Final Project: Secure Network Design

Submitted by Vivian Choe

ENPM 686 – Information Assurance

May 16, 2016

Assumptions are made that the company hasn't invested in any security systems or enabled any security settings within their components or systems.

TABLE OF CONTENTS

The network supports an organization that focuses on promoting database access, and an online platform to advanced the trends and activities within restaurants globally. Customers include restaurant owners and managers from small, medium and large restaurants who are invested in using advanced software to further their business and profits. The company continues to support existing platforms and pushes out new releases of software with updates to better support restaurants all over the world. Regrettably, the organization has undergone a significant and persistent attack that has resulted in the compromise of data within the compromised hosts of the network. The network has been under attack for several months undetected therefore the company doesn't know the breadth of information that has been compromised. However, they have decided due to this breach to raise the level of security of their systems by preventing such attacks like this.

Additionally, the company system currently consists of a network of Linux computers and another network of Windows computers. Also, the company relies on the web server to advertise and sell some of its products. The assets the company wants to protect consist of their network, the web server, the computers (Windows & Linux), database, switches and firewalls. Each of these pieces of hardware and software are pertinent for business operations and if they are compromised it creates a disruption in the company workforce as well as their business operations as each piece of hardware and software are a key component to making the business successful. The computers contain company research and also administrative controls, if these are breached with malware or are exploited not only will the computers need to be wiped and re-imaged, important information about the business will be lost. The web server may not contain vital information as it is mainly used for advertising and marketing products, however if not protected it would impact the business as it would pause advertisements and the selling of their

platform and product, which would affect their profits. If attackers compromise the databases, the confidentiality of data would be lost as the most imperative information is stored within the database such as reservations, clients' credit card transactions, etc. This would result in for the company to restructure their network and all systems, which would halt customers from using their platform, which in turn would cease their operations. The network is one of the company's biggest assets as without the network global operations for the business would cease to even exist. The network is what connects all the other assets together, it's the center of it all, without it there would be no way to connect the database, computers and web servers together so that they can seamlessly run. In addition, if the network is compromised it affects all systems, which stops all operations. In order to protect the network, web server, computers, and databases the business has a firewall, the firewall is used to protect the network so that unwanted users are avoided in the network. If the firewall is compromised, all systems can be compromised easily, which creates a big disruption to business operations. The company prioritizes their assets with the most important asset to the least, which starts with the network and the firewall as they affect all systems within the company operations. Following those the database and web server should be protected next, as these affect not only operations but also profits. The network of computers are the least damaging to the company therefore they are the last when it comes to prioritizing their assets.

Currently, the network has been recently compromised as it has been under attack for the last several months. In this current state, the network is vulnerable to different attacks as there is no intrusion detection or prevention system in place to stop the attacks from happening. In addition, the attackers have exploited not only the network vulnerabilities, but also the host (computer) vulnerabilities. Thus, not only is the network exposed to many attacks, it is similarly

an easy target as both host and network services have been compromised, which puts the business at risk. These host and network exploitations were caused by weak implementations of security of the operating system, firewall, and network settings. Additionally, without intrusion detection and prevention systems it is harder to detect and prevent exploits from happening. The likely causes for the attacks and exploits of the network and host is that the there are too many ports and services running within the host, network and web server that it is easily susceptible to attacks. Equally, even though the network has been under attack for several months, there are security enforcements that can improve the host and network and web server security by enforcing new security policies and equipment to strengthen the security of all systems within the business.

One of the many security design changes that ought to be considered is to intensify the security of company systems is to create a more secure network design. This includes two firewalls for both the Linux and Windows computers that are connected to the different networks. Furthermore, the web server should be hardened so that there is a smaller attack surface for attacks and exploits to occur. It requires a network administrator to run network logs and utilize Nmap and other resources to decrease the number of ports and services that are active on the web server. Another suggestion to improve the security of the host systems is to implement access control lists, anti-virus programs, and rules and policies to limit privileged information to only those who properly have access to them. Resulting in having rules for different roles within the organization, in turn this would confirm that those who access certain files do indeed have the rights and permissions to access those files.

However, to implement these changes to the system there is need for prioritization, which should be organized by order of importance dependent on the core business operations of the

company. The suggested changes to the system may be prioritized based on the core business operations by taking a look at what's the most important for the business. And continue to strive to provide those services while making changes. Although, each business has their own core business operations and principles, the importance of securing systems to continue to provide clients' services is to be highly considered. Yet, the type of business affects how system changes will be prioritized as each company has their own objectives. Ultimately, it matters what type of company it is and what their primary concern may be. The company provides restaurants with a reservation management system that also contains a POS system (point of sale). In addition, it helps restaurants to replace existing paper reservations. This affects their priorities in that they will protect the most important piece of hardware or software first.

In order to start implementing changes to create a better network design, an inventory of current systems and equipment is needed to assess how they are being used and what systems are already in place. A network of Linux and Windows systems are already installed, however there is a gap as these systems have been compromised due to the lack of access control lists being enabled and anti-virus systems as well as comprehensive host firewalls. An administrator can quickly configure access control lists in order to increase security within host-based networks. The business relies heavily on their web server in order to advertise and sell their products; however there isn't any network security controls configured or unused ports that are closed. In addition to the changes mentioned above, new equipment and personnel will be needed to make these changes happen. These include: two firewalls, two intrusion detection systems, two threat detection systems and two new administrators, which include a network administrator and a security administrator. These changes to the security plan and infrastructure would start to help strengthen the network within the company.

The current network design has made it easier for attackers to infiltrate and exploit the system. It contains secure networks, web servers, and many host systems; however, within the network there contain open ports that make these systems extra vulnerable and easy to attack. Furthermore, since there is no intrusion detection or prevention systems in place there is no method to prevent or detect attacks on the system, which resulted in the system being under attack for several months without any warnings. Additionally, with no security administrators it is difficult to monitor the networks and make sure that all systems are secure.

Moreover, before discussing the proposed network design, attack surfaces should be mentioned. Attack surfaces are the sum of all paths for data/commands into and out of the applications and operating systems, the code that protects these paths (including resource connection and authentication, authorization, activity logging, data validation and encoding), all valuable data used in the application, including secrets and keys, etc.[1] To sum it up, it is all the open ports services and other vulnerabilities that make it easier for the attacker to be able to infiltrate the system due to the attack surface. Yet, in order to help harden the operating system the attack surface should be modeled with different types of users, which include roles, privileges and access controls. An attack surface model should help to envision the different endpoints that make it possible for the attacker to gain access to the applications, networks and operating systems via these vulnerabilities. As a result, this will help to envision the risk and map the areas that are of high risk, which can lead to better understanding of when the risk profile of the applications, networks, and operating systems has changed. This can help to gauge the performance of the integration of the current systems with the new network design and systems.

The proposed network design to improve the network and all other systems within the

[1] "Attack Surface Analysis Cheat Sheet." OWASP. Accessed May 5, 2016. https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet.

business is to not only utilize current systems in place such as the web server, network of Linux computers and the network of Windows computers but to also expand equipment and security procedures and policies as needed. In order to begin proposing an updated and new network design, a new security policy should be put in place. A security policy reflects the goals of the company and an assessment of the risks faced and the resources that should be made available.[2] A security policy for the business has been constructed as the following:

- Secure any gaps within the current security configurations
- Educate users on security awareness
- Secure the host and network from intrusions and attacks
- Enforce access control lists, permissions and file system encryption
- Secure all web servers, DNS servers and mail servers
- Provide systems for logging, intrusion detection, prevention and threat detection
- Secure all communications from Linux and Windows networks
- Provide new firewall systems to improve security of host and networked systems
- Enforce an incident response framework to enhance responses as incidents happen
- Enforce a password rotation policy
- Include 2 administrators: 1 network administrator and 1 security administrator to strengthen network and system operations

The new systems that are being provided total $400,000, this includes 2 firewalls, which include spam blockers, gateway antivirus, web blockers, APT blockers and an intrusion prevention system. It also includes an intrusion detection system that provides both host and network

[2] Oxenhandler, Daniel. "Designing a Secure Local Area Network." Designing a Secure Local Area Network. Accessed May 5, 2016. https://www.sans.org/reading-room/whitepapers/bestprac/designing-secure-local-area-network-853.

intrusion detection and a threat detection and response system that provides for automated incident response. The security policy stated above will help to integrate the new network design as well as help to better secure host and network systems that are pertinent to business operations.

The proposed network design would include a trust model that is concentrated on creating the smallest threat vector in order to avoid having attackers infiltrating the system. The network will be designed with the following equipment: two firewalls for the two networks that consist of Linux and Windows computers, two intrusion detection systems, two intrusion prevention systems and two threat detection and response systems. Prioritizing from the network policy, the first design that should be enforced is to see what the current security configurations are and what should be incorporated. The two networks need to be able to communicate with each other securely by using SSH, which runs on port 22. Also, other configurations that could be implemented with the current configurations are to create access control lists and permissions to be defaulted as the principle of least privilege so that no one is granted unauthorized access. Yet, while the principle of the least privilege is being set, so should the file permission security. Additionally, anti-virus programs should be installed in all the host computers for both Windows and Linux computers, this would help from having viruses, worms or malware from being exploited within these systems.

In addition, to further secure the network all users of the business database and platform should be educated on security awareness. Security awareness is training employees to be cautious online so that they will be less susceptible to being attacked by various forms of cyber attacks.[3] It is another line of defense, however it doesn't mean that it will make the systems 100% secure. Also, security awareness training should be mandatory for all employees

[3] Bejtlich, Richard. "The Importance of Security Awareness « Threat Research Blog." Accessed May 10, 2016. https://www.fireeye.com/blog/threat-research/2012/10/importance-security-awareness.html.

and should be done every quarter to make sure that employees understand the risks of not being cautious on the Internet. Also, there should be a contract that states that all employees are to abide by what they learned in training and each employee should sign it.

To supplement the configurations mentioned above, the next step to continue to secure the network is to secure the host (computers) and the network from intrusions and attacks. Implementing anti-virus programs within host computers as well as a spam blocker and a web blocker can help to secure host computers. In addition, firewalls should be placed outside of the network perimeter to help mitigate attacks from happening. To further protect the hosts from intrusions, a password rotation policy should be enforced. The password rotation policy would state that every three months user would be required to change their passwords. In accordance to the policy, the last five passwords couldn't be repeated. And if the user forgot their password, a one-time pad would be issued so they could reset their password; however, this would be after they identified themselves with something that they had or knew. To secure the network from intrusions and attacks a smaller threat vector and attack surface should be implemented, this would only keep necessary ports and services open and all others would be closed. In addition, host and network intrusion detection systems will be implemented, which will be discussed further another section.

Along with these improvements, another implementation to increase security is to secure all web servers, DNS servers and mail servers. Web servers can be secured by only implementing needed ports such as port 80 and 443 for HTTP and HTTPS, which would help to mitigate attacks from happening. Mail servers should only have ports 25, 587,143, and 110 for SMTP, IMAP and POP3 respectively. These three protocols are most commonly used for mail servers and should be the only ones allowed when using a mail server so that the server will be

less vulnerable to attacks. Lastly, in order to secure DNS (domain name system) server's DNS forwarding should be implemented; this is the process where another DNS performs queries on behalf of another DNS. This technique is implemented to protect the DNS server especially if the DNS server also hosts the internal DNS server all within one server. Another way to secure DNS servers is to disable zone transfers; zone transfers make it easier for attackers to configure DNS servers to dump the entirety of the zone database files. This in turn can then let the attacker know the naming schema of the organization and attack key infrastructure services within the organization. In conclusion, the zone transfers should be disabled when using DNS servers.

Lastly, systems for logging, intrusion detection, intrusion prevention and threat detection will be provided within the new network infrastructure, which will help to further secure the network. In addition, an incident response framework should be enforced to enhance responses as they happen. This will be discussed further in the next section. Although, these new features and implementations will help to secure the network and systems within the company it is also extremely helpful to have people who understand how these systems work. Therefore, two administrators should be hired as well to help implement this network plan and also oversee operations to continue to keep these systems as secure as possible. A network administrator should be hired to deal with any troubleshooting and networking issues that arise and a security administrator should be hired to help to continually secure all systems within the company. This would help to not only secure the systems, but to continue to be responsive to problems and attacks that may occur further down the line.

Subsequently, an incident response framework should be implemented, so that not only the administrators know how to respond, but so do company employees. Incident response is the reaction to an identified occurrence whereby responders classify an incident, investigate and

contain the incident.[4] It is important to have an incident response framework in place so that when incidents do occur it doesn't cause a permanent business interruption due to the incident, but rather a pause in the business instead. If the incident response program is executed correctly it will help to minimize loss, mitigate weaknesses, and restore services and processes. With the addition of an incident response framework it put the company at a better position, as it tries to mitigate weaknesses and restore services and processes quickly.

With incident response, there are six steps, which include the following:

- Preparation
- Identification and scoping
- Containment
- Eradication
- Recovery
- Lessons Learned [5]

These six steps will help to create an incident response framework that will structure how the security administrator handles incidents and also how quickly incidents are contained and systems are recovered. However, with a limited team of network administrators and security administrators it makes it harder to be able to manually create an incident response framework to abide by. Therefore an alternative to creating a manual incident response framework would be to use an automated one. However, even with the use of an automated incident response it would still be advisable to prepare and identify the weaknesses within the company infrastructure. An automated incident response system contains automated remediation for incidents and provides

[4] Brennan, Tom, and Jason Jolo. *Top 10 Considerations For Incident Response*. December 2, 2015. https://www.owasp.org/index.php/OWASP_Incident_Response_Project

[5] Torres, Alissa. *Incident Response: How to Fight Back*. August 2014. https://www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342.

faster investigations and mitigation steps, which help to prevent high-risk compromises from becoming bigger risks than they already are.[6] An automated system also contains integration into the IT environment, which makes it easier to integrate into both the network of Windows and Linux systems. And it contains automated testing and minimal cost and complexity compared to manually creating one's own incident response framework, this makes it possible to have a smaller team of administrators and still be able to detect, contain and eradicate incidents.

Respectively, some threats the company wants to protect against are SQL injection within their databases, DNS zone dumping, web server attacks, network breaches and bypassing the firewall. These can be protected by threat modeling and threat detection which are equally important as incident response or if not maybe more important. Threat modeling is a method of depicting system attack surface, threats, and assets.[7] Threat modeling is done so that software can be secure by design, but also to think like an attacker so that there are less ways to penetrate the system through vulnerabilities. A predominant method used to strategize threats is done by the STRIDE method, which was created by Microsoft. It's a method that can be used without being an expert by using the diagram elements. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, and Elevation of Privilege.

Using STRIDE to manage threats will help to mitigate attacks and help to design secure software and hardware techniques. Spoofing happens when an attacker is impersonating to be someone or something else. Cookie authentication or digital signatures to authenticate code or data can stop this. Tampering is when data or code is modified, which violates the integrity of the data or code. To stop code or from being modified access control lists and Windows Mandatory Integrity Controls should be enabled. Repudiation is the act of claiming to not have

[6] "SmartResponse." LogRhythm, The Security Intelligence Company. Accessed May 10, 2016. https://logrhythm.com/pdfs/datasheets/lr-smartresponse-datasheet.pdf.
[7] Dobrawsky, Ido. "Week 10- ENPM 695." Lecture.

performed an action. This can be mitigated with digital signatures and secure auditing. Information disclosure is defined as leaking data or exposing data that isn't authorized for others to see. This can be mitigated by encryption and access controls as well. Denial of service attacks deny users from accessing services by creating multiple requests to keep users from being able to access needed resources. This can be mitigated with filtering, access controls and quotas. Lastly, within the STRIDE methodology is elevation of privilege; this is when an unauthorized user accesses and gains abilities without the proper authorization. Mitigations for elevation privilege are input validation, privilege ownership and group or role membership. While enforcing the STRIDE methodology helps to identify threats and diminish them other methods of threat management and detection are still needed and should be applied.

Other techniques to manage threats include utilizing a threat management and detection system. However, knowing how the security lifecycle works should be a priority to managing threats. The three aspects of the security lifecycle are protection, detection, and response, which include: perimeter protection, risk and vulnerability assessment, penetration testing, intrusion detection, and security policies.[8] Prevention is thinking about how to protect company assets before an attack penetrates critical and important company infrastructure and services. Firewalls are beneficial to protecting the network perimeter, however having firewalls present within the network doesn't guarantee that the network is protected. Firewalls create the first barrier between the network and attackers, however other barriers are necessary to secure the network. The second element to protection is the assessment; this consists of vulnerability assessments and penetration tests. These two assessments help to reveal risk levels and vulnerabilities that need to be corrected. The assessments don't only show network and host risk levels but also the overall

[8] King, Mark. "Security Lifecycle: Managing the Threat." January 2002. https://www.sans.org/reading-room/whitepapers/basics/security-lifecycle-managing-threat-592.

security risks within the organization. Detection is the stage where firewalls and intrusion detection systems are monitoring network traffic for attack signatures and reports for any incidents that have occurred or if there have been any breaches. The firewall is a detection measure as it can check the logs to see if there has been any suspicious activity that has happened recently. Lastly, implementing a security policy to investigate the security breaches and occurrences and to quickly contain them covers response. By looking into the perimeter protection, vulnerability assessment, penetration tests and intrusion detection logs, a proper response is made to the breach and how to contain it and quickly recover all systems back to their normal status. Threat modeling and management is important for the company infrastructure as a whole because without it there would be no system in place to make sure that threats are being logged and moderated to keep all services up and running.

Accordingly, in addition to threat modeling and threat management there also are techniques for threat detection that are to be advised. The LogRhythm security intelligence platform not only provides for automated incident response, but also methods to detect threats within the network and operating system perimeter. Using their platform allows for real-time monitoring, which allows for expedited investigations and allows for quicker threat detection, as threats are detected as they happen. [9] Additionally, other features that are available on the platform are having the knowledge of which applications are in use, a full packet captures, capturing network sessions and much more. These tools make it easier to be able to monitor the network and likely threats within the perimeter as they are happening. Without a system like the LogRhythm SIEM (security intelligence platform), a security administrator wouldn't be able to see real-time threats and try to prevent the attacks and threats from happening within the

[9] "Network Monitoring & Network Forensics." LogRhythm, The Security Intelligence Company. Accessed May 10, 2016. https://logrhythm.com/products/network-monitoring/.

network.

Furthermore, LogRhythm also contains a case management system that assists to provide techniques to integrate data and analyzing threats and allows for analyst workflow that allows for end-to-end threat detection and response. Additionally, it provides methods to accelerate the discovery and qualification of threats, reduce investigation effort and increase threat recognition accuracy, and successfully mitigate threats with aggregated threat details and orchestrated workflows.[10] These features assist to create a threat detection lifecycle with ease and the platform can be handled with a smaller team in place, due to its interface. The platform is highly recommended as it contains a threat detection lifecycle, which consists of threat detection, case creation, investigation, collaboration and mitigation and response. The systems works by being alerted by any concerning activity or a real-time alarm that notifies them that a threat has been detected. Next, a case is created to qualify these threats in the incident response process. Thirdly, alarm details, log data and notes are added into the investigation file, so that threats and alarms can be dealt with properly. Fourthly, real-time collaboration can be enabled so that incident recognition and response. Lastly, countermeasures and containments are implemented to mitigate the risks and threats that were caused by the alarms and threats that were detected.

In conclusion, the LogRhythm SIEM platform is a great platform that helps to automate and quickly contain alerts, threats, and incidents. Due to its automation, it is ideal for smaller security teams to integrate and implement the services offered within the platform to assist in securing the network perimeter as well as all company infrastructure that is impacted by incidents and threats. Also, their focus on expediting threat detection and response helps with company revenue and operations, since the earlier a threat is detected and resolved, it will cause

[10] "Case Management." LogRhythm, The Security Intelligence Company. Accessed May 10, 2016. https://logrhythm.com/pdfs/datasheets/lr-case-management-datasheet.pdf.

fewer disruptions within company operations. Therefore, it will diminish the amount of revenue loss for the company as well.

Correspondingly, to protect the network and other systems intrusion detection systems should be use in conjunction with firewalls, incident response frameworks and threat modeling and management platforms. Intrusion detection is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.[11] Intrusion detection systems complement firewalls as firewalls protect companies from attacks from the Internet, while an intrusion detection system detects if an attacker tries to break through the firewall. There are three major components to intrusion detection systems, which are the management console, sensors, and the database of attack signatures. The management console is the management and reporting console. The sensors are the agents that monitor host and networks in real-time. Lastly, the database of attack signatures contains the attack signatures, which are patterns of different types of previously identified attacks.[12] If the sensors detect any suspicious activity, it tries to match the packets to any previously known attacks. If the sensors match the packets then the management console is notified.

Moreover, there are two different types of intrusion detection systems; they are identified as host based intrusion detection systems (HIDS) and network based intrusion detection systems (NIDS). Host based intrusion detection systems main goals are to protect the host where it monitors system audit and event logs to see if there are any file changes that aren't authorized and compares new log entries based off of attack signatures. On the other hand, network based intrusion detection systems focus on networks and threats that are targeting vulnerable systems

[11] "Intrusion Detection Systems Challenges." Accessed May 11, 2016. https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343.
[12] Ibid.

on the network.

There are many different intrusion detection platforms on the market however, the AlienVault IDS system integrates both host based intrusion detection and network based intrusion detection into one platform. The conciseness of the platform makes it easier for small security teams to be able to monitor both systems such as computer and networks. Also, the AlienVault system is open source; therefore it can be applied to any operating system that supports it. In order to implement the AlienVault IDS for host based IDS the user can download the ISO file of AlienVault IDS and install it on the target system. After installation has been completed an agent must be added in order to monitor the target system. Once completed, then the configuration file on the agent can be changed to specify which files, folder, registry keys should be monitored.[13] Some benefits of a host based intrusion detection systems are easier since there's only an installation file compared to that of a NIDS. Additionally, the host based intrusion detection system has the capability of detecting malware and rootkits being installed on host systems.

As mentioned before AlienVault also provides an NIDS within the same platform as the HIDS. The network based intrusion detection system is enabled by default with the interfaces and monitored networks once configured in the Getting Started Wizard.[14] Some benefits of the network based intrusion detection system are the ease of deployment as there is no need for installation. It also can collect data from multiple devices compared to the host based intrusion detection system. Lastly, it can work in many different network architectures and can be easily moved to a different location. In conclusion, the AlienVault IDS provides an easier solution to dealing with intrusions for both host based and network based systems.

[13] "Intrusion Detection System (IDS)." Accessed May 11, 2016. https://www.alienvault.com/solutions/intrusion-detection-system.
[14] Ibid.

In conjunction with intrusion detection systems there is a need for intrusion prevention systems, so that there is a way to not only detect attacks and exploits, but also prevent them. An intrusion prevention system is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.[15] The intrusion prevention system often sits behind the firewall and is a corresponding layer of analysis that selects dangerous content so that these can be avoided and prevented from exploiting the network. Compared to an intrusion detection system that sifts through host and network data looking for threats, intrusion prevention systems actively examining automated actions on all traffic flows that enter the network. An intrusion prevention system is known as an inline, which means that it has direction communication between the source and the destination. In addition, the intrusion prevention system performs these actions to mitigate attacks from happening on systems such as sending an alarm to an administrator, dropping malicious packets, and blocking traffic from the source address.[16]

Likewise, there are many different types of intrusion prevention systems on the market today. However, there isn't a collection of open source intrusion prevention systems that provide support to both Linux systems and Windows systems like Snort. Snort is an open source intrusion prevention system that performs real-time traffic analysis and packet logging on IP networks. Also, it implements protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, SMB probes, OS fingerprinting attempts, and many more services.[17] Snort can be installed and implemented in many different ways, as it is open source and supports different operation systems. In order for

[15] "What Is an Intrusion Prevention System?" Accessed May 10, 2016. https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-prevention-system-ips.
[16] Ibid.
[17] "Snort." Home. Accessed May 9, 2016. https://www.snort.org/.

Snort to be installed on Linux systems there are a few different methods, which include source and Fedora, Centos and FreeBSD. The source technique is mostly used by more experienced programmers who are more familiar with the command line. The source instructions are to type these commands to install Snort:

- ```
  wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
  wget https://www.snort.org/downloads/snort/snort-2.9.8.2.tar.gz
  ```
- ```
  ar xvfz daq-2.0.6.tar.gz
  cd daq-2.0.6
  ./configure && make && sudo make install
  ```
- ```
  tar xvfz snort-2.9.8.2.tar.gz
  cd snort-2.9.8.2
  ./configure --enable-sourcefire && make && sudo make install
  ```

In addition to these commands, Snort suggests that user sign up get Oinkcode so that they stay updated with the latest detections. While installing the Snort programs different Snort rules should also be configured so that vulnerabilities may be detected, however in order to configure these rules there must be a deep understanding of how the particular vulnerabilities work.[18] To use Snort for Windows systems the user or administrator that is installing the software is to execute `Snort_2_9_8_2_Installer.exe` in order to install the program onto the system. Afterwards, the same steps as the source installation is recommended where users should get the Oinkcode to get the latest detections and user packages.

In conclusion, Snort is the best intrusion prevention system choice for both Linux and Windows systems as it is the premier open source intrusion prevention system of date. It is also malleable to the administrator who installs Snort as rules can be enforced for known vulnerabilities, as well as updates for the latest detections can be accessed. Also, since the Snort software is open source it keeps the budget lower since the software is free.

[18] Ibid.
  ```

Finally, as recommendations of new software, hardware and network design have been made such as utilizing firewalls, intrusion detection system, intrusion prevention system, threat modeling, threat management and detection, and incident response framework has been suggested. All these new improvements without hardening the operating systems, network, and web server will be meaningless. Some hardening techniques for networks and web servers have already been mentioned in previous sections. Hardening is defined as the process of securing the system and reducing the attack surface so that the amount of vulnerabilities exposed and exploited are limited. In order to provide a more secure operating system the first step is to disable and remove all unnecessary services and applications.[19] Removing unnecessary services reduces the amount of logs, which makes it easier to detect intrusions. The next step is to configure user authentication, which consists of removing or disabling accounts that are no longer needed. Also, default usernames and passwords should be changed as well. A RBAC (role based access control) should be enforced to create groups based on each user's roles, which would limit access to unauthorized files or folders. To weaken the attack surface, two factor authentication and encrypted authentication should be required. To further secure files and folders file system security should be enforced such as read-only access. All other access such as chroot for Linux and read, write, and execute settings should be given very carefully. In both Windows and Linux systems, systems should be configured with the principle of least privilege before any other access controls or privileges are granted to the user.

In summary, these are techniques that should be configured to all systems within the network to guarantee that all necessary prevention techniques were used to lower the chance of vulnerabilities and risks being exposed or exploited within the systems.

---

[19] "Host Hardening - Purdue University." Accessed May 11, 2016. http://www.purdue.edu/securepurdue/images/training/HostHardening.pdf.

In conclusion, the network of the company was weak, which cause for several computers within the company to be compromised. Therefore, a new network design was suggested, which included a security policy, updated hardware and software solutions to assist in creating a more secure network to prevent the majority of further attacks. The new network plan required for any gaps to be secured within the current security configurations as well as educate the users on security awareness. These were the first two priorities when it came to constructing the security policy, as using currently enforced hardware and software as much as possible is a good means to securing the network. Also, users are usually the biggest culprits when it comes to having systems' vulnerabilities exposed or exploited. The next steps that were taken were to secure hosts and networks from intrusions as well as enforce access control lists, permissions and file system encryption. Other measures were taken to provide systems for logging, intrusion detection, prevention, and threat detection and management. Most of the measures that were taken to secure the network, hosts and web server won't affect the operation of the company, as they will be configured throughout the evening hours when employees aren't present.

Lastly, the recommendations to improve the security of the network are the best solutions proposed. All improvements proposed within the security policy are methods, which will secure the network to provide the best level of security for company operations. The maximum cost of software and hardware was limited to $500K; only $400K was needed to allocate these changes, as many were collaborated within one platform. However, it is advised to have at least one network administrator and one security administrator if not more. The software, hardware and methods recommended are the easiest to implement within a short amount of time and the least amount of staff, as requested by the company.

REFERENCES

"Attack Surface Analysis Cheat Sheet." OWASP. Accessed May 5, 2016. https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet.

Bejtlich, Richard. "The Importance of Security Awareness « Threat Research Blog." Accessed May 10, 2016. https://www.fireeye.com/blog/threat-research/2012/10/importance-security-awareness.html.

Brennan, Tom, and Jason Jolo. *Top 10 Considerations For Incident Response*. December 2, 2015. https://www.owasp.org/index.php/OWASP_Incident_Response_Project

"Case Management." LogRhythm, The Security Intelligence Company. Accessed May 10, 2016. https://logrhythm.com/pdfs/datasheets/lr-case-management-datasheet.pdf.

Dobrawsky, Ido. "Week 10- ENPM 695." Lecture.

"Host Hardening - Purdue University." Accessed May 11, 2016. http://www.purdue.edu/securepurdue/images/training/HostHardening.pdf.

"Intrusion Detection Systems Challenges." Accessed May 11, 2016. https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343.

"Intrusion Detection System (IDS)." Accessed May 11, 2016. https://www.alienvault.com/solutions/intrusion-detection-system.

King, Mark. "Security Lifecycle: Managing the Threat." January 2002. https://www.sans.org/reading-room/whitepapers/basics/security-lifecycle-managing-threat-592.

Kral, Patrick. *Incident Handlers Handbook*. December 5, 2011. https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.

"Network Monitoring & Network Forensics." LogRhythm, The Security Intelligence Company. Accessed May 10, 2016. https://logrhythm.com/products/network-monitoring/.

Oxenhandler, Daniel. "Designing a Secure Local Area Network." Designing a Secure Local Area Network. Accessed May 5, 2016. https://www.sans.org/reading-room/whitepapers/bestprac/designing-secure-local-area-network-853.

"SmartResponse." LogRhythm, The Security Intelligence Company. Accessed May 10, 2016. https://logrhythm.com/pdfs/datasheets/lr-smartresponse-datasheet.pdf.

"Snort." Home. Accessed May 9, 2016. https://www.snort.org/.

Torres, Alissa. *Incident Response: How to Fight Back*. Incident Response: How to Fight Back. August 2014. https://www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342.

"What Is an Intrusion Prevention System?" Accessed May 10, 2016. https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-prevention-system-ips.