

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Student:

Sadam Hashi

Email:

smhashi@asu.edu

Time on Task:

14 hours, 53 minutes

Progress:

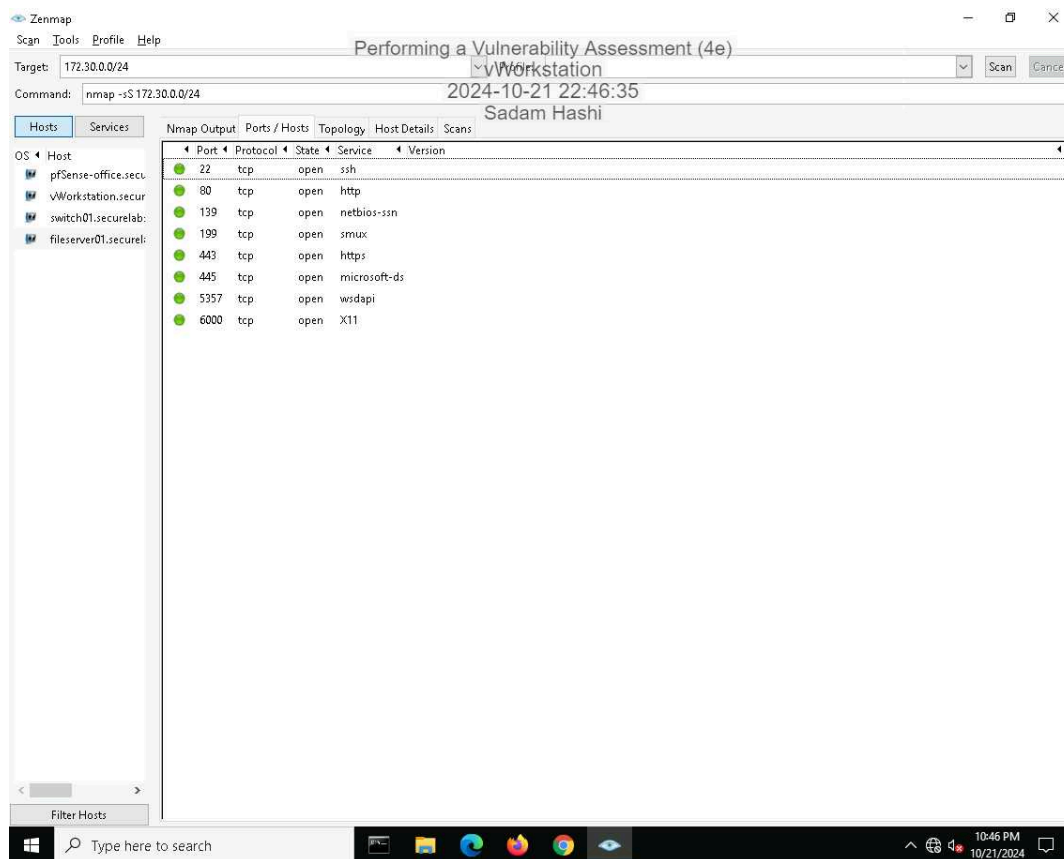
100%

Report Generated: Thursday, October 24, 2024 at 1:38 AM

Section 1: Hands-On Demonstration

Part 1: Scan the Network with Zenmap

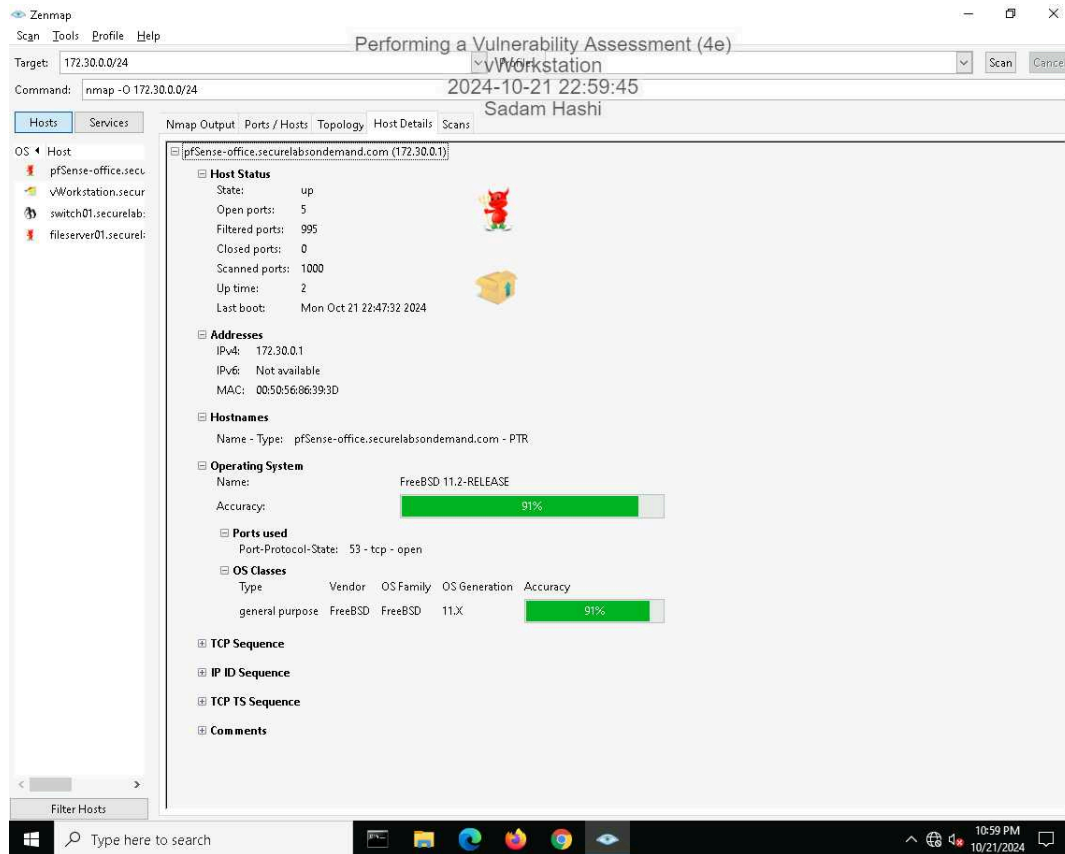
9. **Make a screen capture** showing the contents of the **Ports/Hosts** tab from the **SYN** scan for **fileserver01.securelabsondemand.com**.



Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

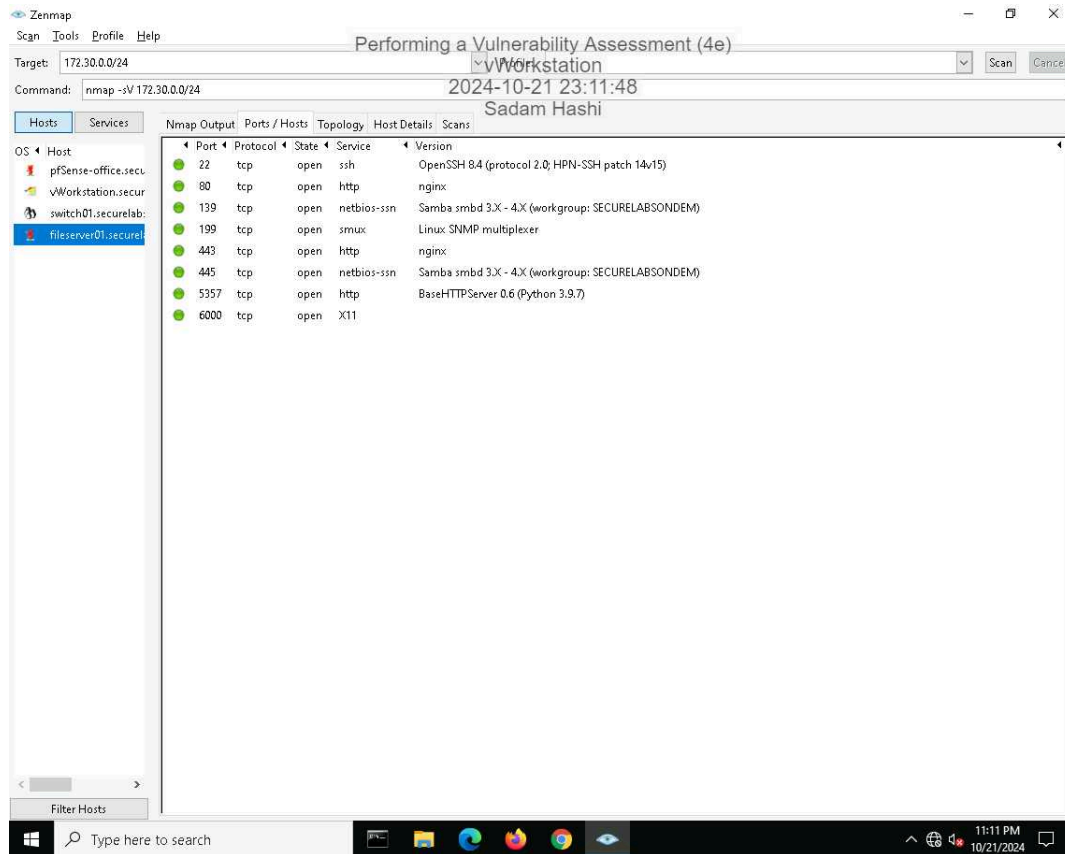
15. **Make a screen capture** showing the contents of the **Host Details** tab from the OS scan for **fileserver01.securelabondemand.com**.



Performing a Vulnerability Assessment (4e)

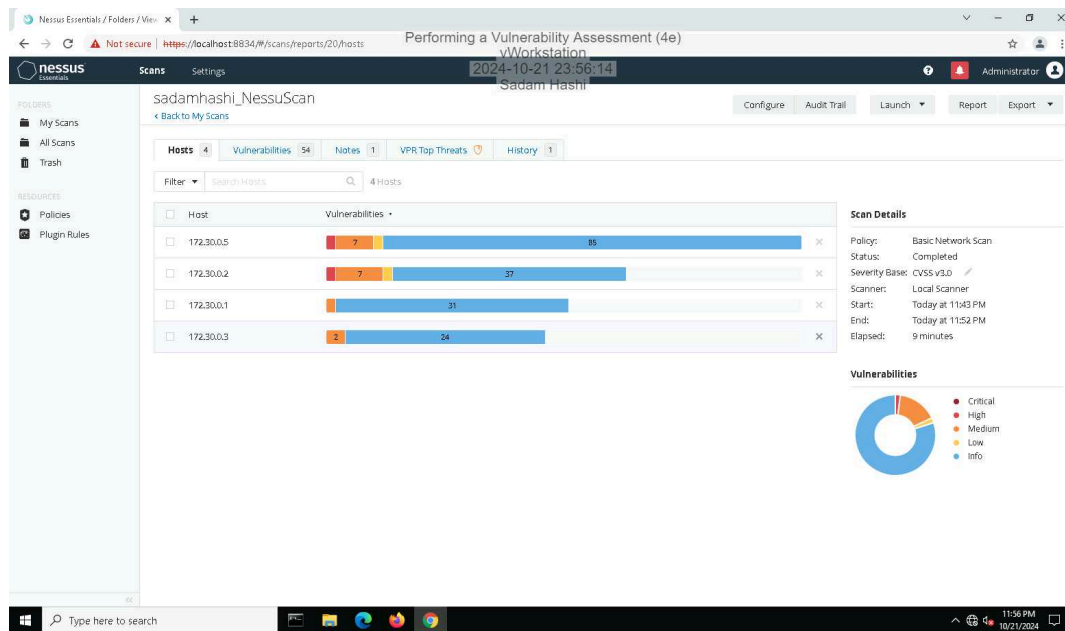
Fundamentals of Information Systems Security, Fourth Edition - Lab 02

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.

Vulnerability: SSH Weak Algorithms Supported

Nessus Plugin ID: 90317

CVSS: 4.3

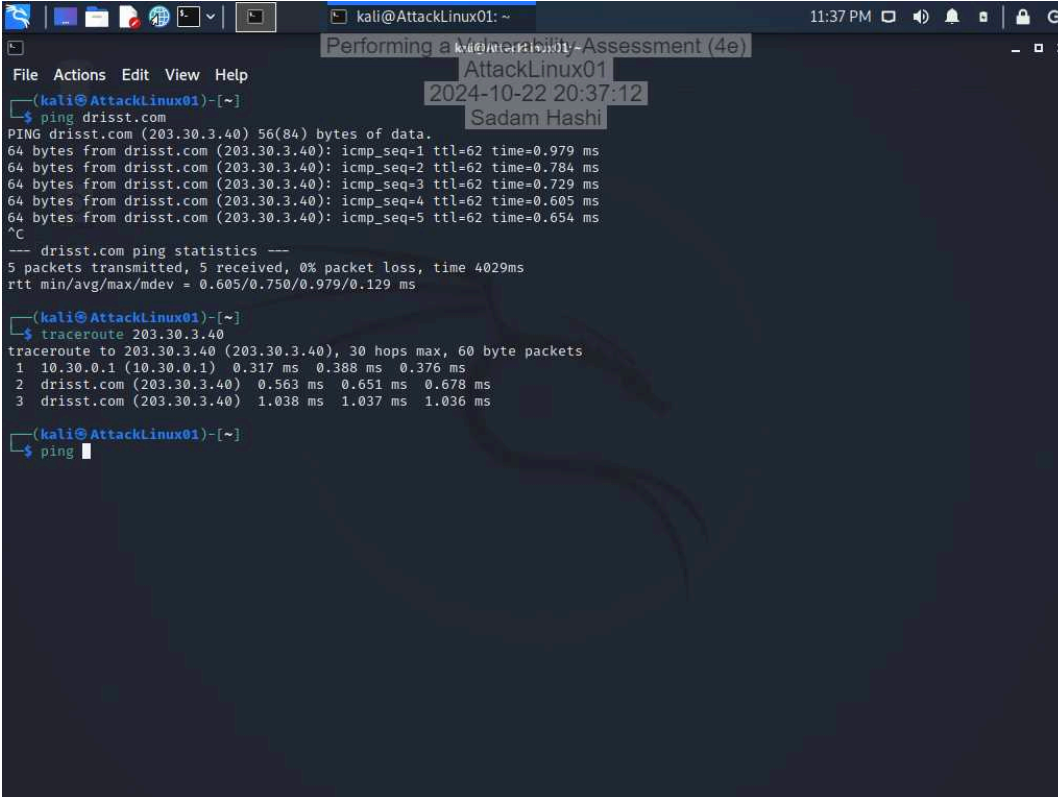
Summary: The vulnerability Nessus identified suggests that the remote Secure Shell (SSH) is configured to support weak encryption algorithms such as "Arcfour" or no encryption at all. The Arcfour cipher is known to have issues with weak keys and be vulnerable to attacks.

Mitigation strategy: Remove Arcfour stream cipher and configure SSH server to a robust cipher. Contact the vendors for guidance or review product documentation.

Section 2: Applied Learning

Part 1: Scan the Network with Nmap

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

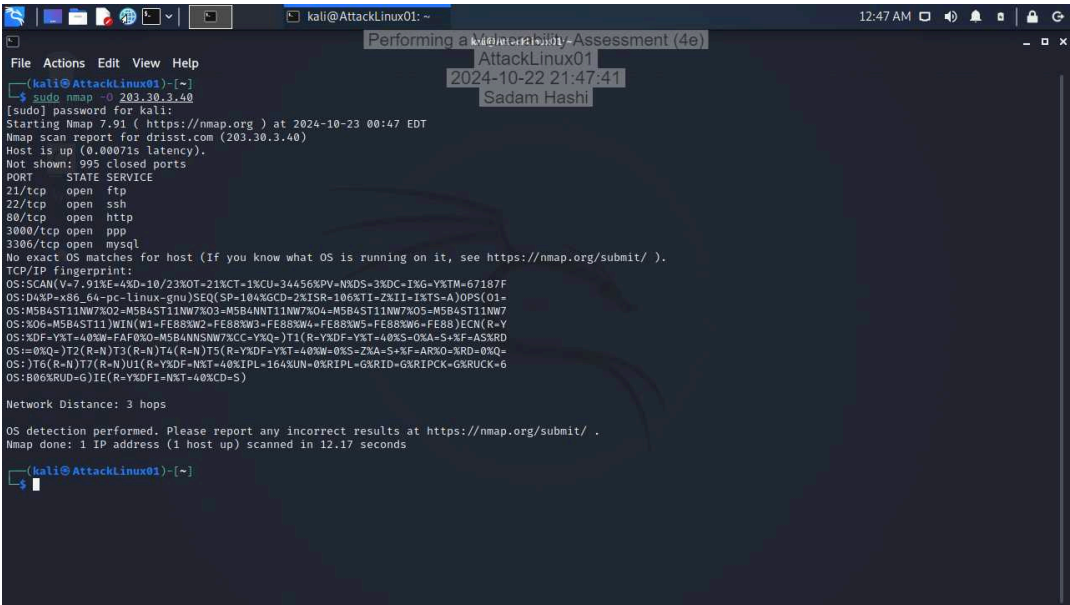


The screenshot shows a Kali Linux terminal window with the following content:

```
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=0.979 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=0.784 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.729 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=0.605 ms  
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=0.654 ms  
^C  
--- drisst.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4029ms  
rtt min/avg/max/mdev = 0.605/0.750/0.979/0.129 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)  0.317 ms  0.388 ms  0.376 ms  
 2 drisst.com (203.30.3.40)  0.563 ms  0.651 ms  0.678 ms  
 3 drisst.com (203.30.3.40)  1.038 ms  1.037 ms  1.036 ms  
  
(kali@AttackLinux01)-[~]  
$ ping
```

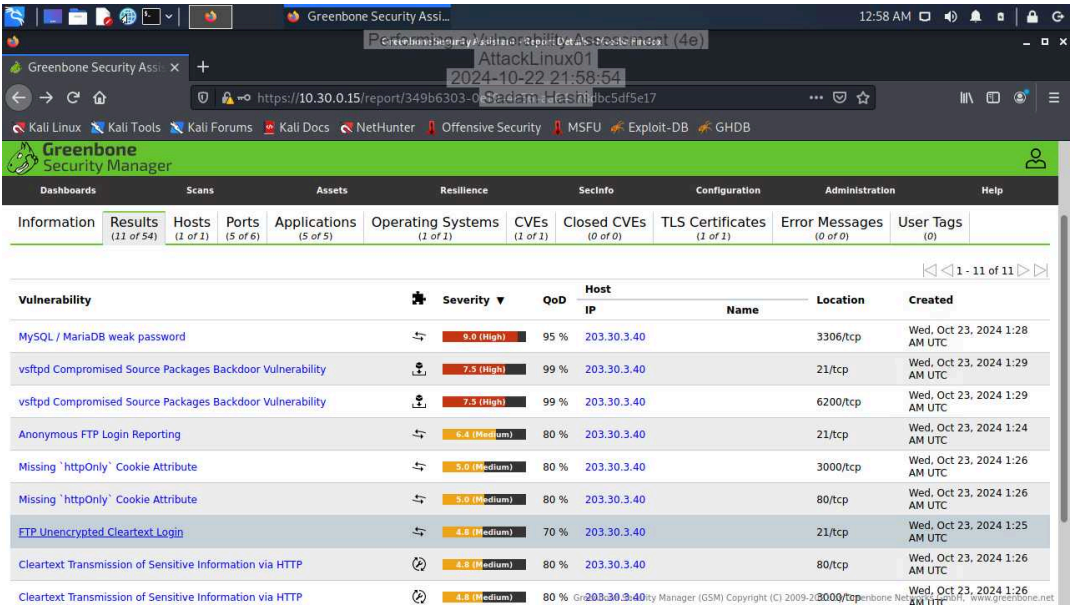
Overlaid on the terminal window are three semi-transparent labels: "Performing a Vulnerability Assessment (4e)" at the top, "AttackLinux01" in the middle, and "2024-10-22 20:37:12" and "Sadam Hashi" at the bottom.

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

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Target

Insert the target here.

The target for this penetration test is a web server hosting drisst.com, which is operated by Secure Labs on Demand, and the main goal of this test is to identify security vulnerabilities through a vulnerability scan.

Completed by

Insert your name here.

Sadam Hashi

On

Insert current date here.

10/23/2024

Purpose

Identify the purpose of the penetration test.

The purpose of this penetration test is to identify any security weaknesses present in the drisst.com server. By assessing the vulnerabilities present in the system, certain measures will be taken to enhance the organization's current security stance.

Scope

Identify the scope of the penetration test.

The scope of this penetration test is constricted to using OpenVAS and Nmap for a vulnerability scan on the drisst.com web server. The penetration tester has the consent of the organization to identify vulnerabilities in the system without resorting to a destructive scan that negatively affects the web server. This means that the tester is to exclude other services and systems within the organization.

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 1 is "MySQL / MariaDB Weak Password." The CVSS Base(Severity) is 9.0(high). The issue here is that the database Maria is using a weak password, which can be guessed. Any sort of successful exploitation leads to an attacker accessing the database information. The recommendation is to strengthen the MariaDB password immediately. The more complex the password is, the better. Vulnerability 2 is "vsftpd Compromised Source Packages Backdoor Vulnerability." The CVSS Base(Severity) is 7.5(high). The identified issue with a QoD of 99%, is that vsftpd service is utilizing compromised source packages containing a backdoor vulnerability. The attackers can exploit this issue using unpredictable commands, which will compromise the server and allow the attacker to gain control. The recommended solution is to update vsftpd to its latest version and remove any current compromised packages from the system. Vulnerability 3 is "vsftpd Compromised Source Packages Backdoor Vulnerability". The CVSS Base(Severity) is 7.5(high). The issue is the same as the previous one, the vsftpd service is having a backdoor vulnerability due to compromised source packages. The solution is the same as the previous issue, update vsftpd to its latest version and remove any compromised source packages.

Conclusion

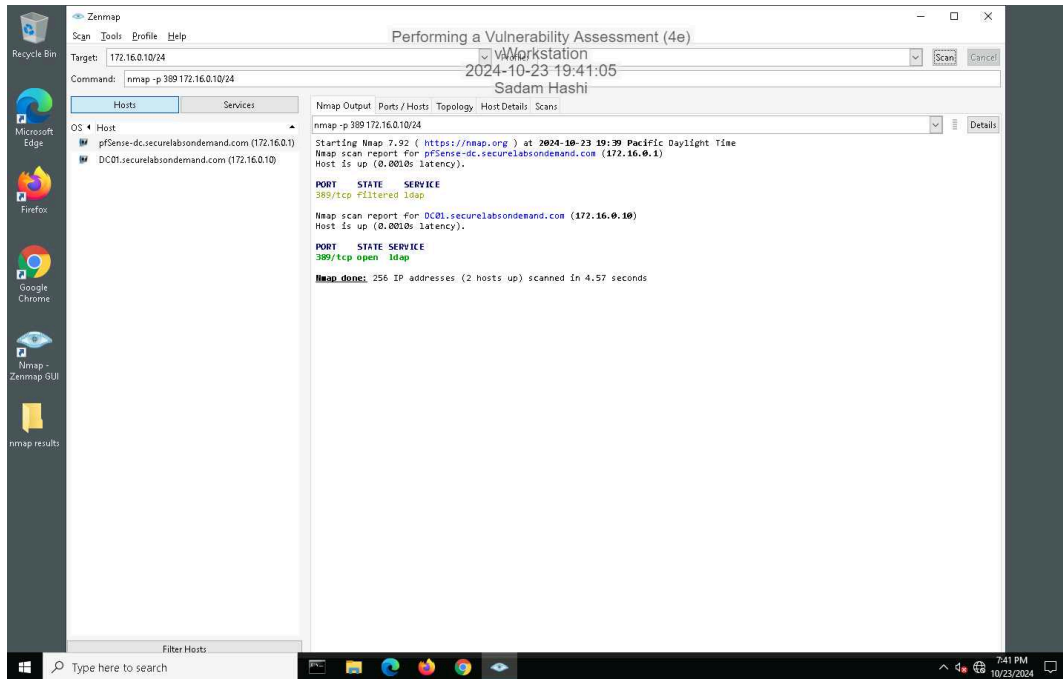
Identify your key findings.

This penetration test has successfully revealed 3 high-severity vulnerabilities in the drisst.com web server. Each of these vulnerabilities poses a serious risk to the organizations overall security. The organization should mitigate these high-severity risks by implementing provided solutions such as strengthening the current SQL / MariaDB password and updating vsftpd to its latest version while deleting any compromised packages from the system. These solutions need to be implemented immediately. The organization should conduct more vulnerability scans and penetration tests in order to reduce any future risks that will compromise and detriment the organization's security.

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.

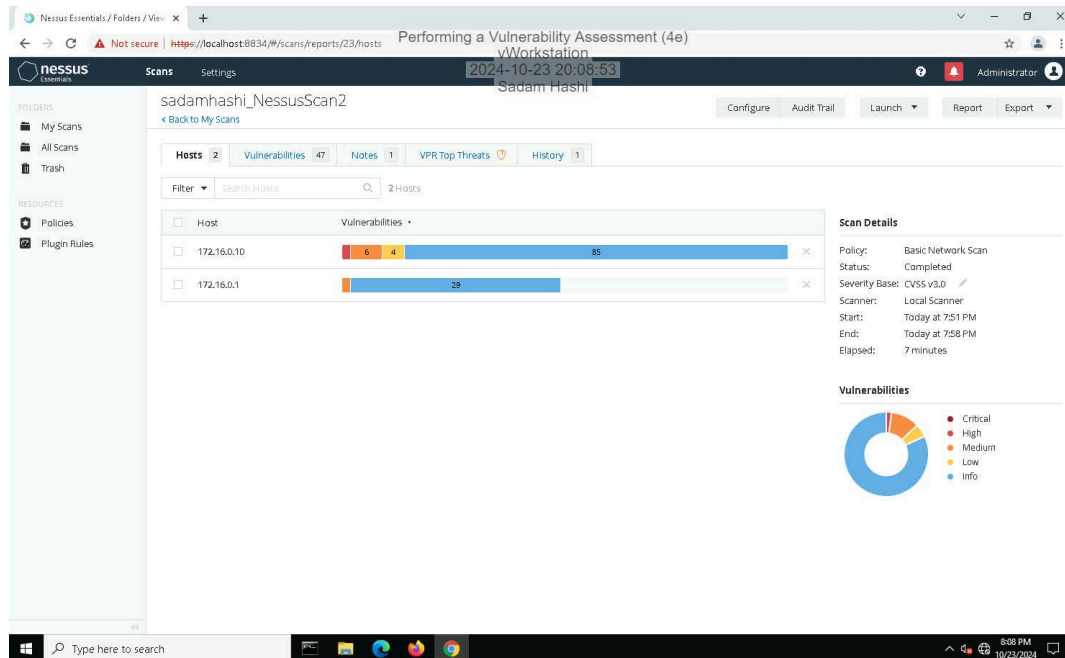


Part 2: Scan the Domain Controller with Nessus

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.

The target of this penetration test is the domain controller labeled DomainController01(IP address: 172.16.1.10) which is a server managing network for Secure Labs on Demand. The objective of this test was to assess for any security vulnerabilities through a regular network scan.

Completed by

Insert your name here.

Sadam Hashi

On

Insert current date here.

10/23/2024

Purpose

Identify the purpose of the penetration test.

The main purpose of this penetration test to identify any security vulnerabilities on the domaincontroller01 and assess what sorts of risks these vulnerabilities present to Secure Labs on Demand. Domain controllers are very important to any organization's infrastructure. This test is needed in order to halt to or prevent any attacks to the system.

Scope

Identify the scope of the penetration test.

The scope of the penetration test was limited to a network vulnerability scan of DomainController01. Nmap was used to identify any sort of open ports in the domain controller, mostly targeting an LDAP service devices. Then Nessus was used to perform a basic network scan to identify any vulnerabilities. The test was conducted within the confines of not causing any destruction or exploiting the system.

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 is "SSL Medium Strength Cipher Suites Supported (SWEET32)." The CVSS Base(Severity) is 7.5(high). The domain controller service supports the use of medium strength SSL ciphers which is prominent for being vulnerable to SWEET32 attacks, a vulnerability that exploits block cipher collisions. This vulnerability comes from the use of encryption that uses key lengths at least 64 bits and less than 112 bits or even 3DES which a black cipher that encrypts data. A CVE released a major security vulnerability in the 3DES, advising the any usage of it. An attacker can decrypt some portions of an encrypted data due to this vulnerability. The recommendation is to disable the use of the 64 64-bit block cipher suites, including 3DES on the domain controller. Reconfigure the system with more secure secure cipher suites to negate any compromises to the server.

Conclusion

Identify your key findings.

The penetration test was conducted on behalf of Secure Labs on Demand to identify a high-severity vulnerability in DomainController01. Any exploitation due to this vulnerability will expose sensitive information to the attacker and possibility of an unauthorized misuse of the information. The recommended solution was to get disable the 64-bit black cipher suites including 3DES, and implement robust encryption method. Consistent vulnerability scans is required to maintain a strong security stance and keep the system's integrity intact.