Premium House Lights Incident Report

By: Derek Mayen

Table of Contents

Executive Summary

There has been communication via email with the company “Premium House Lights” of an attacker claiming they have been able to access the customer information database, and have taken their information hostage and provided a ransom of 10 BTC to be deposited in a secure wallet ID by a certain time and date. The attackers have provided an example list of data they have collected from the database. After a thorough investigation of the access logs, database logs, and traffic to the server, we can determine how long this attack has been taking place, and how they managed to infiltrate the network.

The Current timeline of the attack is as follows:

19th February 2022 at 21:56:11 UTC -0500 (Eastern Standard Time)

- The attacker, with the help of a CrawlerBot, used this bot to gather information about the webserver.

19th February 2022 at 21:58:32 :“301” Code Indicates Data Moved

- The attacker managed to copy the database and moved the information to a new place, while deleting the local database copy.

19th February 2022 at 21:59:04

- The attacker inserted a malicious script to move information to a new location.

19th February 2022 at 21:59:47 : Network Scan Took Place

- The attacker used a scanning method named “nmap” to scan the network for any vulnerabilities and access they can take to infiltrate the database.

19th February 2022 at 22:00:19 : Brute Force Attack

- The attacker failed a login attempt multiple times before gaining access to the database.

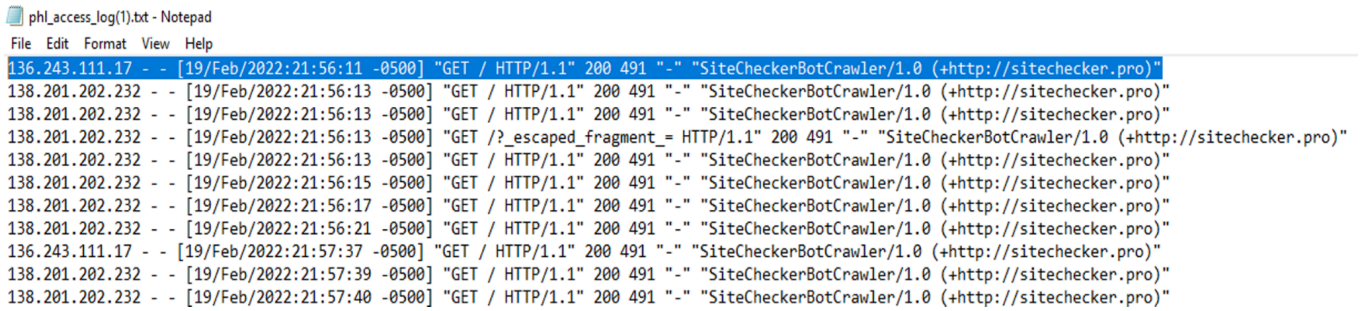
19th February 2022 at 22:02:36 : Local Database Copy was Deleted

- Using a linux command, the attacker was able to copy the database contents of customer information, and send it to themselves before deleting the local copy.

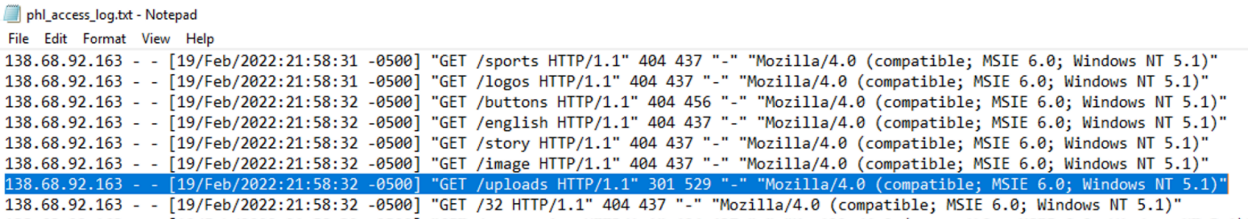
21st February 2022 at 09:04:21 : Customer Support Received Email

- The ransom email was received by Customer support with proof of data breach.

Technical Analysis

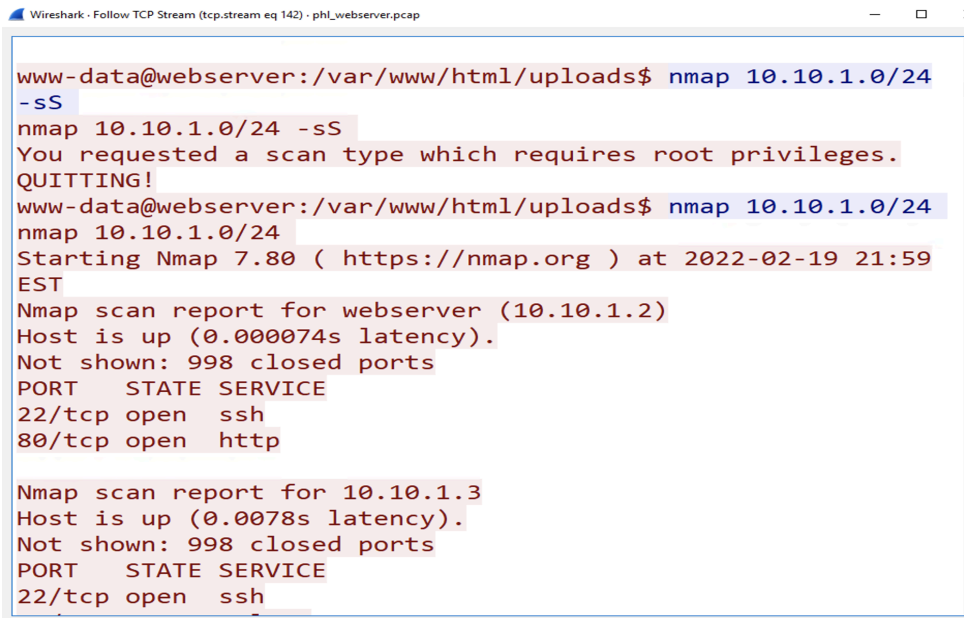


From the first reconnaissance attack located in the first access log, commenced at 9:56 pm EST using a CrawlerBot. This type of attack targets websites mainly and can be used to test web servers and is frequently used to gather intel for a company wanting to see what kind of information can be gathered from their server. In this case however, the attacker used the “CrawlerBot” to inspect the webserver and gain access to private information that could be left vulnerable. From the fourth line which mentions “?_escaped_Fragment_” this is an indication that information has been requested from the server, in which case the bot will turn the information into a readable snapshot for the attacker to view. A further indication of the reconnaissance being successful, is the status code reading as “200” which indicates a successful request.We can also see that there was an indication of a successful data transfer to a new location at 9:58:32 pm EST. This IoC (Indicator of Compromise) is from another status code reading as “301”.

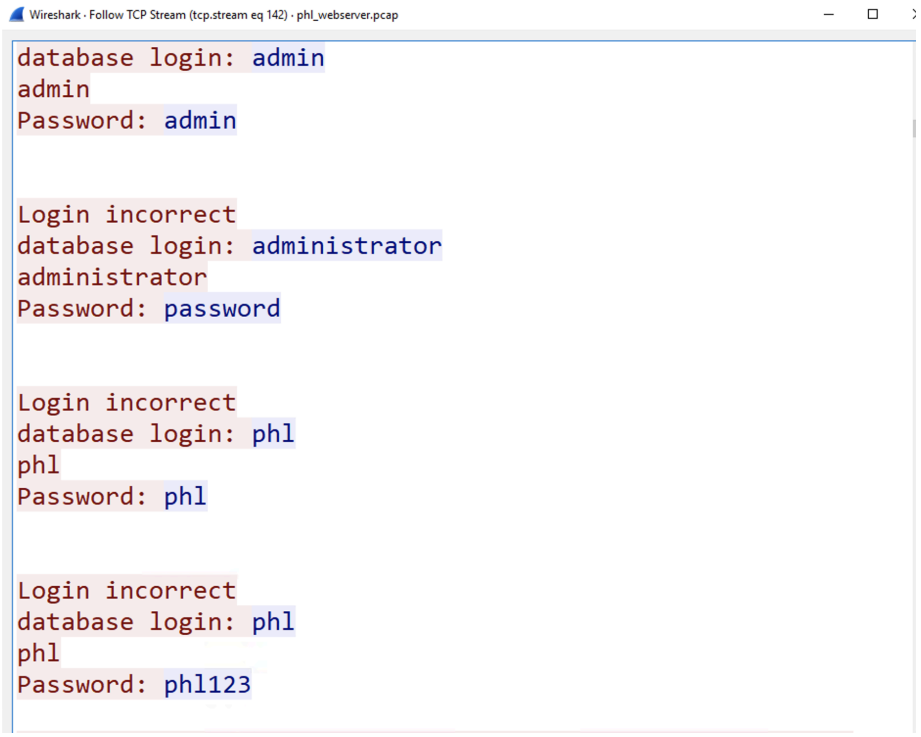


From the wireshark capture of the phl database, we can also see evidence of our second IoC of a reverse shell command that enables a python script that runs on the database, through port 54950. This indicates that the attacker remotely accessed the database in order to insert a malicious program to gather information and move them to another location. This script was executed at 9:59:04 EST.

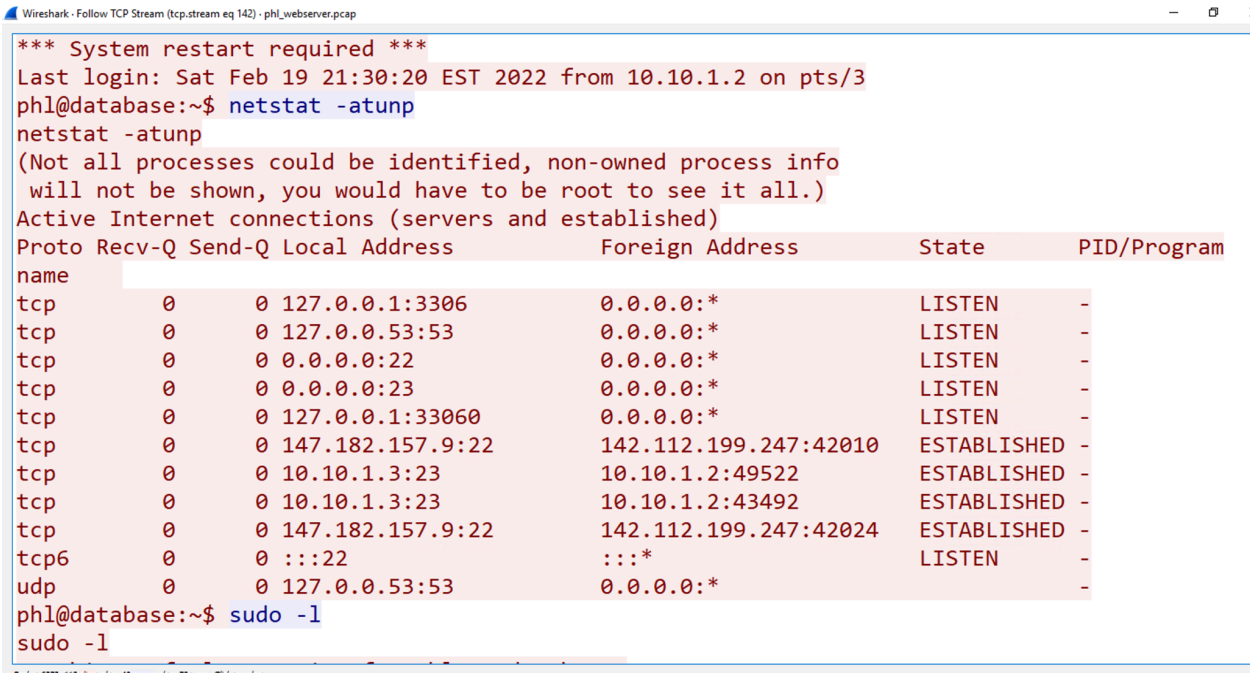
Our third IoC comes from another wireshark capture that was caught when a network scan was conducted on the customer subnet according to the topology provided (10.10.1.0/24). When the scan concluded, it revealed the open devices managing the subnet and what vulnerabilities they contained for any breaches. The attackers then chose a target to begin their brute force attack to gain access to the machine “10.10.1.3”.



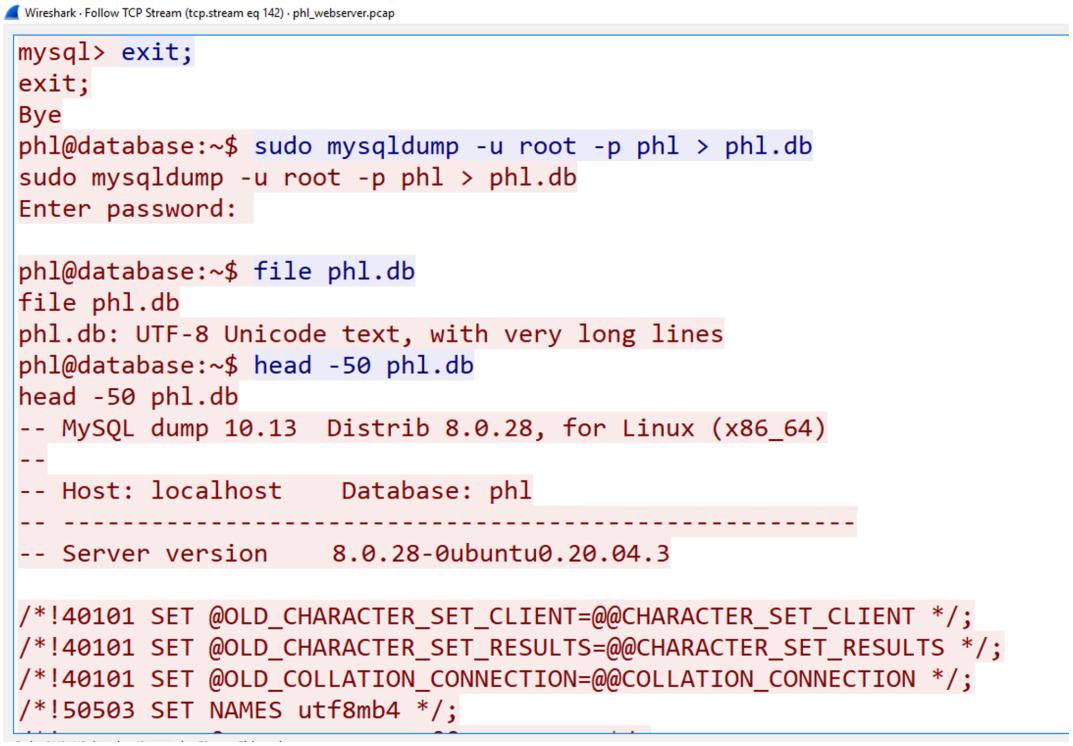
The investigation further into the Wireshark capture will reveal the attempts the attackers made when trying to access the machine, and when they were successful at 22:00:19 on February 19th 2022. The attackers attempted 4 total logins 3 of which were unsuccessful. The screen capture provided below will show the attacker attempting the login credentials until they have discovered the username and password username: “phl” and password: “phl123”.



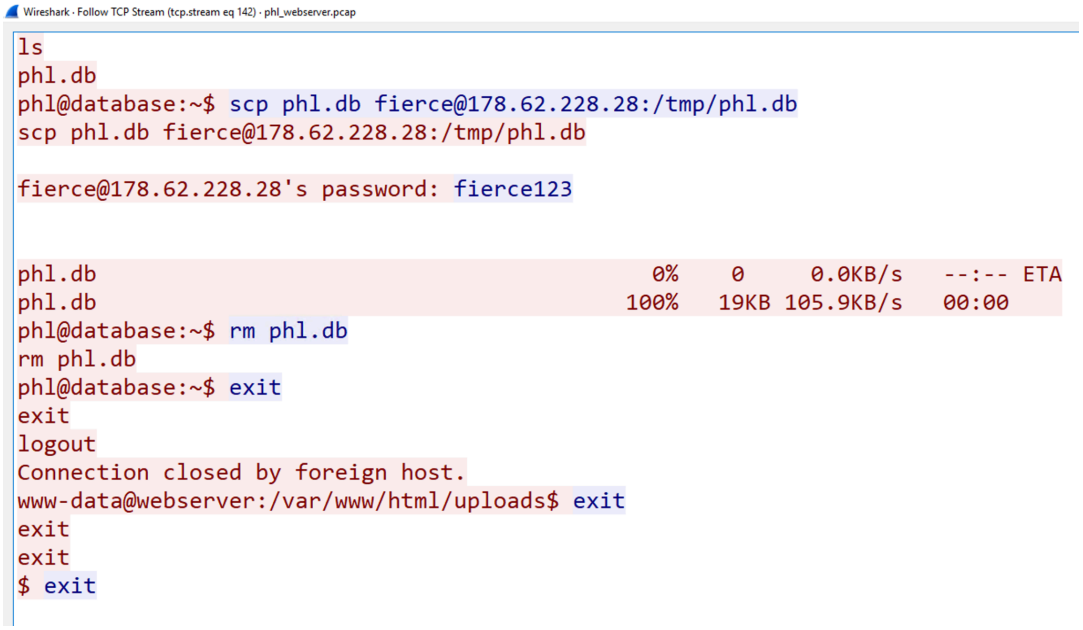
After gaining access to the located machine, they began to run commands in which to gather more information about any accounts with admin privileges at 9:30:20 EST. The first command the attackers ran was “netstat - atunp”, which was used to gather more information about the network, its connections, and access ports. The next command used was “sudo -l”, this command lists the users who have access to the device, this allowed the attackers to gain information on which users have admin privileges as well as the configuration of the server’s security. The next command the attackers used was “sudo mysql -u root -p” which allowed the attackers access to the database without the need for a password.



After the attackers gained their admin privileges, they continued to examine the database in order to discover the location of the customer data and where it was kept. Once the attackers found what they were looking for, they began the extraction process with the command “sudo mysqldump -u root -p phl > phl.db”. After securing the copy of the database, they confirmed the contents and began to transfer the data to a new location.



On the 19th of February 2022 at 9:02:36 EST, the attackers used the “scp phl.db fierce-” command was used to move the extracted data from the database to the attackers secure IP address “178.62.228.28” and to remove the original copy of the database they used the “rm phl.db” command to remove the contents of the database.



Incident Response

After investigating the incident that has happened to Premium House Lights, the first step would be to organize a plan of action or workflow in order of priority. The first thing that should be done is to handle the response after the attack. For the purposes of this document we will refer to the NIST (National Institute of Standards and Technology) Incident Response Framework. This framework will be the cornerstone of the process of what to do after the attack which goes as follows:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Discovery
4. Post-Incident Activity

The first step of the Framework “Preparation” is about setting up the proper tools necessary to detect or prevent attacks when they occur, this would be the proactive threat hunting that would bolster security for the company to stop attacks similar to the previous incident that occurred. For example, adding MFA (Multi-Factor Authentication) methods when a user is attempting to login to their account. Using MFA would prevent brute force attacks which depend on unprotected or very low security on accounts and their login information. Enabling MFA would alert the account user if any login attempt was made on their account, and if it is an unauthorized user, the account owner may change their login details, to prevent data breaches. Other methods of preparation for incidents related to brute force attacks, are frequent security audits. Frequent security audits are made to investigate the network's traffic and log data, in order to investigate signs of possible data breaches and suspicious activity.

The second step of the NIST framework is called “Detection and Analysis”. This step of the framework is dedicated to the detection of possible Indicators of Compromise (IoC’s) which will alert the security team to possible breaches on the network. This can be done by many methods, in terms of brute force attacks, the process would be similar to the steps taken from the previous section of this document. In order to make this step efficient, the proper tools are required to enable the security team to be able to fully investigate every aspect of the network. This can be done through applications such as “Wireshark” which monitors network traffic and provides the communication between IP addresses. These can be used to investigate abnormal traffic and processes that have been placed on the network. Other forms of data analysis can be to keep stored access log files, and database log files, that can be stored on a separate database or server only to be accessed when security audits or a suspected attack has taken place. This will allow security analysts to sort through log files to find possible IoC’s as seen in the previous section of this document.

Containment, Eradication, and Discovery, is the next step of the NIST Framework in which the affected areas will be confined to minimize infected areas of the network and mitigating service disruptions. This stage is effective to implement when the network topology is segmented, meaning that the network is divided into smaller segments to act as their own smaller networks. This prevents any lateral movement between the network. Lateral movement is caused when an attacker is able to access a network through a vulnerability, and is able to navigate through the network across multiple databases, which the attacker in the incident was able to do. Through network segmentation, the security teams are able to deactivate breached areas and minimize the effects and risks of attackers being able to go to other databases that hold more sensitive information. This stage utilizes security measures and tools already in place and helps develop more awareness of possible improvements to be made to the detection of attacks similar to the one above as well as other attacks.

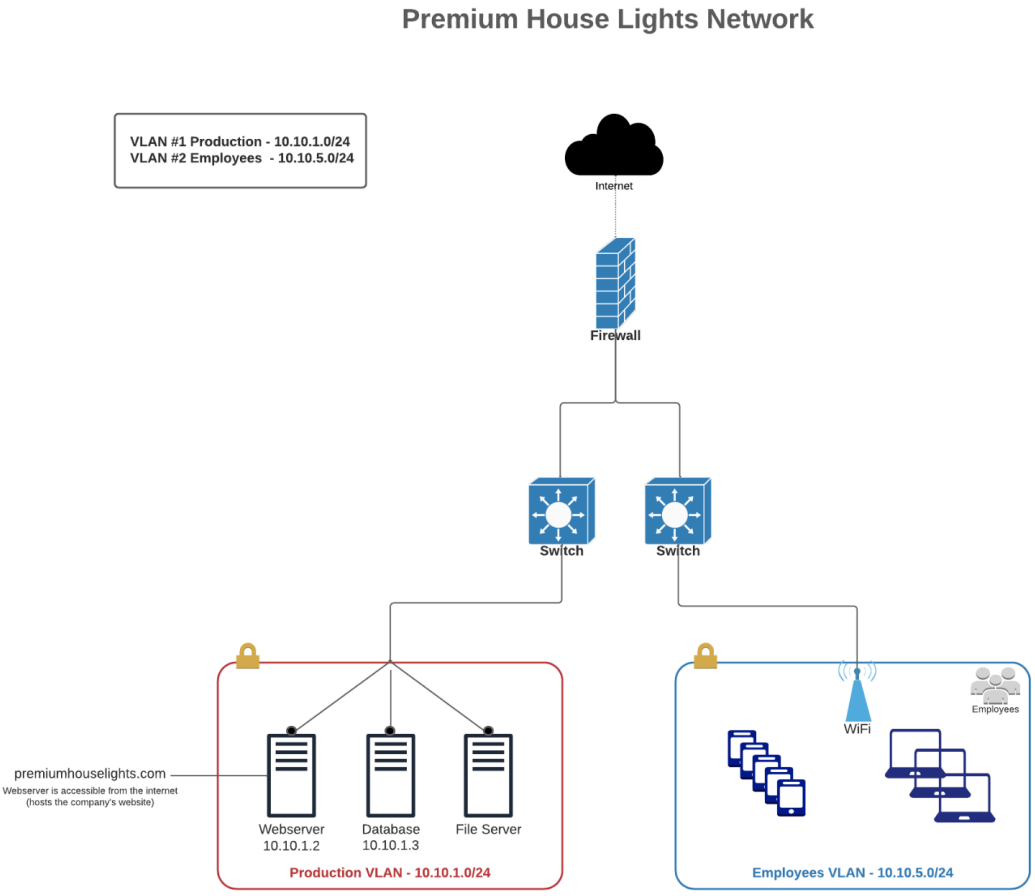
The final stage of the NIST incident response framework is “Post-Incident Activity”, this is where documentation of the incident and response to the incident are thoroughly documented and reported to proper management or authorities if needed. After reviewing the incident and the response to the attack on Premium House Lights, we can compile the documentation and make necessary adjustments to procedure, policy, and security measures, to prevent a similar attack from happening. Improvement for policies such as adding additional security authentication methods (MFA Policy) to verify the identity of the user attempting to log in to their account, as well as password expiration policy to have employees update their login details periodically. The industry best practice for this policy is every 60-90 days. Implementing other security measures such as segmentation of the network, enabling monitoring systems for failed login attempts to the network, which would alert the user and the security team, which would enable a fast and efficient response to brute force attacks. And finally establishing an encrypted service to the databases which contain sensitive employee and customer details, to further halt the advances of attackers being able to read the sensitive data without the encryption key. Making the necessary adjustments and being able to adapt to the new threat landscape will enable Premium House Lights to prevent more attacks and develop better security and procedures as the company grows and becomes more susceptible to vulnerabilities as well as attacks.

Post-Incident Recommendations

In conjunction with the preventative measures implemented above, these are the following recommendations that I would recommend Premium House Lights integrates into their network architecture as well as their security framework. The recommendations are as follows:

1. Network Segmentation

- Network segmentation provides a better network structure for minimizing affected databases, and minimizes the scope in which an attacker is able to maneuver through a network to obtain sensitive data. As shown from the Premium House Lights topology shown below, we can see that once the attacker was able to identify what belonged on the subnet through the crawl bot they were able to run scans to determine what was connected to the web server subnet. Network segmentation would only show what is attached to the web server subnet while the sensitive data will be stored on another subnet.



2. Implementing Data Encryption

- Data encryption of sensitive customer data and employee data is a security measure that prevents the readability of encrypted data. Only authorized users with the decryption key will be able to access the data and read it in its entirety. This ensures that even if the data files are stolen the integrity of the files will be kept intact and more difficult to read for unauthorized users.

3. Implementing Principle of Least Privilege Policy

- Principle of Least Privilege is an industry best practice where users only have access to certain areas of the network or files on a database, depending on what is needed of them. In which case a store employee cannot access the security aspect of the company and adjust the security measures. The security team will have access to files and data that pertain to their work area, as a store employee will have access to store applications provided.

4. Enabling MFA (Multi-Factor Authentication Methods)

- Multi-Factor Authentication is a method in which there are 2 or more levels of authentication methods to verify the owner of a user account. Common practices include verification codes sent to various contact methods such as a phone number or email, Captcha test to ensure that the user attempting to login to an account is not a program but in fact a user, and finally security questions that rely on personal information pertaining to the user. Implementing this security measure will help prevent attacks such as brute force attacks and allow the owner of their account to report suspicious activity.

5. Frequent Security Audits

- Implementing Frequent security audits periodically as needed or required by any governing law will help proactive threat detection through analyzing network data in order to discover possible Indicators of Compromise (IoC's). This can be implemented as a policy in which the security audits are done as a mandate by the company and by law. The policy can be adaptable to the growing size of Premium House Lights to enable the quick detection of possible threats and IoC's and allow for preventative measures to be enacted in an effective and timely manner.

6. Updating Firewalls and Devices

- Updating Firewalls to prevent unauthorized scans and block suspicious IP addresses. This preventative measure will help mitigate the unauthorized scan of the network or any exposed subnet such as the webserver. In this case, the "SiteCheckerBotCrawler" can be blocked from scanning the web server to make any connected database harder to detect. Minimizing certain operations of open access ports on a machine through the firewall can also deny unauthorized network scans from taking place, making the attacker unable to undergo an accurate network scan.
- Secondly, updating software along with patches for devices will decrease the vulnerability of the current devices and software that are housed on the machines that access certain databases. Security updates and patches are constantly being pushed on devices as they tend to patch certain exploits that may be available on the previous software version. Therefore, a simple action of updating software frequently will lead to even more secure devices that access aspects of the network.

Conclusion

In conclusion, Premium House Lights as a company is required to update their security procedures, policies, and incident response procedure, in order to adapt to the changing threat landscape. Though there are more methods to better secure and protect customer and employee sensitive information, as well as the assets of Premium House Lights, implementing the recommendations, policies, and procedure that are contained within this document will further the security measures, incident response effectiveness and efficiency, and furthermore protect the network from being breached as easily as the incident of investigation during the tech analysis. Adapting from this incident is how Premium House Lights can learn how to increase the effectiveness of their security and prevent other incidents of this nature from happening again.

Work Cited

Atlassian. (n.d.). *Get to know the incident response lifecycle*. https://www.atlassian.com/incident-management/incident-response/lifecycle#incident-response-lifecycle

GeeksforGeeks. (2022a, September 8). *Most popular methods used by hackers to bypass firewalls*. GeeksforGeeks. https://www.geeksforgeeks.org/most-popular-methods-used-by-hackers-to-bypass-firewalls/

Computer Security Division, I. T. L. (n.d.-a). *NIST Risk Management Framework: CSRC*. CSRC. https://csrc.nist.gov/Projects/Risk-Management

Inci, D. (2022, November 28). *Why & how to prevent bots/crawlers from crawling your site*. Digital Marketing and eCommerce Development Company |. https://www.optimum7.com/blog/prevent-bots-from-crawling-your-website.html#:~:text=Preventing%20certain%20bots%20from%20crawling%20your%20site%20can,can%20be%20a%20serious%20problem%20for%20website%20owners.

guy mograbiguy mograbi 27.6k1616 gold badges8585 silver badges123123 bronze badges, & LeoLeo 14.6k22 gold badges3737 silver badges5656 bronze badges. (1960, December 1). *What part omits the hash fragment from the URL or why crawlers do not simply send the fragment?*. Stack Overflow. https://stackoverflow.com/questions/26011050/what-part-omits-the-hash-fragment-from-the-url-or-why-crawlers-do-not-simply-sen#:~:text=In%20order%20to%20be%20able%20to%20request%20that,an%20ajax%20request%20coming%20from%20a%20user%27s%20browser.

NeedAnswersNeedAnswers 1, & alepagealepage 32611 silver badge88 bronze badges. (1960, August 1). *What is a HTML snapshot (for Google Crawler)*. Stack Overflow. https://stackoverflow.com/questions/23773017/what-is-a-html-snapshot-for-google-crawler#:~:text=A%20HTML%20snapshot%20is%20the%20static%20HTML%20code,applications%29%2C%20the%20HTML%20changes%20without%20reloading%20the%20page.

Peters, A. (2021, July 31). *Find out what mysqldump is, what it's for, and how you can use it*. Lifewire. https://www.lifewire.com/using-mysqldump-4173962

McKay, D. (2023, October 4). *How to use the SCP command on linux*. How. https://www.howtogeek.com/804179/scp-command-linux/

MozDevNet. (n.d.). *301 moved permanently - http: MDN*. MDN Web Docs. https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/301

What is network segmentation?. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation