INDIVIDUAL ASSIGNMENT

CT128-3-2-ISC

IMPLEMENTATION OF SECURE SYSTEM

APU2F2111CS(CYB)- APD2F2111CS(CYB)

HAND OUT DATE: 10 MAY 2022

HAND IN DATE: 18 JULY 2022

WEIGHTAGE: 50%

INSTRUCTIONS TO CANDIDATES:

1. **Assignment is to be submitted through online submission (Moodle).**
2. **Students are advised to underpin their answers with the use of references (cited using APA Referencing).**
3. **Late submission will be awarded zero (0) unless Extenuating Circumstances (EC) are uphelp.**
4. **Cases of plagiarism will be penalized.**
5. **You must obtain 50% overall to pass this module.**

NAME:	**KHALED WALID ALI ELSAYED RADWAN**
TP NO:	**TP063017**

Table of Contents

“For Word Count, Please Refer to the Page (12)”

“For Video Demo Attachment, Please Refer to the Page (13)”

1. Introduction

According to the recent incident occurred to SEPA as the organization faced phishing attacks by hackers, strengthening and using VPN has become a crucial step in the world nowadays as there are many similar cases to this incident being faced by cyber security in worldwide every day. This is mostly because many vulnerabilities existing in the system and potential attacks that may happen using only one person among an organization as a vulnerability to access this organization's email servers. According to that, each individual person or employee should carefully protect himself primarily, as the email server is a very fundamental element of any organization, and if accessing this server is permitted to any external party, there might be significant errors in the organization's system. Thus, there are some techniques and practices required in order to struggle against this category which are also called cyber criminals, and VPN can be considered as one of these techniques used to struggle the cyber criminals.

VPN is the abbreviation of the term "Virtual Private Network”. It is a network connection that is protected from using the public networks. VPN hides the online identity of a user and can also prevent the online activities that he does from tracing. This is mainly by encrypting the user's Internet Protocol address, so that a user can open sites that include tracers and cookies with less caution. Thus, it becomes more difficult for the third party to track the user's activities and steal his personal data (Kaspersky, 2020).

To further understand, think of a VPN as hiding user's real location by making it appear as though he is somewhere else. It primarily builds a data tunnel that connects the local network with an exit node located in another area. As a result, neither the Internet Service Provider (ISP) nor another party will be able to track user's browser actions, including the history of user's browsing or any data have been transmitted by him.

Advantages of VPN

- allow accessing Regional Content

Some places may not always have access to regional websites. Many times, the content on such these websites and service is accessible only from specified regions. The user's location is determined using a regular connection using a local server in the region specified. This means that neither the content from user's home country nor any other country can be accessed when user is at home. For instance, the user might be unable to access some websites and programs, such as Facebook, Google, Instagram, and others. The user can get access to these contents using VPN. However, not all countries are permitted to use VPN, and even some countries may take legal action when someone is detected using VPN, so it is important to take this into consideration (Kaspersky, 2020).

- Provide Secure Encryption

An encryption key is required in order to read the content data. In case this key is not existed, it might take centuries in the event of brute force attack that targets computer in order for this computer to complete the code deciphering. User's internet actions are concealed with a VPN, even in public networks (Kaspersky, 2020).

- Significantly improve security

Regularly used websites and apps track user's online actions continuously and analyze the information they gather, such as IP address, location, passwords, and personal information.
When a user uses VPN, the VPN can stop internet browsers, websites, cable companies, and even Internet service providers (ISP) from following the user.

- Disguise user's location

A Virtual Private Network server primarily works as user's online proxy. User's precise location cannot be identified since there is a server in another region originates the demographic location data. Additionally, most VPN services do not keep records of user's actions. On the other side, some services track user's behavior without disclosing it to outside parties. This implies that any possible record of user's user behavior is kept secret forever (Kaspersky, 2020).

2. Overview of topic

2.1. Recent Issues

- Establishing Tunnel Connections

The failure of user's VPN client to create a tunnel connected with the servers has a couple of recognized causes. The first reason is that User's router always filters IP packets. In most cases, establishing IP tunnel traffic might be challenging due to filtering IP packets. In such scenario, user must look for IP packet filters on the VPN server or client as well as any other connected devices. For checking the server or the client, user must access the page of TCP/IP properties in the advanced settings of the device targeted by user, then the user must choose "filtering", and last thing is to disable the option by clicking the button "properties" (Joel Timothy, 2022).

- Accepting unauthorized or risky connection

Even though it does not happen often, this blunder can have catastrophic consequences. This happens as it significantly jeopardizes user's security and privacy. Check the "Remote Access Policy" to find the solution. The Dial-In tab of the user's sheet of properties in the "Active Directory Users and Computers console" contains the option. If the user wants to stop unauthorized connections, the user can deactivate this feature (Joel Timothy, 2022).

2.2. Challenges

- Limited Physically

The number of individuals who can be hosted by an on-premises device used in standard VPNs is often limited by device. Numerous companies used remote work statistics many years ago to decide the specs for their VPN devices, which left them unready for the spike in working remotely that COVID-19 caused. VPNs are failing, and businesses are having trouble scaling to handle many multiple users. Businesses are using innovative methods. However, these are not long-term solutions. Examples include restricting VPN use to certain employees, buying a backup solution, implementing contradictory standards, etc. (W et al., 2020).

- Failing to Balance Security and Productivity

VPN does not offer a practical answer to the age-old argument between productivity and security. Do businesses encourage access and productivity at the expense of security? Or is it that all traffic sent via infrastructure of security in order to be filtered, overtaxing the VPN, firewalls and Web gateways, while also having a detrimental impact on productivity due to the poor user experience? Users of VPNs will say that they complete half the task in double the period. Then there are the IT professionals, who cite innumerable instances of workers who have jeopardized important data by failing to utilize the proper security precautions or infected their company laptops with malware. The conflict between security and productivity cannot be resolved with conventional VPNs (W et al., 2020).

3. Vulnerabilities & Potential Attacks

In the modern age, even who have taken security precautions cannot be completely assured of their security, so what would it be like for those who do not ever take any kind of security precautions? The DDoS attack threats are highly potential threats associated with using the VPN. The attacks of DDoS have been carried out by the cybercriminals and they were using trojan, or the computer networks infected with a malware.

Due to this, it is challenging to link the user to a specific individual. A DDoS attack would be us ed by cybercriminals for a number of reasons. The hacker can use DDoS attacks to extort businesses and establish a name for themselves in the hacker’s community. DDoS attacks are another tactic used by cyberterrorists to lag websites.

Another Expected assault is a man in the middle attack, so that the hacker positions himself in the middle between the dialogue of an application and a user. Once it is the day end, important information is stolen, including credentials, banking account information, and numerous other pieces of personal data and information. This action is either done with the intent to spy or to assume and act like the other party, making transactions such as trades appear normal while they are in progress. So using a VPN might not always be safe in light of all of this.

The next weakness is infected with Trojan horses and Worms. A Trojan is a client-server-based application that enables access to users' resources, identities, and credentials through the back doors of the end-user network-connected computers. Worms can be defined as self-replicating programs that are designed in order to infect the resources shared such as several drives, involving network and portable drives, and other resources of network. The client will be more damaging right now if it is connected to any VPN. Because infected VPN users and internally connected network services will make the entire business network very susceptible to Trojan and worm infections.

4. Techniques

A software called VPN is created to shield devices from hackers. This is so that IP addresses can be concealed, and traffic and data can be encrypted. This capability makes it challenging for hackers to attack a user. Nevertheless, there seem to be a few procedures to follow to guarantee that VPN can effectively safeguard users from intruders.

- Using strong authentication methods in all connections of VPN

This method is excellent for boosting security. Implementing this technique to user's VPN connection will make it more challenging for the hacker to gain access into the user's computer system. Using multi-factor authentication, for instance, across all VPN connections. Two-factors authentication adds another layer of protection (Heller, 2006).

- Not trusting all providers of VPN

In the event that the organization does not provide remote VPN access, this is the ideal technique for the organization's users. Whenever using free services of VPN, a decent VPN should be able to conceal user's online activity and information; otherwise, it will collect everything. As a result, users who use free services of VPN need to exercise caution and choose reliable services of VPN.

- Testing the VPN limitation

A company will employ a sizable number of people. In order to ensure that all employees can access to the VPN, it is crucial to evaluate the VPN the organization uses. By following this procedure, the employee is less likely to use other free VPN services. Additionally, verifying the restrictions enables IT security staff to identify any existing issues with the VPN software's ability to safeguard stored data. Additionally, it may enable the IT security team to make some adjustments to ensure that the data can be effectively safeguarded by the VPN.

- Using remote VPN when the network is not trusted

This procedure is crucial when an individual connects to and uses a public Wi-Fi network, like one at a hospital, coffee shop, school, hotel, and so on. This is due to the possibility that it is unknown who installed and connected to this public network. Therefore, if a user does not use a remote VPN whenever he connects to a public network, this user's personal information will be leaked without his knowledge.

5. Conclusion

In conclusion, a Virtual private network has more advantages than disadvantages, which is why using one is advised. For example, it enhances online security. By remotely using the encrypted network, the user may protect his Internet Protocol address, location, passwords, and information against potential attackers, major technological companies, and other people who might try to take advantage of the user. Even the user's (ISP) will not be able to see what the user is doing, but they can view statistics from the user’s encrypted server of VPN. The user and others can share files for extended lengths of time without worrying about data being stolen or exposed if a VPN is accessible.

6. References

Kaspersky. (2020, November 3). What is a VPN and how does it work? Www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

Cisco. (2019). *What Is a VPN? - Virtual Private Network*. Cisco. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

What is a VPN? - Definition, How It Works & More | Proofpoint US. (2021, July 29). Proofpoint. https://www.proofpoint.com/us/threat-reference/vpn

5 Common VPN Problems and How to Fix Them. (n.d.). WizCase. https://www.wizcase.com/blog/how-to-fix-common-vpn-issues/

W, M. J. C. P. of P. S. at, eraMay 15, & 2020. (2020, May 15). 4 Challenges with Existing VPNs. Dark Reading. https://www.darkreading.com/vulnerabilities-threats/4-challenges-with-existing-vpns

Heller, M. (2006, October 2). 10 tips to secure client VPNs. Computerworld. https://www.computerworld.com/article/2547058/10-tips-to-secure-client-vpns.html

7. Appendix

WORD COUNT

- Introduction – 637 words
- Overview – 410 words
    - Recent Issues – 187 words
    - Challenges – 223 words
- Vulnerabilities & Potential Attacks – 329 words
- Techniques – 361
- Conclusion – 112

Total – 1849 words

Video Demo Attachment