Assignment name	**Information Security**
Student name	**Pham Van Kien**
Student ID	**Kienpvbhaf180165**
Tutor	**Lê Văn Thuận**

Table of Contents

Introduction

This is information security. I have a duty to master your basic knowledge and learn well but the risks and the The organization security procedures and practices of various techniques to improve network security

P1. Identify types of security risks to organizations.

There are ten common security risks:

1. Computer virus

Figure 1 Showing computer virus

A computer virus is a software program that is able to copy itself from one infected object to another (the infected object may be program files, text files, etc.). After infecting the computer, the virus can slow down the computer, corrupt infected files, lose data, cause system errors ...

The virus may also use the victim's computer to illegally advertise, send spam, annoy users, cause insecurity, steal personal information, account information, and numbers. credit cards ... Some viruses also take advantage of a victim's computer to create a botnet (network of ghost computers), to attack server systems, other websites ...

Here are some signs when a computer is infected with a virus:

+ Accessing files, opening slow application programs.

+ When browsing strange web pages appear automatically.

+ Browse slowly, the content of web pages displayed on the browser is slow.

+ The ad page automatically pops up (pop up), the Desktop screen is changed.

+ The right corner of the screen appears the yellow triangle warning: "Your computer is infected", or the "Virus Alert" window appears ...

+ Strange files automatically generated when you open the USB drive.

+ There appear files with the extension .exe with the names of the folders.

In addition, there are many viruses that run in the background with the system and there are no special or unusual signs, so it is difficult for users to know whether the computer is infected with a virus or not.

Therefore, to ensure safety for your computer, you should choose a good antivirus software to install and use regularly and permanently for your computer. Good antivirus software must meet all criteria: copyrighted software, regularly updated with new versions, with direct technical support from the manufacturer when there is a virus-related problem.

2. Rogue security software

Figure 2 Showing rogue security software

Rogue security software is a form of malicious software and Internet fraud that misleads users into believing there is a virus on their computer, and to pay money for a fake malware removal tool (that actually introduces malware to the computer). It is a form of scareware that manipulates users through fear, and a form of ransomware

3. Trojan horses

Figure 3 Showing symbolic of trojan horse

Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an email attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else. Although their payload can be anything, many modern forms act as a backdoor, contacting

a controller which can then have unauthorized access to the affected computer. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can also delete a user's files or infect other devices connected to the network. Ransomware attacks are often carried out using a Trojan.

4. Adware and spyware

Figure 4 Showing an example of spyware – keylogger

Adware conveys promoting content in a way that is surprising and undesirable by the client. Once the

adware malware moves toward becoming installed, it regularly shows promoting pennants, popup

advertisements, or opens new internet browser windows aimlessly interims

5. Computer worm

Figure 5 Showing symbolic of computer worm

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

6. DOS and DDOS assault

A DoS assault is performed by one machine and its web association, by flooding a site with bundles and

making it incomprehensible for genuine clients to get to the substance of the overflowed site. Luckily,

you can't generally over-burden a server with a solitary other server or a computer any longer. In the

previous years, it hasn't been that normal in the event that anything, at that point by blemishes in the

convention.

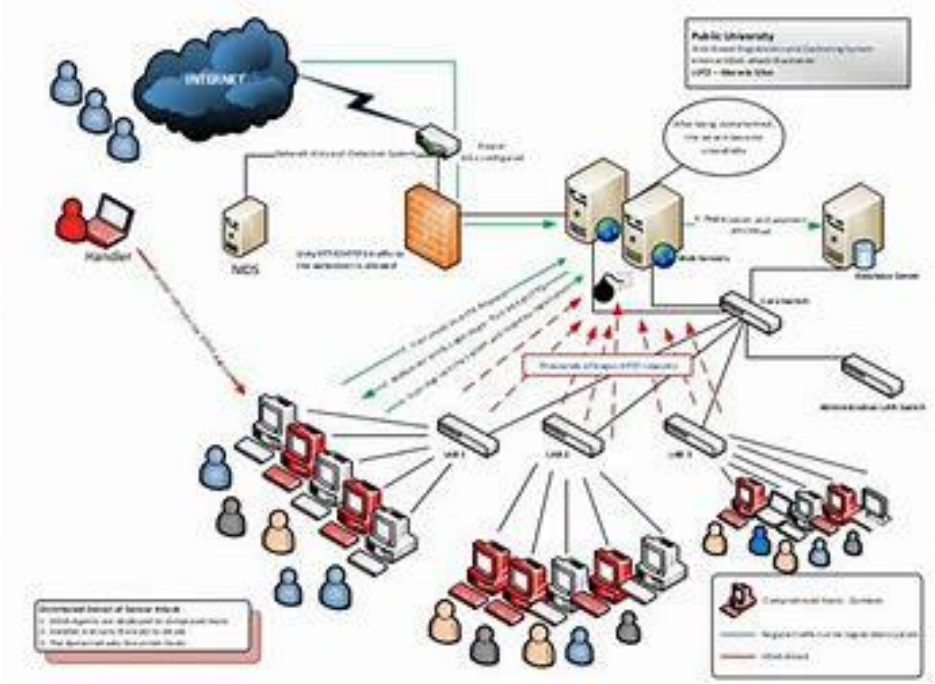

Figure 6 Showing how DoS and DdoS attacks

7. Phishing

Figure 7 Showing computer phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

8. Rootkit

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software. The term rootkit is a portmanteau of "root" (the traditional name of the privileged account on Unix-like operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.

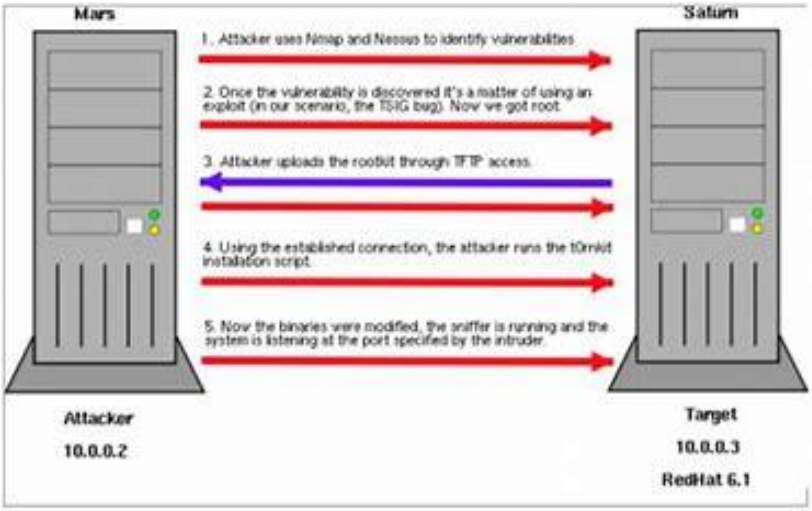

Figure 8 Details rootkit

9. SQL Injection attack

SQL injection is a type of attack that can give an adversary complete control over your web application database by inserting arbitrary SQL code into a database query.

The good news? SQL injection is the lowest of the low-hanging fruit for both attackers and defenders. SQLi isn't some cutting edge NSA Shadow Brokers kit, it's so simple a three-year old can do it. This is script kiddie stuff—and fixing your web application to mitigate the risk of SQLi is so easy that failure to do so looks more and more like gross negligence

Figure 9 Showing attack overview of SQL injection attack

10. Man-in-the-middle attacks

Man-in-the-middle attacks are cybersecurity assaults that enable the aggressor to listen stealthily on the

correspondence between two targets. It can tune in to correspondence which should, in typical settings,

be private. (www.imperva.com)

For instance, a man-in-the-center assault happens when the assailant needs to capture correspondence

between individual An an individual B. Individual A sends their open key to individual B, however, the

aggressor blocks it and sends a fashioned message to individual B, speaking to themselves as A, yet

rather, it has the assailants open key. B trusts that the message originates from individual An and

scrambles the message with the assailants open key, sends it back to A, yet aggressor again catches this

message, opens the message with private key, conceivably modifies it, and re-encodes it utilizing the

Figure 11 Showing how man-in-the-middle attacks work

P2. Organizational security procedures.

2.1. Definition

Security procedures are detailed step-by-step instructions on how to implement, enable, or enforce security controls as enumerated from your organization's security policies. Security procedures should cover the multitude of hardware and software components supporting your business processes as well as any security related business processes themselves

2.2. The Purpose of Security Procedures

The purpose of security procedures is to ensure consistency in the implementation of a security control or execution of a security relevant business process. They are to be followed each time the control needs to be implemented or the security relevant business process followed. Here is an analogy. As part of every aircraft flight, the pilot will follow a pre-flight checklist. Why do they do this? Simply put, they do it to ensure that the aircraft is ready to fly and to do everything possible to ensure a safe flight. Although pilots may have flown thousands of hours, they still follow the checklist. Following the checklist ensures consistency of behavior each and every time. Even though they may have executed the checklist hundreds of times, there is risk in relying on memory to execute the checklist as there could be some distraction that causes them to forget or overlook a critical step.

Much like pre-flight checklists, security procedures guide the individual executing the procedure to an expected outcome. One example is server hardening. Even though a system administrator has built and hardened hundreds of servers, the

procedure to harden the server still needs to be followed to ensure the server is hardened correctly and to a level that still allows operability with the system of which it is a part. If the hardening procedure is not followed, the system administrator could leave out a step that results in an unacceptable exposure of the server or data (e.g., leaving unneeded ports open on the server or the permissions on a directory open to unauthorized users). The best option would be to automate the hardening procedure through scripts or other automation tools

P3. Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.

A virtual private network (VPN) is programming that creates a safe, encrypted connection over a less secure network, such as the public internet. A VPN uses tunneling protocols to encrypt data at the sending end and decrypt it at the receiving end. To provide additional security, the originating and receiving network addresses are also encrypted.

VPNs are used to provide remote corporate employees, gig economy freelance workers and business travelers with access to software applications hosted on proprietary networks. To gain access to a restricted resource through a VPN, the user must be authorized to use the VPN app and provide one or more authentication factors, such as a password, security token or biometric data.

VPN apps are often used by individuals who want to protect data transmissions on their mobile devices or visit web sites that are geographically restricted. Secure access to an isolated network or website through a mobile VPN should not

be confused with private browsing, however. Private browsing does not involve encryption; it is simply an optional browser setting that prevents identifiable user data, such as cookies, from being collected and forwarded to a third-party server.

Potential impact to IT security:

- There might lead to a data breach by creating a hole in the network and the third person could take
- advantage of that breach and steal the sensitive files Desired traffic could not land it's wanted destination.

- The traffic reaches a destination it should have not reached

Figure 11 Showing how VPN works

P4. How different techniques can be implemented to improve network security.

1. Definition of static IP

A static IP address is a 32-bit number that is assigned to a computer to be its address on the internet. This number is in the form of a dotted quad and is typically provided by an internet service provider (ISP).

First, an IP address (internet protocol address) acts as a unique identifier for a device that connects to the internet. Computers use IP addresses to locate and talk to each other on the internet, much the same way people use phone numbers to locate and talk to one another on the telephone. An IP address scan provide information such as the hosting provider and geographic location data.

11. How static IP works

At the point when Static IP Addresses are used. Static IP locations are essential for gadgets that need steady access.

12. Real situation

Static IP would be great in the classroom. They can share a printer over a network by using static IP.

13. NAT – Network Address Translation

Definition

In this Explicit Networking Training Tutorial series, we explored the Differences between Modem and Router in detail in our previous tutorial.

In this tutorial, we will explore the concept of network address translation (NAT) by analyzing the need for introducing it, benefits, types and methods of implementation.

How Network Address Translation Works

In the computer networking system, NAT is introduced as a rescue methodology when the IPv4 address space was getting exhausted.

Network Address Translation helps improve security by reusing IP addresses. The NAT router translates traffic coming into and leaving the private network. See more pictures of computer networking.

Conclusions

Finally, with identifying the type of security risks for organizations. The organization security procedures and practices of various techniques to improve

network security. I was able to master the basics of security and at the same time overcome the risk of information theft.

References

https://linfordco.com/blog/security-procedures/

https://searchnetworking.techtarget.com/definition/virtual-private-network