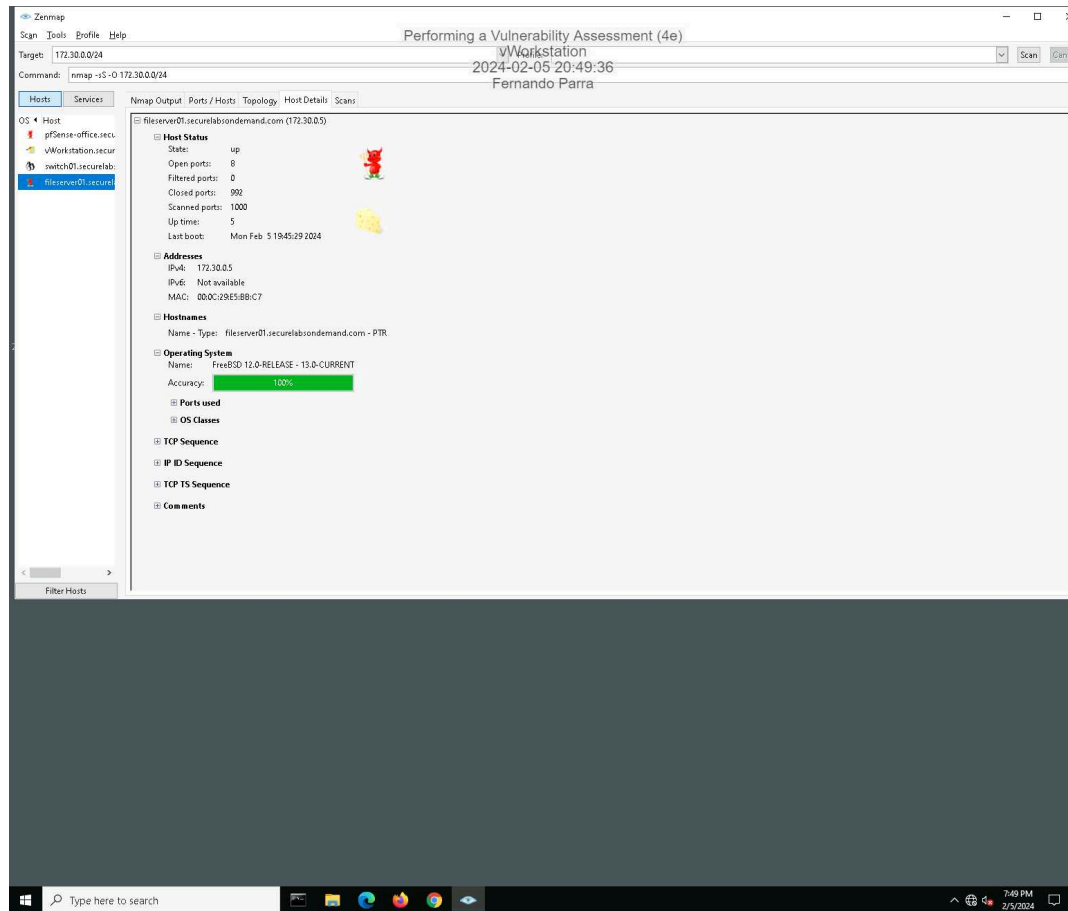
9. **Make a screen capture** showing the contents of the **Ports/Hosts** tab from the **SYN** scan for **fileserver01.securelabsondemand.com**.



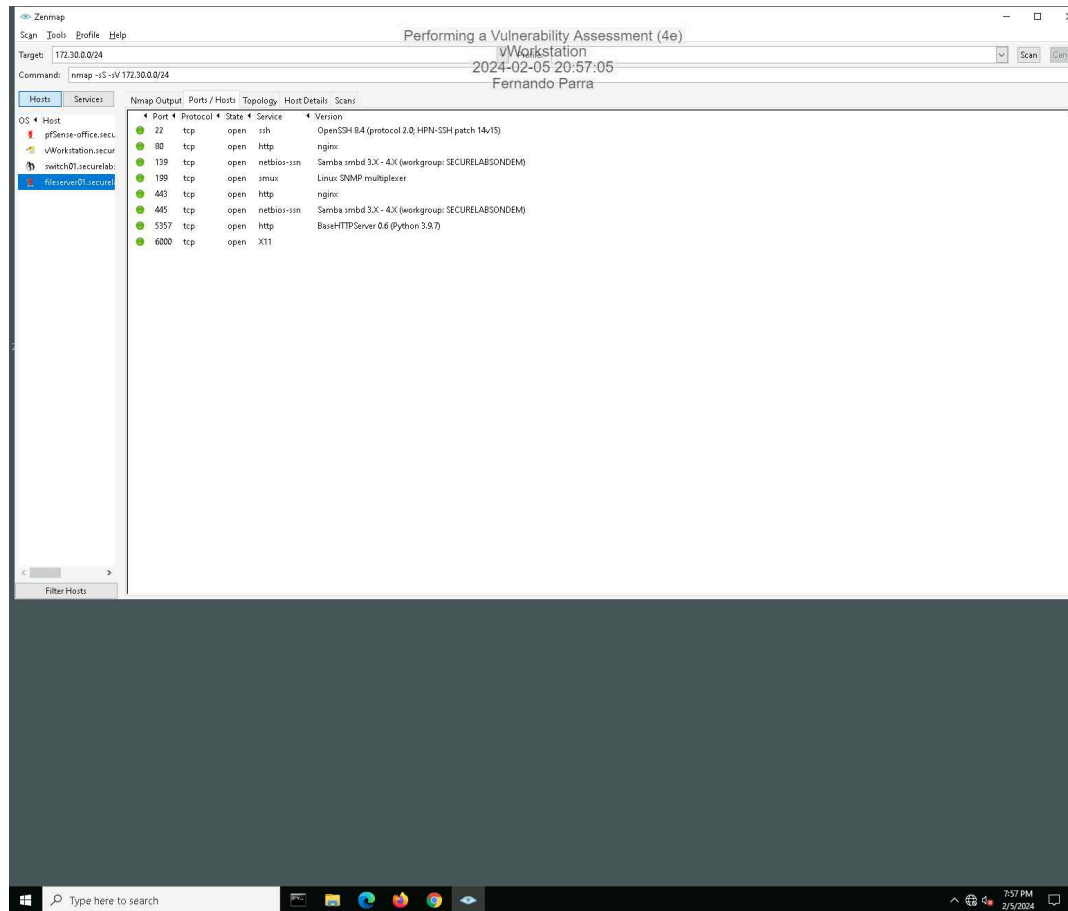
# Performing a Vulnerability Assessment (4e)

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**.

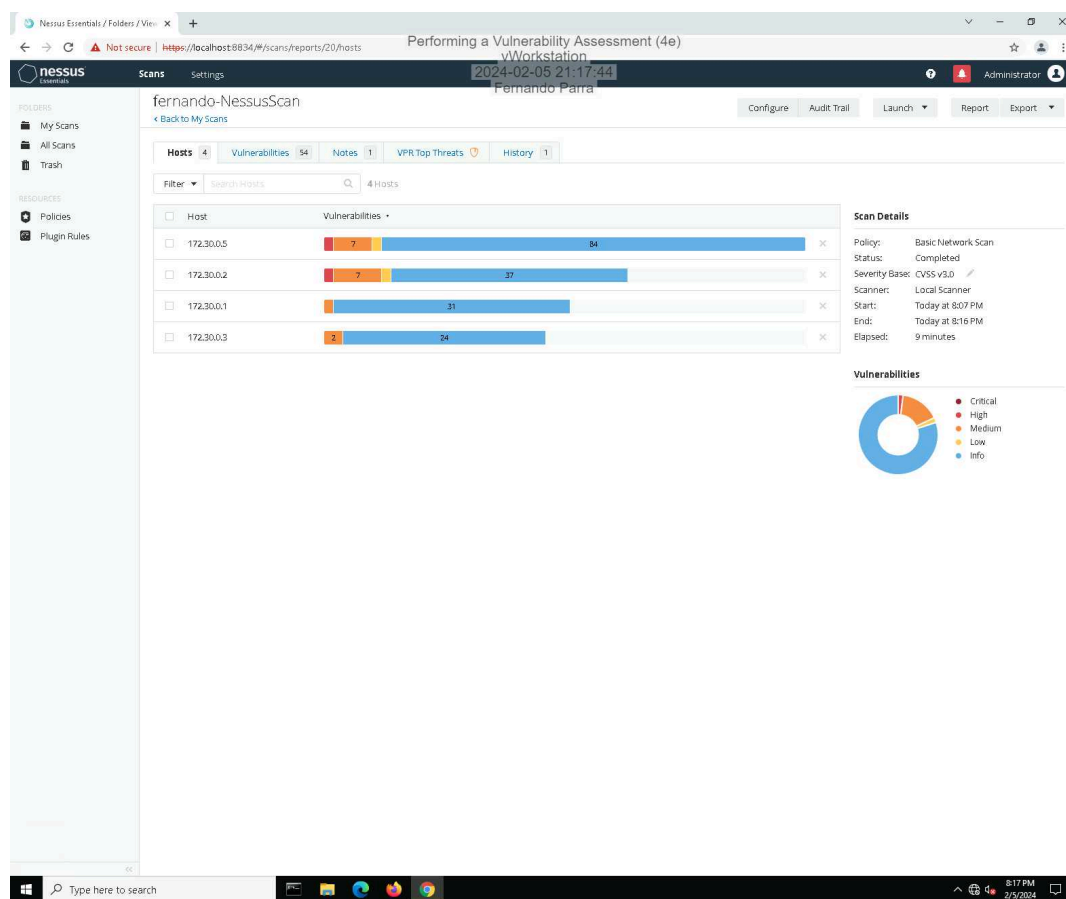


19. **Make a screen capture** showing the details in the **Ports/Hosts** tab from the **Service scan** for **fileserver01.securelabsondemand.com**.



## Part 2: Conduct a Vulnerability Scan with Nessus

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



## Part 3: Evaluate Your Findings

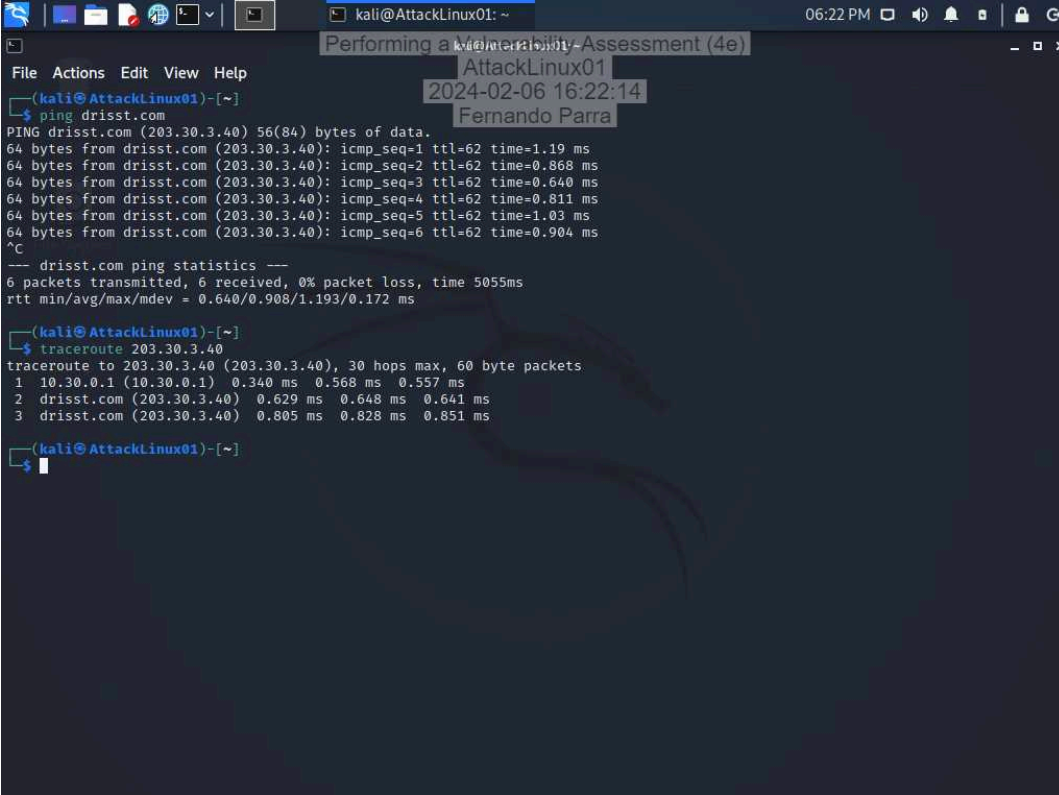
### 11. Summarize the vulnerability you selected, including the CVSS risk score, and recommend a mitigation strategy.

I have chosen the vulnerability with a medium rating, which is identified as 90317 or SSH Weak Algorithm Supported. This vulnerability means that the SSH protocol is configured with a weak or no encryption algorithm, thus making it vulnerable to remote attacks. The access vector is through the network, the access complexity is medium, there is no need for authentication, and it only partially impacts confidentiality.

## Section 2: Applied Learning

### Part 1: Scan the Network with Nmap

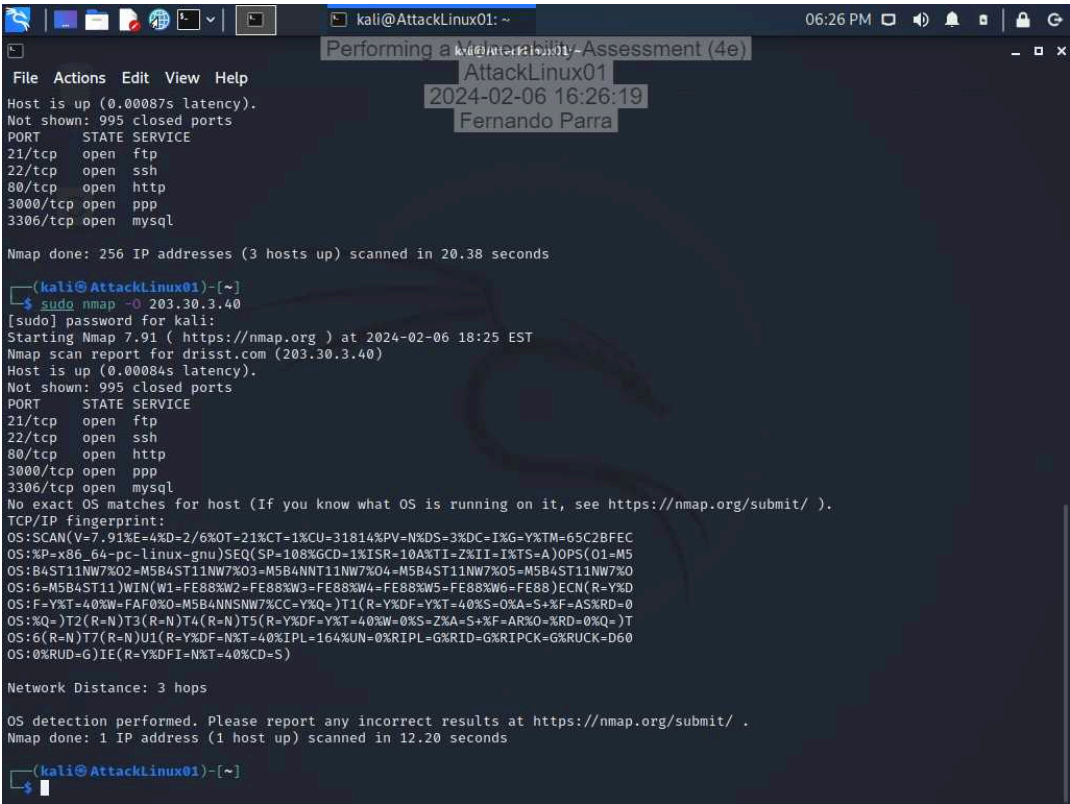
6. Make a screen capture showing the results of the traceroute command.



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

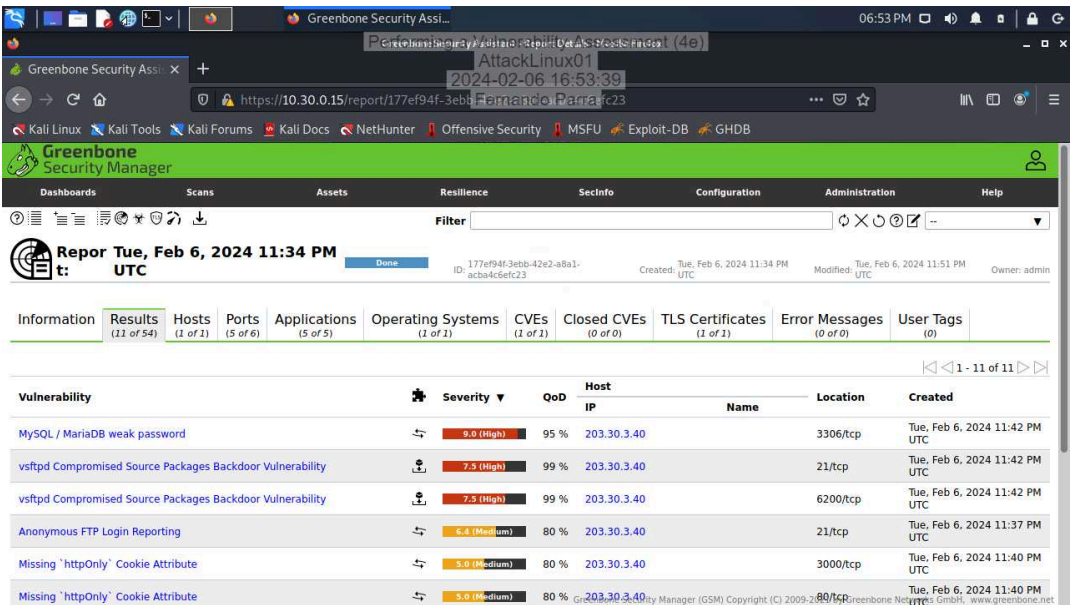
```
kali@AttackLinux01: ~  
File Actions Edit View Help  
AttackLinux01  
2024-02-06 16:22:14  
Fernando Parra  
kali@AttackLinux01:~  
$ ping drisst.com  
PING drisst.com (203.30.3.40) 56(84) bytes of data:  
64 bytes from drisst.com (203.30.3.40): icmp_seq=1 ttl=62 time=1.19 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=0.868 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.640 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=0.811 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=1.03 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=6 ttl=62 time=0.904 ms  
^C  
--- drisst.com ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5055ms  
rtt min/avg/max/mdev = 0.640/0.908/1.193/0.172 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) 0.340 ms 0.568 ms 0.557 ms  
2 drisst.com (203.30.3.40) 0.629 ms 0.648 ms 0.641 ms  
3 drisst.com (203.30.3.40) 0.805 ms 0.828 ms 0.851 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.

Website: drisst.com

IP Address: 203.30.3.40

#### Completed by

Insert your name here.

Fernando

#### On

Insert current date here.

February 6th, 2024

#### Purpose

Identify the purpose of the penetration test.

The purpose of this penetration test was to identify vulnerabilities within the web server of drisst.com that could potentially be exploited to compromise system integrity, confidentiality, or availability.

#### Scope

Identify the scope of the penetration test.

The scope of the test was restricted to a non-destructive vulnerability scan of the drisst.com web server. The tools used were Nmap for network mapping and OpenVAS/GSM for vulnerability scanning. The emphasis was on determining exploitable vulnerabilities without disrupting the live environment.

### 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.

The examination commenced with an Nmap scan to enumerate services, followed by an OpenVAS vulnerability scan focusing on those services to identify potential weaknesses. A total of 11 vulnerabilities were uncovered during the scanning process, with 3 identified as high severity for their potential impact on the system security: MySQL MariaDB Weak Password. This vulnerability is due to the deployment of a weak password policy in the MySQL MariaDB service, making it sensitive to brute-force attacks. vsftpd Compromised Source Packages (Backdoor Vulnerability) Two instances of the vsftpd service were found to be susceptible to compromise with backdoor vulnerabilities, likely due to the installation of manipulated source packages. This could allow unauthorized remote access to the server.

To mitigate the identified vulnerabilities and improve the security posture of the drisst.com web server, the organization should enforce strong password policies for all services, especially MySQL MariaDB, to prevent brute-force attacks. Passwords should meet complexity requirements and be changed regularly. Examine the source of the vsftpd packages to pinpoint and remove compromised versions. Ensure future installations are obtained from trustworthy repositories and verify their integrity. Regularly perform security scans and assessments to identify new vulnerabilities. Implement continuous monitoring tools to detect and alert on suspicious activities.

### Conclusion

Identify your key findings.

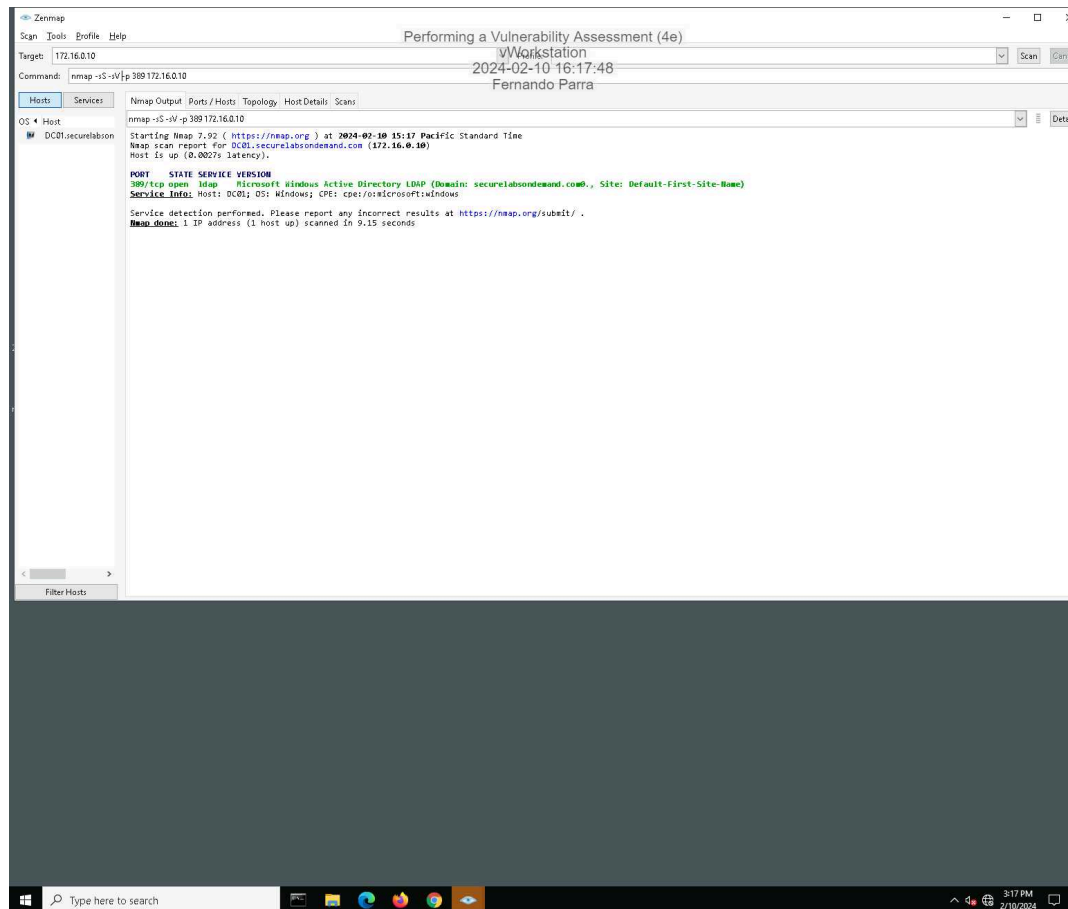
The penetration test was successful in determining crucial vulnerabilities within the drisst.com web server. Notably, the weak password policy applied to the MySQL MariaDB and two compromised vsftpd packages pose substantial security risks. These vulnerabilities could allow attackers to gain unauthorized access, manipulate data, or exploit the integrity of the web server. By managing these vulnerabilities promptly and adopting a proactive security posture, drisst.com can significantly decrease its exposure to potential cyber threats and safeguard its digital assets.



### Section 3: Challenge and Analysis

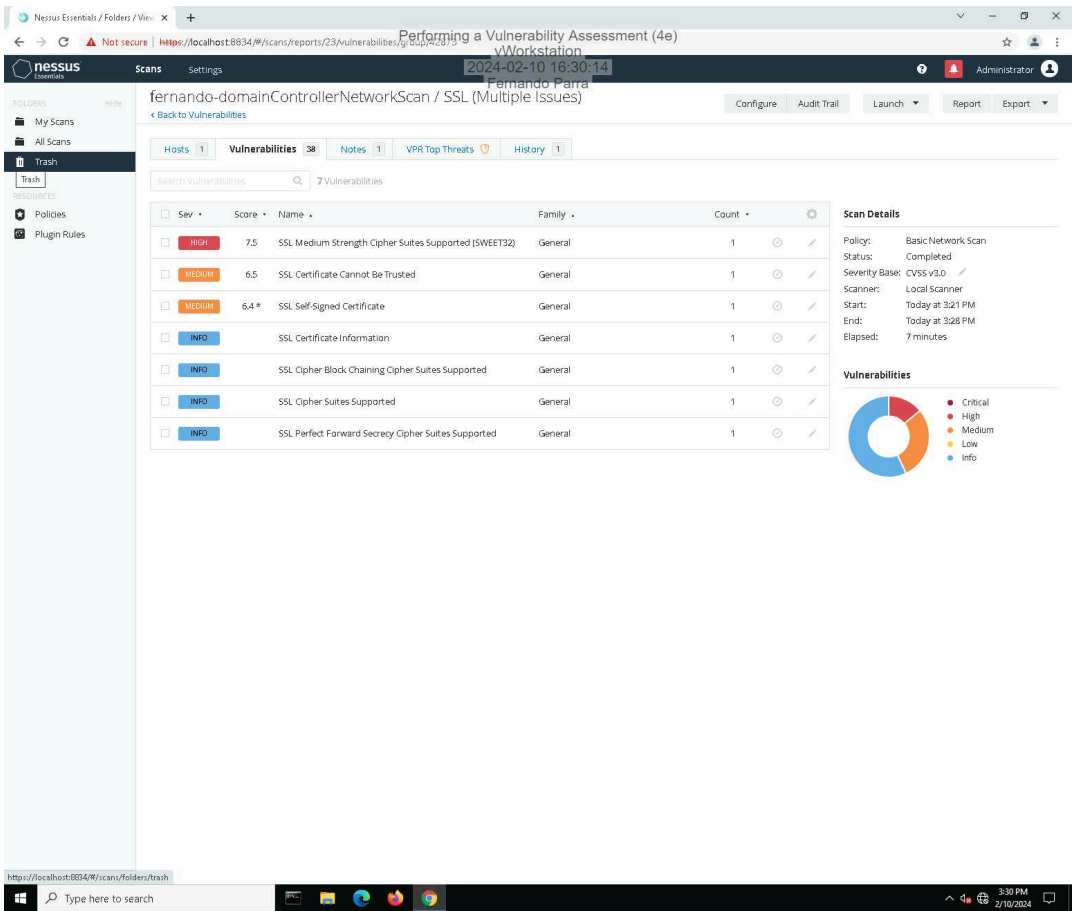
#### Part 1: Scan the Domain Controller with Nmap

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.

DomainController01/172.16.0.10

Completed by

Insert your name here.

Fernando

### On

Insert current date here.

February 10th, 2024

### Purpose

Identify the purpose of the penetration test.

The objective of conducting a penetration test is to assess the ability of domainController01 to withstand potential cyber threats. This includes evaluating its susceptibility to unauthorized access, data breaches, and manipulation of critical system settings through open ports and vulnerabilities like SSL Medium Strength Cipher Suites Supported (SWEET32), which can be exploited as attack vectors.

### Scope

Identify the scope of the penetration test.

The scope of the test encompassed utilizing Nmap and Nessus to conduct a basic network scan evaluation, this approach aimed to gain an understanding of the network's layout and potential vulnerabilities that could be exploited by attackers.

### 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.

During the penetration test, several vulnerabilities were identified, each with varying severity levels. Open Port: LDAP (Port 389) with a high severity according to CVE-2022-0918 LDAP (Lightweight Directory Access Protocol) is an open port that could potentially expose the device to denial of service attacks. Remediation could be to implement firewall rules and update LDAP configurations to ensure security best patches are installed. Additionally, the open port 3389 with Microsoft Windows Based Terminal puts the device at risk of SSL Medium Strength Cipher Suites Supported (SWEET32) detected by Nessus. The high severity of the vulnerability is mainly due to its medium-strength SSL ciphers, it is recommended to update the SSL/TLS configuration to disable support for weak or deprecated cipher suites. Use strong cryptographic algorithms and key lengths and regularly update SSL/TLS libraries and monitor for security advisories to stay informed about emerging threats and vulnerabilities.

### Conclusion

Identify your key findings.

In summary, it is crucial to take prompt action to address the high-severity vulnerabilities detected in the LDAP (Port 389) and Microsoft Windows Based Terminal (Port 3389) to enhance the overall security of the system. This requires implementing firewall rules, updating the LDAP configurations, and disabling support for weak SSL/TLS cipher suites.