Network Security Proposal

Prepared for:
University of Maryland University College

Prepared by:
Dmitry Landy

I. Analysis and Planning

A. Vulnerability Assessment

Requirements

A vulnerability assessment is a process that identifies known vulnerabilities to a network or a system [1]. One tool that can be used in a vulnerability assessment is a vulnerability scanner, which is a comprehensive tool suite that performs a variety of tests on devices in search of any vulnerabilities. These vulnerabilities can be things such as open ports, outdated operating system software, misconfigurations, and default passwords [2]. Other tools include port scanners, network mappers, password crackers, and ping scanners. To find open ports, a port scanner conducts a two-way handshake (or half-open scan) to see if a port responds. Port scanners output a socket pair, which includes an IP address and its port number. To identify the devices in a network, a network mapping tool can be used to do both ping sweeps and scan port. To determine the strength of a password and its encryption, a password cracker can be used. To discover systems in a network that are vulnerable to ICMP floods, then a ping scanner can be used to find devices that reply to ICMP echo requests. All of these tools are needed to assess various vulnerabilities of a network.

Proposed Solution

One option for effectively performing vulnerability assessments can be to use a paid vulnerability scanner such as Nessus [3]. The tools within Nessus can be run individually to perform a specific scan. However, Nessus also includes an option to create “policies”, which are created to perform a combination of different scans against specified targets. There are a series of premade policy scans that perform common combinations of scans. If these premade scans do not meet the assessment needs, then a custom policy can be created. The resulting policy scans will reveal both an overview of the vulnerabilities discovered as well as the specifics, such as the vulnerability target, severity, and description. If cost is an issue then the community edition of Retina can be used to conduct many similar scans [4].

Another option, though not as effective, can be to use Nmap, or its graphic version Zenmap, to conduct vulnerability assessments [5]. Similarly to Nessus, Nmap can identify a target or series of targets to perform a variety of scans on. Thes scans include ping scans, port scans, and network mapping. Information about devices in a network can be discovered using nMap, such as MAC addresses, operating systems, open ports, and

service versions. This is a tool that offers effective options for conducting quick and simple vulnerability assessments.

Justification

The use of vulnerability scanners is an extremely effective and efficient method of conducting a vulnerability assessment. Since vulnerability scanners give users the flexibility to customize scans in anyway they want, they can be set up to scan very targeted areas of a network. Additionally, specific scans can be selected to identify certain types of vulnerabilities in a network, such as just open ports. If a summary of all network vulnerabilities is needed, then a comprehensive result can be made after the appropriate scans are run. The results reveal the exact vulnerability and its location, which reduces the time needed to locate the vulnerability. Depending on the budget and needs that the University of Maryland University College has for its network, a paid vulnerability scanner, such as Nessus, might be better than a free scanner, such as Retina, due to extended features and functions available.

B. Security Policy

Requirements

To ensure proper security measures are followed, policies should be put in place. This collection of policies should outline the security considerations for various aspects of the University of Maryland University College's (UMUC) organizational and functional structure. The security policy will address the following security management categories and security documentation [6]:

- Acceptable Use Policy (AUP)
- Privacy Policy
- Authorized Access Policy (AAP)
- Change and Configuration Management Policy
- Human Resources Policy
- Password Policy
- Data Retention Policy
- Physical Security Policy

Proposed Solution

To create a thorough security policy for the University of Maryland University College (UMUC), the collection of documents listed in the "Requirements" section should be created. The following identifies each document and areas of focus that should be addressed when creating

each document:

- The acceptable use policy (AUP) should outline the boundaries an employee and student has in terms of company property, such as equipment and system use [6]. The specific role and function of the equipment/system should be explained. Then, the limits of the user with concerning the equipment/system should be detailed. This document must explain the extent of any monitoring that is done on systems to ensure the users are fully aware.

- The privacy policy explains how private information of employees and students will be secured. This policy should list exactly what kind of private information is being secured as well as any laws that apply to the security of that information [6]. It is also important to include how the information is being secured. Some information that will have to be secured is names, phone numbers, email addresses, physical addresses, social security numbers, date of birth, and student identification number [8]. The adherence to the Patriot Act and provide the appropriate private information to authorized law enforcement should be mentioned in the policy [6].

- The authorized access policy (AAP) specifies the access boundaries of an individual or group in a certain position [6]. This access includes both physical access to rooms and equipment as well as access to network resources, such as files [9]. The specific accesses to resources and equipment should be explained for each role.

- The purpose of the change and configuration management policy is to create a procedure for implementing changes to assets safely and securely [6], [7]. The procedure should include the specified target, the proposed change, reason for the change, associated risks, controlled testing method, a rollback plan, documentation, and change impact analysis. Additionally, methods to track documentation and personnel involved in the change should be included.

- Human resource policies mitigate future security issues by ensuring that incoming employees are qualified for job responsibilities [6]. A hiring policy should be included to make sure that appropriate steps are taken to evaluate all job candidates properly. This means that pre-employment screening could be implemented to evaluate the background of the employee. A termination policy should be included that outlines the process to ensure that UMUC's property is returned, access to assets is removed, legal documents are signed and handled, and exit interviews are conducted.

- A password policy should outline the password length, appropriate characters, authorized sequences, authorized attempts, and the time frame between password changes [6]. A specific work section should be designated and specified for addressing password-related issues [9]. The password requirements should not be so complex that users can not remember it and write it down or end up using a predictable pattern to

meet the criteria [10].

- A data retention policy identifies the duration of time certain types of data will be stored to meet business and legal requirements [11]. When the time limit for the data is reached, specific procedures for handling the destruction of data should be outlined in this policy. Additionally, procedures for handling data needed for investigation should be clearly defined in the policy as well. Data classification could be implemented in conjunction with this policy to assist in data retention and destruction process.

- Physical security involved the securing of physical assets keeping them safe from physical threats [7]. The policy should outline what type of areas, such as classrooms and server rooms, require what kind of physical security measured. Possible ways to implement physical security is adding locks for doors, adding video surveillance cameras inside and outside a building, hiring security guards, and having appropriate fire extinguishers in rooms [12]. Defense-in-depth is a concept that should be implemented for physical security to ensure that there is not a single point of failure.

Justification

Every proposed document for the security policy serves a security-related function that benefits University of Maryland University College. The following will explain this function for each document:

- The acceptable use policy (AUP) provides boundaries to system and equipment use that keep both the user and assets safe [6]. Additionally, UMUC is legally secured since an expectation to the user's privacy is properly set.

- The privacy policy provides users, students, and employees with an explanation of how their private information is going to be secured[6]. As long as the information is secured properly and follows the appropriate laws, this policy gives legal security to UMUC. Additionally, it gives the users, students, and employees a sense of security so that they can focus on their required tasks.

- The authorized access policy (AAP) designates the type and level of access individuals have to ensure that UMUC's assets are safe. Restricting access to places such as the server room to only authorized personnel ensures non-authorized personnel aren't allowed to wander in and damage themselves or the equipment. Through this policy, UMUC's equipment, systems, data, and personnel are secured.

- The change and configuration management policy create a specific procedure for guiding changes to assets to avoid possible damage [6]. Changes to UMUC's assets will have to be approved and tested before being implemented. This minimizes the

chances of damage to assets since issues should be caught during the approval or testing step. However, if a change that is implemented does cause issues, a rollback allows assets to be configured to the previous state to prevent further damage.

- The human resources policies are critical to the security of UMUC's assets because they ensure qualified individuals operate in the appropriate jobs [6]. An unqualified individual could severely damage UMUC's assets due to mishandling. A pre-employment screening could reveal a candidate with a dangerous background which could prevent an insider threat issue. A termination policy ensures that an employee can't get unauthorized access to UMUC's resources after being terminated. Additionally, an exit interview could reveal security issues not previously addressed.

- A password policy that outlines the criteria for a strong, but memorable password ensures that unauthorized personnel can't have network access so easily. Making sure that the password criteria is something that is memorable for employees allows passwords to be unique and effective.

- A carefully created data retention policy is critical for ensuring the legal security of UMUC by providing the appropriate procedure for locating data during an investigation [6]. Properly stored data reduces the time, and therefore cost, of locating the needed data during an investigation. Removing expired data keeps storage devices uncluttered and allows available space to be made for other necessary data.

- A physical security policy focuses on protecting physical assets from harm. By securing server rooms with locks that require keys or RFID cards, only authorized personnel with the appropriate key or card can access the server room. This prevents accidental or intentional damage to UMUC's assets. Additionally, proper implementation of physical security can protect UMUC from liability issues if something like a laptop with private information is stolen [12].

C. Risk Management

Requirements

Risk management is a process of identifying risk, reducing the risk via countermeasures, and then dealing with the residual risk [13]. To properly identify a risk, assets and their values have to be assigned. This can include the cost of replacing a device, such as a server, or the cost produced from the downtime of a device, such as a disabled router. Next, threats and vulnerabilities should be identified for each asset. Each risk can be assessed and assigned a

qualitative or quantitative value. Determining the quantitative risk requires the use of the following formula: single loss expectancy (SLE) * annualized rate of occurrence (ARO) = annual loss expectancy(ALE). Lastly, management techniques to handle each risk should be determined. These techniques are an avoidance of risk, reduction of risk, transfer of risk, and retention. Once this is decided, then appropriate security controls can be determined and implemented [14]. A security control should be compatible with the existing infrastructure, effectively deal with the risk, and is compliant with regulations and policies. Additionally, a cost benefit analysis should be performed to ensure that this security control balances cost, performance, and security.

Proposed Solutions

Proper risk management for the University of Maryland University College's (UMUC) infrastructure should be done meticulously and not rushed. It is suggested that every asset should be identified and be given a value [13]. This is known as asset valuation and it is needed to determine the level of protection appropriate for the asset [15]. The value of each asset can be physical, but also digital or functional. Both should be considered when conducting asset valuation. Once the asset has had a value assigned to it, threats and vulnerabilities of the asset will need to be determined. Threats can be internal (within the organization), external (outside the organization), natural threats (such as fires), or disasters (such as floods). Each type of threat will need to be determined by evaluating the physical location, access to the asset, and the function of the asset as well as its function. Asset vulnerabilities, which are exploitable weaknesses of that asset (such as poor physical security), will have to be determined as well.

The next step is to perform a qualitative or quantitative risk assessment. The difference between the two is that qualitative risk assessment involves approximation of risk occurrences and costs whereas quantitative risk assessment involves calculating exact numbers [15]. Qualitative risk assessments are used to determine risks and their relative ranking to one another. This can be used when determining the quality of physical security in various sections of a building. Quantitative risk assessments are used to determine exact costs regarding a risk. This is done by multiplying the value of an asset, which is the single loss expectancy (SLE), by the likely rate of occurrence in a year, or the annual rate of occurrence (ARO), to determine the annual loss expectancy (ALE) of the asset. If there is data from previous years, then that data can be used to better calculate the ALE.

Once the risk assessment has been successfully conducted, risk response will have to be evaluated and decided on. However, before deciding the response method, a cost benefit analysis should be done for each type of method. This is used to determine if the cost of protecting the risk is worth it [14]. Risk response for each asset is done by accepting, transferring, deterring, or rejecting the risk [15]. Accepting risk means that even though the risk is known and calculated, it is decided that nothing will be done. This could be due to the low likelihood of a risk, the cost of protecting it is too high, or both. Transferring the risk is done by

getting insurance for the asset. If the cost of the insurance is less than the cost determined by the risk assessment, then this may be a good choice. Deterring the risk is done by posting warnings or notices at a physical or logical entry point that states the consequences of unauthorized access or use. Rejecting or avoiding the risk is done by denying or ignoring the risk. This type of risk response method should be avoided. It is highly unlikely that risk can be completely removed, but instead should be mitigated. The level of risk remaining, or residual risk, should be at an acceptable level.

Justification

Going through the risk management process is a critical process to the security of assets and continued functionality of the University of Maryland University College (UMUC). Various levels of risk can be found for every one of UMUC's assets. One way or another, those risks will eventually become a reality and being able to deal with that is crucial. The risk management process allows UMUC to be properly prepared to handle such situations. Back up plans to replace assets or restore their functionality can be made by being aware of the risks of the assets. Determining the value of assets as well as the threats and vulnerabilities they are exposed to allow for qualitative and quantitative risk assessments to be made. The results of these risk assessments allow plans to be created for responding to these risks. A qualitative risk assessment can reveal weaknesses in policies and allow security measures to be better implemented. A quantitative risk assessment can determine a final cost that can be calculated into a yearly budget. The risk management process ensures that UMUC is prepared to deal with costly events, not if, but when they occur.

D. Business Continuity Plan

Requirements

A business continuity plan (BCP) is created to prepare for recovery and continuation of significant business functions after a disaster or catastrophic event has occurred [16]. Multiple parts are required to create a successful BCP. The first part is a business impact analysis (BIA) which determines what kinds of losses the business will suffer, as well as the time to recover if certain business functions are down. The second part is a disaster recovery plan (DRP) which determines the appropriate recovery method for every possible failure to a critical function. The BCP should be created in a way that requires the appropriate employees to just follow the instructions in the plan without having to guess various steps [17]. Additionally, employees should be properly trained and prepared to respond to a disaster and carry out the instructions in a BCP. When a disaster does occur, the appropriate employees should be able to follow the BCP and handle the situation in an organized manner. Every step of the BCP should be documented when drafting a BCP so that the final version can be verified to contain the optimal solutions.

Proposed Solutions

For a business continuity plan (BCP) to be effective, it has to be created before a disaster occurs so that it may be used to handle the effects the disaster has on business function [17]. The first part of developing a BCP should be to identify critical business functions (CBFs) and prioritize them in order of importance. Next, timeframes for recovery of each CBF should be determined. These time frames are determined via a business impact analysis which calculates it based on acceptable losses to customers per service level agreements if any. Various solutions should be made to recover the CBF within the allotted time frames. These solutions should be created to suit a variety of situations and should be properly tested. Tabletop, medium, and complex exercises could be used to test possible solutions. Tabletop exercise tests one part of the BCP with a small group, a medium exercise tests multiple parts with a larger group, and a complex exercise simulates a realistic scenario and tests all of the BCP. The BCP should also account for both damaged and undamaged equipment. This means that steps should be specified for the handling and storage of undamaged equipment and the salvaging of damaged equipment.

The next part of business continuity is the business impact analysis (BIA), which determines the acceptable losses that can occur as well as the impact those losses have [17]. The BIA identifies critical functions, systems, and their appropriate threats. Each of the values discussed next has to be carefully calculated in order to set the limits needed to meet business requirements. Various values are determined in the BIA such as the maximum down time (MDT), recovery point objectives (RPO), recovery time objectives (RTO), mean time between failures (MTBF), and mean time to repair (MTTR). MDT is the total time an organization can be down without critical function or asset. RPO is the maximum time an event can go on for before a system stops functioning [18]. RTO is the maximum time a system can be down before failing to meet business requirements. MTBF is the average period of time a device lasts before failing, while MTTR is the average period of time it takes to repair a failed device [19]. These values should be carefully calculated to determine the appropriate time frame and implement the appropriate solutions to meet business requirements. These values also help determine the tangible and intangible loss, such as monetary and trust, respectively, that can occur when devices and business functions fail [17].

The last part of business continuity is the disaster recovery plan (DRP), which plans for restoring critical functions after a disaster occurs [17]. This plan should include every failure possible to critical functions and provide a solution to resume that function, whether through timely repair or replacement. Switching to an alternate operating site as well as going back to

the original should be carefully laid out and explained. The type of site, hot or cold, should be determined based on cost and business function requirements. This plan should also account for the security of information during the transfers. Appropriate training to employees should be conducted to ensure they are prepared for such an event.

Justification

Planning for business continuity is a critical requirement that plans for failures to critical functions [16]. Objects break all the time and being prepared to recover from that is mandatory. A business continuity plan (BCP), business impact analysis (BIA), and disaster recovery plan (DRP) prepare an organization to continue functioning after a significant break to operation occurs. These plans allow recovery to occur within a time limit that ensures that business requirements and objectives are met. Additionally, intervals between device failure, which will eventually occur, is planned for and appropriate steps are prepared to resolve the failure in a BIA. In case of a major disaster, a DRP explains the transfer to a cold or hot site in order to resume business functions on a large scale. Without a BCP, small and large disasters will cause extreme tangible and intangible damage to the organization and its business associates.

E. Access Controls

Requirements
identification, authentication, need to know, least privilege, implicit deny, separation of duties, job rotation, AAA

Access controls are put in place to control the type and amount of data someone has access to [20]. Depending on the type of information that is being secured, various methods can be used to secure access from unauthorized users. Managing certain aspects of job functions is an important process to pay attention to. This involves both separation of duties and job rotation [21]. Separation of duties is used to separate or divide a duty or responsibility to multiple people so that a single person is not responsible for the whole task. Job rotation involves the cross-training of multiple users on multiple job positions so that job responsibilities can be rotated. This is used to control the amount of access and knowledge an individual can have at a single time.

Another way to control access is through authentication, authorization, and accounting (AAA), which is a security framework used to control access to resources [22]. Authentication involves the identification and verification of a user. Identification is described as something, such as a username, that lets one claim who or what they are. Verification is described as the proof that is provided in order to ensure the identity is legitimate. Authorization is a process of determining whether someone or something is allowed to have access to a resource, which

involves privilege. Accounting is the process of monitoring the actions of someone or something to ensure everything is functioning appropriately and no security issues have arisen. To best manage this framework, a server needs to be configured with appropriate information involved in AAA, such as user, group, and permissions.

Proposed Solutions

Proper access controls have to be put in place to ensure the security of University of Maryland University College (UMUC). To limit the amount of control an individual can within their respective positions, separation of duties and job rotation should be implemented. Separation of duties can be implemented through the principle of least privilege [22]. This principle ensures that an individual is only given the necessary permissions needed to accomplish their tasks. If an individual changes positions, then their permissions change accordingly. Unnecessary permissions should be removed to avoid privilege escalation. Another practice for separation of duties can be to ensure that no single individual has complete control over a full process to avoid compromise. A task should be split into multiple sub-tasks that are performed by different individuals. Along with separation of duties, job rotation ensures that different personnel perform the same job in various cycles. This helps limit the possibility of fraud and compromise in a certain position as multiple people will perform the job in limited intervals.

Implementing the authentication, authorization, and accounting (AAA) framework can help automate access control [22]. Multi-factor authentication can be implemented to more securely authenticate someone. This can be done by requiring two or more pieces of information that differ in their type. For example, a password, which is something known, can be provided with a code on a token, which is something that is had. Mutual authentication, which is more secure than one-way authentication, can also be configured where the user and server both authenticate each other. Authorization is determined by the permissions that are configured for each user and group. Once again, it is important to keep in mind the principle of least privilege when configuring these permissions. These permissions need to be reconfigured when a user's job position or specification changes. Logging of various activities, such as logins and accessing files, should be carefully done to make sure that the appropriate amount of information is logged. Configurations should be done carefully since a poorly configured AAA server could cause more security issues.

Justification

Implementing access controls ensures that data and access to it are appropriately controlled which increases security. Separation of duties and job rotation reduces the possibility of fraud and compromise for a single process [22]. Identifying the exact amount of privilege and the duration of that privilege is a significant part of assigning permissions and is critical in ensuring individuals do not have access to unnecessary information. Configuring AAA servers allows for

automatic access control management in a centralized location. This reduces the risk of error and increases management oversight since multiple groups of people can be managed simultaneously.

II. Securing Boundary Devices, Hosts, and Software

A. Physical Security

Requirements

Physically securing systems is the practice of making physical systems more difficult to access by implementing various security measures [23]. For physical security to be effective, it should use the defense-in-depth concept. Defense-in-depth is the practice of using multiple layers of security to create a stronger defense. This involves implementing perimeter security, access security, inter-facility security, and intrusion detection. When implementing security systems, additional measures have to be taken to allow intrusions in areas to also be detected as well. This ensures that a response to that intrusion can occur. After an attack has occurred, a recovery process has to start. Recovering from attacks involves understanding the issues that allowed the attack, whether that was the security mechanisms or the policies set in place.

Proposed Solution

There are many aspects to consider when implementing physical security at the University of Maryland University College (UMUC). It should always be done using defense-in-depth practice [23]. One of the first areas to protect is the physical perimeter, because it is the outermost and most vulnerable layer of UMUC's building. Perimeter security protects the physical perimeter of UMUC to prevent entrance. Fences, guards, video cameras, barriers, and bollards can all be used to prevent or deter unauthorized access. Posting signs to inform individuals of the repercussions of unauthorized access is also a good way to deter unauthorized access [25].

The perimeter does have to allow authorized personnel to enter, so perimeter access point should be used. Perimeter access points are the areas that allow entrance, or access, inside the perimeter [23]. This should have proper security measures put in place to authenticate individuals that use it, known as access security. Physical access points, such as entrances to a building, should use multiple modes of verification, such as PIN pads as well as security guards to verify the person's identity. Some unauthorized personnel will try to take advantage of the perimeter access point to gain access by tailgating or piggybacking [24]. Tailgating is the technique of following an authorized person through an access point without consent. Piggybacking is similar to tailgating, but is done with the authorized person's consent, such as

holding a door for the unauthorized individual. Both can be prevented by educating users, implementing turnstiles, and mantraps. Areas susceptible to these attacks should be identified and proper security measures should be put in place. The amount of traffic should be a consideration when choosing what security measures to implement.

In addition to perimeter security, inner-facility security and detection should be implemented to regulate who gets to have access to what resources [23]. Inner-facility security can include implementing devices such as door, door locks, keypad locks, smartcard readers and biometric scanners. Methods to detect intrusions should be implemented by including motion sensors, infrared detectors, and proximity alarms. Access logs can also be implemented to have everyone entering an area sign in [25]. Inner-facility security has to be implemented even more carefully because it deals with securing resources from unauthorized personnel who are already inside the perimeter.

Justification

Preventing an attack is easier than recovering from one. Therefore, implementing proper security measures to help prevent attacks should be done with a high priority [23]. Ensuring the safety of resources within an organization is generally less expensive than having to replace those resources or dealing with the repercussions of having them stolen or damaged. Properly implementing physical security can not only discourage people from accessing physical systems but also prevent them. Physical security can protect from malicious attacks, vandalism, theft, and natural disasters [26]. It also allows an organization to be better aware of various risks and then plan to prevent or minimize those risks. More control is given to the organization's resources as well as proper authentication, authorization, and accounting is possible when physical security is appropriately implemented.

B. Mobile Device Security

Requirements

Modern computer networks will typically include mobile devices, which are portable computer devices such as tablets and phones [27]. Before security measures for mobile devices can be put in place, the types of mobile devices as well as who gets to use them should be determined. The organization and the various positions it has will need to be evaluated to see what positions will have mobile devices as well as the function it will serve. An understanding of the risks mobile devices pose to the security of an organization and its network should be understood before allowing mobile devices. Since mobile devices can connect to wireless access points and use a cellular connection to send and receive data, traditional network security, such as firewalls and IDSs, can be easily bypassed. This presents an increased risk of an insider attack. University of Maryland University College should be properly prepared to

handle this risk appropriately.

Proposed Solutions

After establishing who gets to use what mobile devices, a request process needs to be put in place to account for all the devices [28]. Each device should be carefully identified and inventory control measures should be put in place. This means that specifics about the device itself, the people using it, the function it is used for, and the duration of the use should be carefully kept track of. Being accountable and creating boundaries of use for these devices is a significant process in ensuring network security. An acceptable use policy (AUP) for mobile devices should be created and should specify what the mobile devices are allowed to be used for as well as any time specifications [27]. The AUP should define who owns what data if personal mobile devices are allowed to be used for business purposes.

To ensure that mobile devices connected to the network are safe, Network Access Control (NAC) can be implemented to have the appropriate software installed on the device before allowing it on the network [27]. Another option to manage mobile devices could be to install a guest network, which allows some network access to these devices, but is separate from the production network. To ensure the security of mobile devices, those devices can use mobile device management (MDM) infrastructure. MDM can regulate the strength of the passwords or pins used, lockout configurations that need to be set, and any device encryption that is used. For extreme cases, a remote wipe feature can be configured to remove sensitive data from the device if that device is lost. With that being said, a reporting procedure for lost or stolen mobile devices has to be in place to allow users to report the issue. This ensures the accountability of devices and allows steps to be taken to secure that data or at least account for it.

Justification

Properly implementing security measures to manage mobile devices allows for an organization to manage the security risks that come along with such a device [27]. The policies put in that that specifies the extent of use for mobile devices can protect an organization from liability if that device is used inappropriately. The organization's data can be made more secure by specifying what data belongs to the organization on a personal mobile device. Proper device management and implementation of Network Access Control (NAC) for network devices can prevent foreign malware to spread on to the network. To make the network even safer, a guest network for mobile devices can be created to keep the production network and the data within secured from any threats that mobile devices may pose while still allowing the devices a network connection.

Any mobile device being used has to have security measures to protect the data inside. Appropriate password, lockout, and encryption configurations can keep unauthorized personnel from getting access to sensitive data [27]. Additionally, if the data is in more danger, a remote wipe option can remove all data from that device to ensure that it doesn't get into the wrong

hands. Implementing a reporting process for stolen or missing mobile devices and educating users on it allows the issue to be dealt with quickly and decreases the time unauthorized personnel have to get into the device. If a remove wipe feature has been implemented, then it would be used in such a situation to ensure sensitive data isn't leaked.

C. Perimeter Defenses

Requirements

The network perimeter is the boundary of a network that separates the private network from the public network [29]. Since the network perimeter is exposed to the outside, appropriate perimeter defenses should be set up. Perimeter defenses should be implemented to defend against attacks that the organization is open to [30]. These vulnerabilities can be discovered by conducting active and passive reconnaissance of a network. Perimeter defenses for the network depend on the vulnerabilities found through the reconnaissance [31]. A variety of actions can be taken to better secure the perimeter, such as software and hardware implementations or restructuring the network. Creating new parts of a network, such as DMZs (demilitarized zones), honeynets, and guest networks can separate the network to secure sensitive network resources from publically available resources.

Proposed Solutions

Before setting up the appropriate defenses to the network perimeter, research, in the form of reconnaissance, about the perimeter should be conducted [30]. Both passive and active reconnaissance of the network should be conducted to see what an attacker would be able to see. Passive reconnaissance involves techniques and actions that don't touch anything in the network. This can be done by visiting a company's website or searching through the job listing to see what kind of devices are used in the company. Advanced search engine searches can also reveal special information about a website or organization. Active reconnaissance involves actively interacting with network devices to gather information about various systems in the network. This can be done by scanning the network for open ports and sending ICMP (Internet control message protocol) echo requests to check for active devices. Various tools such as Nmap, Metasploit, Nessus, and Wireshark can be used to perform active reconnaissance.

After gathering as much information about network perimeter weaknesses, solutions for those weaknesses can be implemented [31]. A wide variety of hardware and software solutions exits to enhance network perimeter security. Proxy servers can be set up to handle requests from the private network to the public network on behalf of the private network. When this is done, the public sees only the IP of the proxy server and not any other device. The proxy server can be configured to cache web pages so that users don't have to make multiple requests for the same

public web page. Instead, users only have to go as far as the proxy server to retrieve their web page. Servers can be configured to filter the contents of network traffic requested to prevent malicious sites from being visited.

Sometimes, the network structure has to be moved around or changed by adding security zones to provide additional security [32]. A DMZ (demilitarized zone) is a part of the network that allows both internal and external network connections, and is separated from the internal and external network via firewalls. These firewalls determine what type of traffic is allowed to access the DMZ from both networks to ensure security. Honeynets, which are dummy networks that are set up to present a target for attackers to attacks, can also be set up. This allows network administrators to see what types of attacks are being used against the honeynet and find defenses against them in the real network. Guest networks can be created to allow devices to gain network connectivity to a network separate from the production network with heavy restrictions to resources.

Justification

Understanding the vulnerabilities in the network defense is vital to being able to manage the risk associated with those vulnerabilities. Conducting passive and active reconnaissance is a critical task that allows an organization to understand what the public can see [30]. By understanding the security gaps present in their network, an organization can implement appropriate security measures. If security measures can't be implemented (perhaps due to the service being provided), then at least the organization is aware of the risk and can monitor the vulnerability for unusual or malicious activity. For example, if the network is found to have allowed ICMP echo requests from the public, then the organization can prepare itself for an ICMP flood attack.

To make the network perimeter more secure, a proxy server should be implemented. Implementing a proxy server can make the network more secure by masking the devices within [31]. Additionally, cached data in the server can make the network less vulnerable by reducing the bandwidth costs as well as user exposure to the public network. Configuring a server with content filtering allows bandwidth use to be reduced, but more importantly, secures the network by restricting access to safe and appropriate sites.

Defense in depth can be applied to the security of network perimeters by creating security zones [32]. Introducing security zones allows a network and its resources to be segregated. This segregation of resources creates multiple points of failure and allows for better control of access to resources. Additionally, the traffic that goes through security zones is monitored, which makes detection of malicious activity more probable.

D. Network Defense Devices

Requirements

A variety of devices, both software and hardware can be implemented into a network to increase network security. Each network device has different features and functions, which means that they have different vulnerabilities. These vulnerabilities should be understood before installing the devices in the network [34]. For example, the difference between managed and unmanaged switches is that one gives administrators great control in what is allowed to pass through the switch, while the other does not. This difference is significant and determines what administrators can and cannot do. It is vital to understand the full extent of these devices to know how to properly manage them. Proper planning of devices in the network should be done to prepare security measures for the functions they provide [35]. The devices' roles in the network determine how other devices and users will interact with the network device. Any function that will not be used should be properly secured.

Physical devices can be added to a network to provide additional security to a network, such as intrusion prevention systems and intrusion detection systems [37]. Assessments of the network should be conducted periodically to check on the network's overall security and health [2]. Vulnerability assessments check the network for known vulnerabilities and identify them so that they may be fixed. This has to be done to maintain the required level of security in the network.

Proposed Solutions

A good first step when introducing new systems into the network that are manageable is to change any default accounts [33]. Something like a switch can be initially assessed for management by inputting the default username and password. During initial access, the account management area should be located and the default information for the account should be changed. Additional administrator accounts can be created to allow multiple people to manage the device. However, only those that need to manage the device should be allowed to manage it.

When implementing the devices in the network, it should be understood, in great detail, what that device can and should do [34]. Although some functions of an access switch and core switch are the same, their place in a network is different in many ways. Properly implementing such devices in the network can ensure that they provide the appropriate function, and therefore can be managed appropriately.

After understanding the functions of a network device, the vulnerabilities that come with them should be understood next [34]. For example, a layer 2 switch and a layer 3 switch differ

because a layer 3 switch can work with IP addresses, while a layer 2 switch only works with MAC addresses. This increased functionality for a layer 3 switch allows it to be susceptible to layer 3 attacks, such as ping floods. When these attacks are understood, proper security measures can be configured for the device. These network devices should be configured to provide only the functions it needs to successfully play their role in a network and nothing more [35]. A switch that doesn't require remote access from outside the network should be configured to deny any such attempts. Additional configurations can be made to routers to prevent unauthorized traffic from going in or out of the network [36]. Configuring access control lists (ACLs) on the router ensures that traffic does not get routed to unauthorized areas of the network or even at all.

Intrusion prevention systems(IPS) and/or intrusion detection systems (IDS) should be implemented in the network to detect and prevent malicious attacks in a network [37]. An IDS is configured to only detect malicious attacks, log the activity and maybe alert the network administrator. It does this by analyzing network traffic and log files for matching criteria. An IPS, or active IDS, can do the same as an IDS, but will also attempt to stop the activity.

Vulnerability assessments should be conducted periodically (depending on the network) to ensure known vulnerabilities are properly addressed [2]. There are a wide variety of vulnerability assessment tools available depending on budget restricted. Nessus is a high-end vulnerability assessment product that provides a suite of tools that can be customized to efficiently scan the network and the devices within [3]. Resulting scans will reveal identified vulnerabilities, where to find them, how to fix them, and the level of concern for that vulnerability. A wide variety of scans can be performed depending on the desired result. These scans can check to see if the policies are up to a certain standard or if devices have the appropriate updates.

Justification

Network defense devices that are misconfigured are more of a security risk than not having it at all. Therefore, it is important to understand each device and configure it appropriately. Changing default account access information is critical to ensuring authorized access [33]. By creating additional accounts with strong passwords, access to the device can be properly managed. Understanding the functionality of network devices helps in understanding its vulnerabilities as well [34]. These vulnerabilities have to be accounted for and handled appropriately to secure the network. However, without a full understanding of the devices' functions, this can not be done correctly. Poor security configuration for network devices will result in vulnerabilities that can be taken advantage of [35]. Forgetting to disable remote access to a router from outside the network can result in unauthorized access that can jeopardize the whole security of the network.

Implementing intrusion detection systems and intrusion prevention systems can provide significant security to a network by detecting and preventing suspicious activity in a network [37]. However, network administrators should be careful in configuring them as they can provide

false positives and false negatives that result in preventing authorized traffic and allowing unauthorized traffic (respectively). These configurations can be checked to meet various criteria with vulnerability assessment tools. Vulnerability assessments reveal a range of issues in a network efficiently so that they may be properly addressed [3]. These assessments can be customized to reveal specific issues with certain devices, or they can be done to check on the overall security of a network.

E. Host Defenses

Requirements

[38] A host is a vital part of a network as they are a device that provides a service to users or other devices on the network [38]. Due to the role that they play in the network, they have to be carefully protected to ensure they continue to provide that function in their role. Like any other device, hosts can also be infected by malware [39]. It is important to know what different types of malware are out there and how to prevent devices from getting infected. Malware is malicious software that is deployed to a system for malicious purposes, such as gathering information, allowing unauthorized access, preventing access to resources, or destroying resources [40]. Malware is typically made to spread to systems, preserve itself, remain undetected, and perform its purpose. The advancements of malware have made them more difficult to detect and much more dangerous when installed.

Since users are the ones that work with the hosts, an education system has to exist to educate the users on various topics involving host security [39]. Additionally, Access to hosts has to be managed carefully as well as their permissions when they do access the host device [41]. The operating systems of host devices should be kept up to date as appropriately as possible [42]. The network size should be considered when deciding how to manage the devices. Host devices have to be managed effectively and efficiently to protect the network.

Proposed Solutions

Since hosts are an important part of a network and can be infected by malware, steps should be taken to protect host devices from getting infected [39]. One step to prevent malware is to ensure that the operating system and web browser are up to date. This protects the device from attacks to known vulnerabilities. Another critical step is to make sure that anti-malware software and firewalls are installed and active. After they are installed, they need to be configured carefully to identify malicious traffic and protect against it. With that, the definitions should be kept updated to make sure that the newest attacks are being protected against. It's important to schedule full scans of systems periodically to make sure nothing malicious got through to the system.

Host devices can’t do their job if there are no users to make sure they are configured properly and are functional. Users should be well educated on malware as well as the best practices to prevent them from getting into the network [39]. Users should also be educated on appropriate password security, such as password complexity and length [41]. Poor passwords can lead to unauthorized access to the system.

As mentioned earlier, updating the operating system is a critical part of the security of a host [42]. However, other measures can be taken to harden the operating system. When a new manageable device is added to the network, any default login information should be changed. With that, the personnel that are allowed to manage that device with extended privileges should be limited to only the necessary personnel. Those devices should include all the software it needs to properly function, but should not include anything unnecessary. Unnecessary services should be disabled or removed. The host should have a configuration and security baseline that should be ensured periodically. If the device doesn't meet the baseline, then it should be quarantined until the requirements are met.

Due to the large number of host devices present in the University of Maryland University College's network, group policy objects (GPOs) should be used to effectively manage the devices [43]. GPOs can establish the requirements for all types of criteria relating to device security in a domain. These criteria should be identified and set accordingly to ensure the hosts are properly secured. When the GPOs are configured, any device that is added to the domain will be automatically configured to the GPOs configurations.

Justification

Recovering from malware is extremely difficult and costly since the damage that is done is often irreversible [39]. Therefore, preventing malware from getting on the system is well worth it to ensure the security of the devices and data in the network. Malware can still get on the network if users are uneducated and unaware of the dangers that come with malware. Properly educating users on the subject will decrease negligent or ignorant acts that comprise the network.

The rest of the network defense are meaningless if unauthorized users can guess passwords successfully. Ensuring that passwords can be and are implemented correctly protects the network from unauthorized access [41]. If password requirements are too complex that users can't remember their passwords, then shortcuts will be taken to meet those requirements. Those shortcuts are likely known by attackers, who can use them to gain access inside the system by guessing the passwords. Default passwords are even easier to guess. Changing default passwords to new host devices prevents unauthorized access via default login information [42]. Allowing only necessary users to logon to those devices with escalated

privileges prevents inappropriate access and secures resources from mishandling.

To avoid misconfiguration masses of devices individually, group policy objects should be implemented. GPOs provide an efficient way to manage a large number of devices and reduces the possibility of error and misconfiguration [43]. This centralized system allows hosts to be automatically configured to meet any security and policy baseline. If the baseline changes and new configurations need to be added, then changing the GPOs once will allow all the devices to be updated with that new configuration immediately. This improves security by providing improved control, reducing redundancy, and reducing error.

III. Securing Data at Rest and in Transit

A. Public Key Infrastructure

Requirements

Public Key Infrastructure (PKI) is a foundation that provides security applications and systems in a network through the use of public keys and certificates to provide authentication and security [44]. A PKI is composed of a certification authority (CA), a client, a cryptographic service provider (CSP), and a client [45]. These components of the infrastructure work together to issue certificates. CSP generates key pair via asymmetric encryption for client [45]. The client keeps the private key but sends the public key along with a certificate request to the CA. If the CA approves the certificate request, it will issue the certificate. The certificate does have a lifespan and will have to be renewed at a certain point. Additionally, to ensure fake certificates are not trusted, the CA signs every certificate, which is checked by the clients before accepting them.

Proposed Solutions

A certification authority (CA) should have policies properly configured to approve/deny certificate requests automatically or have the administrator do it [45]. Having an administrator do it provides additional administrative overhead, which is good for security but is time-consuming. Policies should be put in place to determine what kind of certificates are being issued as well. Certificates should have a specified length of time for how long they are valid for. The Certificate Revocation list should be updated with lost or stolen certificates to ensure only valid certificates are being used. Since the list will only get longer over time, Online Certificate Status Protocol (OCSP) should be used to efficiently check certificates. To make the certification request process more efficient, a registration authority (RA) can be implemented between the client and Certificate authority. The RA acts as a proxy between the two to provide load balancing. This would be a good idea for a large organization like the University of Maryland University College.

A Windows Server 2016 can be set up to be the Certificate Authority (CA) by installing the Active Directory Certificate Authority role [46]. Once the role is installed, it can be configured to manage certificates appropriately by going to Tools> Certificate Authority in Server Manager.

Clients will have to have the “Certificate” snap-in installed on their machines. From there, users can select the type of certificate they need and request it. For additional security, the CA should be configured to hold all requests in a pending state until an administrator manually approves or denies them. Additional functions to revoke and un-revoke certificates can be done using the CA depending on the situation.

To establish a more secure certificate management process, a hierarchical model should be implemented [47]. In this model, there is a root CA at the top of the tree, subordinate CA below it, and issuing CAs at the lowest level. The issuing CAs are the ones that issue certificates to the clients but have to be approved by the subordinate CAs. the subordinate CAs have to be approved by the root CA. This model provides more security in certificate management as multiple CAs have to approve or deny a certificate. This model does provide quite a lot of overhead and should be implemented in larger environments.

Justification

Applications such as email use security protocols that are made secure via PKI [44]. If PKI is not properly implemented, then the security of the network and everything that functions within will be at risk. PKI provides an efficient and effective process for securing systems and applications [44]. PKI allows for there to trust in the network [45]. A web server can be trusted to have secured web pages because it has received an SSL certificate from the CA, which it can use to guarantee its security to the client. Without PKI, this trust may not be there, which would complicate day-to-day operations.

B. Secure Protocol Implementation

Requirements

Computer networks, and the devices within it, function and handle data by following established rules known as protocols [48]. These rules are created for everything that occurs in a network. Since security is a critical part of a network, secure protocols have to be used. Secured Socket Layer (SSL) and Transport Layer Security (TLS) are what provide security for TCP/IP communication [49]. For example, to secure confidential data within a web page, HTTP can be secured with SSL or TLS to encrypt the data.

Protocols can be secured by using certificates issued by a trusted Certificate Authority [49]. This occurs by having a Public Key Infrastructure in place. After the certificate is given, SSL or TLS will use that certificate to encrypt the communication for the protocol. When the protocol is used to send data between the client and server, the client and server conduct the SSL/TLS handshake to establish secured communication before sending any data between each other.

IPsec, which stands for IP security, is another security protocol that can be used to secure TCP/IP traffic in a network [52]. IPsec uses Authentication Header (AH) and Encapsulating Security Payload (ESP) to provide integrity (by calculating checksums), authenticity (by verifying signatures), and confidentiality (through encryption) [53]. Before data can be sent, a Security Association is created for two routers to decide on the method for secure communication [52]. Internet Key Exchange (IKE) is used to help establish SAs. Once the SA is set up, then IPsec can be used to provide a secure communication channel.

Proposed Solutions

[50] If a network provides web services to clients, it should use a secured protocol A web server should be configured to use HTTPS to secure the data being transmitted between it and the client. HTTPS is HTTP that uses SSL or TLS to encrypt its data. [49] Both SSL and TLS have multiple versions that improve the security upon the previous version. TLS is more secure than SSL, but the two are used interchangeably when TLS is being discussed. TLS should be used for protocols when possible to provide the best security. When HTTPS is used, a handshake is done to establish a secure connection before transmitting any data. HTTPS should not be confused with S-HTTP as it is not as secure and uses stateless connections.

HTTPS does provide a security risk to the organization that should be considered. Since HTTPS provides a secure tunnel, administrators can't see what is going on by inspecting packets to ensure malware or other security threats aren't entering the network [50]. To get around this, SSL inspection should be used to decrypt the HTTPS packets going in and out of the network. SSL inspection will intercept the packets, decrypt them, inspect the contents, then repackage them and send them to the destination server.

If a Windows Server 2016 server is providing web services using Internet Information Services (IIS), then it can and should be configured to use HTTPS. IIS Manager can be selected from Server Manager to begin the configuration process. Once the manager window is up, locate the desired website to use HTTPS, right-click and select "Edit Bindings…" [51]. Then click on "Add" and select the certificate for it. If a certificate was not available, then one would have to be requested before the website can use HTTPS. After the certificate is added, the website can use HTTPS until the certificate expires.

To require IPsec to be used as a security protocol for communication in a network, configurations will have to be made to the Windows Firewall [54]. Open Windows Firewall with Advanced Security, right-click on "Connection Security Rules", and select "New Rule…" to begin. When the set-up wizard is displayed choose "Isolation Rule" to restrict communication based on authentication. The next step is to select whether inbound and outbound connections will request or require authentication. The most secure option is to require authentication for both. After the authentication requirement is selected, the next step is to select the authentication method. The remaining steps are to specify the network profile and name the rule. Once the rules are set up, devices meeting the connection criteria will have to meet the

rule requirements before making and inbound or outbound connection.

Justification

Data that is sent using unsecured protocols is in clear text and can be seen by unauthorized personnel. SSL/TLS and IPsec can be used to secure communication and protect data from reaching the wrong hands. IPsec allows secure transmissions to occur for TCP/IP connections and ensures authenticity, integrity, non-repudiation, and confidentiality [55]. It uses Authentication Header and Encapsulating Security Payload to create a secure tunnel for the data to go through. Traffic using SSL or TLS can be monitored in a network by implementing SSL inspection. This ensures that traffic using secured protocols is thoroughly checked to keep malware from entering the network. Services that use secured protocols are more trusted by clients as they better protect client data.

C. File Encryption

Requirements

Sensitive data can be controlled and secured by encrypting files, directories, and drives. If a whole drive needs to be encrypted, BitLocker will have to be used [56]. BitLocker can encrypt a whole drive or volume and all the contents within. New Technology File System (NTFS) provides users the functionality of encrypting files using Encrypting File System (EFS) [57]. The operating system has to be using NTFS version 3 or later to use this function. Other file systems, such as FAT32, can not be encrypted using EFS because they are not NTFS. EFS can encrypt files and directories in a file system, but not whole drives. Full drive encryption is handled by BitLocker.

Encrypting File System (EFS) can encrypt a file by using the symmetric file encryption key (FEK) to encrypt the file [58]. The FEK is then encrypted using the user's public key and then stored in the file header. The decryption process works in reverse by taking the FEK in the header and decrypting it with the public key to get the decrypted FEK. That FEK is then used to decrypt the file.

Files encrypted using EFS can be configured to allow multiple users to access the file's contents [57]. To do this, other certificates have to be added to the file's access list. If the keys are lost or corrupted, then the access to the folder will not be available. To remedy this, a Data Recovery Agent (DRA) should be set up. The DRA can be the administrator or anyone else. The administrator is not the DRA by default, so they will have to be manually defined.

Proposed Solutions

Encrypting a file using Encrypting File System (EFS) can be done by selecting a file,

right-clicking, selecting “properties”, and then select “Advanced”. A screen will appear with an unchecked box that encrypts the contents. That box should be marked and then the “OK” button should be selected. Then, select “Apply” and choose whether the file or the file and parent folder are going to be encrypted. After the selection, the file will be encrypted and any unauthorized users will not be able to view the file. However, other users that should be able to access the file can be added by going to “properties” and then select “Details”. In that new window, other users’ certificates can be added to give access to those users by selecting the “Add” button. The “Remove” button can be used to remove a user from accessing the file.

To ensure that encrypted data can be recovered if the user’s key is lost or corrupted, a Data Recovery Agent (DRA) should be set up [59]. To set up a DRA, go to the command prompt and type “cipher /R:recovery” and press “enter”. This will create the CER and PFX files for the DRA. The DRA can be specified by going to the computer policies and finding “Public Key Policies”. In there, right-click on “Encrypting File System” and select the option to add the recovery agent. When the wizard is loaded, select browse in the windows to find and upload the certificate. That certificate will be used to allow the DRA to decrypt files for recovery purposes

Administrators should be aware that files encrypted by EFS can be decrypted when being transferred to another location with a different file system [57]. The decryption of that file will occur without any warning and could allow unauthorized users to access this. Files can also be decrypted if they are transferred over the network using the SMB protocol. This must be understood before transferring encrypted files to prevent unauthorized access.

To encrypt a disk using BitLocker with a Trusted Platform module, the configuration setting in the BIOS will have to be changed [60]. During the boot-up process, the appropriate key to load the BIOS will have to be pressed. When the BIOS settings are open, the security tab should be looked through to find the TPM section. Then the TPM setting should be turned on, the settings saved, and the BIOS exited. After getting logged in, open the control panel in the tile display and go to “BitLocker Drive Encryption”. When the window is up, locate the drive that needs to be encrypted and click on “Turn On BitLocker”. A window will appear asking where to save the recovery key. That key should not be saved onto the local system, because if the drive is locked out, the key will be useless. The next window will give the option to encrypt only used space in the drive or the whole drive. After the drive is encrypted, there will be a lock icon next to the drive to indicate that it is encrypted.

Justification

Encrypted files protect an organization’s data and prevent unauthorized users from accessing sensitive data. Encrypting File System (EFS) can control data access by encrypting files and directories.BitLocker ensures that if a hard drive is stolen, it will not function if it’s not on the same physical computer [56]. BitLocker on Windows 7 and later conducts integrity checks during the boot process to make sure that the computer hardware isn’t different. If it is different, the contents of the drive will not unlock unless the recovery password is provided. This ensures that only authorized personnel can access the contents of the drive.

D. Hashing

Requirements

Hashing is the process of taking data and creating a string of characters by using a hashing algorithm [61]. This string will change completely if even a single character changes from the original data. This allows data to be verified for integrity. For the hashing process to work, there has to be data and an algorithm. Some algorithms for hashing include Message Digest version 5 (MD5), Secure Hash Algorithm (SHA) 1, and SHA-2. Each algorithm produces a different fixed output: MD5 is 32 hex characters long, SHA-0, and SHA-1 are 40 hex characters long [62]. These different lengths in output determine the strength and complexity of the hash which impacts the security of the data regarding verification.

Proposed Solutions

Although hashing algorithms work very well, they are not perfect. Hashing collisions can occur when two different pieces of data create the same hash [61]. This is more likely when the same hashing algorithm has a shorter hash value but is very unlikely. Regardless, this is something that has to be considered when deciding on which hashing algorithm to use. This is one reason why some prefer to use SHA-2 over SHA-1. Other algorithms such as MD5, RIPEMD, LANMAN, NTLM, and CHAP should all be considered when employing the algorithm [63]. Each provides a different result and different pros and cons. These have to be carefully looked into when deciding which one to use.

When downloading any files from a website, check the website for the file hash and compare it to the hash of the file downloaded [61]. This will verify if the file has been tampered with during the download. The tampering does not always indicate malicious acts and could be a corrupted file. However, if the hashes do not match, the file should be re-downloaded. To check the hash of a file against another, a hashing utility that uses the same algorithm will need to be downloaded [64]. Once the utility is downloaded, select the file of interest and run the utility to create the hash. Each utility will work differently and will have to be understood before using it. When the hash is created, it needs to be verified against the original hash. If there are any differences, then the current file is different from the original. If the hashes are the same, then there is no change to the file.

Justification

Hashing ensures the integrity of data when that data is transferred [63]. It is made secure since it is a one-way function, and is not something that can produce the original message. It is something that can be easily used to ensure that downloaded files are legitimate and full (no missing parts). By verifying the hashes, an administrator can trust the file and the data within. If

the file is an executable, then the administrator can run it knowing that no malicious software is on it. Any sensitive information that is sent from one place to another can use hashes to ensure that all the data was transferred without issues.

E. Backup and Restore

Requirements

Backing up data is a critical part of an organization's operation to prepare for data failure. There are three types of backups: full, incremental, and differential [65]. A full backup, as the name implies, archives everything on a system regardless if its been archived or not. The archive bit, which indicates whether a file needs to be archived, is cleared during the back. However, if there are any changes to that file, the archive bit is reset to indicate the change. An incremental backup will backup only the files that have changed since the last full backup or last incremental backup. It does this by looking for archive bits that are on. A differential backup is similar to an incremental backup, but it backs up all data that has changed since the last full backup, including the changed files that have already been backed up [66]. This reduces the time in the recovery process.

System images can also be used to back up the data [65]. This is done by creating a bit-level mirror of a drive or partition on a drive. This is advantageous over an archive because it can restore a system to a previous state. If malware was on the system, then restoring that drive or partition with a previous system image would remove that malware. However, system imaging is a longer process than a typical backup but is worth it when it comes to the restoration process.

Backups must have integrity checks conducted periodically to ensure that the backed up data is as it should be [65]. This is done by taking a backup into a lab environment and loading that backup. This is an important process that will require a lab environment to be set up so that backups may be tested.

Proposed Solutions

Backups have to be done periodically in an organized way to ensure all system files are backed up appropriately and efficiently [65]. For example, a full backup should not be done every day as it consumes a lot of data and time. Instead, it could be done once a week and then an incremental backup could be done for the rest of the days. This ensures that all files are always backed up, but saves time and storage space while reducing redundancy. The disadvantage with incremental backups lies in the restoration process. To properly restore a system, the incremental backups will have to be done after the full backup is restored. Then, each incremental backup will have to be done in the order they were archived. This is more time

consuming and requires proper organization of the backups to be done. A differential backup would be better in this case because it would only have to be restored once. If these types of backups will be done, the time and organization will need to be considered. Differential and incremental backups should not be mixed because they are different in how they archive the data. This becomes an issue when restoring the data.

Before backing up anything, it should be understood that a Windows 10 compatible backup process is different from a Windows 7 compatible process. To backup a workstation on Windows 10, select the Windows icon, click the gear icon for the settings, and select “Update & Security” [67]. When the window is up, select “backup” on the left side and then click on “Add a drive”. Select the appropriate drive to back up. The settings should be more specific for the backup schedule by going to “more options” and configuring the settings there. To create a Windows 7 compatible backup, open the control panel, go to “Backup and Restore (Windows 7)”, and then select “Set up backup”. When the window appears, select the appropriate drive to backup and proceed to select what in the drive will be backed up. Then decide on how often and if a system image will be created. After that is done, the backup can be created.

There are two ways to restore a backup file: through file history and the backup utility [68]. To restore a file on Windows 10 using file history, go to the Windows start icon and type then select “Restore your files with File History”. Then, browse to the location of the desired file, select it, and click on the restore button. The file will then appear in the location where it was last in. To restore using the backup utility, go to the control panel and select “Backup and Restore (Windows 7)” under “System and Security”. When the window appears, select the “restore my files” button and then select “search” to find the appropriate files to backup. Then, select the location where to restore the file and restore the file.

Justification

Backing up data allows an organization to be prepared in case of a system crash or file corruption. These events do occur, and they occur without warning. Additionally, natural disasters can cause a system to be damaged or destroyed. Being able to recover the data and resume function is critical to an organization. The backup process is fairly straightforward and gives a lot of flexibility to the administrator regarding the schedule of the backup and how long the backups are stored before deletion. Windows provides different options to backup and restore files depending on the versions of Windows in the network. This allows different versions of Windows to be used to restore backed up files.

References

[1] TestOut Corp, “6.9.1 Vulnerability Assessment”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[2] TestOut Corp, “6.9.2 Vulnerability Assessment Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[3] TestOut Corp, “6.9.3 Scanning a Network with Nessus”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[4] TestOut Corp, “6.9.4 Scanning a network with Retina”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[5] TestOut Corp, “6.9.9 Performing Port and Ping Scans”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[6] TestOut Corp, “3.1.4 Security Documentation Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 4, 2019]

[7] TestOut Corp, “3.1.5 Security Management Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 4, 2019]

[8] J. Stacey and J.R. Petro, “Personally Identifiable Information Protection Policy”, Colorado Dept. of Edu. Apr. 2018. [Online]. Available: https://www.cde.state.co.us/dataprivacyandsecurity/piiprotectionpolicy [Accessed Nov. 4, 2019]

[9] J. Perkins, “Access Control Policy”, The London School of Econ. and Political Sci. Nov. 2018. [Online]. Available: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/accConPol.pdf [Accessed Nov. 4, 2019]

[10] Y. Guo, Z. Zhang, and Y. Guo, “Optiwords: A new password policy for creating memorable and strong passwords”, *Computers & Security*, vol. 85, pp. 423–435, Aug. 2019. [Online]. doi: 10.1016/j.cose.2019.05.015 [Accessed Nov. 4, 2019]

[11] TestOut Corp, “3.1.7 Data Retention Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 4, 2019]

[12] D. Hutter, “Physical Security and Why It Is Important”, Sans Inst. Inform. Security Reading Room, Jun. 2016. [Online]. Available: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120 [Accessed Nov. 4, 2019]

[13] TestOut Corp, “3.2.1 Risk Management”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[14] TestOut Corp, “3.2.2 Security Controls”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[15] TestOut Corp, “3.2.3 Risk Management Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[16] TestOut Corp, “3.3.1 Business Continuity Planning”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[17] TestOut Corp, “3.3.2 Business Continuity Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[18] P. Kaushik, “Security+: Business Impact Analysis Concepts”, Infosec, 2019. [Online]. Available: https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/risk-management-in-security/business-impact-analysis-concepts/ [Accessed Nov. 5, 2019]

[19] P.C.T Gomes, “MTTR And MTBF, What Are They And What Are Their Differences?”, OPServices, Aug. 2015. [Online]. Available: https://www.opservices.com/mttr-and-mtbf/ [Accessed Nov. 5, 2019]

[20] TestOut Corp, “2.3.1 Identity and Access Management”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 5, 2019]

[21] TestOut Corp, “2.3.3 Access Control Best Practices”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov. 5, 2019]

[22] TestOut Corp, “2.3.2 Authentication, Authorization, and Accounting”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 5, 2019]

[23] TestOut Corp, “4.1.1 Physical Security”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[24] TestOut Corp, “4.1.2 Tailgating and Piggybacking”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[25] TestOut Corp, “4.1.3 Physical Security Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[26] S. Moses and D.C. Rowe, “Physical Security and Cybersecurity: Reducing Risk by Enhancing Physical Security Posture through Multi-Factor Authentication and other Techniques”, *Int. J. for Inform. Security Res. (IJISR)*, vol. 6, no. 2, pp. 667 -676, Jun. 2016.

[Online], Available: https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/Physical-Security-and-Cybersecurity-Reducing-Risk-by-Enhancing-Physical-Security.pdf [Accessed Nov. 23, 2019]

[27] TestOut Corp, “3.8.1 Mobile Device Management”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[28] TestOut Corp, “3.8.2 Mobile Device Security Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[29] “Network Perimeter”, Barracuda, n.d. [Online]. Available: https://www.barracuda.com/glossary/network-perimeter [Accessed Nov. 23, 2019]

[30] TestOut Corp, “5.1.1 Reconnaissance”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[31] TestOut Corp, “5.3.1 Security Solutions”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[32] TestOut Corp, “5.3.2 Security Zones”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[33] TestOut Corp, “6.2.4 Securing a Switch”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 5, 2019]

[34] TestOut Corp, “6.5.1 Switch features”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[35] TestOut Corp, “6.7.1 Router Security”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[36] TestOut Corp, “6.7.2 Router ACLs”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[37] TestOut Corp, “6.8.1 Intrusion Detection”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 23, 2019]

[38] “What is a Host”, Computer Hope, Oct. 2019. [Online]. Available: https://www.computerhope.com/jargon/h/hostcomp.htm [Accessed Nov 25, 2019]

[39] TestOut Corp, “7.1.3 Malware Protection Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 25, 2019]

[40] “MalwareRisks and Mitigation Report”, BITS Financial Services Roundtable, Jun. 2011. [Online]. Available https://www.nist.gov/system/files/documents/itl/BITS-Malware-Report-Jun2011.pdf

[41] TestOut Corp, “7.2.2 Password attack Facts”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 25, 2019]

[42] TestOut Corp, “7.3.1 Operating System Hardening”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 25, 2019]

[43] TestOut Corp, “7.4.1 Hardening Enforcement with GPOs”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Nov 25, 2019]

[44] J.Weise, “Public Key Infrastructure Overview”, Sun BluePrints Online, Aug. 2001. [Online]. Available: https://pdfs.semanticscholar.org/6439/5a36e7eedfdf60f885ad013ac125dc6e37de.pdf [Accessed Dec. 6, 2019]

[45] TestOut Corp, “9.8.1 Certificates”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 6, 2019]

[46] TestOut Corp, “9.8.2 Managing Certificates”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 6, 2019]

[47] TestOut Corp, “9.8.5 CA Implementation”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 6, 2019]

[48] “What is a Protocol”, ComputerHope, Oct. 2019. [Online[. Available: https://www.computerhope.com/jargon/p/protocol.htm [Accessed Dec. 6, 2019]

[49] TestOut Corp, “9.10.1 Secure Protocols”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 6, 2019]

[50] TestOut Corp, “9.10.2 Secure Protocols 2”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 6, 2019]

[51] TestOut Corp, “9.10.4 Adding SSL to a Website”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 6, 2019]

[52] TestOut Corp, “9.10.6 IPsec”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 6, 2019]

[53] M. Elezi and B. Raufi, “Conception of Virtual Private Networks Using IPsec Suite of Protocols, Comparative Analysis of Distributed Database Queries Using Different IPsec

Modes of Encryption", *Procedia - Social and Behavioral Sciences*, vol. 195, pp. 1938-1948, Jul. 2015 [Online]. Available: https://doi.org/10.1016/j.sbspro.2015.06.206 [Accessed Dec. 6, 2019]

[54] TestOut Corp, "9.10.8 Requiring IPsec for Communications", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 6, 2019]

[55] TestOut Corp, "9.10.7 IPsec Facts", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 6, 2019]

[56] TestOut Corp, "9.7.6 BitLocker and Database Encryption", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[57] TestOut Corp, "9.7.1 Encrypting File System", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[58] A. Vij, "Encrypting File System (EFS) on Windows 10 explained"The Windows Club,Aug. 2018. [Online]. Available: https://www.thewindowsclub.com/encrypting-file-system-efs-windows-10

[59] TestOut Corp, "9.7.2 Securing Files Using EFS", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[60] TestOut Corp, "9.7.7 Configuring BitLocker", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[61] TestOut Corp, "9.9.1 Hashing", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[62] TestOut Corp, "9.9.2 Hashing Algorithms", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[63] TestOut Corp, "9.9.3 Hashing Facts", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[64] TestOut Corp, "9.9.4 Using Hashes", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[65] TestOut Corp, "9.13.1 Backup and Restore", TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[66] E. Sullivan, "Full vs. incremental vs. differential: Comparing types of backup",TechTarget, Jul. 2019, [Online]. Available: https://searchdatabackup.techtarget.com/tip/Data-backup-types-explained-Full-incremental-differential-and-incremental-forever-backup

[67] TestOut Corp, “9.13.4 Backing Up Workstations”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]

[68] TestOut Corp, “9.13.6 Restoring Workstation Data from Backup”, TestOut Security Pro, 2019. [Online]. Available: http://www.testout.com [Accessed Dec. 7, 2019]