

## **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.....	4
Roles and Obligations .....	5
The stages of Forensic Investigation.....	6
<b>Extraction-</b> .....	6
<b>System logs:</b> .....	6
<b>Wireshark:</b> .....	6
<b>PROPOSAL DESCRIPTION:</b> .....	7
Logs analysis:.....	8
<b>Auth.log</b> .....	8
Fig 1.1 Failed Login Attempts .....	8
Fig 1.2 First Login Successfully .....	8
Fig 1.3 Second Login Successfully.....	8
<b>Suricata logs:-</b> .....	8
Fig 1.4 Telnet Connection Attempt .....	9
<b>Kernel logs:</b> .....	9
Fig 1.5 kernal.log .....	9
<b>System logs</b> .....	9
Fig 1.6 Syslog .....	10
Analysis.....	11
Fig 2.0 Conversation .....	11
Fig 2.1. View The Website .....	12
<b>Recommendation</b> .....	12
Ensure that your software is updated .....	12

Fig 2.2 request and reply.....	13
Fig 2.3 started dictionary attack.....	13
Fig 2.4 Filed Password attempt.....	14
Fig 2.5 Successfully logging using a dictionary attack.....	14
<b>Recommendation:</b> .....	15
Password protection .....	15
Analysis of Activity Log.....	16
Fig 3.1 Attacker Run Commands.....	16
Fig 3 3 employee-details.txt.....	17
Fig 3.4 email-password-recovery-code.cs .....	17
Fig 3.5 copy and removing files .....	17
Fig. Ccredit-card-info.txt .....	18
<b>Recommendation:</b> .....	18
Compromise Phase.....	19
Fig 4.3 SSH Encrypted Conversation .....	20
Recommendation .....	20
Graphical Time-Line events .....	21
Document the results: .....	22
Conclusion .....	24
References .....	25

## **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-yoghurt
```

**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 8<sup>th</sup> at 14:35:46**.



## Kernel logs:

[illegible]

## 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** can be seen in the following image.

```

File Edit View

Mar 8 14:37:43 frozenyoghurt-pc kernel: [ 1028.372750] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55045 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:43 frozenyoghurt-pc kernel: [ 1028.393177] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=55046 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:44 frozenyoghurt-pc kernel: [ 1029.317245] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=54 TOS=0x10 PREC=0x00 TTL=64 ID=55047 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:44 frozenyoghurt-pc kernel: [ 1029.319563] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=55048 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:44 frozenyoghurt-pc kernel: [ 1029.327345] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=55049 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:44 frozenyoghurt-pc kernel: [ 1029.327775] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=55050 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:44 frozenyoghurt-pc kernel: [ 1029.329860] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=55051 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:44 frozenyoghurt-pc kernel: [ 1029.428394] iptable logN-emp88 OUT= MAC= SRC=10.0.0.215 DST=224.0.0.251 LEN=73 TOS=0x00 PREC=0x00 TTL=255 ID=22657 DF PROTO=UDP SPT=5353 DPT=5353 LEN=53
Mar 8 14:37:44 frozenyoghurt-pc kernel: [ 1029.508048] iptable logN-emp88 OUT= MAC= SRC=192.168.56.102 DST=224.0.0.251 LEN=73 TOS=0x00 PREC=0x00 TTL=255 ID=22657 DF PROTO=UDP SPT=5353 DPT=5353 LEN=53
Mar 8 14:37:49 frozenyoghurt-pc kernel: [ 1034.733867] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55052 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:49 frozenyoghurt-pc kernel: [ 1034.908071] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55053 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:50 frozenyoghurt-pc kernel: [ 1035.180515] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55054 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:50 frozenyoghurt-pc kernel: [ 1035.332308] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55055 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:50 frozenyoghurt-pc kernel: [ 1035.548953] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55056 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:51 frozenyoghurt-pc kernel: [ 1036.356770] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55057 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:51 frozenyoghurt-pc kernel: [ 1036.516892] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55058 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:51 frozenyoghurt-pc kernel: [ 1036.660115] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55059 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:51 frozenyoghurt-pc kernel: [ 1036.796810] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55060 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:51 frozenyoghurt-pc kernel: [ 1036.924380] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55061 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:52 frozenyoghurt-pc kernel: [ 1037.061052] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55062 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:52 frozenyoghurt-pc kernel: [ 1037.189017] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55063 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:52 frozenyoghurt-pc kernel: [ 1037.420443] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55064 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:52 frozenyoghurt-pc kernel: [ 1037.572340] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55065 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:52 frozenyoghurt-pc kernel: [ 1037.692559] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55066 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:53 frozenyoghurt-pc kernel: [ 1038.084537] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55067 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:53 frozenyoghurt-pc kernel: [ 1038.333855] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55068 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:53 frozenyoghurt-pc kernel: [ 1038.548262] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55069 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:53 frozenyoghurt-pc kernel: [ 1038.860989] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=54 TOS=0x10 PREC=0x00 TTL=64 ID=55070 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:53 frozenyoghurt-pc kernel: [ 1038.861899] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=55071 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:56 frozenyoghurt-pc kernel: [ 1041.564561] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=53 TOS=0x10 PREC=0x00 TTL=64 ID=55072 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:56 frozenyoghurt-pc kernel: [ 1041.564890] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=55073 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:57 frozenyoghurt-pc kernel: [ 1042.053030] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=54 TOS=0x10 PREC=0x00 TTL=64 ID=55074 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:57 frozenyoghurt-pc dbus-daemon[1271]: [session uid=1000 pid=1271] Activating via systemd: service name='org.freedesktop.Tracker1.Miner.Extract' unit='tracker-extract.service' requested by ':1.2' (uid=1000 pid=1264 comm='/usr/libexec/trac
Mar 8 14:37:57 frozenyoghurt-pc system[1255]: Starting Tracker metadata database store and lookup manager...
Mar 8 14:37:57 frozenyoghurt-pc kernel: [ 1042.057886] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=55075 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:57 frozenyoghurt-pc kernel: [ 1042.058851] iptable logN-emp88 OUT= MAC=08:00:27:6d:47:d4:0a:00:27:00:00:00:00:00 SRC=192.168.56.1 DST=192.168.56.102 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=55076 DF PROTO=TCP SPT=53248 DPT=23
Mar 8 14:37:57 frozenyoghurt-pc dbus-daemon[1271]: [session uid=1000 pid=1271] Successfully activated service 'org.freedesktop.Tracker1'
Mar 8 14:37:57 frozenyoghurt-pc tracker-extract[2477]: Set scheduler policy to SCHED_IDLE
Mar 8 14:37:57 frozenyoghurt-pc tracker-extract[2477]: Setting priority nice level to 19
Mar 8 14:37:57 frozenyoghurt-pc dbus-daemon[1271]: [session uid=1000 pid=1271] Successfully activated service 'org.freedesktop.Tracker1.Miner.Extract'
Mar 8 14:37:57 frozenyoghurt-pc system[1255]: Started Tracker metadata extractor...

```

Fig 1.6 Syslog



Network Packet Capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>F

Time	Source	Src Port	Destination	Des Port	Protocol	Identification	Info
2022-03-08 14:29:25.245358054	192.168.56.1	60682	192.168.56.102	80	HTTP	0xc4af (50351)	GET / HTTP/1.1
2022-03-08 14:29:25.248441892	192.168.56.102	80	192.168.56.1	60682	HTTP	0xb3a8 (936)	HTTP/1.1 200 OK (text/html)
2022-03-08 14:29:25.294641383	192.168.56.1	60682	192.168.56.102	80	HTTP	0xc4b1 (50353)	GET /css/style.css HTTP/1.1
2022-03-08 14:29:25.295054230	192.168.56.1	60684	192.168.56.102	80	HTTP	0x0c3d (3133)	GET /css/mobile.css HTTP/1.1
2022-03-08 14:29:25.295374658	192.168.56.1	60686	192.168.56.102	80	HTTP	0x0cab (3243)	GET /js/mobile.js HTTP/1.1
2022-03-08 14:29:25.296724869	192.168.56.102	80	192.168.56.1	60686	HTTP	0x2ac1 (10945)	HTTP/1.1 200 OK (application/javascript)
2022-03-08 14:29:25.297132774	192.168.56.102	80	192.168.56.1	60684	HTTP	0xe4ee (58606)	HTTP/1.1 200 OK (text/css)
2022-03-08 14:29:25.297623655	192.168.56.102	80	192.168.56.1	60682	HTTP	0x03ac (940)	HTTP/1.1 200 OK (text/css)
2022-03-08 14:29:25.297886583	192.168.56.1	60684	192.168.56.102	80	HTTP	0xb4c0 (3136)	GET /images/logo.png HTTP/1.1
2022-03-08 14:29:25.297886654	192.168.56.1	60686	192.168.56.102	80	HTTP	0xb4cd (3245)	GET /images/bg-home.jpg HTTP/1.1
2022-03-08 14:29:25.297978616	192.168.56.1	60682	192.168.56.102	80	HTTP	0xc4b5 (50357)	GET /images/yogurt.jpg HTTP/1.1
2022-03-08 14:29:25.299899798	192.168.56.102	80	192.168.56.1	60686	HTTP	0x2ac3 (10947)	HTTP/1.1 304 Not Modified
2022-03-08 14:29:25.300095370	192.168.56.102	80	192.168.56.1	60684	HTTP	0xe4f0 (58608)	HTTP/1.1 304 Not Modified
2022-03-08 14:29:25.300918742	192.168.56.102	80	192.168.56.1	60682	HTTP	0x03bc (956)	HTTP/1.1 200 OK (JPEG JFIF image)
2022-03-08 14:29:25.306244480	192.168.56.1	60682	192.168.56.102	80	HTTP	0xc4c4 (50372)	GET /images/icons.png HTTP/1.1
2022-03-08 14:29:25.306735042	192.168.56.102	80	192.168.56.1	60682	HTTP	0x03be (958)	HTTP/1.1 304 Not Modified
2022-03-08 14:29:25.316283846	192.168.56.1	60682	192.168.56.102	80	HTTP	0xc4c6 (50374)	GET /fonts/lato-regular-webfont.woff HTTP/1.1
2022-03-08 14:29:25.316833788	192.168.56.102	80	192.168.56.1	60682	HTTP	0x03c0 (960)	HTTP/1.1 304 Not Modified
2022-03-08 14:29:25.317326609	192.168.56.1	60682	192.168.56.102	80	HTTP	0xc4c8 (50376)	GET /fonts/quick-sand-bold-webfont.woff HTTP/1.1
2022-03-08 14:29:25.317420018	192.168.56.102	80	192.168.56.1	60682	HTTP	0x03c1 (961)	HTTP/1.1 304 Not Modified
2022-03-08 14:29:25.318506828	192.168.56.1	60682	192.168.56.102	80	HTTP	0xc4ca (50378)	GET /fonts/lato-bold-webfont.woff HTTP/1.1
2022-03-08 14:29:25.318591269	192.168.56.102	80	192.168.56.1	60682	HTTP	0x03c2 (962)	HTTP/1.1 304 Not Modified
2022-03-08 14:29:25.319266777	192.168.56.1	60682	192.168.56.102	80	HTTP	0xc4cc (50380)	GET /fonts/magna-bold-webfont.woff HTTP/1.1
2022-03-08 14:29:25.319352137	192.168.56.102	80	192.168.56.1	60682	HTTP	0x03c3 (963)	HTTP/1.1 304 Not Modified
2022-03-08 14:29:25.319450631	192.168.56.1	60684	192.168.56.102	80	HTTP	0xb4c2 (3138)	GET /fonts/roboto-regular-webfont.woff HTTP/1.1
2022-03-08 14:29:25.319604544	192.168.56.102	80	192.168.56.1	60684	HTTP	0xe4f2 (58610)	HTTP/1.1 304 Not Modified
2022-03-08 14:29:25.331640457	192.168.56.1	60690	192.168.56.102	80	HTTP	0x7ec8 (32456)	GET /login HTTP/1.1
2022-03-08 14:29:25.331875350	192.168.56.102	80	192.168.56.1	60690	HTTP	0xfdb5 (64949)	HTTP/1.1 404 Not Found (text/html)
2022-03-08 14:30:12.069647146	192.168.56.1	60692	192.168.56.102	80	HTTP	0x9263 (37475)	GET /admin HTTP/1.1
2022-03-08 14:30:12.070436637	192.168.56.102	80	192.168.56.1	60692	HTTP	0x1854 (6228)	HTTP/1.1 404 Not Found (text/html)
2022-03-08 14:30:17.258842449	192.168.56.1	60694	192.168.56.102	80	HTTP	0xb0f0 (3845)	GET /login.php HTTP/1.1
2022-03-08 14:30:17.259059230	192.168.56.102	80	192.168.56.1	60694	HTTP	0x2435 (9269)	HTTP/1.1 404 Not Found (text/html)
2022-03-08 14:30:22.279760886	192.168.56.1	60696	192.168.56.102	80	HTTP	0x528b (21131)	GET /robots.txt HTTP/1.1
2022-03-08 14:30:22.280480256	192.168.56.102	80	192.168.56.1	60696	HTTP	0xd1e8 (53736)	HTTP/1.1 404 Not Found (text/html)
2022-03-08 14:30:27.187184320	192.168.56.1	60696	192.168.56.102	80	HTTP	0x528d (21133)	GET /about.html HTTP/1.1
2022-03-08 14:30:27.189215826	192.168.56.102	80	192.168.56.1	60696	HTTP	0xd1eb (53739)	HTTP/1.1 200 OK (text/html)

**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:deff::5353	5353	ff02::fb	5353	MDNS	0x224b (8779)	Standard query 0x0000 PTR_pgkey-hkp._tcp.local, "QM" question
2022-03-08 14:32:43.959242805	192.168.56.102	5353	224.0.0.251	5353	MDNS		Standard query 0x0000 PTR_pgkey-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 TSecr=0
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 14:32:45.293362695	192.168.56.102	23	192.168.56.1	53210	TCP	0xd303 (54019)	Telnet Data ...
2022-03-08 14:32:45.293362695	192.168.56.102	23	192.168.56.1	53210	TCP	0xd7f9 (18425)	23 → 53210 [ACK] Seq=1 Ack=28 Win=65152 Len=0 TSval=2706851792 TSecr=3581394409
2022-03-08 14:32:45.386379283	192.168.56.1	53210	192.168.56.102	23	TCP	0xd7fa (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	TCP	0xd7fb (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	TCP	0xd306 (54022)	Telnet Data ...
2022-03-08 14:32:45.386678609	192.168.56.102	23	192.168.56.1	53210	TCP	0xd7fc (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	TCP	0xd7fd (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	TCP	0xd308 (54024)	Telnet Data ...
2022-03-08 14:32:45.387127224	192.168.56.102	23	192.168.56.1	53210	TCP	0xd7fe (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	TCP	0xd7ff (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	TCP	0xd800 (18432)	Telnet Data ...
2022-03-08 14:32:45.389568591	192.168.56.1	53210	192.168.56.102	23	TCP	0xd30a (54026)	Telnet Data ...
2022-03-08 14:32:45.389577929	192.168.56.102	23	192.168.56.1	53210	TCP	0xd801 (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 14:32:45.390456257	192.168.56.102	23	192.168.56.1	53210	TCP	0xd802 (18434)	Telnet Data ...
2022-03-08 14:32:45.390835324	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	TCP	0xd30d (54029)	Telnet Data ...
2022-03-08 14:32:47.675270169	192.168.56.102	23	192.168.56.1	53210	TCP	0xd803 (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	TCP	0xd804 (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	TCP	0xd30f (54031)	Telnet Data ...

Fig 2.3 started dictionary attack

```

.....#.#".....#.'.....!...Ubuntu 20.04.4 LTS
frozenyoghurt-pc login: ..ffrroozzeenn--yyoogghuurtt
-
Password: touch
-
Login incorrect
frozenyoghurt-pc login: ffrroozzeenn--yyoogghuurtt
-
Password: tom
-
Login incorrect
frozenyoghurt-pc login: ffrroozzeenn--yyoogghuurtt
-
Password: admin
-
Login incorrect
frozenyoghurt-pc login: ffrroozzeenn--yyoogghuurtt
-
Password: rooot
-
Login incorrect
frozenyoghurt-pc login: ffrroozzeenn--yyoogghuurtt
-
Password: freeze
-
Login incorrect
Maximum number of tries exceeded (5)

```

**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.

```

Wireshark - Follow TCP Stream (tcp.stream eq 2) - Network Packet Capture.pcapng
.....#.....".....#....."!.....!...Ubuntu 20.04.4 LTS
frozenyoghurt-pc login: ..ffrroozeenn--yyoogghhuurtt
.
Password: password
.
Login incorrect
frozenyoghurt-pc login: ffrroozeenn--yyoogghhuurtt
.
Password: yoghurt
.
Login incorrect
frozenyoghurt-pc login: ffrroozeenn--yyoogghhuurtt
.
Password: lisahanks
.
Login incorrect
frozenyoghurt-pc login: ffrroozeenn--yyoogghhuurtt
.
Password: admin1
.
Login incorrect
frozenyoghurt-pc login: ffrroozeenn--yyoogghhuurtt
.
Password: frozen
.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-30-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

18 updates can be applied immediately.
11 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Mar  7 17:09:58 GMT 2022 from 1.capita.vpn.port.ac.uk on pts/4
frozen-yoghurt@frozenyoghurt-pc:~$
116 client pkts, 114 server pkts, 166 bytes.

```

### 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

```

Wireshark · Follow TCP Stream (tcp.stream eq 25) · Network Packet Capture.pcapng

.....!..".'.#.....#..'.!..".'.#.....'.O.....38400,38400....#.df1-
bk-24:1.....'.DISPLAY.dfl-bk-24:1.....xterm-256color.....Ubuntu 20.04.4 LTS
frozenyoghurt-pc login: ffr.. ...ffrroozzeenn--yyoogghhuurtt
Password: frozen
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

18 updates can be applied immediately.
11 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Mar  8 14:35:08 GMT 2022 from 1.capita.vpn.port.ac.uk on pts/6
[j0;frozen-yoghurt@frozenyoghurt-pc: ~/.[01;32mfrozen-yoghurt@frozenyoghurt-pc.[00m$ llss
auth.log                                fast.log
credit-card-info.txt                    kern.log
.[0m.[01;31mcredit-card-info.zip.[0m    .[01;34mMusic.[0m
.[01;34mDesktop.[0m                    .[01;34mPictures.[0m
.[01;34mDocuments.[0m                  .[01;34mPublic.[0m
.[01;34mDownloads.[0m                  syslog
electronic-card-transactions-january-2022-csv-tables.csv .[01;34mTemplates.[0m
email-password-recovery-code.csv        .[01;34mVideos.[0m
employee-details.txt

```

**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.





- 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.

```

[0;31mcredit-card-info.zip
[credit-card-info.zip] credit-card-info.txt password: cred .....frozen
replace credit-card-info.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: yy
inflating: credit-card-info.txt
]0;frozen-yoghurt@frozenyoghurt-pc: ~.[01;32mfrozen-yoghurt@frozenyoghurt-pc.[00m:.[01;34m~.[00m$
]0;frozen-yoghurt@frozenyoghurt-pc: ~.[01;32mfrozen-yoghurt@frozenyoghurt-pc.[00m:.[01;34m~.[00m$ ll...[K..llss
auth.log
credit-card-info.txt
fast.log
kern.log
.[0m.[01;31mcredit-card-info.zip.[0m
.[01;34mDesktop.[0m
.[01;34mDocuments.[0m
.[01;34mDownloads.[0m
.[01;34mMusic.[0m
.[01;34mPictures.[0m
.[01;34mPublic.[0m
syslog
electronic-card-transactions-january-2022-csv-tables.csv .[01;34mTemplates.[0m
email-password-recovery-code.csv .[01;34mVideos.[0m
employee-details.txt
]0;frozen-yoghurt@frozenyoghurt-pc: ~.[01;32mfrozen-yoghurt@frozenyoghurt-pc.[00m:.[01;34m~.[00m$ ccaatt cccree .dit-card-info.tt xt
Name: frozen yoghurt ltd
credit card details: 4658 1234 0909 9876 0000
CVV: 124
Sort code: 406921
Bank: Capital Bank

Name Frozen Youghurt Ltd
Credit card details: 4658 0909 1234 5432 6789
CVV: 135
Sort code: 306129
Bank: Bank of West England
]0;frozen-yoghurt@frozenyoghurt-pc: ~.[01;32mfrozen-yoghurt@frozenyoghurt-pc.[00m:.[01;34m~.[00m$ ss...[K.....ccdd DDesskk
top/

```

**Fig 3.6 Ccredit-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.

2022-03-08 14:44:23.945222452	0a:00:27:00:00:00	Broadcast	ARP	Who has 192.168.56.102? Tell 192.168.56.100 (duplicate use of 192.168.56.100 detected!)
2022-03-08 14:44:23.945239071	PcsCompu_6d:47:d4	0a:00:27:00:00:00	ARP	192.168.56.102 is at 08:00:27:6d:47:d4 (duplicate use of 192.168.56.100 detected!)

**Fig 4.1 Duplicate IP detected**

Time	Source	Src Port	Destination	Dest Port	Protocol	Identification	Info
2022-03-08 14:44:23.945391237	192.168.56.100	36548	192.168.56.102	22	TCP	0xe14f (57679)	36548 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=270357142 TSecr=0 WS=128
2022-03-08 14:44:23.945416363	192.168.56.102	22	192.168.56.100	36548	TCP	0x0000 (0)	22 → 36548 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2270269434 TSecr=270357142
2022-03-08 14:44:23.945530581	192.168.56.100	36548	192.168.56.102	22	TCP	0xe150 (57680)	36548 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=270357142 TSecr=2270269434
2022-03-08 14:44:23.945723682	192.168.56.100	36548	192.168.56.102	22	SSHv2	0xe151 (57681)	Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-dubuntu0.4)
2022-03-08 14:44:23.945734587	192.168.56.102	22	192.168.56.100	36548	TCP	0x0520 (1312)	22 → 36548 [ACK] Seq=1 Ack=42 Win=65152 Len=0 TSval=2270269434 TSecr=270357142
2022-03-08 14:44:23.951470094	192.168.56.102	22	192.168.56.100	36548	SSHv2	0x0521 (1313)	Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-dubuntu0.4)
2022-03-08 14:44:23.951596165	192.168.56.100	36548	192.168.56.102	22	TCP	0xe152 (57682)	36548 → 22 [ACK] Seq=42 Ack=42 Win=64256 Len=0 TSval=270357148 TSecr=2270269440
2022-03-08 14:44:23.951765083	192.168.56.100	36548	192.168.56.102	22	TCP	0xe153 (57683)	36548 → 22 [ACK] Seq=42 Ack=42 Win=64256 Len=1448 TSval=270357148 TSecr=2270269440 [TCP se...
2022-03-08 14:44:23.951765120	192.168.56.100	36548	192.168.56.102	22	SSHv2	0xe154 (57684)	Client: Key Exchange Init
2022-03-08 14:44:23.95176872	192.168.56.102	22	192.168.56.100	36548	TCP	0x0522 (1314)	22 → 36548 [ACK] Seq=42 Ack=1490 Win=64128 Len=0 TSval=2270269440 TSecr=270357148
2022-03-08 14:44:23.951804909	192.168.56.102	22	192.168.56.100	36548	TCP	0x0523 (1315)	22 → 36548 [ACK] Seq=42 Ack=1554 Win=64128 Len=0 TSval=2270269440 TSecr=270357148
2022-03-08 14:44:23.952507216	192.168.56.102	22	192.168.56.100	36548	SSHv2	0x0524 (1316)	Server: Key Exchange Init
2022-03-08 14:44:23.952595407	192.168.56.100	36548	192.168.56.102	22	TCP	0xe155 (57685)	36548 → 22 [ACK] Seq=1554 Ack=1098 Win=64128 Len=0 TSval=270357149 TSecr=2270269441
2022-03-08 14:44:23.953958856	192.168.56.100	36548	192.168.56.102	22	SSHv2	0xe156 (57686)	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
2022-03-08 14:44:23.953969929	192.168.56.102	22	192.168.56.100	36548	TCP	0x0525 (1317)	22 → 36548 [ACK] Seq=1098 Ack=1602 Win=64128 Len=0 TSval=2270269443 TSecr=270357150
2022-03-08 14:44:23.956961056	192.168.56.102	22	192.168.56.100	36548	SSHv2	0x0526 (1318)	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=...
2022-03-08 14:44:23.957238530	192.168.56.100	36548	192.168.56.102	22	TCP	0xe157 (57687)	36548 → 22 [ACK] Seq=1602 Ack=1606 Win=64128 Len=0 TSval=270357153 TSecr=2270269446
2022-03-08 14:44:23.958658272	192.168.56.100	36548	192.168.56.102	22	SSHv2	0xe158 (57688)	Client: New Keys

**Fig 4.2 ssh connection failure**

```

SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4
....
...y..3HQ.K.....curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-
hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-
c....ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ecdsa-
sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,sk-ssh-
ed25519-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,sk-ecdsa-
sha2-nistp256@openssh.com,ssh-ed25519,sk-ssh-ed25519@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh-rsa....lchacha20-
poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com....lchacha20-
poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com....umac-64-etm@openssh.com,umac-128-
etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-
sha1....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib.....
...le%q.i....q.3....curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-
hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256....Arsha-
sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519....lchacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com....lchacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-
gcm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-
sha1....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib.....
...h....ecdsa-sha2-nistp256....n....z....d....E>....rTe....h.R#....-AM....@6e....k>8....g.N...}.y.i?
5.....~.....@....d....ecdsa-sha2-nistp256....I....I....u]"x.].*....5.a.7).JQR.q#R..l....V....f....Oq.fR),..A....k..6.....
.....rGIW.bfi....vk.@....c.....N9....>%.O.r.n.h.sJ...[.oG.....U....o.../..vy0v..D..p..1b.....(..o/x..lgMk...e..
0..).%....4./....p.....T..s_@.....e.;7....c'$.M...j[....Z..
..N....f.....
.....t..n..v.%F..C.....V...%...<PC..Y.[....3vc..0.....L...E.M3.@.....T..m.....a..._Z6.i.B.ni).x...=...
6..l.....i.'w/..<Ko(cfv..
.....%.0d.....I.B.G.....ke.y;77).HI:....'D.$.....(.....$.
4.5^..".%M18".5..-|($#a.i<.y..l.DB..8.IH.<z.....],.....s....+0..Z..V....y\X...cU.>..H..V...?..5.....u.:).RX[U..
..TV.u..C..F.M.1.I..-..}.._..

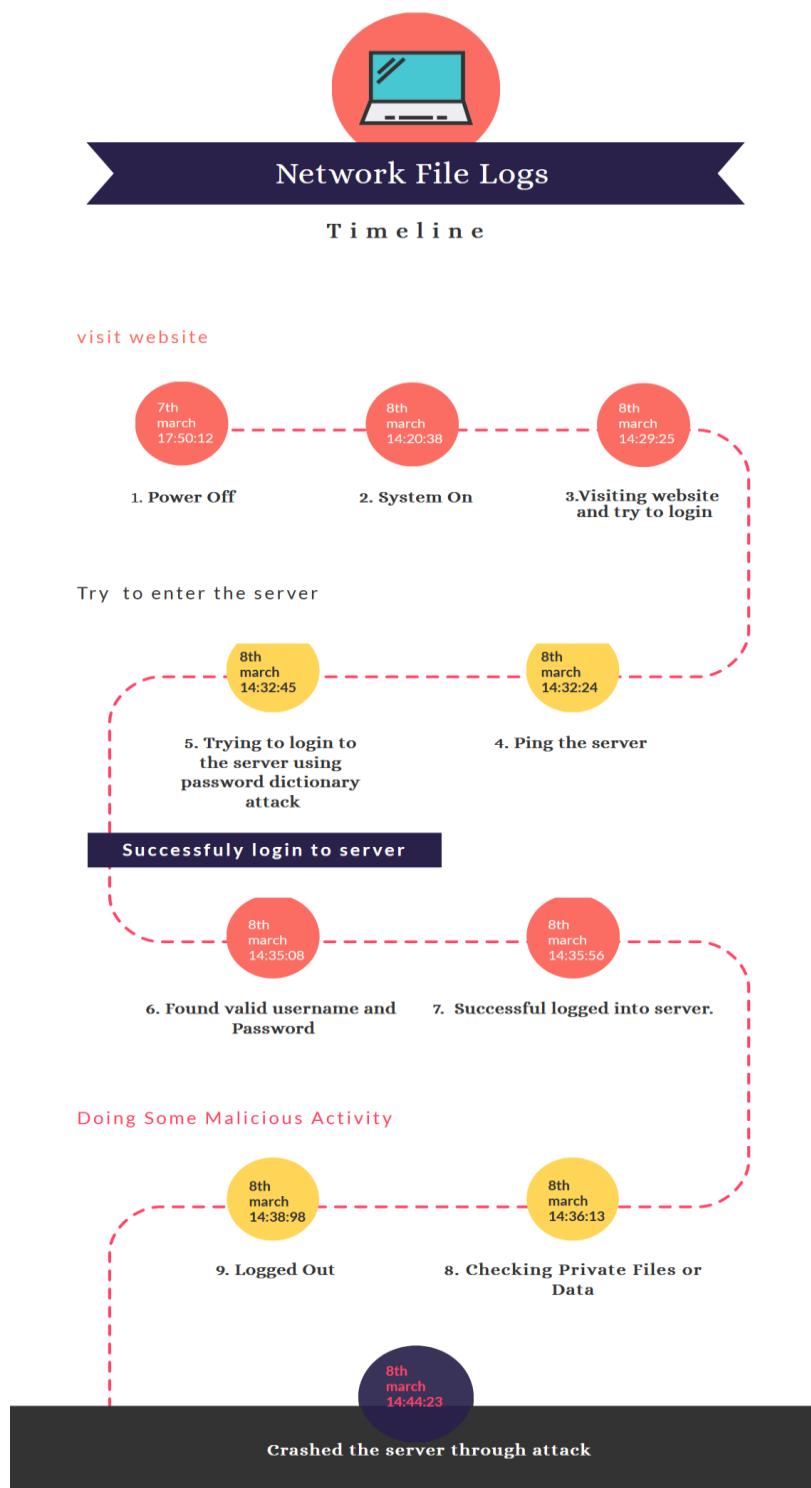
```

**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 <b>High</b>	If any port number is open . <b>High</b>	Serves <b>Critical</b>	All services(website, email,etc.)will be unavailable for at least 3 hours. <b>Critical</b>	<b>High</b> Website data can be stole	<b>High</b> 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 <b>High</b>	Company name related Password attack <b>High</b>	Website <b>Critical</b>	Website resources will be unavailable. <b>Critical</b>	<b>Medium</b> Dictionary attack was discovered once in 2 years.	<b>Medium</b> 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 <b>High</b>	The server room is in the shop. <b>Low</b>	Server. <b>Critical</b>	All services will be unavailable. <b>Critical</b>	<b>Low</b> The last flood in the area happened 10 years ago.	<b>Low</b>	Back up your data on the cloud(AWS) Or try to do multiple Regine instance for hosting
Accidental human interference – accidental file deletions <b>High</b>	Permission is configured properly; IT auditing software is in place; backups are taken regularly. <b>Low</b>	Files on a file share <b>Medium</b>	Critical data could be lost but almost certainly could be restored from backup. <b>Low</b>	<b>Medium</b>	<b>Low</b>	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](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](https://www.researchgate.net/publication/228911072_Network-Based_Dictionary_Attack_Detection)