American college of Technology

Data Communication and Computer Networking

Group Member	ID Number
1. Alazar Demmelash	004/BSc-B2/20
2. Biruk Bogale	RDCS/119/20A
3. Habtamu Tesfaye	010/BSc-B2/20
4. Mikiyas Mebrate	024/BSc-B2/20
5. Nolawit Sefie	020/BSc-B2/20
6. Yemisrach Ermiyas	028/BSc-B2/20

Supervisor: Ms. Yordanos Fessehaye

Submission Date: 27/12/22

Content

Introduction

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become “wired”, an increasing number of people need to understand the basics of security in a networked world. Businesses are more technologically advanced than ever before, and as technology progresses, so must organizations’ security postures. Network protection is becoming increasingly relevant as more devices connect over wired, wireless, or cellular networks. We’ll look at what network security is and what its main features are and its functions.

1. What is network security?

It is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

Network security is a level of guarantee that all the machines in a network are working optimally and the users of these machines only possess the rights that were granted to them. This include the following:

- Preventing unauthorized people from acting on the system maliciously
- Preventing users from performing involuntary operations that are capable of harming the system.
- Securing data by anticipating failures
- Guaranteeing that services are not interrupted

1.1. Basic Network Security

When connecting a matching to a network, we need to make sure no one will easily break in to it. Even if you don't think anyone will try to break into your machines – chances are that someone might try. Crackers often run network scan utilities that check a large range of IP addresses, and automatically try to find machines running servers with security holes. To protect against that, one could simply disable any unnecessary network service they are running.

1.2. Type of network security

There are two type of network security this are:

1.2.1. Wi-Fi Protected Access (WPA)

- WPA encrypts information, and checks to make sure that the network security key has not been modified.
- WPA also authenticates users to help ensure that only authorized people can access the network.

1.2.2. Wired Equivalent Privacy (WEP)

- WEP is an older network security method that is still available to support older devices, but it is no longer recommended.
- When you enable WEP, you set up a network security key.
- This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

1.3. Network security authentication

One-factor authentication – This is "Something a user knows." The most recognized type of one-factor authentication method is the password.

Two-factor authentication – In addition to the first factor, they require additional proof of your identity next to your password, which makes it more complex.

Three-factor authentication – is the use of identity-confirming credentials from three separate categories of authentication – typically, the knowledge (something you know), possession (something you have) and inherence (something you are) factor.

1.4. How does network security work?

Network security typically consists of three different controls:

A. **Physical Network Security** – controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on. Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.

B. **Technical Network Security** – controls protect data that is stored on the network or which is in transit across, into or out of the network. Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

C. **Administrative Network Security** – controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

2. What is a network security threat?

Are threats that try to access unauthorized information without the knowledge of the owner or breaking through the security or through its vulnerability? Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.it can be:

A. **Software attacks** means attack by Viruses, Worms, and Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

B. **Malware** is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

3. Different ways you can secure your network

We have talked about the different types of network security controls. Now let’s take a look at some of the different ways you can secure your network.

3.1. Network Access Control

To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices. Network access control (NAC) can be set at the most granular level. For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.

3.2. Antivirus and Antimalware Software

Antivirus and antimalware software protect an organization from a range of malicious software, including viruses, ransomware, worms and Trojans. The best software not only scans files upon entry to the network but continuously scans and tracks files.

3.3. Firewall Protection

Firewalls, as their name suggests, act as a barrier between the untrusted external networks and your trusted internal network. Administrators typically configure a set of defined rules that blocks or permits traffic onto the network. For example, Forcepoint's Next Generation Firewall (NGFW) offers seamless and centrally managed control of network traffic, whether it is physical, virtual or in the cloud.

3.4. Virtual Private Networks

Virtual private networks (VPNs) create a connection to the network from another endpoint or site. For example, users working from home would typically connect to the organization's network over a VPN. Data between the two points is encrypted and the user would need to authenticate to allow communication between their device and the network. **Force point’s Secure Enterprise SD-WAN** allows organizations to quickly create VPNs using drag-and-drop and to protect all locations with our Next Generation Firewall solution.

4. Describe of threats

4.1. Password Attack

It’s a type of cyberattack where hackers attempt to access a file, folder, account, or computer secured with a password. Password attack is illegal purpose to gain unauthorized access. To retrieve password for authorize access purpose (misplacing, missing) due various reason.

For example:

- **Brute Force attack** means trying every possible combination. In a brute force attack, hackers steal passwords with the hit-and-try method using special software. You can prevent this by using a secure password manager.

4.2. Phishing

It is essentially the act of getting someone to click on a link which either allows a malicious actor to gain access to personal information or downloads malware onto a user’s device.

Phishing attacks often work by disguising malicious communications as originating from a trustworthy entity, like a bank or phone provider.

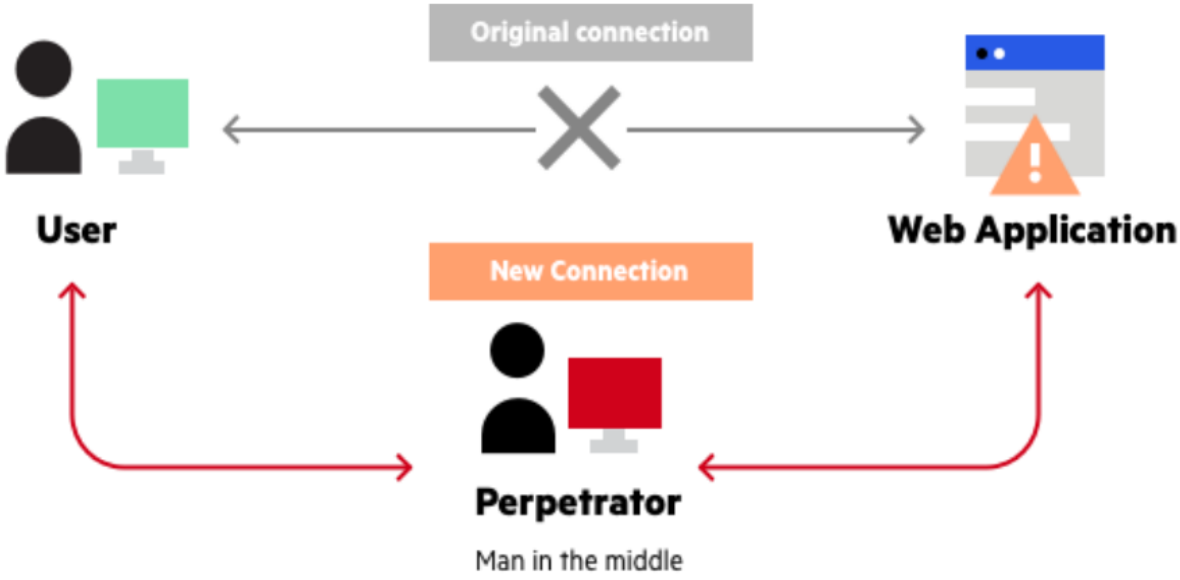
Phishing attack examples

The following illustrates a common phishing scam attempt:

- A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.
- The email claims that the user’s password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.

4.3. MIM attacks

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.



4.4. File-less attacks

File-less malware is a type of malicious activity that uses native, legitimate tools built into a system to execute a cyber-attack. Unlike traditional malware, file-less malware does not require an attacker to install any code on a target's system, making it hard to detect. This file-less technique of using native tools to conduct a malicious attack is sometimes referred to as living off the land or LOL-bins.

5. Common File-less Malware Techniques

Exploit kits Exploits are pieces of code, sequences of commands, or collections of data, and exploit kits are collections of exploits. Adversaries use these tools to take advantage of vulnerabilities that are known to exist in an operating system or an installed application.

Exploits are an efficient way to launch a file-less malware attack because they can be injected directly into memory without requiring anything to be written to disk. Adversaries can use them to automate initial compromises at scale.

An exploit begins in the same way, regardless of whether the attack is file-less or uses traditional malware. Typically, a victim is lured through a phishing email or social engineering.

The exploit kit usually includes exploits for a number of vulnerabilities and a management console that the attacker can use to control the system. In some cases, the exploit kit will include the ability to scan the targeted system for vulnerabilities and then craft and launch a customized exploit on the fly.

A. Registry resident malware

Registry resident malware is malware that installs itself in the Windows registry in order to remain persistent while evading detection.

Commonly, Windows systems are infected through the use of a dropper program that downloads a malicious file. This malicious file remains active on the targeted system, which makes it vulnerable to detection by antivirus software.

File-less malware may also use a dropper program, but it doesn’t download a malicious file. Instead, the dropper program itself writes malicious code straight into the Windows registry.

The malicious code can be programmed to launch every time the OS is launched, and there is no malicious file that could be discovered – the malicious code is hidden in native files not subject to AV detection.

The oldest variant of this type of attack is Poweliks, but many have emerged since then, including Kovter and GootKit. Malware that modifies registry keys is highly likely to remain in place undetected for extended periods of time.

B. Memory-only malware

Memory-only malware resides only in memory. An example of memory-only malware is the Duqu worm, which can remain undetected because it resides exclusively in memory. Duqu 2.0 comes in two versions; the first is a backdoor that allows the adversary to gain a foothold in an organization.

The adversary can then use the advanced version of Duqu 2.0, which offers additional features such as reconnaissance, lateral movement and data exfiltration. Duqu 2.0 has been used to successfully breach companies in the telecom industry and at least one well-known security software provider.

C. File-less ransomware

Adversaries do not limit themselves to one type of attack. They use any technology that will help them capture their payload. Today, ransomware attackers are using fileless techniques to embed malicious code in documents through the use of native scripting languages such as macros or to write the malicious code directly into memory through the use of an exploit. The ransomware then hijacks native tools like PowerShell to encrypt hostage files without ever having written a single line to disk.

D. Stolen credentials

Attackers may commence a file-less attack through the use of stolen credentials so they can access their target under the guise of a legitimate user. Once inside, the attacker can use native tools such as Windows Management Instrumentation (WMI) or PowerShell to conduct their attack. They can establish persistence by hiding code in the registry or the kernel, or by creating user accounts that grant them access to any system they choose.

E. Computer Virus

A computer virus is a malicious piece of computer code designed to spread from device to device. A subset of malware, these self-copying threats are usually designed to damage a device or steal data.

Think of a biological virus – the kind that makes you sick. It's persistently nasty, keeps you from functioning normally, and often requires something powerful to get rid of it. A computer virus is very similar.

Designed to replicate relentlessly, computer viruses infect your programs and files, alter the way your computer operates or stop it from working altogether.

How does a computer get a virus?

Even if you're careful, you can pick up computer viruses through normal Web activities like:

- Sharing music, files, or photos with other users
- Visiting an infected website
- Opening spam email or an email attachment
- Downloading free games, toolbars, media players and other system utilities
- Installing mainstream software applications without thoroughly reading license agreements

What are the symptoms of a computer virus?

- Your computer may be infected if you recognize any of these malware symptoms:
- Slow computer performance
- Erratic computer behavior
- Unexplained data loss
- Frequent computer crashes

What is the recommended solution for those threats?

A. Educate your team about security threats and best practices

Regularly train your employees in proper security procedures, and make the case for why it is important. Make sure they know what to do if they notice something suspicious, or if they become aware of a security lapse. Enforce best practices and demonstrate that they are important to the company.

B. Keep your software up to date

Scheduled, automated updates can take the burden off individuals for keeping up with new software releases and security patches.

C. Enable two-factor authentication and Enforce Strong Password Policies

While many users seem to be immune to calls to choose stronger passwords, two-factor authentication can add an extra layer of security independent from poor passwords.

And Ensure your password has a minimum of 8 characters and contains special characters, capital letters, and small letters. You shouldn't use guessable words or names like your nickname, pet's name, favorite food, holiday destination, birth dates, etc. People who know you personally might crack such passwords. Also use unique passwords for every account, device, and file. Otherwise, hackers might use the credential stuffing technique to attempt password attacks.

D. Have a mobile and personal device policy

There are two ways to handle this problem: Either provide employees with laptops and mobile devices and prohibit file sharing off these devices, or require employees to harden any personal devices they may use to access your corporate network. Also be sure to instruct users on how to access the Internet securely when they're working remotely.

E. Put up a firewall

A firewall is designed to block downloads from anywhere but trusted sources. Firewalls can also restrict access to insecure websites, or limit access to only those on an approved list.

F. Install anti-malware software

Anti-malware software is designed to identify and remove anything malicious that gets on your computer. Make sure your anti-malware software isn't just running, but is also up to date and that the security settings are at the right levels.

G. Install breach monitoring software

Even if you have software in place to combat known errors, you may need extra detection software to monitor your whole system and keep an eye out for suspicious activity. If a firewall is like locking your front door, and anti-malware software is like having a security guard on site, breach detection is like having security cameras installed. They're all pieces of the puzzle to keep your network secure.

H. Restrict access to sensitive data

Keep sensitive data apart from non-sensitive data. This prevents sensitive data from being shared accidentally, and it keeps data breaches compartmentalized. For instance, if you keep your sensitive financial data in secure location A and R&D documents in secure location B, then a breach to location A won't compromise location B.

I. Regularly backup your files

If you have a regular backup of your data, it significantly reduces the risks you face from a data breach. With back up data, you can get your organization back on its feet quickly.

Conclusion

Network security is an important field that is getting more and more attention as the internet expands. The security threats and internet protocol should be analyzed to determine the necessary security technology. The security technology consists of mostly software based, as well as various hardware devices. In addition network Security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined together. Securing the network is just as important as securing the computers and encrypting the message. Points that must be considered when developing a secure network are

- **Confidentiality:** Information in the network remains private
- **Authentication:** Ensure the users of the network are who they say they are
- **Integrity:** Ensure the message has not been modified in transit
- **Authorization (access):** providing authorized users to communicate to and from a
- **Non-repudiation:** Ensure the user does not refute that he used the network. An effective network security plan should be developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack. Tools to reduce the vulnerability of the computer to the network include encryption, authentication mechanisms, intrusion-detection, security management and firewalls.

In addition to protecting the network from outside threats, enforcing company network usage policies can prevent internal users from pulling in threats due to misuse

Reference

https://www.webroot.com/

https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/

https://www.forcepoint.com/cyber-edu/network-security

https://www.crowdstrike.com/

https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

https://www.chathamhouse.org/

https://www.comparitech.com/net