Assessing Information System Threats and Vulnerabilities

(Spring 2023 Individual Assignment for Weeks 1-9)

The Scenario

This assignment covers the first 9 weeks of material you experienced in class and is based the material we covered and your own research throughout the class including my weekly thought questions and your insights from the MBSA security scan analysis and Cain & Abel password cracking experience.

Make believe that you are an information assurance management officer (IAMO) at an organization/company of your choosing.

1. Choose a real or make up a fictitious company/organization and give it a name.
2. Identify and describe your company and the industry it is in (e.g., transportation, financial, medical, etc.) within the Security Assessment Report (SAR) report which you will provide for this assignment.
3. All aspects of the company, it's security issues and strengths are purely up to you and your imagination.
4. Please, however, make sure they are rooted in the real aspects of networks and security systems and that you do allow for security issues or vulnerabilities.

One morning, as you're getting ready for work, you see an email from your manager. You are being asked to come to their office as soon as you arrive at work. When you arrive, you are told that there's been a security breach at the Office of Personnel Management (OPM). Your manager is worried about your own organization and says "we don't know how this happened, but we need to make sure it doesn't happen here." You are to use the information about this breach as well as your knowledge of other cyber threats and vulnerabilities to assess the information system vulnerabilities at your organization. Security requirements for your company or organization can be assessed and modified based on your assessment.

After you have studied the OPM OIG report, you found that the hackers were able to gain access through compromised credentials. The security breach could have been prevented if the OPM had abided by previous auditing reports and security findings, written access security requirements and implemented them. In addition, access to the databases could have been prevented by implementing various encryption schemas and could have been identified after running regularly scheduled scans of the systems. You realize that your manager is worried because your organization uses similar network and system access and has similar databases and data base management systems (DBMS) as the OPM does.

You are being asked to analyze your organization's network and systems (the databases and DBMSs in particular) and to compile your findings into a Security Assessment Report, or SAR. You will identify the threats and vulnerabilities and the different means for remediation. You are not being asked to determine the risks, likelihoods of occurrence, remediation costs or to select the preferred remediation for your organization, however.

In what follows, I have provided high-level descriptions of important network, system and cyber security terms. You may already have researched these in the current literature, if you thought about my weekly thought questions. Each part that I cover is another step that one would undertake to complete an SAR.

I have provided a template for your SAR that you should use. It greatly simplifies what you need to write. Do not remain at a high level since your manager needs you to give them specific information about the threats and vulnerabilities in their network and systems that

they can take action on. Open the SAR template to see exactly what you need to cover in each section. Then use the following material for background and source information as well as questions you should be asking yourself when you fill in the SAR template.

Introduction

The security posture of the information systems infrastructure of an organization should be regularly monitored and assessed (including software, hardware, firmware components, governance policies, and implementation of security controls).

The monitoring and assessment of the infrastructure and its components, policies, and processes should also account for changes and new procurements in order to stay in step with ever-changing information system technologies. These all require that requirements be specified so that among other things, the security is built-in up front.

The data breach at the US Office of Personnel Management (OPM) was one of the largest in US government history. Please read about it in the reported literature and in the April 2021 OIG report, also available online. The literature provides a series of lessons learned for other organizations like yours in industry and the public sector. Some failures of security practices, such as lack of diligence with security controls and management of changes to the information systems infrastructure, were cited as contributors to the massive data breach in the OPM Office of the Inspector General's (OIG) Reports.
Some of the findings in the reports include:

- weak authentication mechanisms;
- lack of a plan for life-cycle management of the information systems;
- lack of a configuration management and change management plan;
- lack of inventory of systems, servers, databases, and network devices;
- lack of mature vulnerability scanning tools;
- lack of valid authorizations for many systems; and
- lack of plans of action to remedy the findings of previous audits.

The breach ultimately resulted in removal of OPM's top leadership. The impact of the breach on the livelihoods of millions of people may never be fully known. If a person had applied for a government clearance, it is highly likely that they were affected. However, every person referenced in the application is also highly likely to be affected.

There is a critical need for security programs that can assess vulnerabilities and provide mitigations.

The deliverable for this assignment is a Security Assessment Report (SAR): This should be an 8-10-page (no longer!!) double-spaced Word document with in-line citations and summary references in APA format. The page count does not include figures, diagrams, tables or summary references.

Part 1: Enterprise Network

Consider the types of networks and their security that may be used in an organization to accomplish the functions of your organization’s mission. Which of these does your organization use or should be using?

Common Computing Platforms

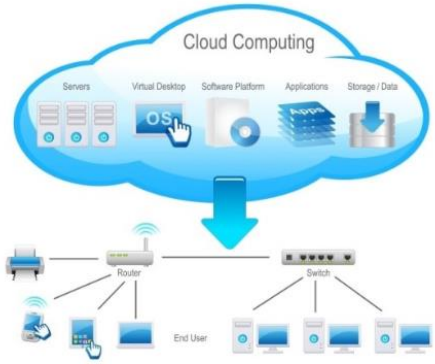
Computing platforms have three main components: hardware, the operating system (OS), and applications. The hardware is the physical equipment/machine that runs the OS and applications. It generally consists of the central processing unit (CPU) or processor, storage,

and memory. The operating system (OS) communicates between the hardware and the applications run by the end user.

Different platforms are used for traditional desktops and laptops and touchscreen phones and tablets. Common processors include Intel Core and AMD (for desktops) and ARM (modified by Apple and Qualcomm to make processors for phones). The most popular operating systems for desktops are Windows and Linux, and for phones, are iOS and Android.

Compatible applications are developed for specific systems by different companies, including Microsoft, Apple, Google, and Adobe

Cloud Computing



Cloud Computing
Source: Microsoft

Cloud computing refers to the use of remote servers over the Internet (instead of via local servers or devices) for the purpose of sharing resources. According to the National Institute of Standards and Technology (Mell & Grance, 2011):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (p. 2)

There are several advantages to cloud computing, including ease of use and upgrades, low capital expenditure, remote access capabilities from several locations, higher security/better data recovery, and optimized use of resources.

Cloud computing servers offer three models: software as a service, or SaaS (use of Internet-based applications through web browsers); platform as a service, or PaaS (use of cloud platforms that can be used to develop applications); and infrastructure as a service, or IaaS (use of remote infrastructure to create platforms and applications).

Cloud computing is a general term for the delivery of hosted services over the Internet. The use of cloud computing can increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software.
Just a few examples of cloud services are:

- Dropbox
- Evernote
- Mozy
- Carbonite

- Google Docs
- Runescape

References

Mell, P., & Grance, T. (2011). Special publication 800-145: *The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology.* National Institute of Standards and Technology. nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Distributed Computing

Distributed computing is a computing model that uses multiple machines or servers connected through a network to share resources and complete tasks. Though the machines can be in different geographical locations, they work and appear as a single entity by communicating through encrypted messages. The latency and bandwidth of the communication channels can, however, have a significant impact on the working of the servers.

Distributed computing models perform tasks by breaking them into subtasks and solving them sequentially or simultaneously (using several machines). Hence, the models can provide greater efficiency and lower risk of failure (as compared with centralized computing models). Distributed computing systems typically use client-server, peer-to-peer, or tier architectures, depending on the functions performed by the servers.

Centralized Computing

Centralized computing refers to a computing model involving a central computer or server with high computing capability and sophisticated applications/software. The central server connects to client computers that have very low processing capability, so when a task needs to be performed, the clients simply send requests to the central server, which then performs most of the processing. The connection between the central server and clients can be either direct or over a network.

As all requests are processed by a central server, the centralized computing model has lower efficiency and higher risk of failure, compared with the decentralized or distributed computing model. However, the centralized model provides higher security and reliability, as all the data is stored and tasks are performed on a central server.

Secure Programming Fundamentals

It is important that software developers follow secure coding methods and adopt safe practices in the development stage, rather than trying to implement them at a later stage.

One of the fundamental secure programming practices is input validation, which is performed to prevent attacks from external sources. The National Institute of Standards and Technology (NIST) also emphasizes its importance for safe programming in its "Guide to Secure Web Services":

Write all web service code in languages that automatically perform input validation, such as Java and C#, or if writing in C or C++, ensure that all expected input lengths and formats are explicitly specified, and that all inputs received are validated to ensure that they do not exceed those lengths or violate those formats. Error and exception handling should be expressly programmed to reject or truncate any inputs that violate the allowable input lengths/formats (Singhal et al., 2007).

Another fundamental practice to ensure security is access control, which is implemented to prevent unauthorized access, resulting in intentional or unintentional changes to the code. In

addition, it is important to include security tools and architectures that can detect code errors and prevent attacks. Finally, it is useful to develop mitigation strategies by modeling possible threats and testing the code.

References

Singhal, A., Winograd, T., & Scarfone, K. (2007). Computer security: Guide to secure web services: Recommendations of the National Institute of Standards and Technology (Special Publication 800-95). *National Institute of Standards and Technology*. http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

Explain the specific local area network (LAN) and wide area network (WAN) and the systems environment that exists at your organization. Be sure to discuss the cyber security aspects of your network and systems.

Part 2: Enterprise Threats

Review the literature and the initial OIG and subsequent OIG reports on the OPM breach. The OIG report and the related articles you find include many security deficiencies that likely left OPM networks vulnerable to being breached.

In addition to those external threats, the report describes the ways OPM was vulnerable to insider threats. The information about the breach could be classified as threat intelligence. Define threat intelligence and explain what kind of threat intelligence is known about the OPM breach.

You just provided background information on your organization and its networks. Next, you'll describe threats to your organization's systems. Before you get started, read about insider threats, also known as internal threats. As you are reading, take note of which insider threats are a risk to your organization.

Insider Threats

An insider threat is a type of threat that comes from within the organization, such as from an employee. These types of threats can also be posed by those with former associations with the organization. Prior and current employees, contractors, business associates, and others with information about the business or its security practices can become an insider threat. The same is true of anyone granted access at any time to the data on the networks and systems of the organization.

Insider threats pose a unique set of challenges. Workers need information in order to do their jobs, but every system's data needs to be protected in order to minimize risk. Every organization has to find a way to strike a balance between these conflicting needs.

Now, differentiate between the external threats to the system and the insider threats. Identify where these threats can specifically occur in your network and systems. Relate the OPM threat intelligence to your organization. How likely is it that a similar attack will occur at your organization?

Part 3: Identify Security Issues

Now it's time to identify the security issues in your organization's networks and systems. As two examples, you will have learned about system vulnerabilities from your MBSA scans and password-cracking in your team project. You and your team members ran individual tests and created a team project report. Provide your analysis of the strength of passwords used by the employees in your organization. Are weak passwords a security issue for your

organization? Provide an analysis of system security issues for the systems in your organization.

Part 4: Firewalls and Encryption

Next, consider firewalls and auditing related to the use of the Relational Database Management System (RDBMS), the database system and data. Also review access control.

Firewalls

Firewalls provide security to network systems by controlling the flow of incoming and outgoing traffic and preventing unauthorized access. The guidelines document of the National Institute of Standards and Technology (NIST) defines firewalls as "devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures" (Scarfone & Hoffman, 2009).

Firewalls are deployed extensively by businesses, educational institutions, government organizations, and end users to prevent cyberattacks and to protect sensitive information.

There are two types of firewall implementation: software and hardware. Software firewalls are installed on individual systems or machines, whereas hardware firewalls are implemented using specialized hardware equipment (on network switches or routers) to provide security to all connected machines. According to one expert:

A firewall can exist as hardware or software (or both). A hardware firewall is a device that is connected to the network and filters the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they at a computer (Bourgeois, 2014) [or system].

References

Bourgeois, D. T. (2014). Information systems for business and beyond. *The Saylor Academy*. http://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond.pdf

Scarfone, K., & Hoffman, P. (2009). *U.S.* Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology: Special Publication 800-41. *National Institute of Standards and Technology*. http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Auditing - RDBMS

Auditing is the process used to keep track of information flow and actions undertaken inside databases. A relational database management system (RDBMS) is used to manage data by organizing it in tables in a way that all data can be accessed without reorganization. This is achieved by connecting the tables' attributes and uniquely identify rows in a table.

The primary advantages of RDBMS over other database management systems have been discussed by Campbell and Shin (2011):

First, each table can now be separately prepared, maintained, and edited. This is particularly useful when one considers the potentially huge sizes of many modern databases. Second, the tables may be maintained separately until the need for a particular query or analysis calls for them to be related. This creates a large degree of efficiency for processing information within a given database.

Consequently, an RDBMS is popular for storage and management of databases.

References

Campbell, J. E., & Shin, M. (2011). Geographic information system basics. http://2012books.lardbucket.org/books/geographic-information-system-basics/s09-02-geospatial-database-management.html

Access Control

Access control is the process by which permissions are granted for given resources. Access control can be physical (e.g., locked doors accessed using various control methods) or logical (e.g., electronic keys or credentials). There are several access control models, to include:

- **Role-based access control:** Access is granted based on individual roles.
- **Mandatory access control:** Access is granted by comparing data sensitivity levels with user sensitivity access permissions.
- **Attribute-based access control:** Access is granted based on assigned attributes.
- **Discretionary access control:** Access is granted based on the identity and/or group membership of the user.

The access control model used is determined based on the needs of the organization. To determine the best model, a risk assessment should be performed to determine what threats might be applicable. This information is then used to assess which model can best protect against the threats.

Determine the role of firewalls, encryption, and auditing for RDBMS in protecting information and monitoring the confidentiality, integrity, and availability of the information in the information systems.

Reflect any weaknesses found in the network and information system diagrams previously created, as well as in your developing SAR.

Part 5: Threat Identification

Now that you know the weaknesses in your organization's network and information system, you will determine various known threats to the organization's network architecture and IT assets.

Get acquainted with the following types of threats and attack techniques. Which are risks to your organization?

- IP address spoofing/cache poisoning attacks
- denial-of-service attacks (DoS)
- distributed denial-of-service attacks (DDoS)
- packet analysis/sniffing
- session hijacking attacks

Spoofing/Cache Poisoning Attacks

Spoofing refers to attacks in which a program pretends to be another program so that it can gain unauthorized access. DNS spoofing is a type of spoofing attack that is performed on DNS records. This type of attack can be carried out in various ways, including through cache poisoning, DNS compromising, and man-in-the-middle attacks.

Cache poisoning attacks involve an attack on the cache of the DNS servers and the replacement of one or more target IP addresses with spoofed ones. The attacker loads these addresses with corrupt content and malicious viruses, which affect the users accessing the cached IP addresses on the DNS server.

IP Address Spoofing

In this type of attack, the attacker sniffs network traffic to identify the pattern of legitimate IP addresses for that particular network. The attacker then forges the IP address in the packet headers. If the network uses the IP address to authenticate the user, the attacker is able to gain access to the network through the packet with the forged IP address. The attacker can then send malicious packets to the network. For example, an attacker may introduce a Trojan or keylogging application to the network after gaining access to it.

IP address spoofing is a network layer attack.

Denial-of-Service Attacks (DoS)
Denial-of-service (DoS) attacks are cyberattacks aimed at making resources (or services) unavailable to users. DoS attacks are implemented through either the exploitation of limitations of communication and application protocols, or an attack on the server involving the transmission of an extensive number of requests meant to overload the server and exhaust its resources.

DoS attacks and their detection are discussed in the guidelines document of the National Institute of Standards and Technology (Scarfone & Hoffman, 2009). They typically lead to significantly increased bandwidth usage or a much larger-than-usual number of packets or connections sent to or from a particular host. Anomaly detection methods can involve monitoring bandwidth or packet or connection numbers and determining whether observed activity is significantly different from expected activity.

The effects of DoS attacks can be mitigated with the installation of appropriate software and the throttling of bandwidth usage.

Distributed Denial-of-Service Attacks
Like denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks are cyber attacks that intend to exhaust network resources. DDoS attacks, however, are launched from several (possibly hundreds or thousands of) devices, which are connected to each other, but distributed over the internet. Hence, a large number of devices simultaneously attack the network infrastructure (as opposed to the single device used in DoS attacks).

Common types of DDoS attacks include bandwidth, traffic, and application attacks. DDoS attacks are harder to prevent and mitigate than DoS attacks, as the multiple attack sources create a large volume of traffic in a short period of time.

Packet Analysis/Sniffing
Sniffing is performed by packet sniffers or network analyzers, which monitor data streams and capture packets for decoding and examination.

According to the National Institute of Standards and Technology (NIST):

> Packet sniffers are designed to monitor network traffic on wired or wireless networks and capture packets. Packet sniffers generally can be configured [to direct] the sniffer to capture all packets or only those with particular characteristics (e.g., certain TCP ports, certain source or destination IP addresses). Most packet sniffers are also protocol analyzers, which means that they can reassemble streams from individual packets and decode communications that use any of hundreds or thousands of different protocols (Mell et al., 2005).

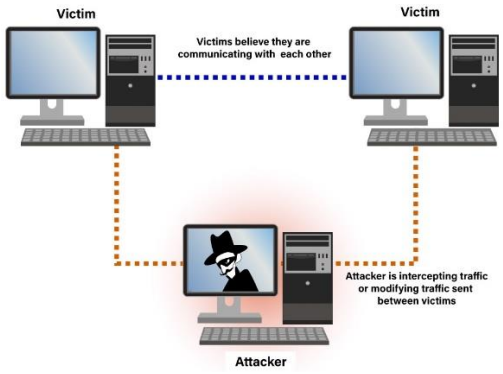
Packet sniffing is performed for several beneficial purposes, which include identifying suspicious activities, finding corrupted or erroneous packets, and analyzing and improving system efficiency. It is, however, also used by hackers for attacking, spying, and collecting information.

References

Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to malware incident prevention and handling: Recommendations of the National Institute of Standards and Technology. (Special Publication 800-83 Rev 1). *National Institute of Standards and Technology. US Department of Commerce.* https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final

Session Hijacking Attacks
When an attacker obtains unauthorized access to a user's session ID or key, the attacker is able to masquerade as the user to access websites. This process is known as session hijacking. The session ID is stored in the cookie and can be stolen using several methods, including sniffing, software codes, and Trojans.

Though it is not easy to identify session hijacking attacks, users can take some precautions to prevent it. Some common steps include using sessions with secure SSL certificates, setting timeouts for sessions, and preventing JavaScripts from accessing session cookies.



Man-in-the-Middle Attack

In identifying the different threats, complete the following tasks:

1. Identify the potential hacking actors of these threat attacks on vulnerabilities in networks and information systems, as well as the types of remediation and mitigation techniques available in your industry and for your organization.
2. Identify the purpose and function of firewalls for organization network systems and how they address the threats and vulnerabilities you have identified.
3. Discuss the value of using access control, database transaction, and firewall log files.
4. Identify the purpose and function of encryption as it relates to files, databases, and other information assets on the organization's networks.

Include these in your SAR.

Part 6 Remediation Possibilities.
Each of the vulnerabilities or threats that you identify may be mitigated or eliminated by employing security measures. The security measures, however, are not specified in the requirements. The requirements just state the security that is desired. Ideally, well before the system is designed and deployed, the requirements are specified and the alternative security measures are considered. Your assessment has uncovered security vulnerabilities which are present because requirements are not written or are insufficient, or the security measures which were implemented were inadequate or poorly administered or for other reasons. Now that remediation is needed, the various measures need to be considered again.

For each of your identified vulnerabilities and threats, be sure to identify several different ways in which they may be addressed; not just one. Security often involves making choices. Normally, you would then do a risk analysis and determine whether any measure should be deployed at all or which specific measure is best for your situation. You are not asked to provide this analysis or choice in this report.

Please use the template I provided separately to complete this Individual Assignment. Although this assignment seems very formidable, the template guides you with the minimum of what is needed and enables you to put a lot of that information into tables. Thus, your writing will be less than you think right now. Please be sure to maintain the given section numbering in the template. Good luck!