

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Student:

Matias Kun

Email:

rkh4zx@virginia.edu

Time on Task:

8 hours, 16 minutes

Progress:

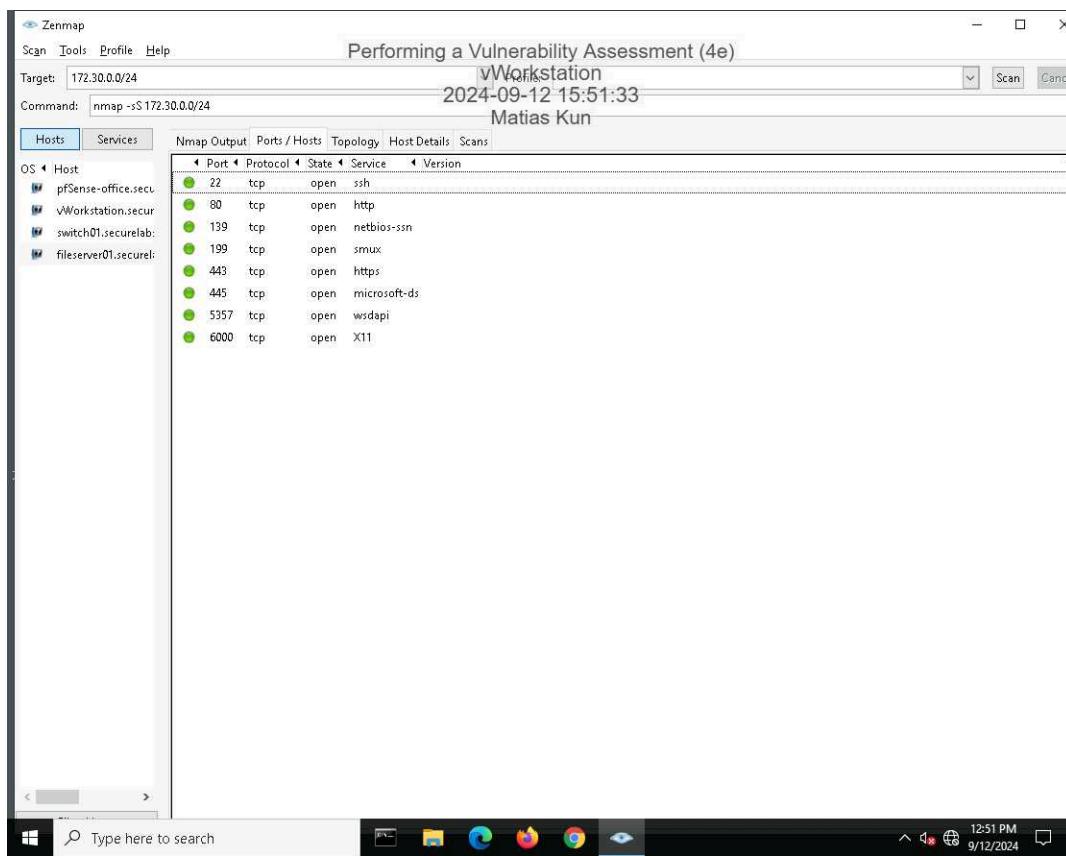
100%

Report Generated: Thursday, September 12, 2024 at 7:50 PM

Section 1: Hands-On Demonstration

Part 1: Scan the Network with Zenmap

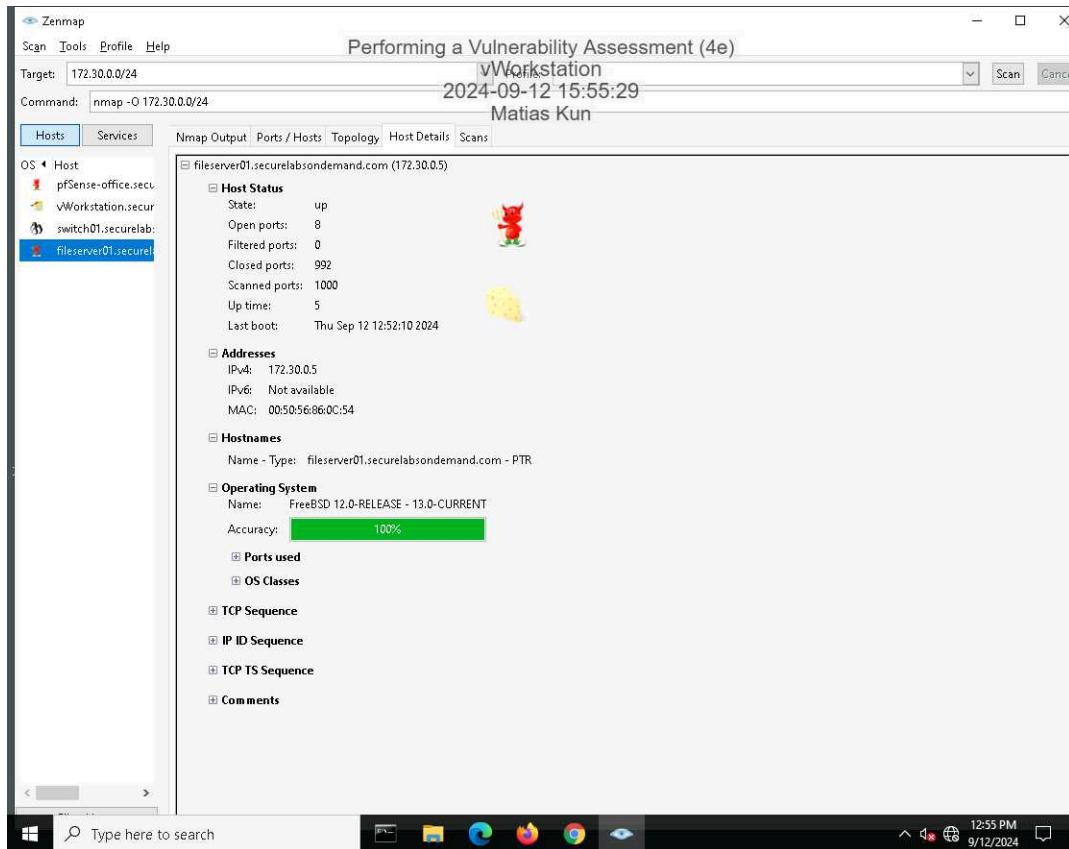
9. Make a screen capture showing the contents of the **Ports/Hosts** tab from the SYN scan for **fileserver01.securelabsondemand.com**.



Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

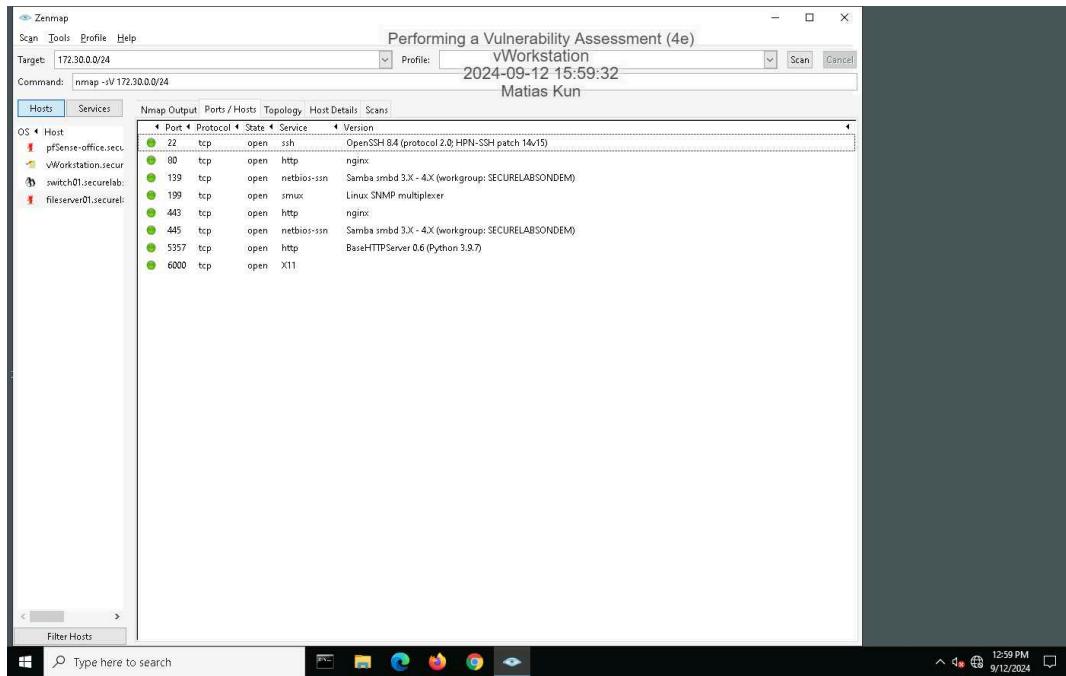
15. Make a screen capture showing the contents of the **Host Details** tab from the OS scan for **fileserver01.securelabsondemand.com**.



Performing a Vulnerability Assessment (4e)

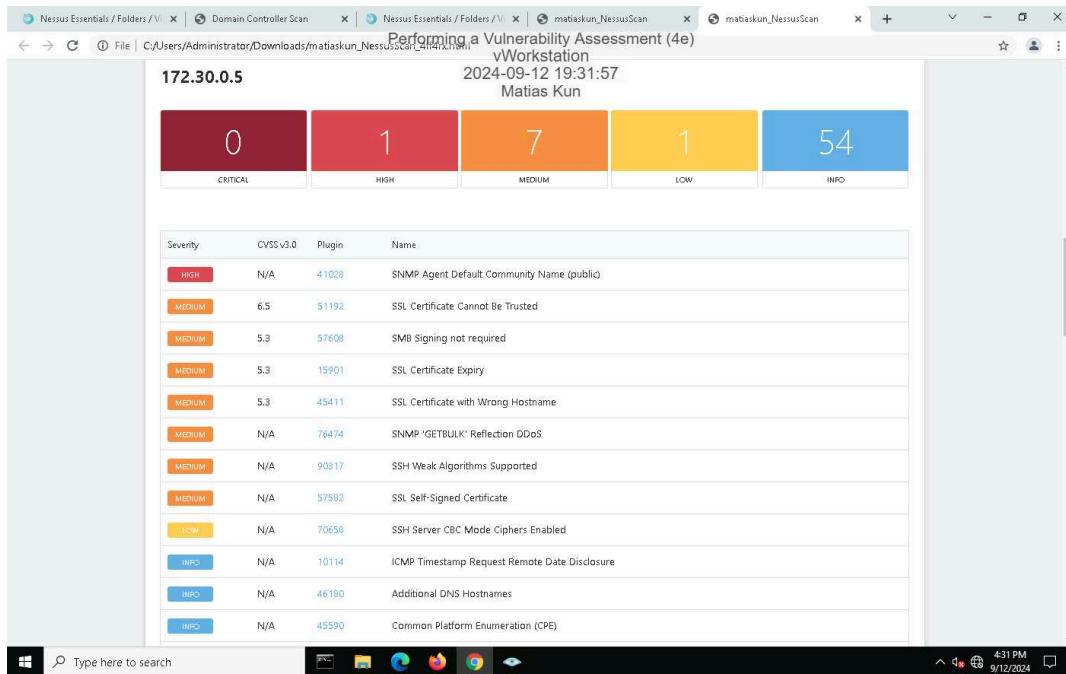
Fundamentals of Information Systems Security, Fourth Edition - Lab 02

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

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

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

The medium vulnerability I have selected, I have selected plugin ID 15901. Plugin ID 15901 is when the SSL Certificate has expired. The CVSS risk score is 5.3 in v3 (equivalent to 5 in v2). The recommended solution or mitigation strategy is to either purchase or generate a new SSL certificate to replace the already expired one. Along with that, a policy implementation for when to replace SSL certificates when expiration is ahead.

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)
File Actions Edit View Help
AttackLinux01
2024-09-12 16:43:39
64 bytes from drisst.com (203.30.3.40): icmp_seq=102 ttl=62 time=0.814 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=103 ttl=62 time=0.717 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=104 ttl=62 time=0.739 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=105 ttl=62 time=1.03 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=106 ttl=62 time=0.853 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=107 ttl=62 time=0.833 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=108 ttl=62 time=1.09 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=109 ttl=62 time=0.723 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=110 ttl=62 time=0.896 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=111 ttl=62 time=0.893 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=112 ttl=62 time=0.754 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=113 ttl=62 time=0.865 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=114 ttl=62 time=0.913 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=115 ttl=62 time=0.988 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=116 ttl=62 time=1.01 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=117 ttl=62 time=0.856 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=118 ttl=62 time=0.855 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=119 ttl=62 time=0.839 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=120 ttl=62 time=0.756 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=121 ttl=62 time=0.624 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=122 ttl=62 time=0.844 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=123 ttl=62 time=0.839 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=124 ttl=62 time=0.714 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=125 ttl=62 time=0.775 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=126 ttl=62 time=0.738 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=127 ttl=62 time=0.879 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=128 ttl=62 time=0.892 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=129 ttl=62 time=0.957 ms
^C
--- drisst.com ping statistics ---
129 packets transmitted, 129 received, 0% packet loss, time 128890ms
rtt min/avg/max/mdev = 0.522/0.884/1.515/0.134 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) 0.274 ms 0.412 ms 0.386 ms
2 drisst.com (203.30.3.40) 0.590 ms 0.873 ms 0.667 ms
3 drisst.com (203.30.3.40) 0.751 ms 0.596 ms 0.598 ms

[(kali㉿AttackLinux01) ~]$
```

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

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

The screenshot shows a terminal window titled "Performing a Vulnerability Assessment (4e)" running on "AttackLinux01". The terminal displays the output of an Nmap scan for the IP address 203.30.3.40. The scan results show various open ports (21/tcp, 22/tcp, 80/tcp, 3000/tcp, 3306/tcp) and services (ftp, ssh, http, ppp, mysql). The OS detection section at the bottom provides a detailed fingerprint of the target system, identifying it as "M5B4ST11NW7%03-M5B4NT11NW7%04-M5B4ST11NW7%05-M5B4ST11NW7%06-FE88" with a confidence level of 91%. The command used was "sudo nmap -O 203.30.3.40".

```
Host is up (0.00047s 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 19.79 seconds

(kali㉿AttackLinux01)~
└─$ sudo nmap -O 203.30.3.40
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-09-12 16:45 EDT
Nmap scan report for drisst.com (203.30.3.40)
Host is up (0.00083s 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=7.91E+4%D=9/12%OT=21%CT=1%CU=40/202%PV=N%DS=3%DC=I%G=Y%TM=66E352D
OS:DPR=x86_64-pc-linux-gnu|SEQ(SP=10%GC=1%SR=10%CTT=1%II=1%TS=A)OPS(O1=M
OS:5B4ST11NW7%02-M5B4ST11NW7%03-M5B4NT11NW7%04-M5B4ST11NW7%05-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%0-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=ARX0=%RD=0%Q=)
OS:T6(R-N)T7(R-N)U1(R=Y%DF=N%T=40%PL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=B4
OS:3%ARUD=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 12.26 seconds
```

Part 2: Conduct a Vulnerability Scan with OpenVAS

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

13. Make a screen capture showing the detailed OpenVAS scan results.

The screenshot shows the Greenbone Security Manager web interface. The title bar indicates the page is 'Performing a Vulnerability Assessment (4e)' and the target is 'AttackLinux01'. The date and time are listed as '2024-09-12 17:09:50'. The main content area is a table titled 'Vulnerability' with the following columns: Severity, QoD, Host IP, Name, Location, and Created. The table lists various security issues found on the target host:

| Vulnerability | Severity | QoD | Host IP | Name | Location | Created |
|--|--------------|------|-------------|-------------|-------------------------------|---------|
| MySQL / MariaDB weak password | 9.0 (High) | 95 % | 203.30.3.40 | 3306/tcp | Thu, Sep 12, 2024 8:59 PM UTC | |
| vsftpd Compromised Source Packages Backdoor Vulnerability | 7.5 (High) | 99 % | 203.30.3.40 | 21/tcp | Thu, Sep 12, 2024 8:59 PM UTC | |
| vsftpd Compromised Source Packages Backdoor Vulnerability | 7.5 (High) | 99 % | 203.30.3.40 | 6200/tcp | Thu, Sep 12, 2024 8:59 PM UTC | |
| Anonymous FTP Login Reporting | 6.4 (Medium) | 80 % | 203.30.3.40 | 21/tcp | Thu, Sep 12, 2024 8:55 PM UTC | |
| Missing 'httpOnly' Cookie Attribute | 5.0 (Medium) | 80 % | 203.30.3.40 | 3000/tcp | Thu, Sep 12, 2024 8:57 PM UTC | |
| Missing 'httpOnly' Cookie Attribute | 5.0 (Medium) | 80 % | 203.30.3.40 | 80/tcp | Thu, Sep 12, 2024 8:57 PM UTC | |
| FTP Unencrypted Cleartext Login | 4.8 (Medium) | 70 % | 203.30.3.40 | 21/tcp | Thu, Sep 12, 2024 8:55 PM UTC | |
| Cleartext Transmission of Sensitive Information via HTTP | 4.8 (Medium) | 80 % | 203.30.3.40 | 80/tcp | Thu, Sep 12, 2024 8:57 PM UTC | |
| Cleartext Transmission of Sensitive Information via HTTP | 4.8 (Medium) | 80 % | 203.30.3.40 | 3000/tcp | Thu, Sep 12, 2024 8:57 PM UTC | |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4.3 (Medium) | 98 % | 203.30.3.40 | 3306/tcp | Thu, Sep 12, 2024 8:56 PM UTC | |
| TCP timestamps | 2.6 (Low) | 80 % | 203.30.3.40 | general/tcp | Thu, Sep 12, 2024 8:56 PM UTC | |

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

The target for this scan is drisst.com (IP address: 203.30.3.40).

Completed by

Insert your name here.

Matias Laszlo Kun

On

Insert current date here.

September 12, 2024

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Purpose

Identify the purpose of the penetration test.

Purpose of this lab is targeting exploitation from an unknown source.

Scope

Identify the scope of the penetration test.

The scope is to identify weak and compromised passwords attackers used. In addition, the source packages could potentially have hidden entrances to bypass basic security functionality. Finally, scanning vulnerability in the internal employee network and determining whether one of the servers are targeted by a malicious actor or hacktivist group.

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.

For the first severe vulnerability (Severity level 9.0), the possibility of logging in high by using a remote MySQL for using weak credentials, like in this case, using "password" as the password. The simplicity of the password makes unauthorized accessing more effective. The password must be promptly and quickly change or else this mitigation solution will be ineffective, as well as Multifactor Authentication (MFA) to secure the MySQL instance.

Another thing to point out the daemon or software program vsftpd being prone to this backdoor attack (Severity level for both vsftpd compromises: 7.5). Vsftpd 2.3.4 source package was affected. The solution is to download and install the patched package from the referenced link, as well as verifying the package signature's validity. All the compromised vsftpd packages must be to the updated, secure version ensuring application stability.

Please ensure password policies with MFA is implemented as well as installing secure, updated vsftpd packages.

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Conclusion

Identify your key findings.

The weak credentials were the primary factor for the attack and should be changed and further heighten its security, like MFA implementation alongside the password or PIN, not just how strong it is. The compromised vsftpd packages were a secondary source for the compromised network and both verifying the signature along with installing the secure, patched version should resolve this vulnerability. There are potential risks of installing beta files that could possibly have unresolved vulnerabilities.

Anonymous remote access to the FTP service, though not as severe as the severe issues listed above, were used in this attack too. Ensuring the employees understand whom they grant access to sensitive files will significantly reduce the likelihood of access to sensitive data. The cookie used Javascript, which is commonly known for session hijackings, as opposed to httpOnly which is more secure. An FTP Encryption could have prevented the sensitive data from transiting through compromised login credentials through unencrypted FTP. Protocol TLSv1.0 was used in the attack. Companies will need to adhere supported protocols to ensure safety and security.

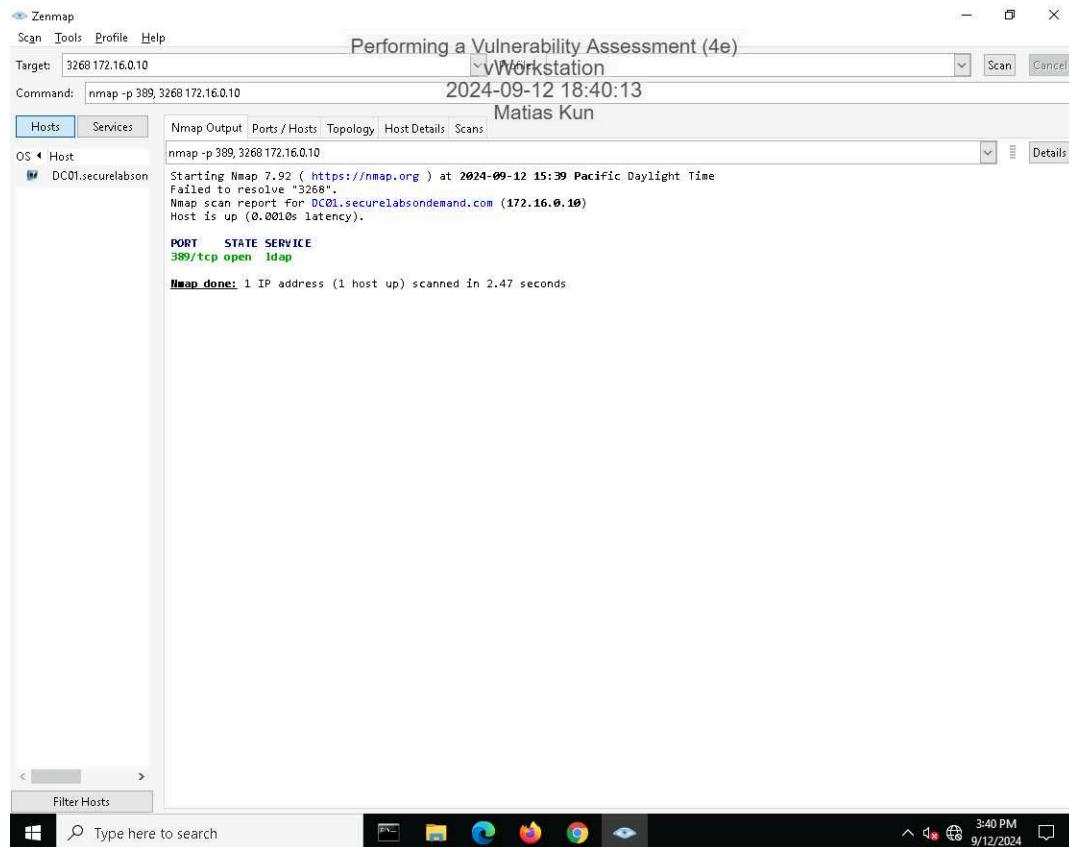
Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

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.



The screenshot shows the Zenmap interface with the following details:

- Scan Tools Profile Help** menu bar.
- Target:** 3268 172.16.0.10
- Command:** nmap -p 389,3268 172.16.0.10
- Scans:** Matias Kun
- Hosts:** DC01.securelabson
- Services:** OS Host, DC01.securelabson
- Nmap Output:** nmap -p 389,3268 172.16.0.10
Starting Nmap 7.92 (https://nmap.org) at 2024-09-12 15:39 Pacific Daylight Time
Failed to resolve "3268".
Nmap scan report for DC01.securelabson-demand.com (172.16.0.10)
Host is up (0.0010s latency).

| PORT | STATE | SERVICE |
|---------|-------|---------|
| 389/tcp | open | idap |

Nmap done: 1 IP address (1 host up) scanned in 2.47 seconds
- Ports / Hosts Topology Host Details Scans** tabs.
- Filter Hosts:** Type here to search
- System Tray:** 3:40 PM, 9/12/2024

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.

Domain Control (172.16.0.10)

Completed by

Insert your name here.

Matias Laszlo Kun

On

Insert current date here.

September 12, 2024

Performing a Vulnerability Assessment (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 02

Purpose

Identify the purpose of the penetration test.

Secure network test and analysis per Secure Labs on Demand's request.

Scope

Identify the scope of the penetration test.

The scope of the penetration test focused on assets within the internal network, including identifying and addressing vulnerabilities, implementing remediation measures, and considering network segmentation.

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 highest vulnerability (CVSS: 7.5) is the SSL Medium Strength Cipher Suites Supported issue. This level encryption is easy for hackers on the same network to bypass and potentially attack. Therefore, the best solution is to reconfigure affected applications and refrain the use of medium strength ciphers if possible. The second highest vulnerability, though on the medium level (CVSS: 6.5), is an untrusted SSL Certificate. Please ensure to purchase and generate a proper SSL certificate. Another medium level issue with the same CVSS score as the second issue is the TLS 1.0 protocol. Ensure to enable support for TLS 1.2+ and disable TLS 1.0 support. Terminal Services Encryption Level is Medium or Low (CVSS v3 severity and score: Medium and 4.0). Medium or Low Terminal Services Encryption eases access for malicious actors to eavesdrop on communications. Ensure to change the level to High and comply with FIPS.

Conclusion

Identify your key findings.

Since SSL Medium Strength Ciphers are easy to bypass on the same network as the hacker, the best course of action from this finding is to disable medium strength Ciphers and enable stronger encryption levels. An unreliable SSL Certificate was discovered. It is crucial to verify and validate the integrity of a purchased or generated SSL Certificate as invalid SSL Certificates can increase vulnerability. As TLS 1.0 is unsupported, it increases the risk of exploitation. TLS 1.2 and above should decrease the risk of exploitation. Since the Terminal Services has used medium or low levels of authentication, adding more authenticity to the Terminal Services and ensuring FIPS compliance should make Terminal Services more secure.