Cyber security Incident Investigation

Mitul Daiya

Cyber Security and Forensic Information Technology MSc, University of Portsmouth – Portsmouth.

M30062-2021/22: Systems, Security and Hacking

Professor (or Dr.) Olufemi Fasunlade

Date 15/04/2022

Table of Contents

Introduction

Cyber security's center work is to ensure the gadgets we all utilize (smartphones, portable workstations, tablets, and computers) and the administrations we get to both online and if all gadgets members of the same network and one device are compromised, hackers can gain access to all others. In this case able to see that Frozen Yoghurt Ltd, UK company which has treated by a hacker and stole or view a piece of information by the hacker and also the central server conjointly hacker crushed all information into the server but somehow company recoup a few log records from the server for examining who stole the information. So, in this case, think about it. We ought to discover who stole the information and at which time this happened. Moreover, how the hacker got the information from the server we must acknowledge in advance sections. In addition, within the final, I will explain about risk assessment strategy and recommendations to mitigate further occasions like this.

Roles and Obligations

The company name is Frozen Yoghurt Ltd and is based in the United Kingdom Portsmouth city. Its primary work is in-shop deals of Frozen Yogurt items and deals of its own product inside the Portsmouth zone of the UK. The company have seven staff member an employee, 1 is a manager, three are a sales representative, one is an IT supporter who can handle server issues, and two are Administrators.

IT Resources	Roles and responsibilities
One remote access to the central server	2 Administrators
Not Provide any access by the central server.	2 Salesperson
One Windows device with access to the central server.	1 Manager
1 tablet which is access central server in this device person can remotely access Sales Database, Stock inventory system	1 Salesperson
Remote connection to the central server	1 IT Support

The central server is found within the shop. The central server has all the databases and Hosting mail, the server that hosted the site. In this case, when a hacker stole or saw a record, the hacker erased all the log records. Some way or another, the log and network records were recuperated.

The stages of Forensic Investigation

The case is divided into the following stages

Extraction-

Extraction includes the recognizable proof, recuperation, and documentation (such as logs) of the data inspected within the gadgets. The company recoups some log records from the main server.

1) Auth.log
2) Syslog
3) Network Packet Capture.pcapng
4) Kern.log
5) Suricata.log

System logs:

These files might be useful in debugging system problems. These files might be useful when troubleshooting system problems. A log's function plays the role of a warning sign when there is an unfavorable situation happening. As a result, when cybercrime occurs, they play a critical part in the investigation.

Wireshark:

Wireshark may be a tool that analyses network conventions and allows you to see what is happening within the arrange at a small level. When using Wireshark, you can see the whole contents of a network packet in real-time. You may also see all of the chats and network broadcasts that have been taking place, with a filter in place, you can get just the information you want to view.

PROPOSAL DESCRIPTION:

The case research was based on simulating a hypothetical event in a hacker used to obtain access to the system. The suspect's network address was captured through authorization in order to record exchange messages between them. There are two detection techniques for network problems and the Wireshark sniffer was utilized for this task.

Logs analysis:

Auth.log - is a collect user login event like authentication logs, including both successful and non-successful individuals' logins and authentication methods, should be stored. At **14:33:30**, we can observe a hacker trying to get access to the central server; but failed many times. After too many attempts, **192.168.56.1** is successfully login two times at **14:35:08** and **14:35:56**.

```
Mar  8 14:33:30 frozenyoghurt-pc sshd[2287]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Mar  8 14:33:46 frozenyoghurt-pc sshd[2287]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Mar  8 14:34:02 frozenyoghurt-pc sshd[2289]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=frozen-yoghurt
Mar  8 14:34:18 frozenyoghurt-pc sshd[2289]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=frozen-yoghurt
```

Fig 1.1 Failed Login Attempts

```
Mar  8 14:35:08 frozenyoghurt-pc login[2299]: pam_unix(login:session): session opened for user frozen-yoghurt by (uid=0)
Mar  8 14:35:09 frozenyoghurt-pc systemd-logind[561]: New session 5 of user frozen-yoghurt.
Mar  8 14:35:09 frozenyoghurt-pc systemd-logind[561]: Session 5 logged out. Waiting for processes to exit.
Mar  8 14:35:09 frozenyoghurt-pc systemd-logind[561]: Removed session 5.
Mar  8 14:35:12 frozenyoghurt-pc login[2298]: FAILED LOGIN (5) on '/dev/pts/3' from '1.capita.vpn.port.ac.uk' FOR 'frozen-yoghurt', Authentication failure
Mar  8 14:35:12 frozenyoghurt-pc login[2298]: TOO MANY LOGIN TRIES (5) on '/dev/pts/3' from '1.capita.vpn.port.ac.uk' FOR 'frozen-yoghurt'
Mar  8 14:35:12 frozenyoghurt-pc login[2298]: pam_mail(login:session): pam_putenv: delete non-existent entry; MAIL
Mar  8 14:35:12 frozenyoghurt-pc login[2298]: pam_unix(login:session): session closed for user frozen-yoghurt
Mar  8 14:35:12 frozenyoghurt-pc login[2298]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/3 ruser= rhost=1.capita.vpn.port.ac.uk  user=frozen-y
oghurt
```

Fig 1.2 First Login Successfully

```
Mar  8 14:35:56 frozenyoghurt-pc systemd-logind[561]: New session 6 of user frozen-yoghurt.
Mar  8 14:38:38 frozenyoghurt-pc login[2388]: pam_unix(login:session): session closed for user frozen-yoghurt
Mar  8 14:38:38 frozenyoghurt-pc systemd-logind[561]: Session 6 logged out. Waiting for processes to exit.
Mar  8 14:38:38 frozenyoghurt-pc systemd-logind[561]: Removed session 6.
```

Fig 1.3 Second Login Successfully

Suricata logs:-

It can analyze your network traffic, detect a range of sophisticated attacks, and alert you if there are any problems. It can check the traffic on your network and will notify you if there are any sophisticated attacks to any problems. This file stores logs of every IP that attempts to log in or connect to the server. I saw that the **192.168.56.1** IP address was logged in using Telnet on **March 8th at 14:35:46**.

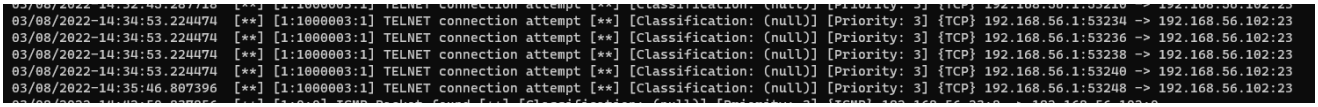


Fig 1.4 Telnet Connection Attempt

Kernel logs:

Kernal logs collect only kernel information like your system logs information about the kernel ring buffer at boot time.

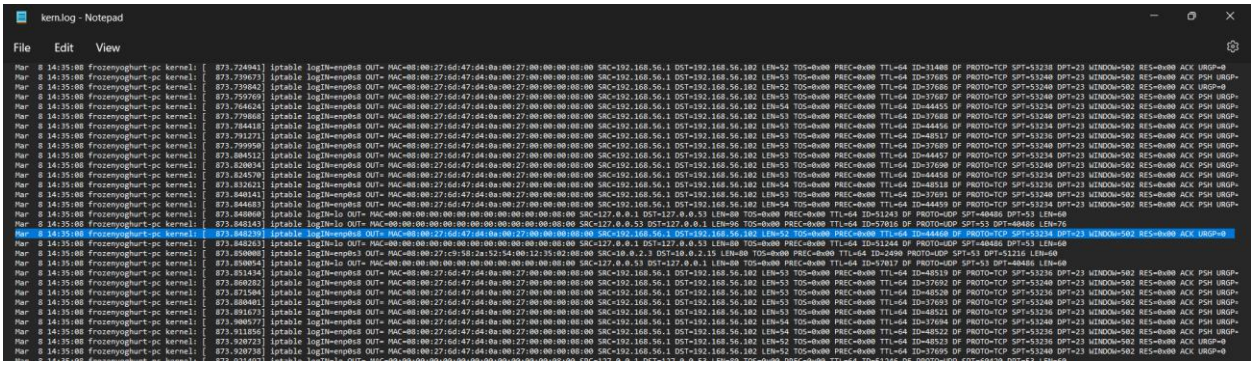


Fig 1.5 kernal.log

System logs**:**

Syslog is a common logging system. It gathers messages from many applications and services, including the kernel, and saves them in a number of log files, often under **/var/log**, depending on the arrangement. Many communications between **192.168.56.1** and **192.168.56.102** an be seen in the following image.

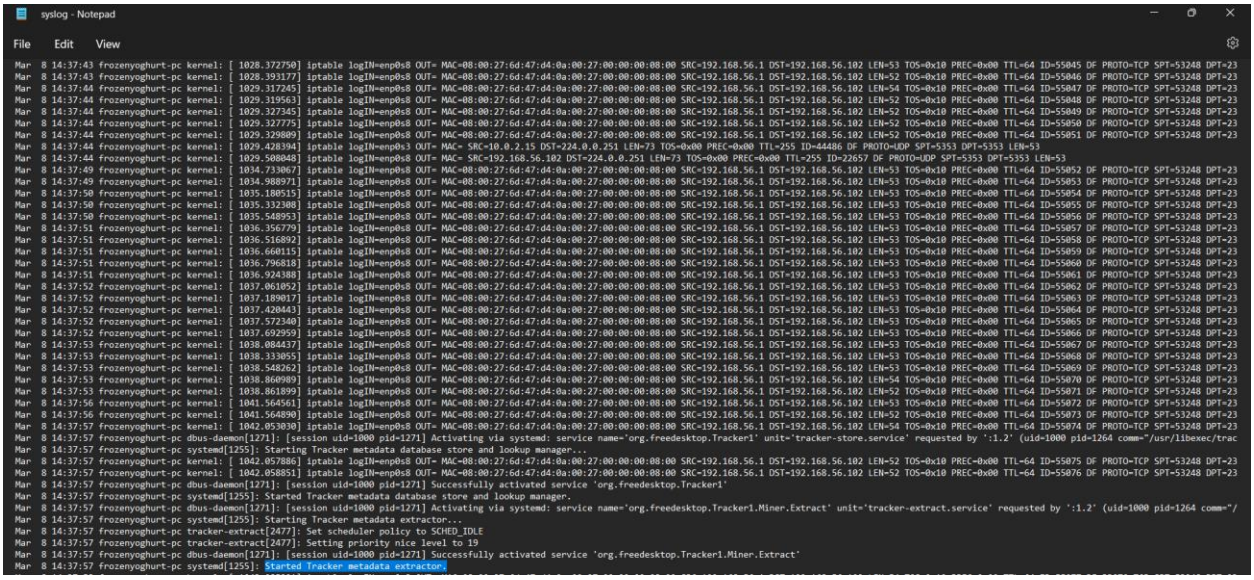
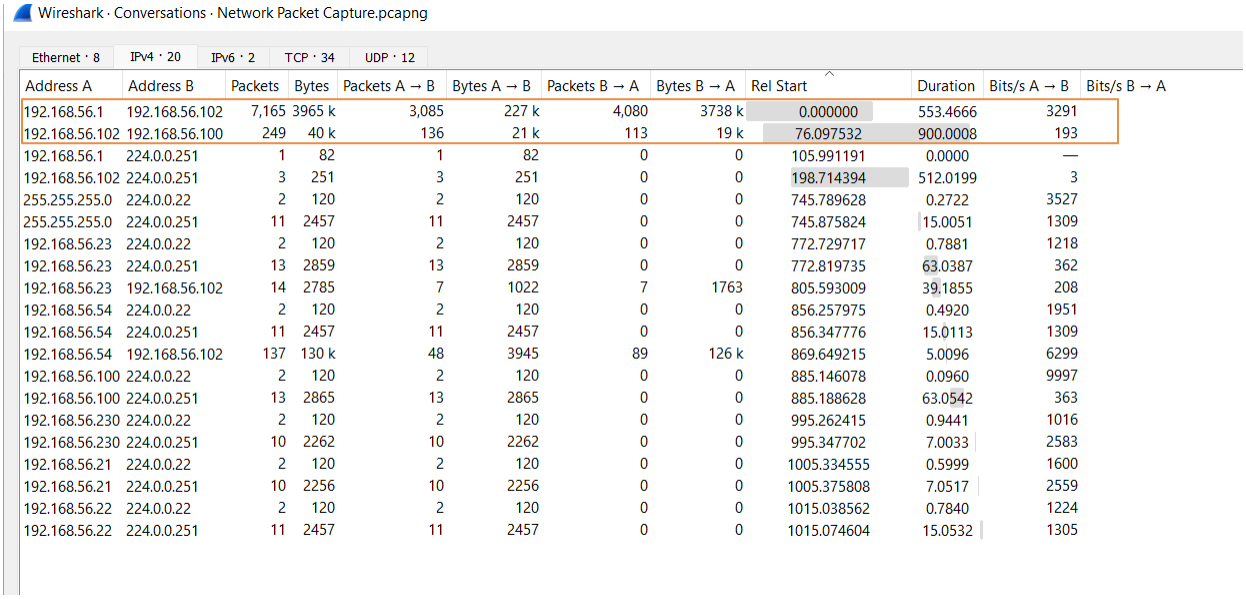


Fig 1.6 Syslog

Analysis

In this analysis, we have to investigate conversations between two different IPs.

First, We should first look through the networkcaputure.pcapng file to see which IP addresses are most frequently used. At the top of the tab, we can see that the majority of the discussions and file transfers occur between **192.168.56.1** and **192.168.56.102**.


Wireshark · Conversations · Network Packet Capture.pcapng

Ethernet · 8 | IPv4 · 20 | IPv6 · 2 | TCP · 34 | UDP · 12

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.56.1	192.168.56.102	7,165	3965 k	3,085	227 k	4,080	3738 k	0.000000	553.4666	3291	
192.168.56.102	192.168.56.100	249	40 k	136	21 k	113	19 k	76.097532	900.0008	193	
192.168.56.1	224.0.0.251	1	82	1	82	0	0	105.991191	0.0000	—	
192.168.56.102	224.0.0.251	3	251	3	251	0	0	198.714394	512.0199	3	
255.255.255.0	224.0.0.22	2	120	2	120	0	0	745.789628	0.2722	3527	
255.255.255.0	224.0.0.251	11	2457	11	2457	0	0	745.875824	15.0051	1309	
192.168.56.23	224.0.0.22	2	120	2	120	0	0	772.729717	0.7881	1218	
192.168.56.23	224.0.0.251	13	2859	13	2859	0	0	772.819735	63.0387	362	
192.168.56.23	192.168.56.102	14	2785	7	1022	7	1763	805.593009	39.1855	208	
192.168.56.54	224.0.0.22	2	120	2	120	0	0	856.257975	0.4920	1951	
192.168.56.54	224.0.0.251	11	2457	11	2457	0	0	856.347776	15.0113	1309	
192.168.56.54	192.168.56.102	137	130 k	48	3945	89	126 k	869.649215	5.0096	6299	
192.168.56.100	224.0.0.22	2	120	2	120	0	0	885.146078	0.0960	9997	
192.168.56.100	224.0.0.251	13	2865	13	2865	0	0	885.188628	63.0542	363	
192.168.56.230	224.0.0.22	2	120	2	120	0	0	995.262415	0.9441	1016	
192.168.56.230	224.0.0.251	10	2262	10	2262	0	0	995.347702	7.0033	2583	
192.168.56.21	224.0.0.22	2	120	2	120	0	0	1005.334555	0.5999	1600	
192.168.56.21	224.0.0.251	10	2256	10	2256	0	0	1005.375808	7.0517	2559	
192.168.56.22	224.0.0.22	2	120	2	120	0	0	1015.038562	0.7840	1224	
192.168.56.22	224.0.0.251	11	2457	11	2457	0	0	1015.074604	15.0532	1305	

Fig 2.0 Conversation

Firstly, the hacker (**192.168.56.1**) came and went to the Website of “frozenyogurt.co.uk” on **8th March at 14:29:25** and the last time at **14:31:56**. He tried to communicate by shaking with the IP address (**192.168.56.102**) means to the central server before the attack. As a result, we can see that **192.168.56.1** has accessed the website's **login.php, admin, etc…** files. We can also see that the request originates from **192.168.56.1** and that the endpoint is **192.168.56.102**, indicating that the website is hosted on the **192.168.56.102** server. This implies that the main server and database are in the central server (**192.168.56.102**).

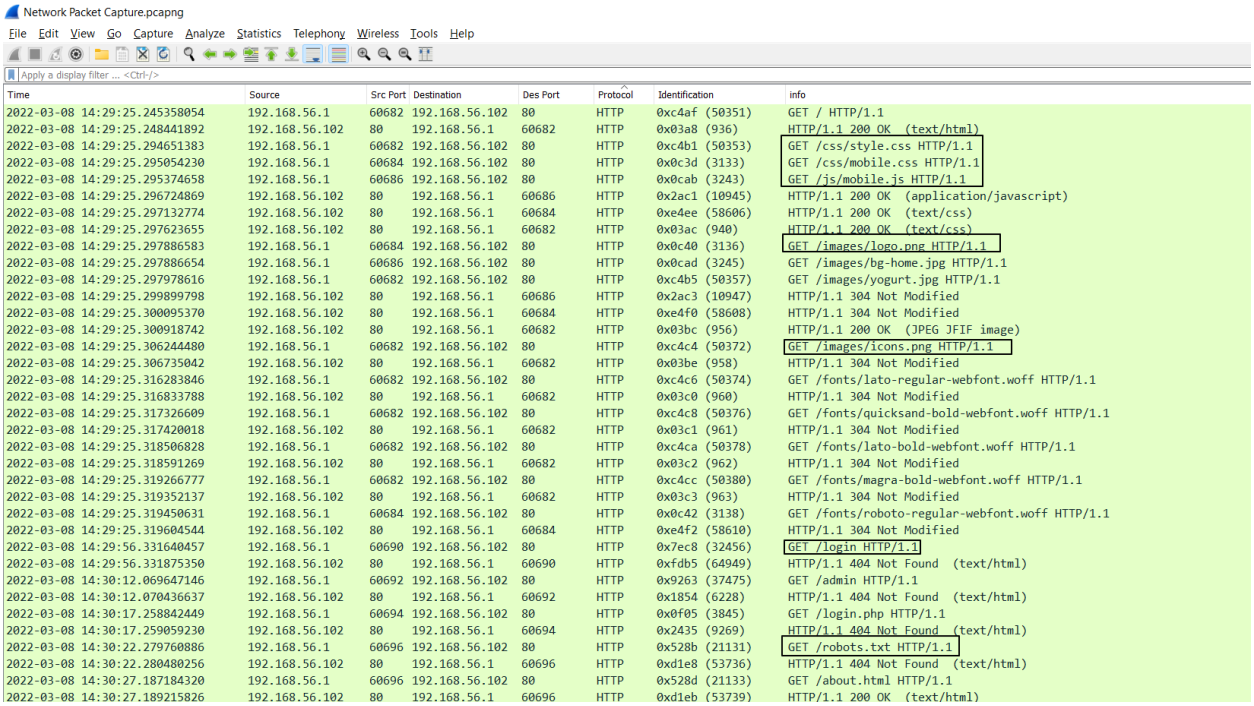
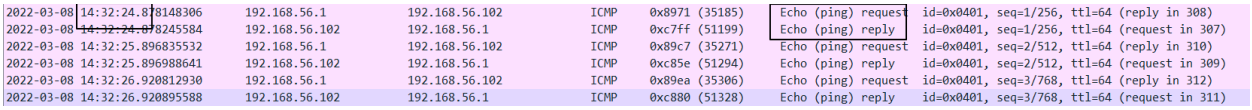


Fig 2.1. View The Website

Recommendation :

Ensure that your software is updated - It's critical to maintain all of your platforms and scripts are up to date. Hackers are effectively seeking after security weaknesses in a prevalent online program that requires program upgrades to close security gaps. Every software product we use should be maintained and updated.

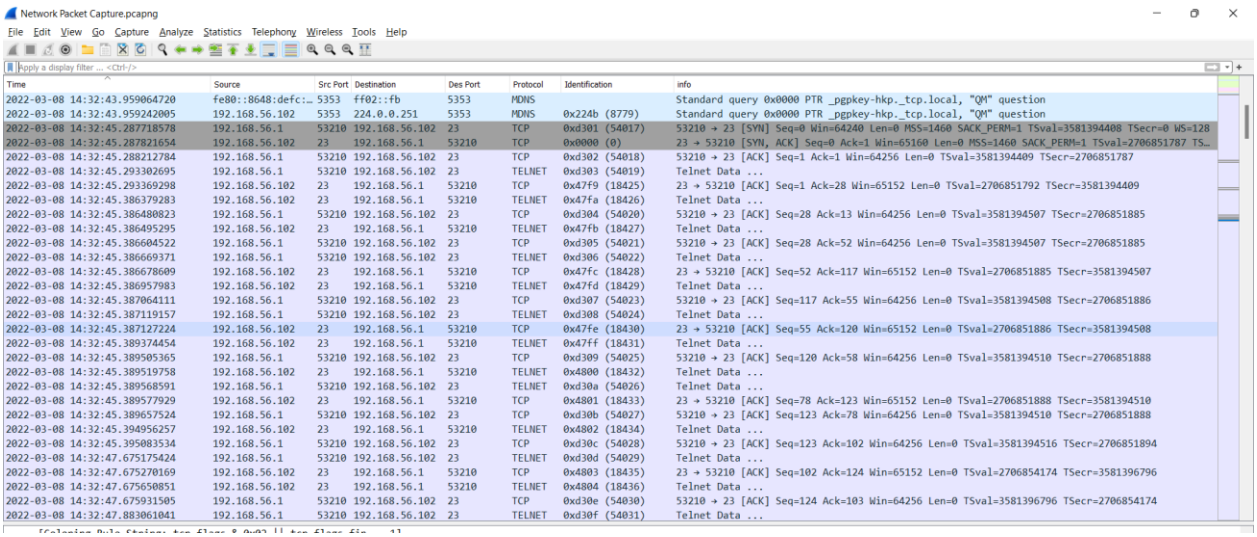
After visiting the website, 192.168.56.1 was requested to the server(192.168.56.102) for connectivity to the server at 14:32:24. The most utilized TCP/IP command for investigating association, reachability, and name determination is ping. It is the most effective method for determining if there are two nodes connecting.



2022-03-08	14:32:24.878148306	192.168.56.1	192.168.56.102	ICMP	0x8971 (35185)	Echo (ping) request	id=0x0401, seq=1/256, ttl=64 (reply in 308)
2022-03-08	14:32:24.878245584	192.168.56.102	192.168.56.1	ICMP	0xc7ff (51199)	Echo (ping) reply	id=0x0401, seq=1/256, ttl=64 (request in 307)
2022-03-08	14:32:25.896835532	192.168.56.1	192.168.56.102	ICMP	0x89c7 (35271)	Echo (ping) request	id=0x0401, seq=2/512, ttl=64 (reply in 310)
2022-03-08	14:32:25.896988641	192.168.56.102	192.168.56.1	ICMP	0xc85e (51294)	Echo (ping) reply	id=0x0401, seq=2/512, ttl=64 (request in 309)
2022-03-08	14:32:26.920812930	192.168.56.1	192.168.56.102	ICMP	0x89ea (35306)	Echo (ping) request	id=0x0401, seq=3/768, ttl=64 (reply in 312)
2022-03-08	14:32:26.920895588	192.168.56.102	192.168.56.1	ICMP	0xc880 (51328)	Echo (ping) reply	id=0x0401, seq=3/768, ttl=64 (request in 311)

Fig 2.2 request and reply

Without further ado after the server reacts to the ping request, **192.168.56.1** attempts to connect to the server utilizing the telnet and ssh service. After that, at **14:32:45**, the hacker uses those services to try to connect with the username and password using some word-listed script like the most popular tool dictionary attacks. Following studying several log files, command run timing is very sort so it has been determined that this is a dictionary attack, as the hacker utilises the company's associated name to create a dictionary file for the attack and the that we can seen in fig



Time	Source	Src Port	Destination	Des Port	Protocol	Identification	info
2022-03-08 14:32:43.959064720	fe80::8648:defc:…	5353	ff02::fb	5353	MDNS		Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
2022-03-08 14:32:43.959242005	192.168.56.102	5353	224.0.0.251	5353	MDNS	0x224b (8779)	Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
2022-03-08 14:32:45.287718578	192.168.56.1	53210	192.168.56.102	23	TCP	0xd301 (54017)	53210 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3581394408 TSecr=0 WS=128
2022-03-08 14:32:45.287821654	192.168.56.102	23	192.168.56.1	53210	TCP	0x0000 (0)	23 → 53210 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2706851787 TS…
2022-03-08 14:32:45.288212784	192.168.56.1	53210	192.168.56.102	23	TCP	0xd302 (54018)	53210 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3581394409 TSecr=2706851787
2022-03-08 14:32:45.293302695	192.168.56.1	53210	192.168.56.102	23	TELNET	0xd303 (54019)	Telnet Data …
2022-03-08 14:32:45.293369298	192.168.56.102	23	192.168.56.1	53210	TCP	0x47f9 (18425)	23 → 53210 [ACK] Seq=1 Ack=28 Win=65152 Len=0 TSval=2706851792 TSecr=3581394409
2022-03-08 14:32:45.386379283	192.168.56.102	23	192.168.56.1	53210	TELNET	0x47fa (18426)	Telnet Data …
2022-03-08 14:32:45.386480823	192.168.56.1	53210	192.168.56.102	23	TCP	0xd304 (54020)	53210 → 23 [ACK] Seq=28 Ack=13 Win=64256 Len=0 TSval=3581394507 TSecr=2706851885
2022-03-08 14:32:45.386495295	192.168.56.102	23	192.168.56.1	53210	TELNET	0x47fb (18427)	Telnet Data …
2022-03-08 14:32:45.386604522	192.168.56.1	53210	192.168.56.102	23	TCP	0xd305 (54021)	53210 → 23 [ACK] Seq=28 Ack=52 Win=64256 Len=0 TSval=3581394507 TSecr=2706851885
2022-03-08 14:32:45.386669371	192.168.56.1	53210	192.168.56.102	23	TELNET	0xd306 (54022)	Telnet Data …
2022-03-08 14:32:45.386678609	192.168.56.102	23	192.168.56.1	53210	TCP	0x47fc (18428)	23 → 53210 [ACK] Seq=52 Ack=117 Win=65152 Len=0 TSval=2706851885 TSecr=3581394507
2022-03-08 14:32:45.386957983	192.168.56.102	23	192.168.56.1	53210	TELNET	0x47fd (18429)	Telnet Data …
2022-03-08 14:32:45.387064111	192.168.56.1	53210	192.168.56.102	23	TCP	0xd307 (54023)	53210 → 23 [ACK] Seq=117 Ack=55 Win=64256 Len=0 TSval=3581394508 TSecr=2706851886
2022-03-08 14:32:45.387119157	192.168.56.1	53210	192.168.56.102	23	TELNET	0xd308 (54024)	Telnet Data …
2022-03-08 14:32:45.387127224	192.168.56.102	23	192.168.56.1	53210	TCP	0x47fe (18430)	23 → 53210 [ACK] Seq=55 Ack=120 Win=65152 Len=0 TSval=2706851886 TSecr=3581394508
2022-03-08 14:32:45.389374454	192.168.56.102	23	192.168.56.1	53210	TELNET	0x47ff (18431)	Telnet Data …
2022-03-08 14:32:45.389505365	192.168.56.1	53210	192.168.56.102	23	TCP	0xd309 (54025)	53210 → 23 [ACK] Seq=120 Ack=58 Win=64256 Len=0 TSval=3581394510 TSecr=2706851888
2022-03-08 14:32:45.389519758	192.168.56.102	23	192.168.56.1	53210	TELNET	0x4800 (18432)	Telnet Data …
2022-03-08 14:32:45.389568591	192.168.56.1	53210	192.168.56.102	23	TELNET	0xd30a (54026)	Telnet Data …
2022-03-08 14:32:45.389577929	192.168.56.102	23	192.168.56.1	53210	TCP	0x4801 (18433)	23 → 53210 [ACK] Seq=78 Ack=123 Win=65152 Len=0 TSval=2706851888 TSecr=3581394510
2022-03-08 14:32:45.389657524	192.168.56.1	53210	192.168.56.102	23	TCP	0xd30b (54027)	53210 → 23 [ACK] Seq=123 Ack=78 Win=64256 Len=0 TSval=3581394510 TSecr=2706851888
2022-03-08 14:32:45.394956257	192.168.56.102	23	192.168.56.1	53210	TELNET	0x4802 (18434)	Telnet Data …
2022-03-08 14:32:45.395083534	192.168.56.1	53210	192.168.56.102	23	TCP	0xd30c (54028)	53210 → 23 [ACK] Seq=123 Ack=102 Win=64256 Len=0 TSval=3581394516 TSecr=2706851894
2022-03-08 14:32:47.675175424	192.168.56.1	53210	192.168.56.102	23	TELNET	0xd30d (54029)	Telnet Data …
2022-03-08 14:32:47.675270169	192.168.56.102	23	192.168.56.1	53210	TCP	0x4803 (18435)	23 → 53210 [ACK] Seq=102 Ack=124 Win=65152 Len=0 TSval=2706854174 TSecr=3581396796
2022-03-08 14:32:47.675650851	192.168.56.102	23	192.168.56.1	53210	TELNET	0x4804 (18436)	Telnet Data …
2022-03-08 14:32:47.675931505	192.168.56.1	53210	192.168.56.102	23	TCP	0xd30e (54030)	53210 → 23 [ACK] Seq=124 Ack=103 Win=64256 Len=0 TSval=3581396796 TSecr=2706854174
2022-03-08 14:32:47.883061041	192.168.56.1	53210	192.168.56.102	23	TELNET	0xd30f (54031)	Telnet Data …

Fig 2.3 started dictionary attack

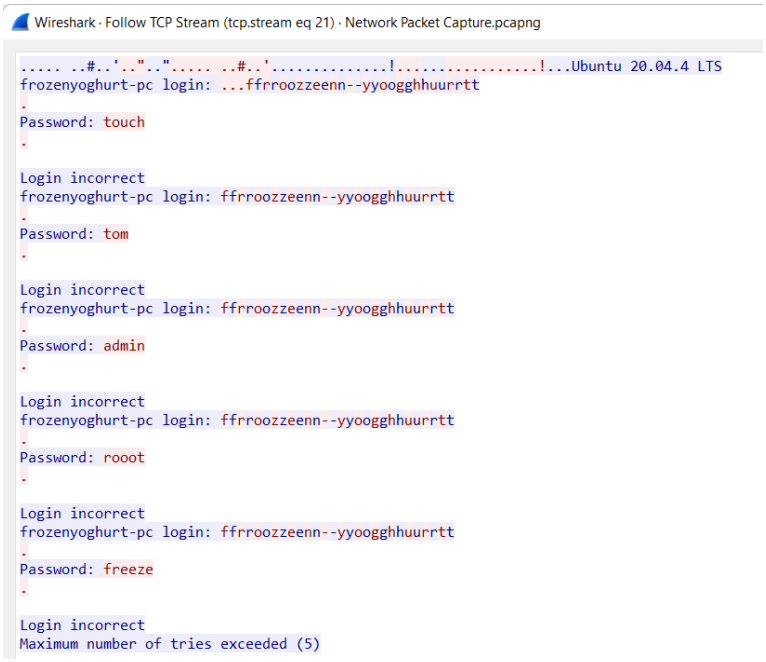


Fig 2.4 Filed Password attempt

At 14:35:08, the attacker discovers the login and password after a long search. The server's username is frozen-yoghuri, while the attacker's password is frozen.

Fig 2.5 Successfully logging using a dictionary attack

Recommendation:

Password protection:

1) **Do not use old password**
2) **Do not use personal information**
3) **Change your password every month**
4) **Use a lengthy password**
5) **Use special characters**

Later, the attacker successfully login to the server at **14:36:56** with a username and password which can be seen in the **auth.log** (Fig 1.2 and 1.3) and **Syslog** (Fig 1.6) files.

Analysis of Activity Log

After logging onto the server successfully, the hacker now attempts to perform some malicious activity on the server. The first attacker finds some files on the desktop and also this main part is done by the attacker executing the following command:

1) First he searches the file on the present directory using "***ls***" command

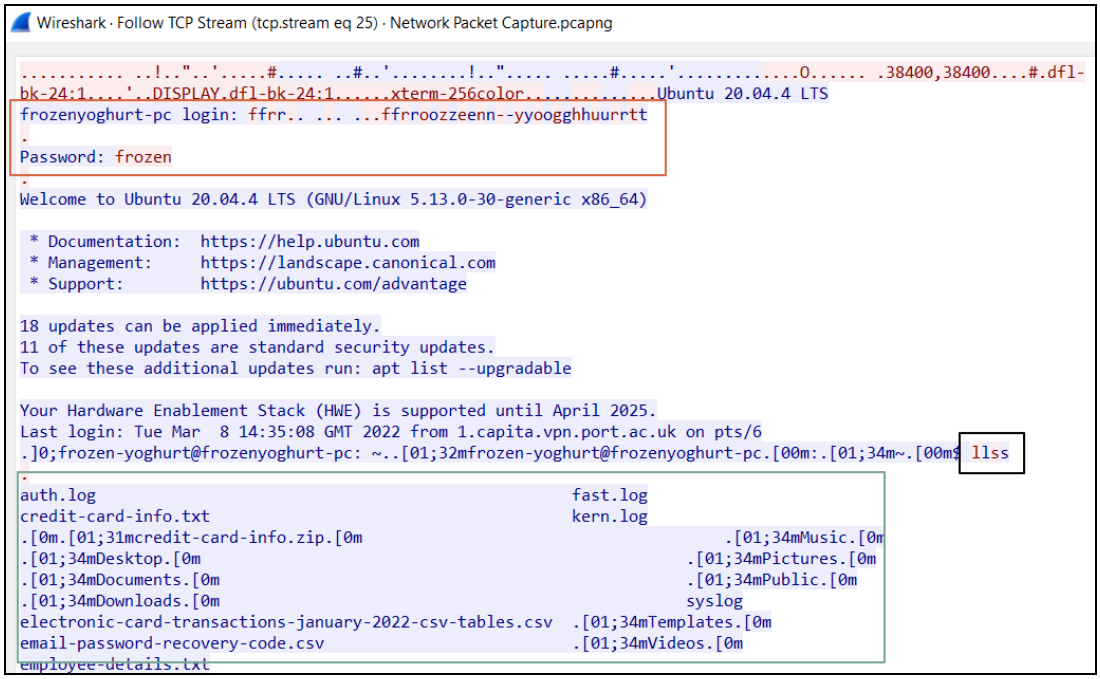


Fig 3.1 Attacker Run Commands

Following the "***ls***" command, we can see that the directory contains a large number of log files as well as some user-related files. We can also notice ***credit-card-info.zip***, which indicates that the zip file contains some clients' confidential data (credit card information).

2) Using the cat command, the attacker examined the **electronic-card-transaction-january-2022-csv-tables.csv, email-password-recovery-code.csv, and employee-details.txt** files.

```
]0;frozen-yoghurt@frozenyoghurt-pc: ~..[01;32mfrozen-yoghurt@frozenyoghurt-pc.[00m:.[01;34m~.[00m$ ccaatt  eelleeccttrroo  nic-card-
ransactions-january-2022-csv-tables.csv
```

Fig 3.2 electronic-card-transaction-january-2022-csv-tables.csv

```
.]0;frozen-yoghurt@frozenyoghurt-pc: ~..[01;32mfrozen-yoghurt@frozenyoghurt-pc.[00m:.[01;34m~.[00m$ ccaatt  eemmpplloo      yee-
details.txt
.

Name: Tom Hanks
Job title: Manager
Employee ID: 0001
Address: No 1 XXX Portsmouth, UK

Name: Lisa Hanks
Job title: Deputy Manager/ Sales
Employee ID: 0002
Address: No 1 XXX Portsmouth, UK

Name: Samuel Jackson
Job title: Administrator
Employee ID: 0003
Address: No 16 XXX Southampton, UK


Name: Bill Graham
Job title: IT Administrator
Employee ID: 0004
Address: No 23 XXX Portsmouth, UK

Name: Lucy Banks
Job title: Sales Representative
Employee ID: 0005
Address: No 66 XXX Fareham, UK
```

Fig 3 3 employee-details.txt

```
.]0;frozen-yoghurt@frozenyoghurt-pc: ~..[01;32mfrozen-yoghurt@frozenyoghurt-pc.[00m:.[01;34m~.[00m$ ccaatt  eemmaaiill      -password-
recovery-code.csv
.
```

Fig 3.4 email-password-recovery-code.cs

3) Remove and copy the files from the server after the hacker has seen all of them. The attacker also removes the **<u>Frozenyogurtshop</u>** file from the existing path, as well as some of the website content shown in the screenshot below.

```
..[K.[A.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.
[C.[C.[C.[C.[C.[C.[C.[C.[C.[A.................[5P.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[A...........[3Pfconfig.[A........ls.[K.[A..sudo rm
-r frozenyogurtshop.[A...........................ls.[K.[A..rm -r frozenyogurtshop.[A......................ls.[K.[A..cd ...[A......
[3Pls.[A..sudo cp -r * ...[A...............[5P.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[A.........d frozenyogurtshop/.[A....................ls.
[K.[A..cd ...[A......[3Pls.[A..sudo cp -r * /...[A.................[5P.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[A..........d
frozenyogurtshop/.[A....................ls.[K.[A..cd /var/www/html/.[A...............[K.[A....[1Pls.[A..sudo rm index.html .
[A...................ls.[K.[A..rm index.html .[A..............ls.[K.[A..cd /var/www/html/.[A.................[25@sudo cp -r
frozenyogurtshop.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[C.[A
```

Fig 3.5 copy and removing files

4) After deleting and copying the file, the hacker attempts to see the credit card zip file, but the file is password protected; somehow, the attacker knows the zip file's password **"frozen"**, the attacker may easily unzip and view the credit card data using **"cat"** command.

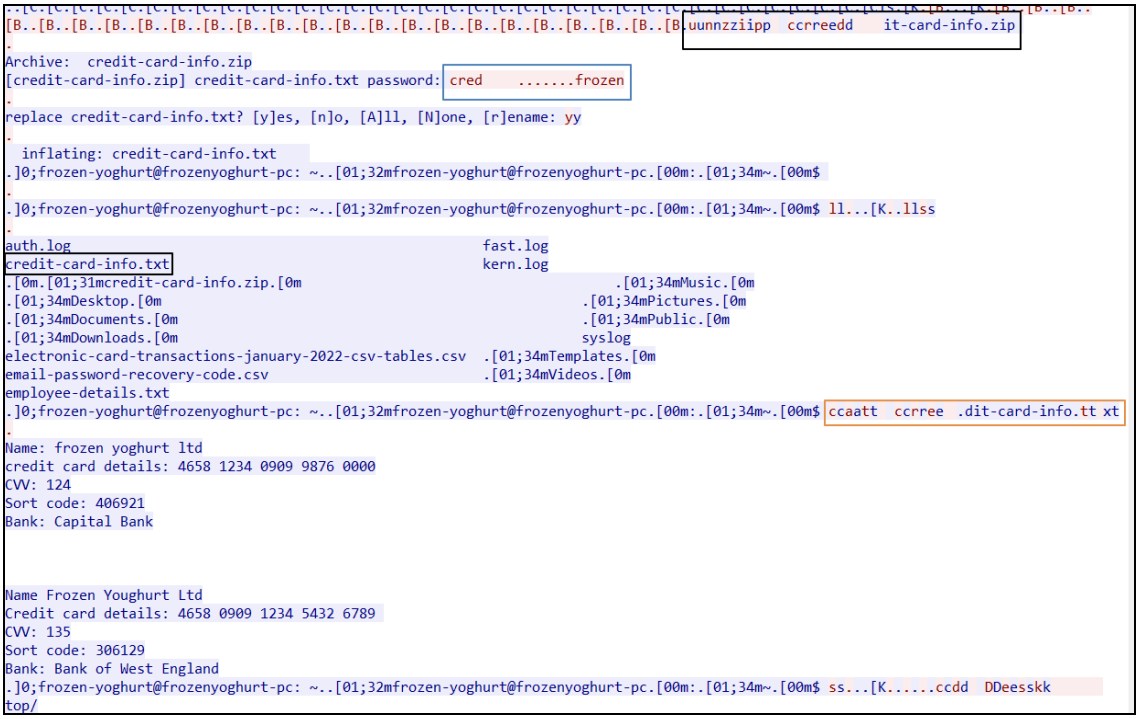


Fig 3.6 Creadit-card-info.txt

Recommendation:

1) **Account lock after too many login attempts**
2) **Cannot access root user via ssh**
3) **Change the default port**
4) **Use two-factor Authentication**
5) **Use WAF (web application Firewall)**

The attacker then went through all of the files and performed some unusual activities on this server before logout at **14:38:38**,and this file log was the final login of this attacker**.**

Compromise Phase

Finally, we notice that at **14:44:23** the address **192.168.56.100** also wants to connect to the server, but **192.168.56.100** was not connected to the server, which was using the SSH service to login, but SSH is entirely encrypted, so we can't see any further information about the interaction between them. In addition, the usage of **192.168.56.100** is duplicated because two separate IPs share the same MAC address. As a result, I believe **192.168.56.1** and **192.168.56.100** have the same Mac address.

Fig 4.1 Duplicate IP detected

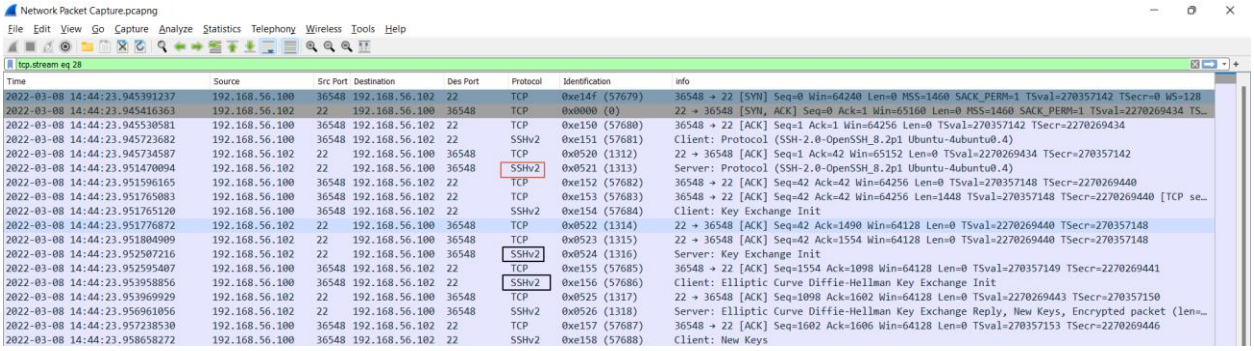


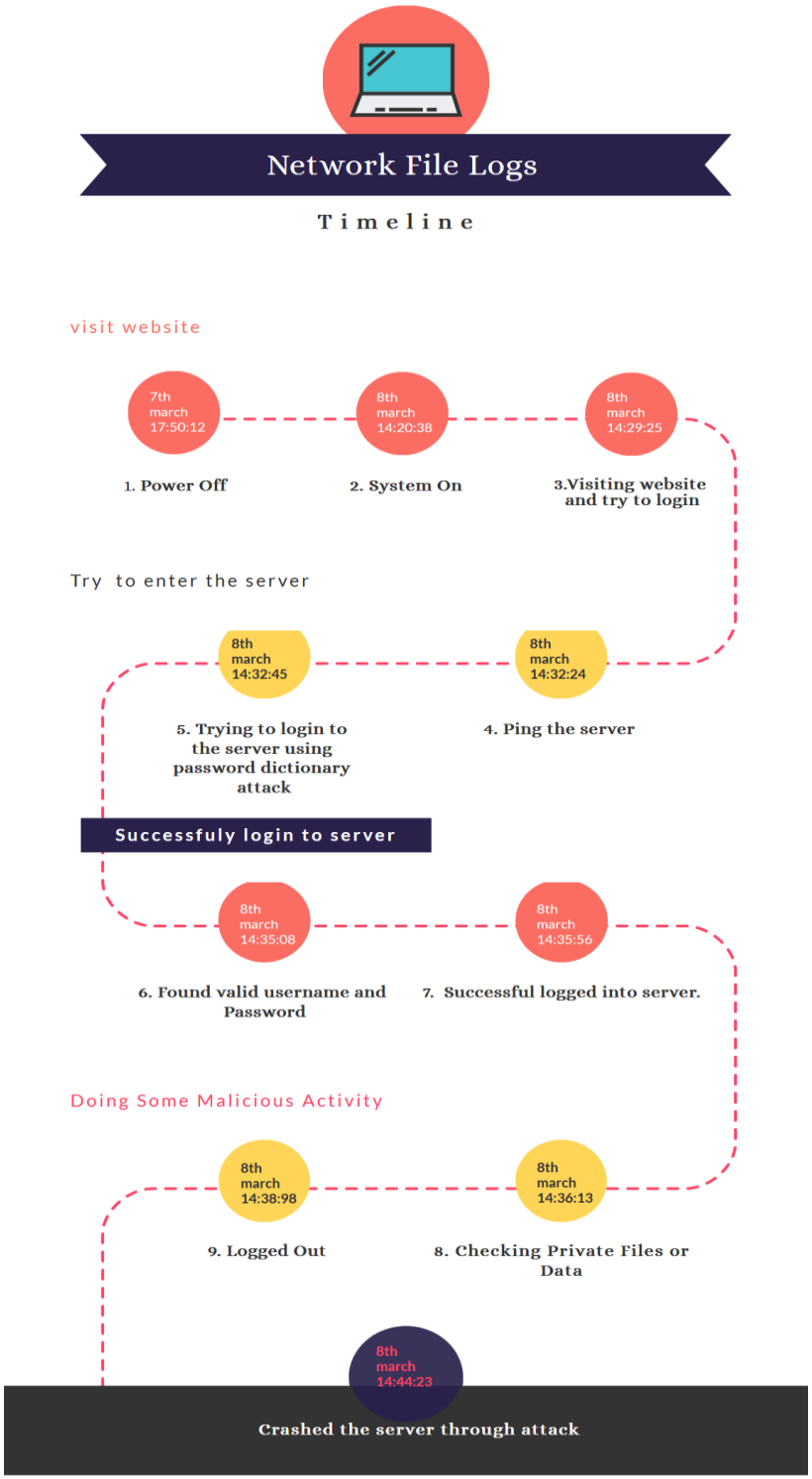
Fig 4.2 ssh connection failure

Fig 4.3 SSH Encrypted Conversation

Recommendation:

1) **Do regular database and website back-up**
2) **Try to separate the database from the file server**
3) **Use HTTPS or TLS to encrypt data just for keeping your customer data secure**
4) **Scan your website for vulnerabilities**
5) **Keep your website clean**

Graphical Time-Line events



Document the results:

A risk assessment report is generated in the final phase to help management make educated decisions regarding the budget, policies, procedures, and other areas of the organization. The report should contain information on each threat's vulnerabilities, assets at risk, impact on your IT infrastructure, the likelihood of occurrence, and proposed remedies, all of which should be included in the final product.

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendations
Website attack High	If any port number is open . High	Serves Critical	All services(website, email,etc.)will be unavailable for at least 3 hours. Critical	High Website data can be stole	High Website data and customer data can be release by hacker	Use HTTPS encryption And use proxy server to prevent this kind of attack.
Malicious human(interference) – Dictionary attack High	Company name related Password attack High	Website Critical	Website resources will be unavailable. Critical	Medium Dictionary attack was discovered once in 2 years.	Medium Potential loss of 5000 to 10000 pounds per hour of downtime	Use the critical password and use a hash function to encrypt the password
Natural disasters flooding High	The server room is in the shop. Low	Server. Critical	All services will be unavailable. Critical	Low The last flood in the area happened 10 years ago.	Low	Back up your data on the cloud(AWS) Or try to do multiple Regine instance for hosting
Accidental human interference – accidental file deletions High	Permission is configured properly; IT auditing software is in place; backups are taken regularly. Low	Files on a file share Medium	Critical data could be lost but almost certainly could be restored from backup. Low	Medium	Low	Continue monitoring permissions changes, privileged users, and backups.

We discovered that attackers attempted to log in using telnet, implying that they should increase their SSL and SSH encryption security, as I suggested in my report. To avoid physical damage such as earthquakes, deploy a cloud-based database, server, and firewall. Also, make a backup of your files and database in case a similar scenario occurs in the future. Furthermore, we may utilize password-protected authentication, such as two-factor authentication, or we can use an automated password change every few weeks to ensure that staff updates their passwords on a regular basis to avoid this type of attack.

Conclusion

In today’s world, computer networks are protected by a wide range of techniques. Despite the fact that these technologies successfully counter many assaults, new attacks continue to slip through the cracks and go undetected. In this scenario, the attacker entered the **192.168.56.102** server via a dictionary attack. After successfully logging into the attacker's view and transferring several files from the central server, we can observe that the attacker performs commands in seconds, implying that the hacker utilizes a scripted password file to do this. The hacker wiped the server after completing his task. It indicates that in this scenario, the attack is a dictionary attack.

References

Combs, G. (1998). *The Wireshark team*. Retrieved from https://www.wireshark.org/

Djukanović, M. (2021, may). Retrieved from https://www.researchgate.net/publication/351485294_Dictionary_Based_Brute_Force_Attack_-_Study_Case_of_Montenegro_and_China

Google. (n.d.). *google cloud* . Retrieved from google.com: https://developers.google.com/search/docs/advanced/security/https

Krause, T. (n.d.). *software.broadcom.com*. Retrieved from Broadcom software : https://www.broadcom.com/info/aiops/network-flow-analysis

Muuss, M. (1983). *Various open-source and commercial developers*. Retrieved from https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping

phoenixNAP. (2018, 12 3). *How To Prevent Brute Force Attacks With 8 Easy Tactics*. Retrieved from https://phoenixnap.com/kb/prevent-brute-force-attacks

ping. (1997). Retrieved from https://www.paessler.com/it-explained/ping

The Knowledge Management. (2022, 1 3). Retrieved from https://kb.iu.edu/d/aayd

Vykopal, J. (2009, march). Retrieved from https://www.researchgate.net/publication/228911072_Network-Based_Dictionary_Attack_Detection