

Student: Brandon Trinkle

Email: btrinkle52@gmail.com

Time on Task: 1 hour, 48 minutes

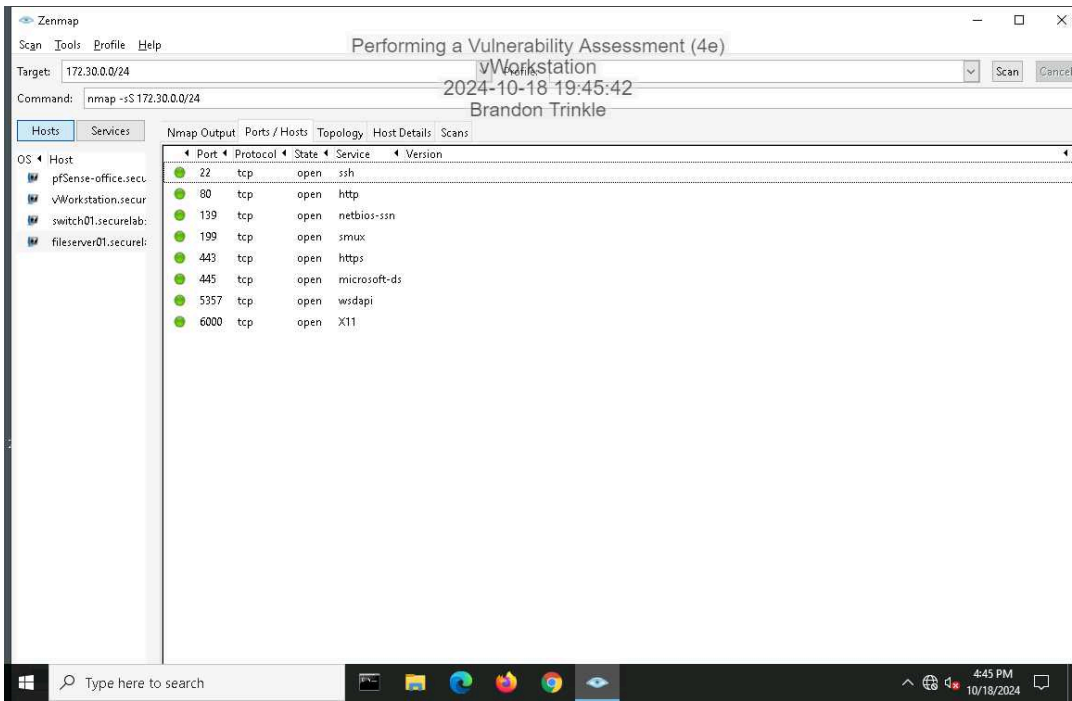
Progress: 100%

Report Generated: Friday, October 18, 2024 at 9:16 PM

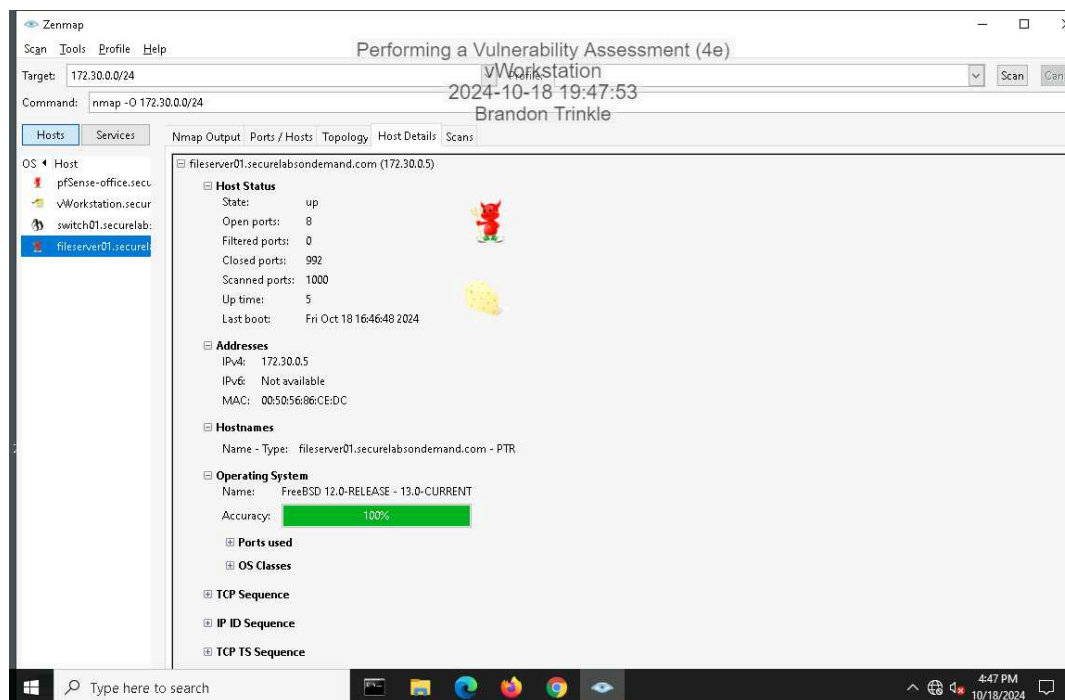
# Section 1: Hands-On Demonstration

## Part 1: Scan the Network with Zenmap

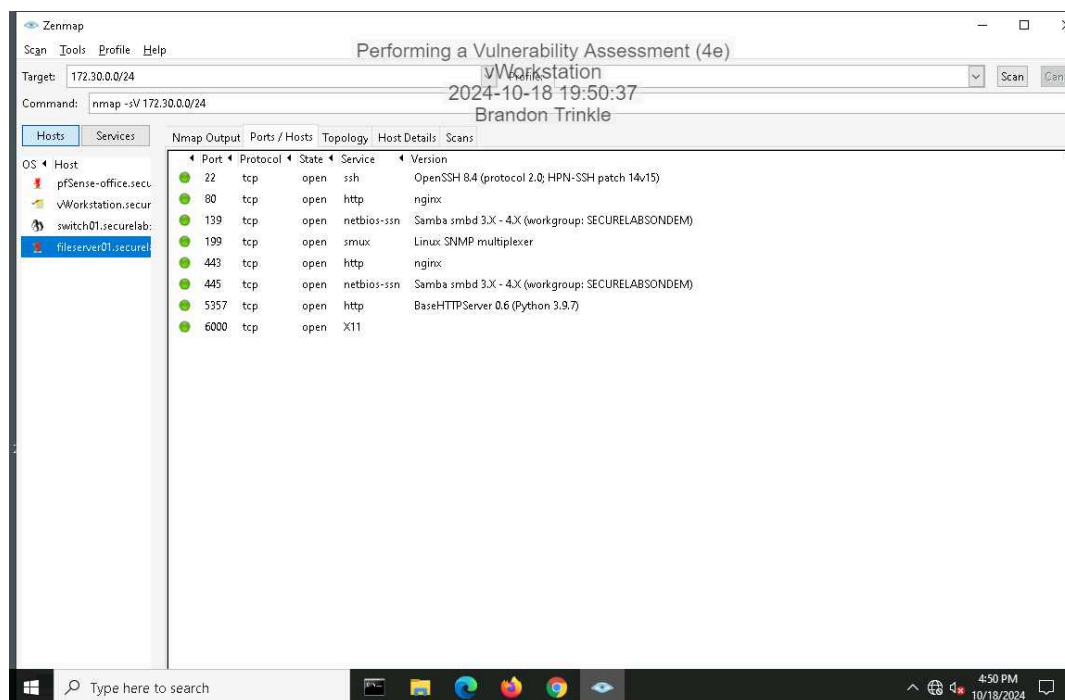
9. Make a screen capture showing the contents of the **Ports/Hosts** tab from the **SYN** scan for **fileserver01.securelabsondemand.com**.



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

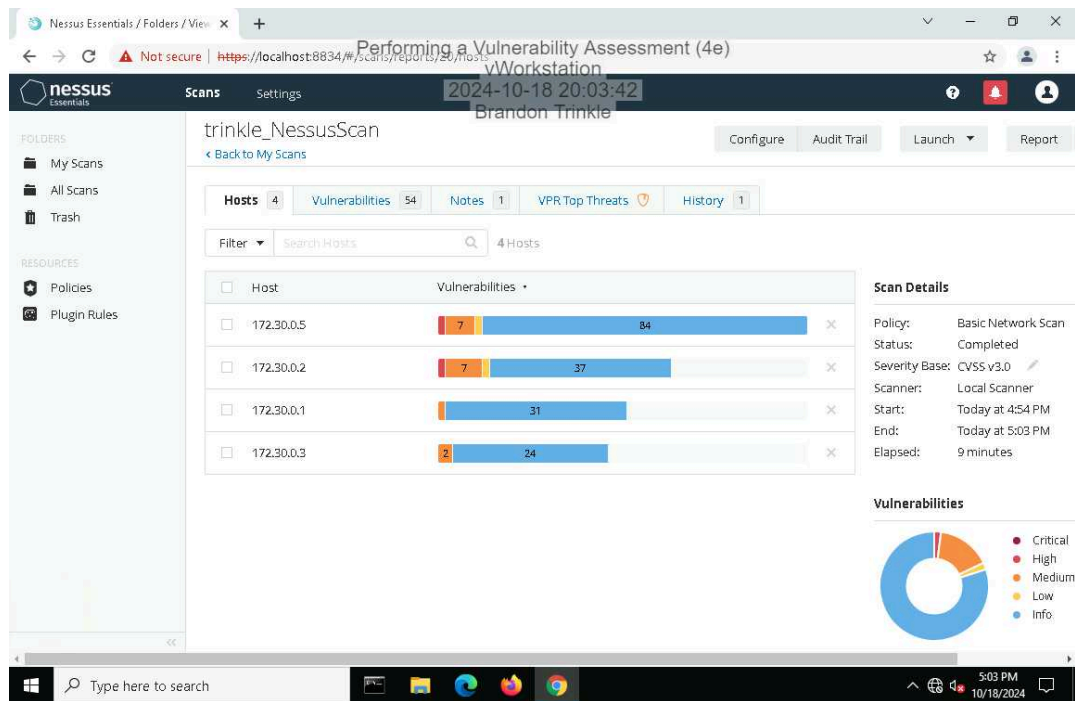


19. Make a screen capture showing the details in the **Ports/Hosts** tab from the **Service** scan for **fileserver01.securelabsondemand.com**.



## 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.

CVE-2016-2183, also known as the Sweet32 attack, is a vulnerability that affects the DES and Triple DES (3DES) encryption algorithms used in protocols like TLS, SSH, and IPsec. An attacker could exploit this flaw to decrypt sensitive information in a session, as demonstrated by attacks against HTTPS sessions that use 3DES in Cipher Block Chaining mode.

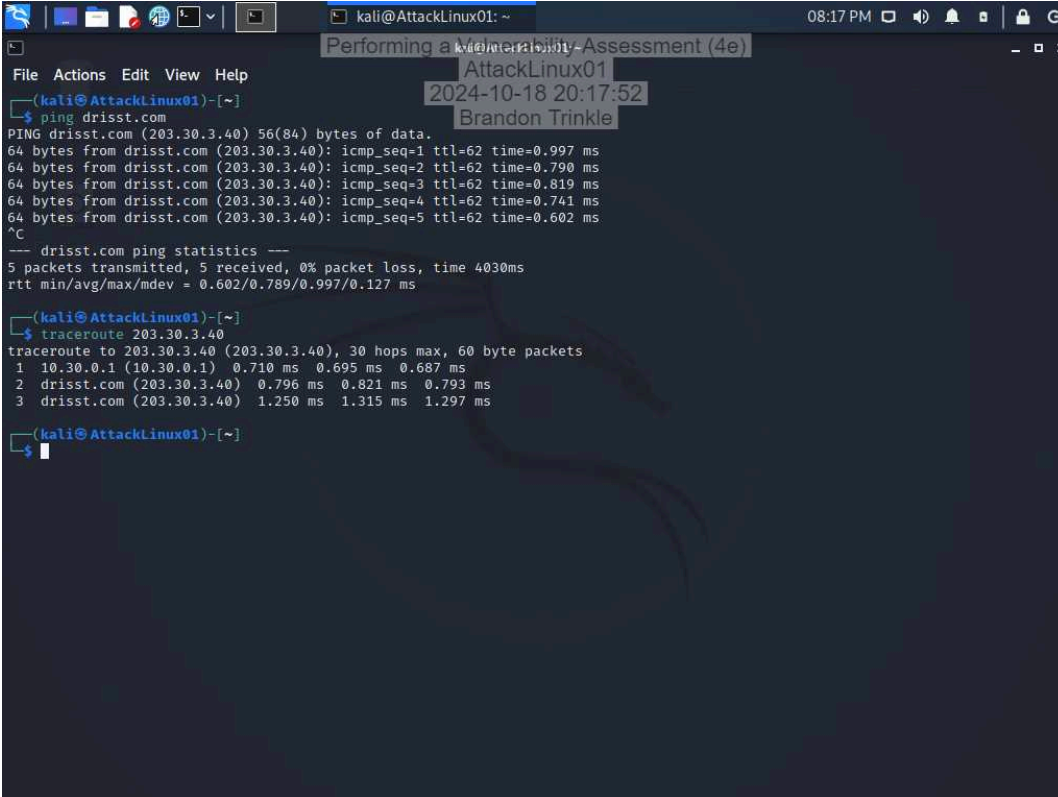
The vulnerability has been given a CVSS v3.1 base score of 7.5, which is considered high. This score reflects the fact that the attack can be carried out remotely over a network, without the need for authentication or user interaction. The primary impact of the attack is on confidentiality, while integrity and availability remain unaffected.

To mitigate this vulnerability, it is recommended to discontinue the use of DES and 3DES in encryption protocols and transition to modern algorithms like AES (Advanced Encryption Standard). For systems where 3DES must still be used, limiting the duration of encrypted sessions can reduce the risk by lowering the amount of data processed, thus decreasing the chance of a successful birthday attack. Additionally, applying security patches from vendors such as Red Hat, Oracle, and Cisco will address this vulnerability and enhance protection.

## Section 2: Applied Learning

### Part 1: Scan the Network with Nmap

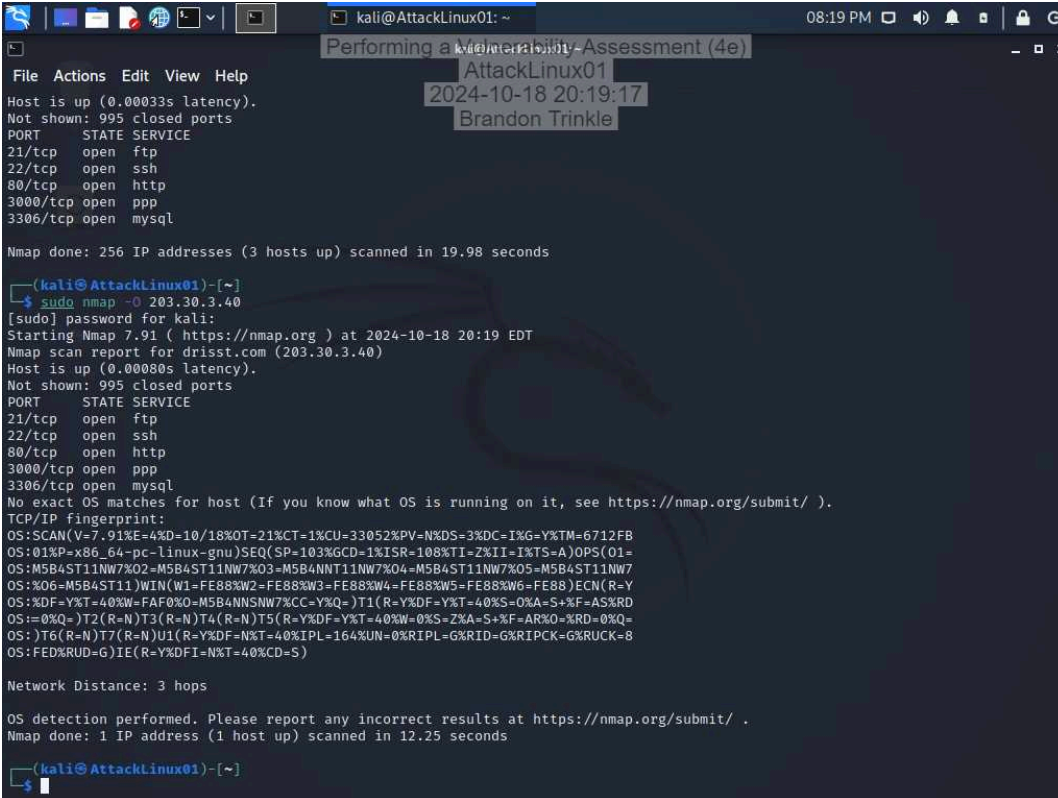
6. Make a screen capture showing the results of the traceroute command.



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=0.997 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=0.790 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.819 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=0.741 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=0.602 ms  
^C  
--- drisst.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4030ms  
rtt min/avg/max/mdev = 0.602/0.789/0.997/0.127 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) 0.710 ms 0.695 ms 0.687 ms  
 2 drisst.com (203.30.3.40) 0.796 ms 0.821 ms 0.793 ms  
 3 drisst.com (203.30.3.40) 1.250 ms 1.315 ms 1.297 ms  
  
kali@AttackLinux01: ~  
$
```

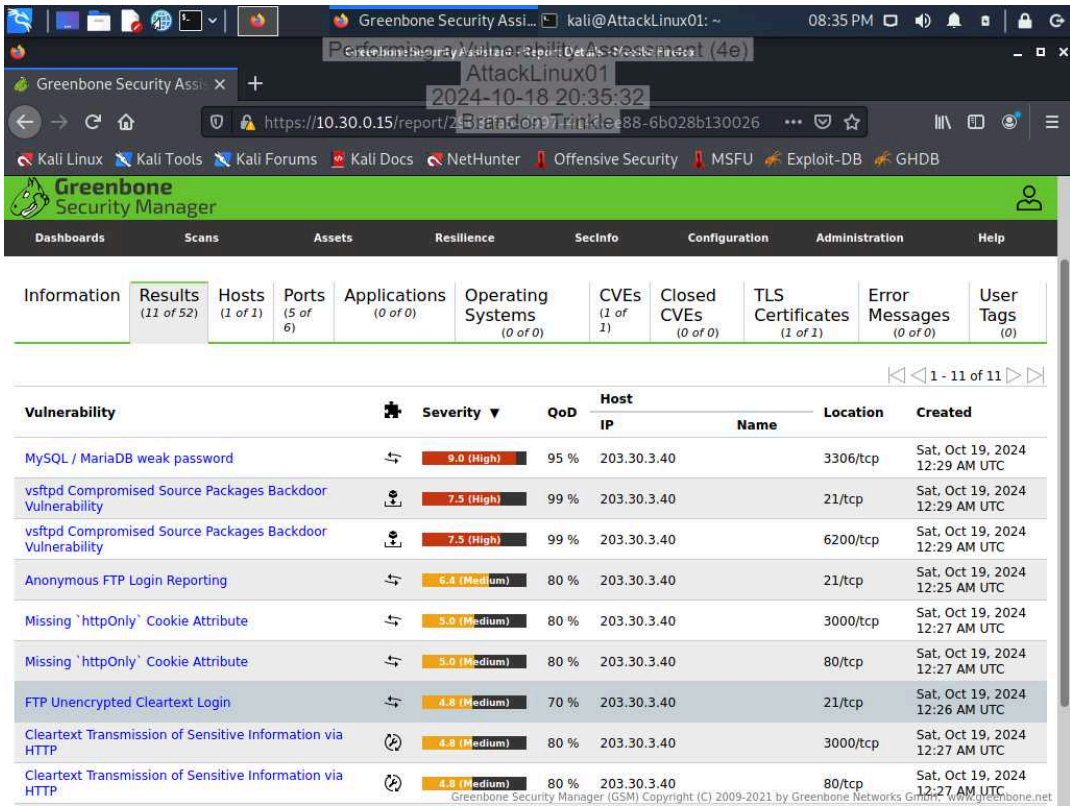
10. Make a screen capture showing the results of the Nmap scan with OS detection activated.



```
kali@AttackLinux01: ~  
File Actions Edit View Help  
Host is up (0.00033s 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 19.98 seconds  
  
kali@AttackLinux01: ~  
$ sudo nmap -O 203.30.3.40  
[sudo] password for kali:  
Starting Nmap 7.91 ( https://nmap.org ) at 2024-10-18 20:19 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=10/18%OT=21%CT=1%CU=33052%PV=N%DS=3%DC=I%G=Y%TM=6712FB  
OS:01%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=108%TI=Z%II=I%TS=A)OPS(O1=  
OS:M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7  
OS:06=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=0%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=8  
OS:FED%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 12.25 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 drisst.com web server. This server hosts several web applications and is critical to the operations of the organization. The test aims to assess the security posture of the server and identify vulnerabilities that could be exploited by attackers.

Completed by

Insert your name here.

Brandon Trinkle

### On

Insert current date here.

10/18/2024

### Purpose

Identify the purpose of the penetration test.

The purpose of this penetration test is to identify and evaluate high-severity vulnerabilities in the drisst.com web server. The test was commissioned by the organization to understand potential security risks and prevent any unauthorized access or data breaches. Specifically, the focus is on testing the server using non-destructive techniques to avoid service disruption while assessing vulnerabilities identified by OpenVAS.

### Scope

Identify the scope of the penetration test.

The scope of this penetration test was defined to ensure that the test was comprehensive yet limited to non-destructive actions. The drisst.com web server was the sole target of the test, and the penetration tester was restricted to using vulnerability scanning tools that did not involve exploit attempts or disruption of service. The focus of the test was to identify three high-severity vulnerabilities as flagged by OpenVAS. These vulnerabilities were evaluated to understand their potential risks and propose mitigation strategies.

### 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.

During the penetration test, several vulnerabilities of varying severity were identified on the drisst.com web server. One of the most critical findings was the presence of weak passwords for the MySQL/MariaDB service, which poses a significant security risk. This vulnerability, classified with a severity score of 9.0 (High), indicates that the database service running on port 3306/tcp is using either weak or default credentials. If exploited, an attacker could potentially gain unauthorized access to the database, leading to data theft, modification, or even full control of the service. It is recommended that strong password policies be enforced immediately, ensuring all database accounts are secured with complex, unique passwords.

Another critical vulnerability, with a severity score of 7.5 (High), relates to a compromised source package in the vsftpd service running on ports 21/tcp and 6200/tcp. This vulnerability suggests that the vsftpd software used by the server may have been backdoored, which could allow an attacker to gain unauthorized access or execute arbitrary commands on the system. To mitigate this risk, it is crucial to verify the integrity of the vsftpd installation and reinstall the service from a trusted source if necessary.

Additionally, the server was found to have a medium-severity issue concerning anonymous FTP login reporting. Although less critical, this vulnerability (severity 6.4) could still allow an attacker to gain insight into the server's directory structure or access non-sensitive files. Remediation for this issue includes disabling anonymous login or properly securing the FTP service to prevent unauthorized access.

### Conclusion

Identify your key findings.

The penetration test of the drisst.com web server uncovered several critical vulnerabilities that require immediate attention to protect the organization from potential security breaches. The most severe issue identified was the use of weak passwords for the MySQL/MariaDB service, which could allow attackers to easily gain unauthorized access to the database, leading to significant data compromise or system manipulation. Additionally, a backdoor vulnerability in the vsftpd service was found, which could enable remote attackers to exploit the server through compromised source packages. Although slightly less critical, the server was also found to allow anonymous FTP logins, which could expose parts of the file system to unauthorized users. These vulnerabilities, if left unaddressed, could lead to data breaches, system compromise, and unauthorized access to sensitive information.

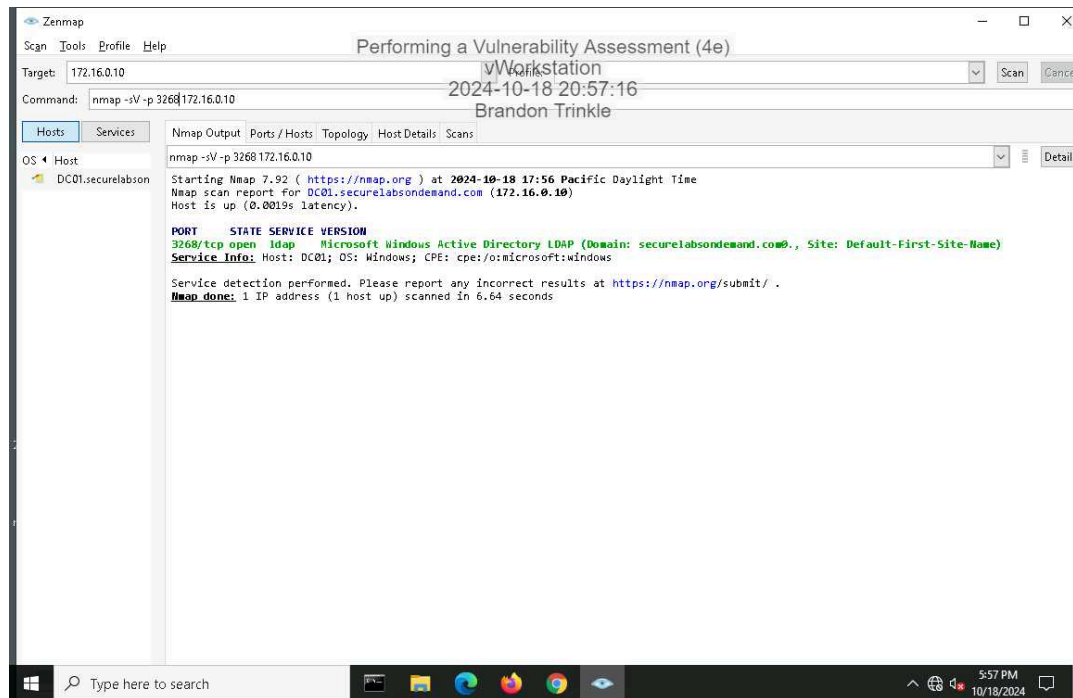
It is recommended that the organization immediately implement strong password policies for all services, verify the integrity of installed software (such as vsftpd), and properly configure the FTP service to disable anonymous logins.



### Section 3: Challenge and Analysis

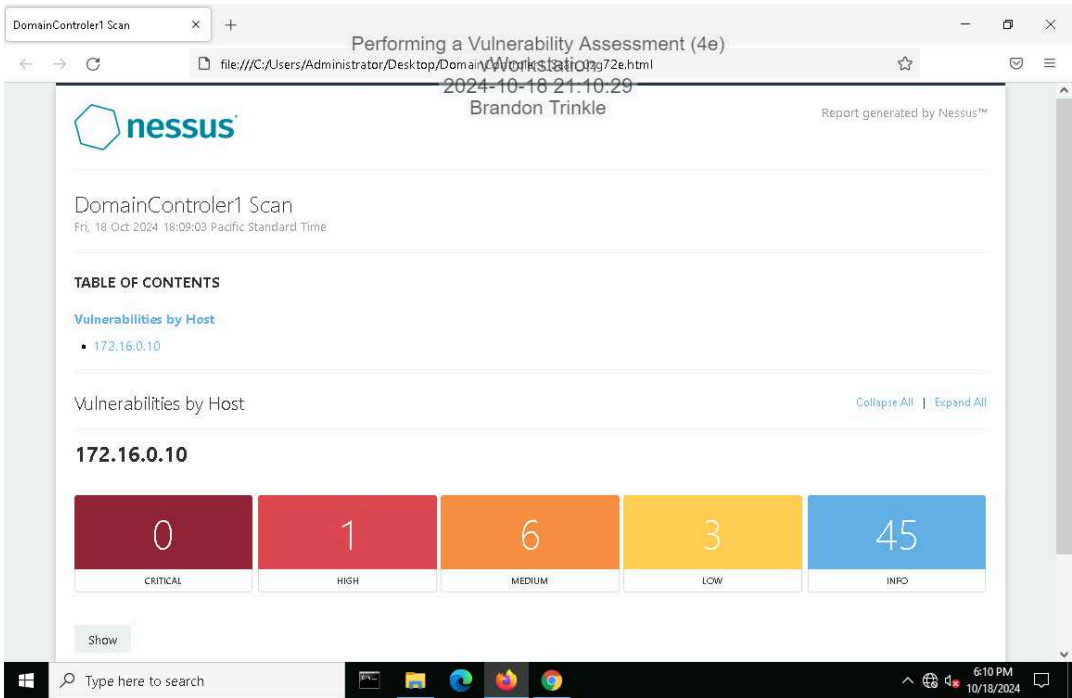
#### Part 1: Scan the Domain Controller with Nmap

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.

The target of this penetration test is the domain controller (IP address: 172.16.0.10).

Completed by

Insert your name here.

Brandon Trinkle

On

Insert current date here.

10/18/2024

### Purpose

Identify the purpose of the penetration test.

The purpose of this penetration test is to evaluate the security posture of the DomainController1. Specifically, the test aims to identify high-severity vulnerabilities that could expose the system to potential attacks or unauthorized access. This assessment follows a request by the organization after the initial test on their web server and focuses on identifying weaknesses within their internal LAN.

### Scope

Identify the scope of the penetration test.

The scope of this test was limited to scanning the domain controller with Nessus for vulnerabilities. The scan was performed with a Basic Network Scan targeting the domain controller (IP: 172.16.0.10) and focused on identifying high-severity vulnerabilities that may affect the security of the system. This test was non-intrusive, and no exploitation of vulnerabilities was conducted.

### 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.

The Nessus vulnerability scan on the domain controller identified a high-severity issue related to the use of medium-strength SSL/TLS cipher suites, specifically the vulnerability known as SWEET32. This vulnerability, with a CVSS score of 7.5, exposes the system to potential attacks that target long-lived SSL/TLS connections using 64-bit block ciphers like 3DES. An attacker could exploit this vulnerability by performing a birthday attack, potentially decrypting sensitive information or compromising the confidentiality of communications over the network. The domain controller's reliance on outdated cryptographic standards increases the risk of sensitive data exposure. To mitigate this risk, it is recommended that the organization disable medium-strength ciphers and enforce the use of stronger, modern encryption algorithms in their SSL/TLS configuration. Regular reviews of cryptographic settings should also be conducted to ensure ongoing compliance with security best practices.

### Conclusion

Identify your key findings.

The Nessus scan revealed a significant vulnerability in the domain controller's SSL/TLS configuration, specifically the support of medium-strength ciphers vulnerable to the SWEET32 attack. This high-severity vulnerability poses a risk to the confidentiality and integrity of sensitive communications. Immediate remediation is necessary to prevent potential attacks, and the organization should update their SSL/TLS configurations to ensure only strong ciphers are used. Addressing this issue will help secure the domain controller and maintain the security of communications within the Secure Labs on Demand network.