

Student: Julie Clarke

Email: clarke323@usf.edu

Time on Task: 7 hours, 52 minutes

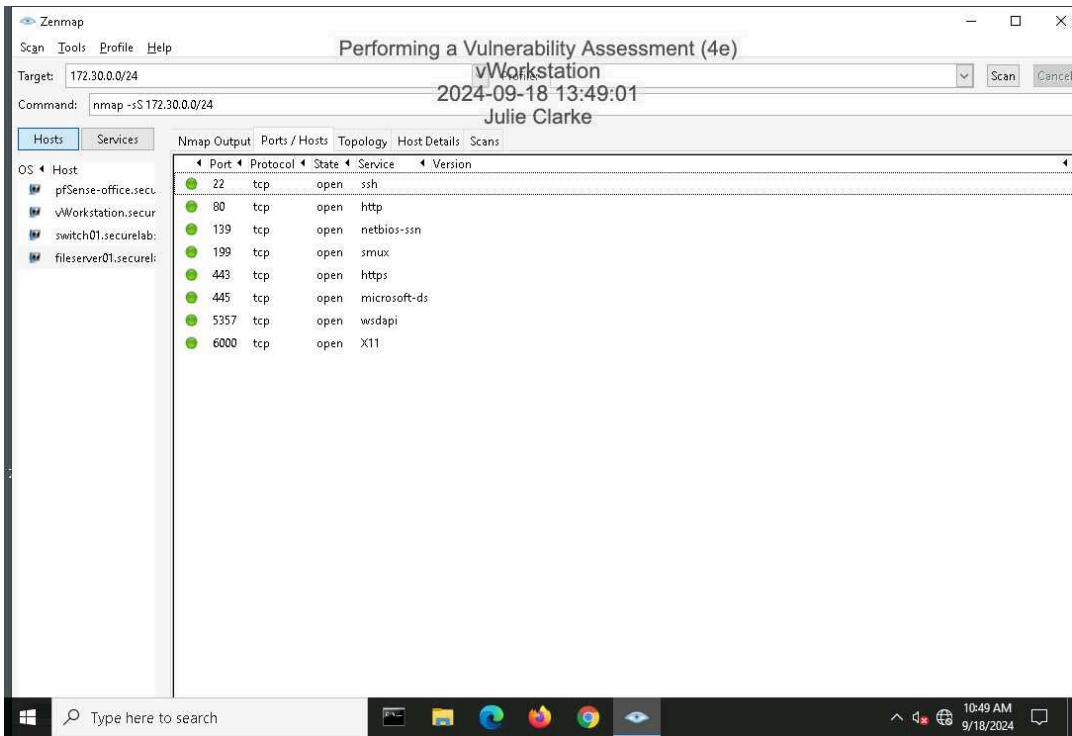
Progress: 100%

Report Generated: Thursday, September 19, 2024 at 12:23 AM

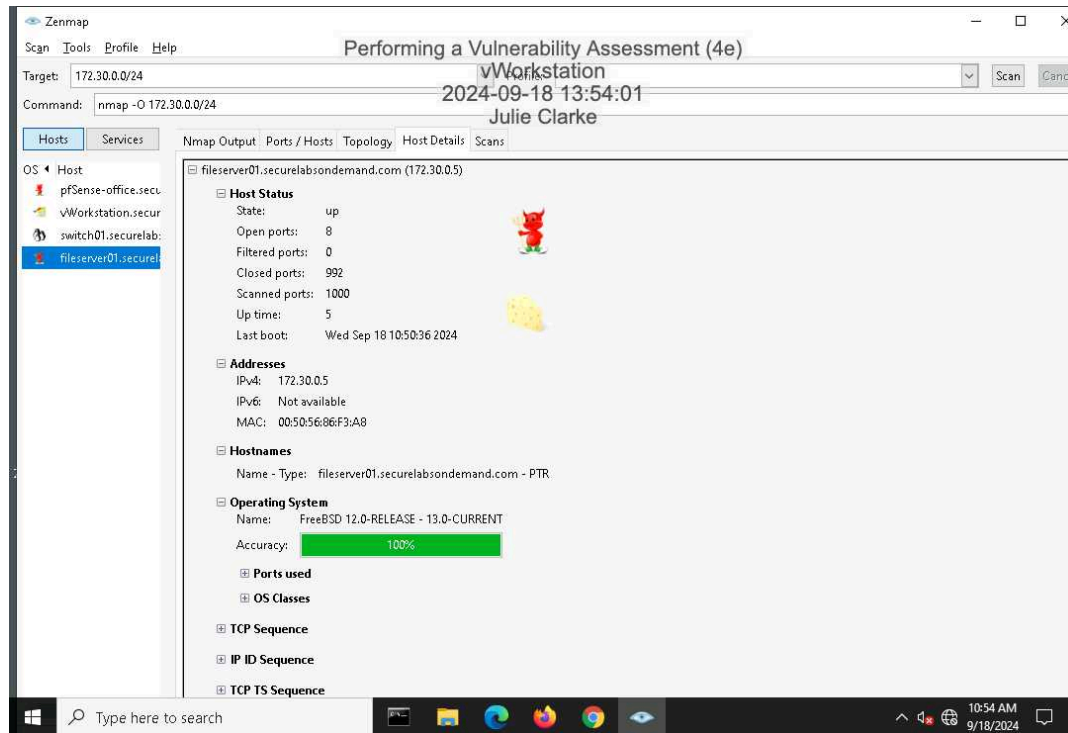
# Section 1: Hands-On Demonstration

## Part 1: Scan the Network with Zenmap

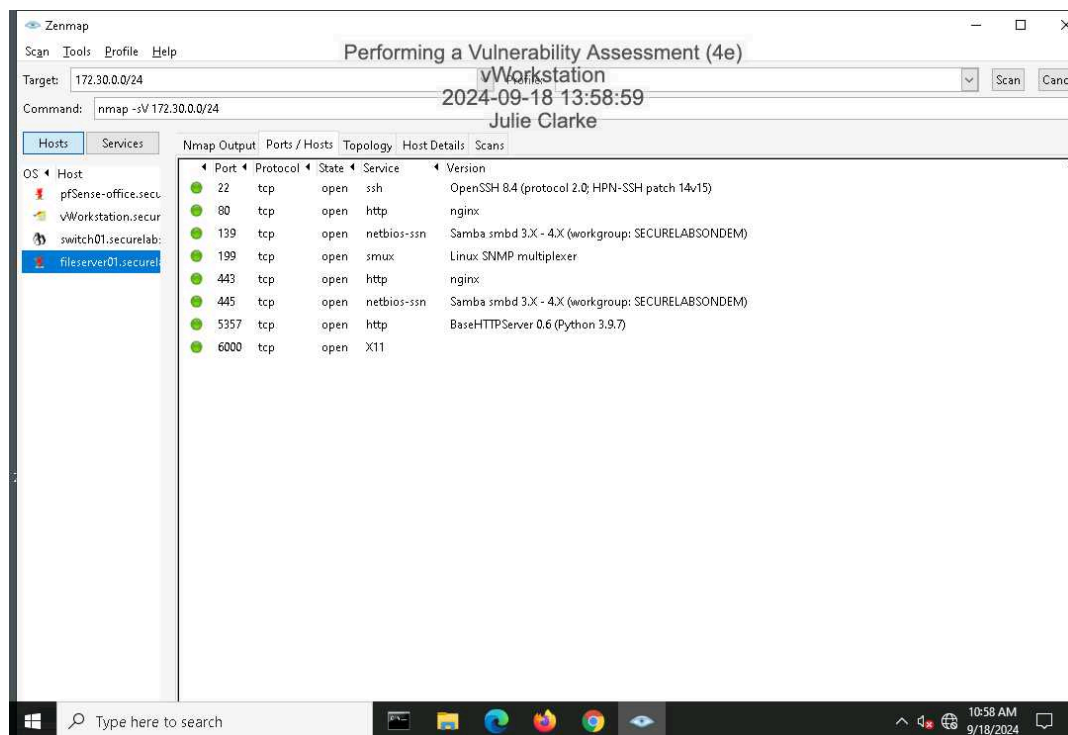
9. Make a screen capture showing the contents of the **Ports/Hosts** tab from the **SYN** scan for **fileserver01.securelabsondemand.com**.



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

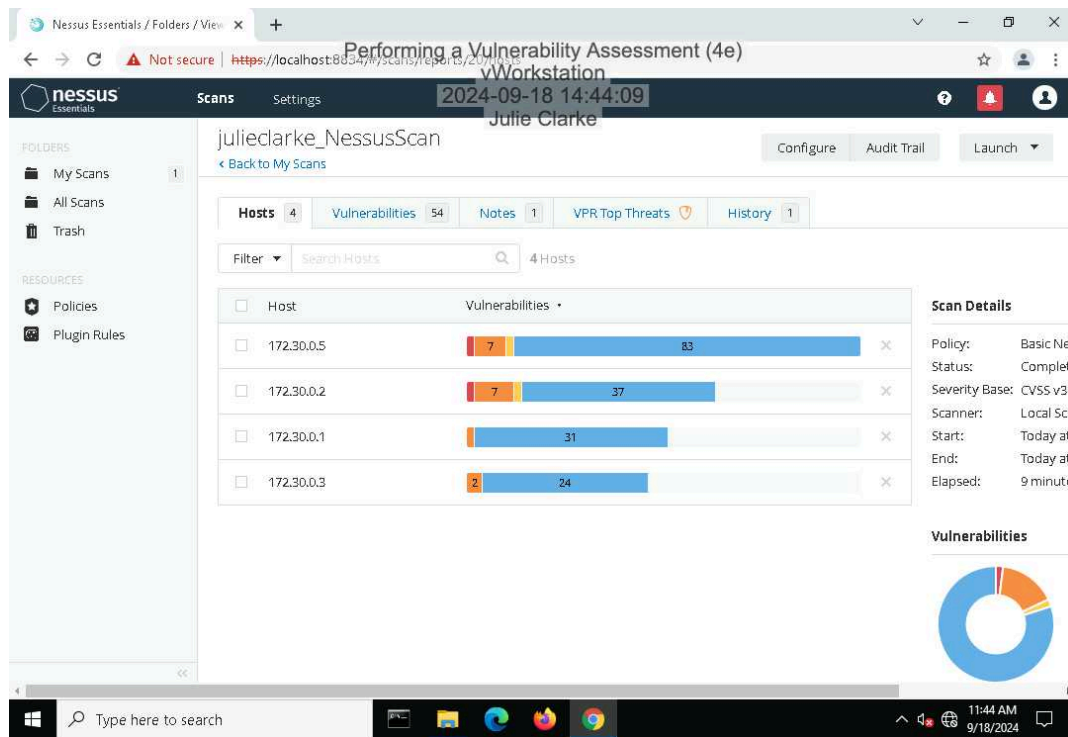


19. Make a screen capture showing the details in the **Ports/Hosts** tab from the **Service** scan for **fileserver01.securelabsondemand.com**.



### 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.

The SNMP Daemon is vulnerable to a 'GETBULK' Reflection Distributed Denial of Service (DDoS) attack, where it responds with a large amount of data to a maliciously crafted 'GETBULK' request.

Attackers can use this to amplify traffic and overwhelm a target, making it a significant security concern with a medium risk rating (CVSS v2 base score: 5)

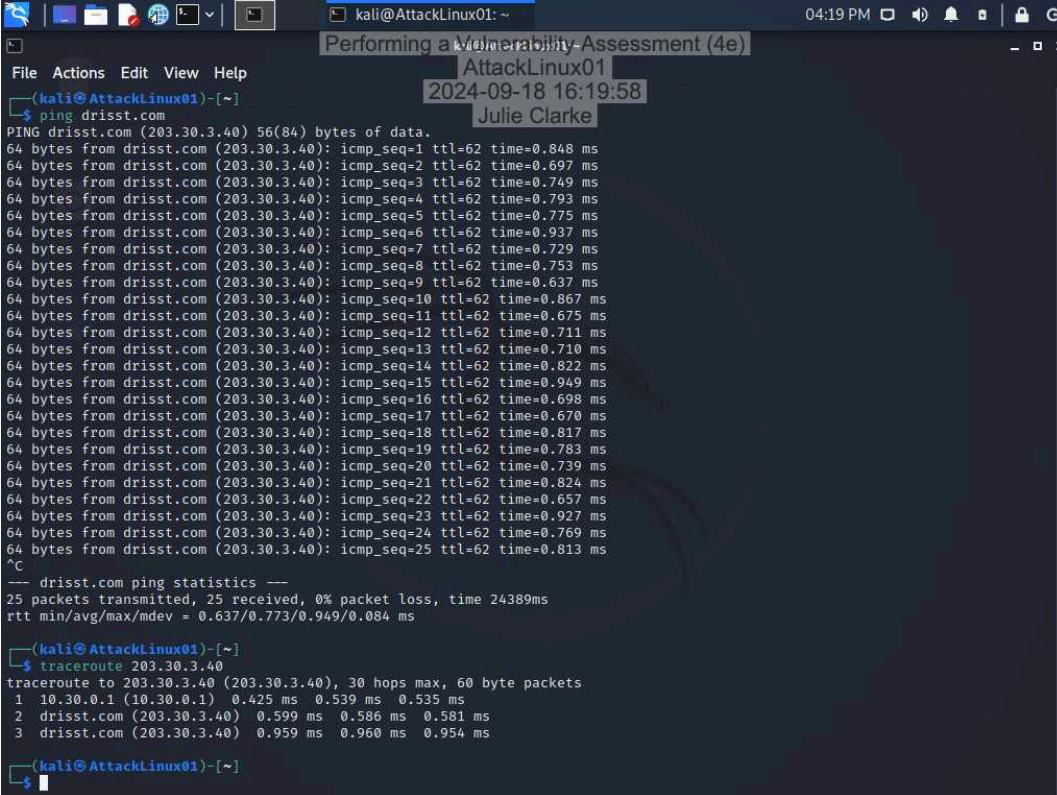
To protect against the SNMP 'GETBULK' Reflection DDoS vulnerability, you should first disable SNMP if it's not needed. If it is required, limit access to trusted users or IP addresses, change the default 'public' community string to something more secure, and configure SNMP to control how much data it sends in response to requests. Additionally, monitor SNMP traffic for any unusual activity, and ensure the software is updated with the latest security patches. These steps will help reduce the risk of exploitation in a DDoS attack.

Extra Vulnerability Info: CVE Dictionary Entry: CVE-2008-4309 ID: 76474 Name: SNMP 'GETBULK' Reflection DDoS Severity: Medium CVSS v2 Risk Score: 5.0

### Section 2: Applied Learning

#### Part 1: Scan the Network with Nmap

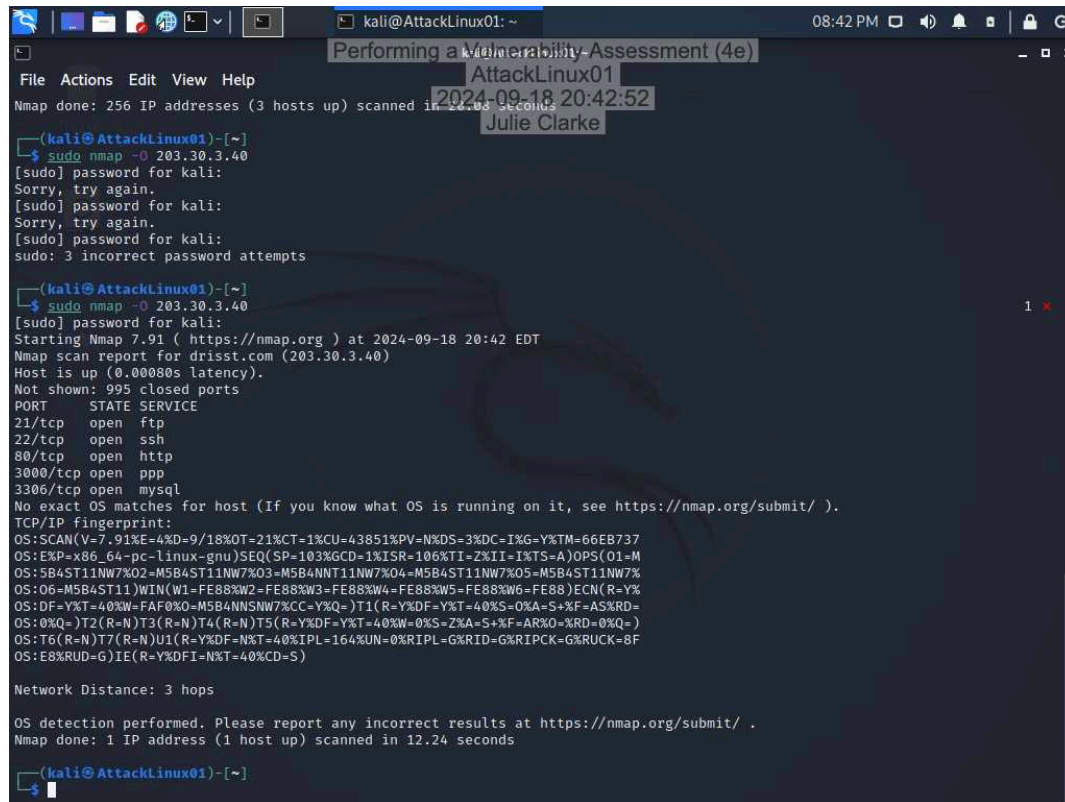
6. Make a screen capture showing the results of the traceroute command.



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

```
kali@AttackLinux01: ~  
File Actions Edit View Help  
AttackLinux01  
2024-09-18 16:19:58  
Julie Clarke  
$ 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=0.848 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=0.697 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.749 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=0.793 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=0.775 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=6 ttl=62 time=0.937 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=7 ttl=62 time=0.729 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=8 ttl=62 time=0.753 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=9 ttl=62 time=0.637 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=10 ttl=62 time=0.867 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=11 ttl=62 time=0.675 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=12 ttl=62 time=0.711 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=13 ttl=62 time=0.710 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=14 ttl=62 time=0.822 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=15 ttl=62 time=0.949 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=16 ttl=62 time=0.698 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=17 ttl=62 time=0.670 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=18 ttl=62 time=0.817 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=19 ttl=62 time=0.783 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=20 ttl=62 time=0.739 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=21 ttl=62 time=0.824 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=22 ttl=62 time=0.657 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=23 ttl=62 time=0.927 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=24 ttl=62 time=0.769 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=25 ttl=62 time=0.813 ms  
^C  
--- drisst.com ping statistics ---  
25 packets transmitted, 25 received, 0% packet loss, time 24389ms  
rtt min/avg/max/mdev = 0.637/0.773/0.949/0.084 ms  
$ 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) 0.425 ms 0.539 ms 0.535 ms  
2 drisst.com (203.30.3.40) 0.599 ms 0.586 ms 0.581 ms  
3 drisst.com (203.30.3.40) 0.959 ms 0.960 ms 0.954 ms  
$
```

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

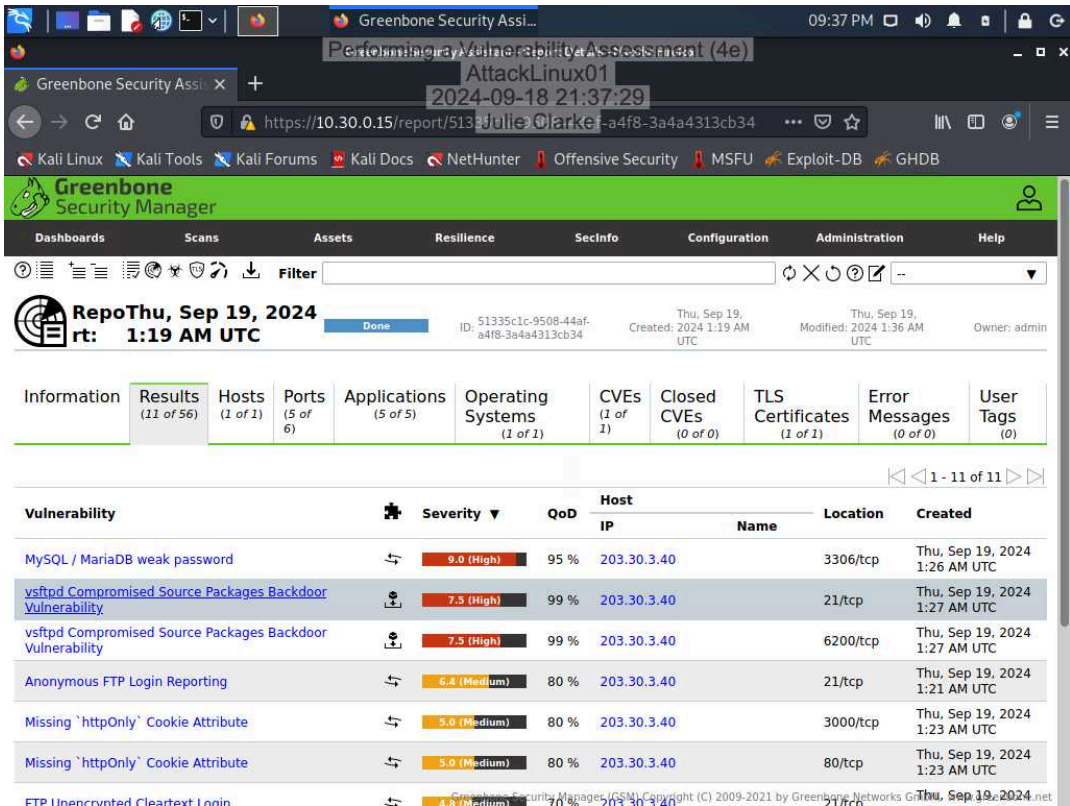


```
kali@AttackLinux01: ~  
File Actions Edit View Help  
Nmap done: 256 IP addresses (3 hosts up) scanned in 12.08 seconds  
[kali@AttackLinux01]~  
$ sudo nmap -O 203.30.3.40  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
sudo: 3 incorrect password attempts  
[kali@AttackLinux01]~  
$ sudo nmap -O 203.30.3.40  
[sudo] password for kali:  
Starting Nmap 7.91 ( https://nmap.org ) at 2024-09-18 20:42 EDT  
Nmap scan report for drisst.com (203.30.3.40)  
Host is up (0.00080s 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=9/18%OT=21%CT=1%CU=43851%PV=N%DS=3%DC=I%G=Y%TM=66E8737  
OS:EXP=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=106%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=8F  
OS:E8%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 12.24 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.

The target of this penetration test is the web server for drisst.com; which serves as a critical component of the organization's online infrastructure. The server was selected due to its public-facing nature, making it a likely target for potential attackers. This test aims to evaluate the security posture of the server by identifying the vulnerabilities that could compromise the server's integrity, which in this case are as follows:- MySQL/ MariaDB weak password (9.0 Risk)- vsftpd Compromised Source Packages Backdoor Vulnerability (7.5 Risk)- vsftpd Compromised Source Packages Backdoor Vulnerability (7.5 Risk)Since the server is responsible for handling external requests and hosting key services, understanding its weaknesses is essential for protecting sensitive data and maintaining system availability.

Completed by

Insert your name here.

Julie Clarke

### On

Insert current date here.

09/18/2024

### Purpose

Identify the purpose of the penetration test.

The purpose of this penetration test is to conduct a thorough security evaluation of the drisst.com web server to identify potential vulnerabilities that may exist. The test is designed to simulate real-world scenarios in which an attacker might attempt to exploit security flaws. By proactively identifying these vulnerabilities, the organization can take steps to strengthen its defenses and reduce the risk of a successful cyberattack. The findings from this assessment will provide the foundation for targeted remediation efforts aimed at improving the overall security of the server.

### Scope

Identify the scope of the penetration test.

The scope of this penetration test is confined to performing a comprehensive vulnerability scan of the drisst.com web server, utilizing tools such as Nmap for network mapping and OpenVAS for vulnerability analysis. The tests will be conducted in a non-intrusive manner, meaning no aggressive scans or actions that could cause system instability or damage will be performed. The goal is to gather detailed information on any security weaknesses present, particularly focusing on the 3 high-severity vulnerabilities. The tester will document all findings without attempting to exploit any identified vulnerabilities, ensuring that the test adheres to ethical guidelines while providing valuable insights into the server's security.

### 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: 9.0 (high)- Issue Description: The MySQL server on the drisst.com web server uses the default root password "password," allowing easy unauthorized root access. This weak credential exposes the database to potential compromise, enabling attackers to execute malicious queries, steal sensitive data, or modify critical information. The vulnerability was detected via the MariaDB/Oracle MySQL method, confirming MySQL version 5.7.34- Recommended remediation: Change the MySQL root password to a strong, complex one immediately. Disable remote root access if not needed. Create a new admin user with limited privileges and implement multi-factor authentication (MFA) if possible. Follow a password rotation policy and monitor for suspicious login attempts- Vulnerability: vsftpd Compromised Source Packages Backdoor Vulnerability- Severity: 7.5 (high)- Issue Description: A backdoor in the vsftpd 2.3.4 source package allows attackers to execute arbitrary commands with the same privileges as vsftpd, potentially compromising the entire system. Exploiting this vulnerability could lead to unauthorized access, privilege escalation, and control over files, making the system susceptible to further attacks within the network- Recommended remediation: Upgrade to a secure, vendor-provided version of vsftpd, replacing the compromised 2.3.4 package. Verify the integrity of the new package by checking its digital signature. Regularly apply updates and security patches, and scan the system for signs of exploitation after applying the fix

### Conclusion

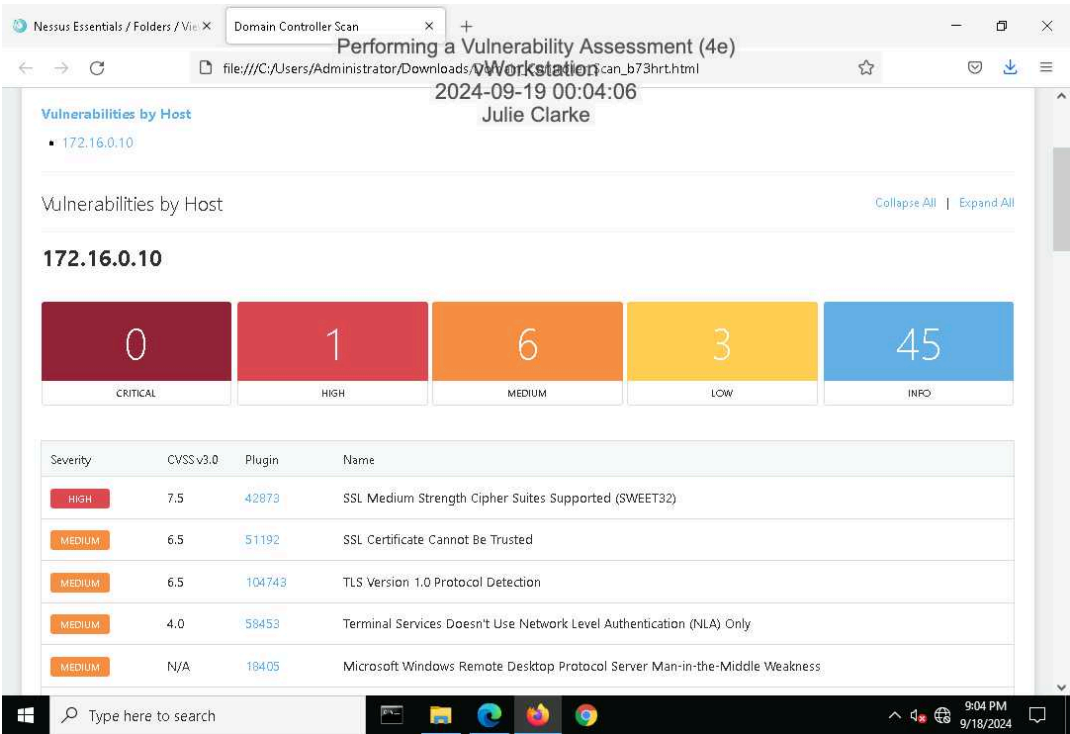
Identify your key findings.

The security penetration test revealed critical vulnerabilities with high severity ratings. The MySQL/MariaDB server was found to be using the default root password "password," posing a severe risk of unauthorized access, data theft, and manipulation. Additionally, a backdoor in the vsftpd 2.3.4 package was identified, allowing attackers to execute arbitrary commands with elevated privileges, potentially compromising the entire system. To address these issues, it is crucial to immediately change the MySQL root password to a strong, complex one, disable remote root access if not needed, create a new admin user with limited privileges, and implement multi-factor authentication. For the vsftpd vulnerability, upgrading to a secure, vendor-provided version, verifying the integrity of the package, and regularly applying updates and patches are essential. Post-remediation, both systems should be thoroughly scanned for signs of exploitation to ensure security.





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.

The target is to test the security of the high severity of the Domain Controller, which in this case that vulnerability is SSL Medium Strength Cipher Suites Supported (SWEET32)

Completed by

Insert your name here.

Julie Clarke

On

Insert current date here.

09/18/2024

### Purpose

Identify the purpose of the penetration test.

The purpose of this test is to find the weak points of SSL Medium Strength Cipher Suites Supported (SWEET32), in order to find ways to improve the system so that the security is maximized and no longer deemed a high severity risk.

### Scope

Identify the scope of the penetration test.

The scope of this vulnerability involves the use of medium-strength SSL ciphers on the remote host. These ciphers provide encryption with key lengths between 64 and 112 bits, or utilize the 3DES encryption suite, which is considered less secure by today's standards. Medium-strength encryption can be easier for attackers to bypass, especially if they are on the same physical network as the target. This vulnerability can put sensitive data at risk, as it allows for the possibility of data interception or decryption. To mitigate this, it's recommended to reconfigure the application to avoid using these weaker ciphers and opt for stronger encryption methods instead.

### 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:** SSL Medium Strength Cipher Suites Supported (SWEET32)  
**Severity:** 7.5 (high)  
**Describe the issue:** The vulnerability involves the remote service supporting SSL ciphers that provide medium-strength encryption. According to Nessus, medium strength refers to ciphers using key lengths of at least 64 bits but less than 112 bits, or encryption suites like 3DES, which are considered outdated by modern security standards. The main risk with medium-strength ciphers is that they are significantly easier to crack, particularly if the attacker is on the same physical network as the target. This makes it possible for an attacker to intercept or decrypt data being transmitted, leading to potential breaches of confidentiality or unauthorized access to sensitive information. Given the relatively low barrier to exploiting this vulnerability, it poses a high security risk for the system. The recommended solution is to reconfigure the affected application, disabling these weak ciphers and replacing them with more robust encryption protocols like AES with higher key lengths, ensuring stronger protection for data in transit.  
**Recommend a remediation:** To resolve the issue of medium-strength SSL ciphers, reconfigure the server to disable these weaker ciphers, such as those with key lengths between 64 and 112 bits or using 3DES. Replace them with stronger options like AES-128 or AES-256, and ensure that the latest version of SSL libraries, such as OpenSSL, is installed. After reconfiguration, test the server to confirm only strong ciphers are in use. Regularly monitor and update the SSL/TLS configuration to maintain compliance with current security standards and reduce the risk of encryption vulnerabilities.

### Conclusion

Identify your key findings.

The vulnerability involving medium-strength SSL cipher suites (SWEET32) presents a significant security risk with a severity rating of 7.5. The issue arises from the remote service supporting SSL ciphers that use key lengths between 64 and 112 bits or outdated encryption suites like 3DES. These ciphers are relatively easy to crack, especially if the attacker is on the same physical network, which could lead to the interception or decryption of sensitive data and potential breaches of confidentiality. To mitigate this high-risk vulnerability, it is crucial to reconfigure the server to disable these weaker ciphers and switch to stronger encryption methods such as AES-128 or AES-256. Additionally, ensure that the latest SSL libraries, like OpenSSL, are used. Post-reconfiguration, thorough testing should confirm that only strong ciphers are in operation. Ongoing monitoring and updates to the SSL/TLS configuration are essential to adhere to current security standards and minimize the risk of similar vulnerabilities in the future.