

Cyber Security Final

by Raoul Enculescu

Submission date: 21-Jul-2023 11:11AM (UTC+0100)

Submission ID: 210503581

File name: 47594_Raoul_Enculescu_Cyber_Security_Final_503767_1020543958.docx (3.08M)

Word count: 2601

Character count: 13249

RAOUL DAN ENCULESCU

2238365

NETWORK AND CYBERSECURITY

ESSENTIALS

ACCA4024_BIRM

ABIDA PERVEEN

21 JULY 2023

THE UNIVERSITY OF WALES

TRINITY SAINT DAVID

QUAY PLACE BIRMINGHAM

CONTENTS

Title.....

Table of content.....

Abstract and conclusions.....

Introduction.....

1. Security Breaches.....

2. Types of Threats, Vulnerabilities, and Attacks.....

3. Security Policy and Digital Space.....

Conclusions.....

References.....

Abbreviations.....

Two months ago, when I started University, I didn't know there are so many "bad" things in the online world. But after a while, I understood how it worked. I used to study networks and servers, the way how to create a peer-to-peer network, I learned about types of cables (P2P), communication, and sharing information. Protocols were an interesting subject, as well as types of layers (OSI). The most important one for me was Cyber Security attacks, hackers, and intruders. I learned about viruses, worms, and trojan horses. Cryptography, access control, and obscuring data made me enjoy this course studied. For this assessment, I will talk about some main problems and explain the way how it works in my opinion. Conclusions about cyber security and cyber attacks can be too many, but I think everyone should be informed well and follow a few essential steps to protect themselves and stay secure.

INTRODUCTION

Cyber Security is when your system or your network is protected well against different kinds of attacks. Sometimes the results might damage our devices, damage hardware, software system, or even data might be in danger. Today I will talk about the main subjects of cyber security, the way how you need to protect yourself against cyber-attacks, what should you do in this kind of situation, and what it means to stay safe. In the world every minute there is a cyber-attack and the best way how to avoid these incidents is to use smart methods against this kind of attack. Everything that is an intentional effort to steal or destroy data or access your network could be fatal. Usually, cyber-attacks are launched by threat actors, and they are using different types of tactics like malware attacks, ransomware, spam, denial of service (DoS), and many more. Hackers have a target, they are trying to break computer networks because they are looking for something important like money, email addresses, personally identifiable information, and business financial data. They want to steal information, disrupt the system or damage a business. It is very hard but not impossible to implement a strategy to protect your system and the people around you. Usually is impossible to know entirely when an attack is coming, but some companies have security monitoring, and they can detect early and flag the cyberattack in progress. Threats are

becoming more advance, and every system should be secure and updated.

1. SECURITY BREACHES

In the last 20 years, lots of small businesses started to be everywhere and the most popular ones are coffee shops where you can sit and enjoy a coffee and work on your computer. Most of them have an internet connection which is very attractive for everyone because gives you free access to the internet and the connection is quite good.

I was reading carefully the story presented and I was disappointed about a few things missing and the way how Mr. Kermit Fogg reacted. If you have a business is very important to have trustworthy people around, you. By opening the business Mr. Fogg came with positive advantages like a free Wi-Fi network for customers and discounts for students and after a while, he started to increase his income.

A security breach is a bad experience where the attacker is accessing your computer data, network, or applications without your authorization. A malware attack is a cyber-attack made intentionally by hackers and can cause disruption to a server, computer, or network.

Meds files are a very dangerous virus, a ransomware infection that encrypted all computers of Mr. Kermit. If I would be a Security Consultant, I will give him a few recommendations which can help him in the future. First is about the way how you interview the people and I think is good to know something about them, to do a history check. But the most important is the way how you protect your business, and the way how you secure it. The first step for him is to install video cameras, this one can record, and he can prove it is necessary. On the market, you can find very professional cameras most of the companies provide good quality products (Nev. N 2017). The second security form is to add a strong password which possibly contains letters, numbers, symbols, and a few capitals (Yenivurt S and Carnovale 2021). But the most important in my opinion is to install a strong anti-virus system. This kind of software can scam and remove viruses from your computer or your network (Johnston R.J. 2009). Another important thing is the way how to keep your documents and where you store them. For Mr. Kermit is important to have a backup and to keep

documents safe. As well I cloud is helpful because, in the case of a cyber-attack, it can recover all documents and information (Puttini R and Mahmood Z 2013). The last thing he can do is firewall protection. (Bock, L. 2022).

Mr. Kermit should analyze this and do it as soon as possible if he doesn't want to protect himself and his business.



2. TYPE OF THREATS, **VULNERABILITY AND ATTACKS**

In the world of cybersecurity threat means something which is weak, and vulnerable and could affect the integrity, and vulnerability of the system, and data and create damage. For example, is that type of

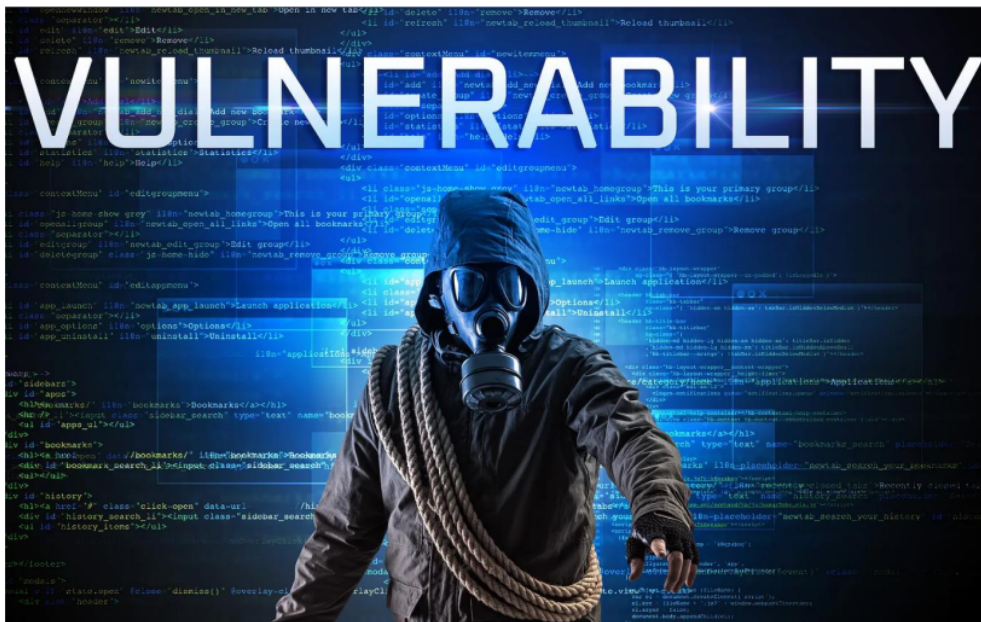
situation when a person called an attacker is taking an opportunity to make a negative impact on a person or a company? They are more types of cyber threats. The last time this kind of threat became more efficient, they can change their tactics daily and attack in a different mode. The most popular types of threats are malware and spyware, password attacks, social engineering, or man in the middle. It is very important for us to keep our integrity and privacy safe by trying to create strong passwords and fully log out after using any type of device. (Gupta, M., Walp, J. and Sharman, R. 2012)

Vulnerability is as well something very important in cyber security. In my opinion, vulnerability is like an unlocked door, something weak which can be opened easily. There are many examples of vulnerability in cyber security but the most common are a weak firewall, unblocked doors, and a lack of security cameras. There is a difference between vulnerability and risk, Cyber security is usually very vulnerable, which means the risk can be low or high. Always you must be one step ahead to prevent malicious attacks, and vulnerability to be detected, identify, analyzed, and verified. After that, we need immediately to remediate vulnerabilities by trying to update the software or fix gaps as soon as possible. (Manzuik, S., Gold, A. and Gatford, C. 2007).

A cyber-attack is something suspicious, an action by threats who are trying to break something or steal by damaging computers, networks, or computing systems. Every second all over the world hackers are trying to steal, destroy and expose information. Hackers can target wide, they can attack usually what is sensitive fragile, and valuable. There are many types of cyber-attacks. Malware attack is the most common one, usually a code or a program created to damage a computer, a network, or a system. They can be trojans, viruses, spyware, or worms. Other types of attacks are DoS, Phishing, Spoofing, Injection attacks, and chain attacks. Protection against these cyber-attacks is very important and every business should have strong security protection, a strong wall to not permit any damage. At the moment most businesses and organizations have infrastructure, applications, and data storage in the cloud. Databases hold very precious and sensitive information and are a high-risk target for attackers. (Geetha, S., Geetha, S. and Phamila, A.V. 2019).

The med's file format is a virus, malicious software, or a program to encrypt files and try to force people or organizations to buy decryption. It is very important to protect ourselves from ransomware infections. As

well is very important to not open suspicious emails from unknown addresses. It is very important to protect our computers by installing good and updated software. Every incident should be reported immediately to authorities, if you provide the correct information as soon as possible authorities will help you to track the cybercrime. If you want to stay safe, I recommend avoiding any contact with intruders because is a big risk. (Krastev, 2023).



3. SECURITY POLICY AND **DIGITAL SPACE**

Security policy and digital space are one of the main problems of our times. Security policy means to be secure, for a business for example means to close the doors, windows, or gates. But cyber security is

different, means protecting yourself, and having privacy when you do something, to protect your information. As well as involved actions to reduce the number of incidents.

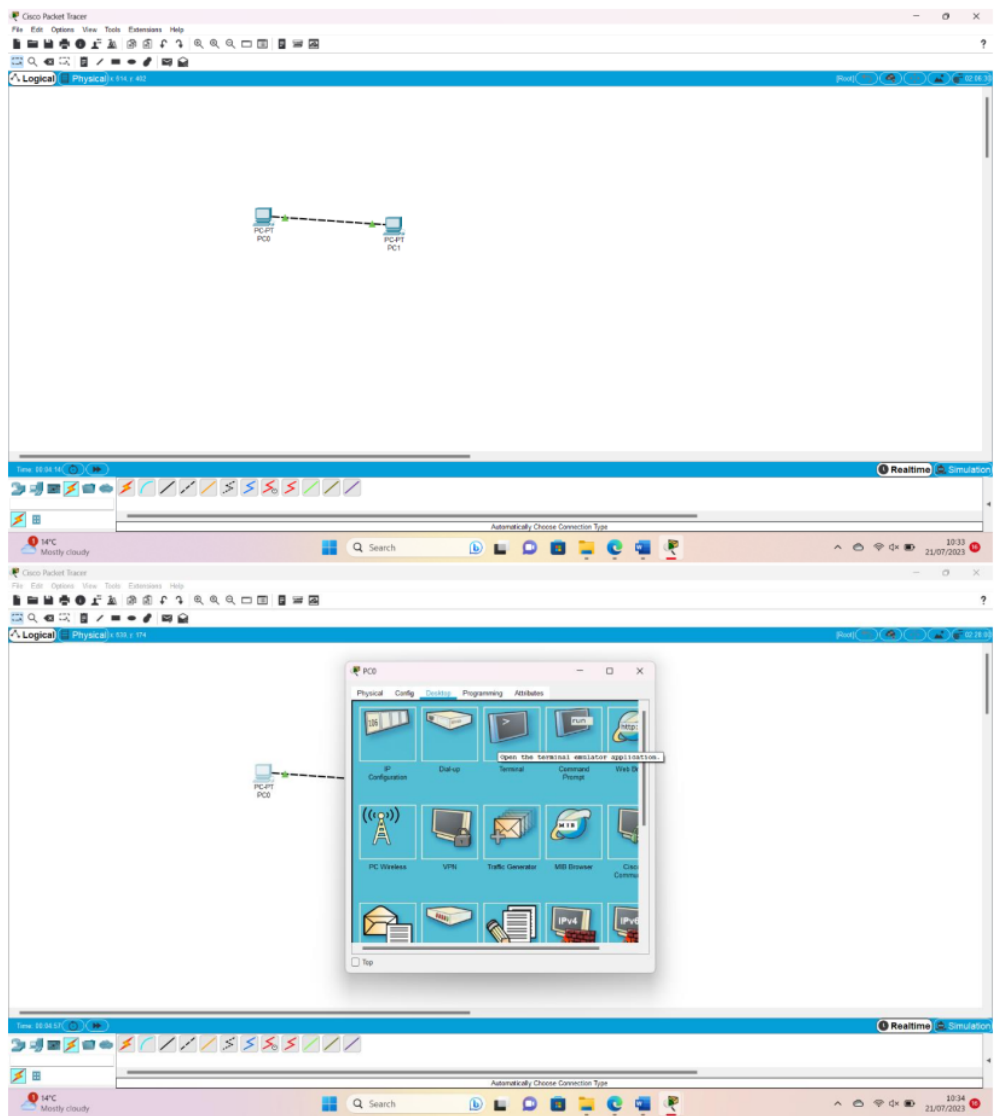
I used to work as a team leader for a long time and I realized is not easy. It's hard work and you need time if you want to see results. But if you have passion for what you are doing and you dedicate yourself you will achieve what you are looking for. Training is very important for your staff, and you must provide it in a professional way, to show and explain what you want from them to do. As a guideline, you need to take care of your staff and first, you need to know how to communicate. In our world almost everything became digital. Big supermarkets are using in-store phones, computers, and tablets to make customer's life easier.

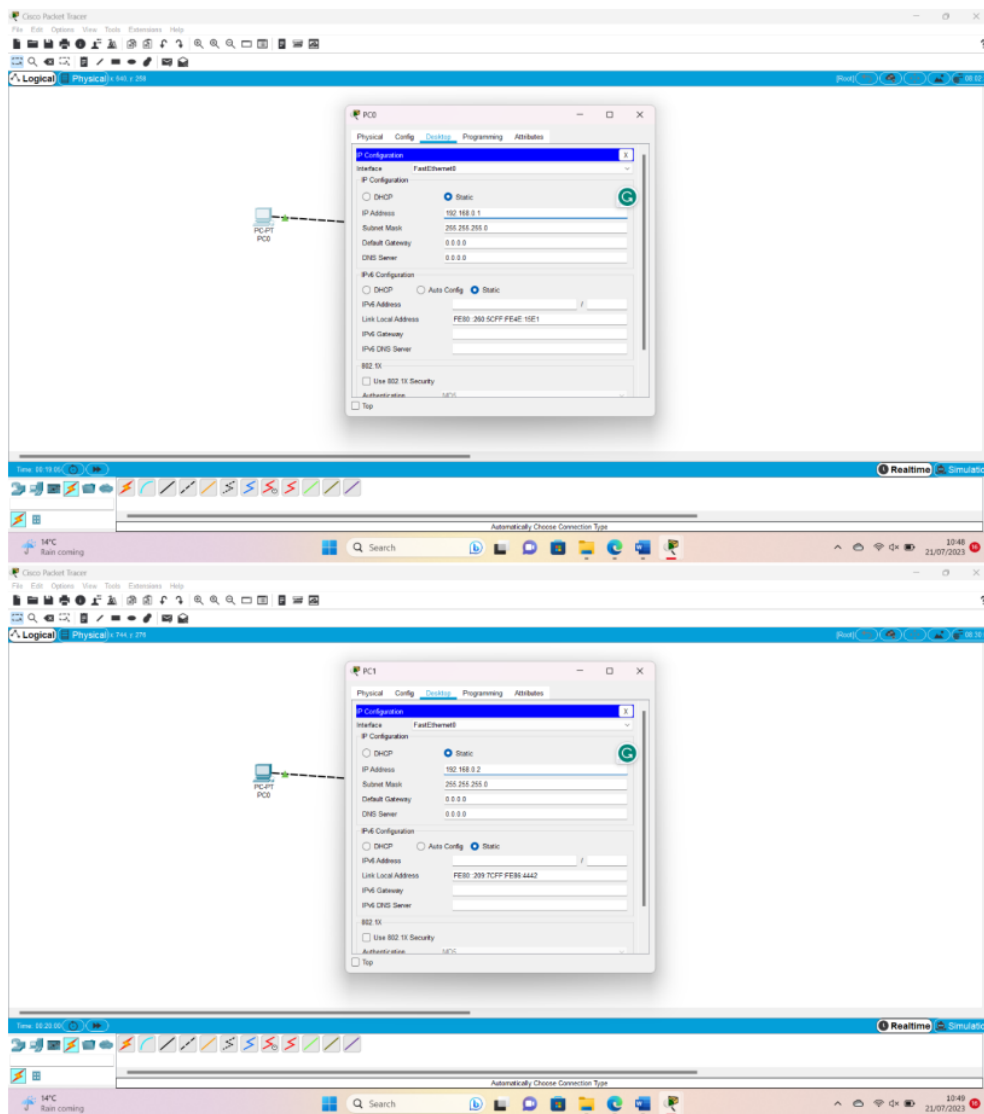
To be a guideline is not complicated, you need to share your knowledge with your staff by providing good training. It's mandatory for a business to have video training where your staff can watch and learn about that. This kind of video is presenting a different kind of software from working on the till, using some application on the tablet, make payments. Most of the banks change their system and they are more secure. For example, debit cards most of are contactless and they have details on the back of the card, they have a pin number, this is just to be more protected and more secure. As well video cameras are very important for security, staff members should check always if there is a problem and if everything is secure. A staff member should always be vigilant and focus on small details, sometimes even small detail matters. Sometimes staff members need more attention and more time, that's why as a guideline need to take time and show small details, especially on the computer part. Every company is using programs, and applications to manage the business well and save time. A staff member should always stay protected and for this one, he needs to secure his phone, laptop, or computer by using a strong password. He had to create an account and a create password, he had to use a long word including numbers, letters, and symbols. He is the only one who knows the password for his security reason. Every person should keep passwords private to not inform other people and to not give them personal details.

Every company has its own policy. In a public place, customers should respect each other. A realistic example for customers is when they are sitting in a queue before to do a payment. There is a rule that should give you privacy and the person who is doing a transaction should know some

important things. They must make sure the next person is approximately two meters away. Also, he should read all instructions and after that do something. After inserting the card, he should protect his card by covering it with his hand and then with the other hand enter the pin number. After the transaction is complete, he could remove his card. I have seen most people are not interested in small details but in my opinion and after I study about cybersecurity, I realized how important is and how easily hackers can steal information from you. Always we are exposed to a cyber-attack and that's why we need to make sure we are protected. It is a big responsibility for a guideline to keep staff focused and provide the right training.

Cisco Packet Tracer is a visual simulation tool designed and created by Cisco Systems and gives you the opportunity to practice computer networks. I started by creating an account which was very easy, and it was completely free. I really enjoyed doing this and I think I took a few screenshots after my work.





Conclusion, recommendation, and future work

After studying so hard I realize how nice is to see your results. It was hard work and a lot of practice and hopefully in the future to be something useful for my future. I learn new things and this course makes me more useful for me and the people around me. Now I have the capacity to share

information with other people to talk more about online, networks, cyber-attacks, and why not to do something in my life. As a person who likes computers, I recommend everyone to try to do computing because, in my opinion, this is the future. I would love to work in this kind of environment for a big company or even open a business. Since I was young, I always liked to build computers, to fix laptops and mobile phones, and I think I would love to build a career based on the hardware part but as well software is an important part of IT. But because I used to work in graphics and design maybe one day I will return. The last word is about security, probably the most important one if you know what to do and how to protect yourself you are safe.

REFERENCES:

1. Whitman, M.E. et al. (2013) Guide to network security. International ed. Australia: Course Technology Cengage Learning.
2. Kumar G., D., Singh, M.K. and Jayanthi, M.K. (2016) Network security attacks and countermeasures. Edited by D. Kumar G., M.K. Singh, and M.K. Jayanthi. Hershey, PA: Information Science Reference. Available at: <https://doi.org/10.4018/978-1-4666-8761-5>.
3. McClure, S., Scambray, J. and Kurtz, G. (2009) Hacking exposed: network security secrets & solutions. 6th ed. New York: McGraw-Hill.
4. Mitra, P. and Mitra, P. (2018) Recent Advances in Cryptography and Network Security. Edited by P. Mitra. Place of publication not identified: Intech Open.
5. Cyber security and threats: concepts, methodologies, tools, and applications (2018). Hershey, PA: Information Science Reference. Available at: <https://doi.org/10.4018/978-1-5225-5634-3>.
6. Reveron, D.S. (2012) Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World. Washington, D.C: Georgetown University Press.

7. Dey, N. et al. (2017) Applied video processing in surveillance and monitoring systems. Edited by N. Dey, A. Ashour, and S. Acharjee. Hershey, Pennsylvania: Information Science Reference. Available at: <https://doi.org/10.4018/978-1-5225-1022-2>.
8. Gupta, B. (2021) Advances in malware and data-driven network security. Edited by B. Gupta. Hershey, Pennsylvania: Information Science Reference. Available at: <https://doi.org/10.4018/978-1-7998-7789-9>.
9. Babulak, E. (2023) Malware : Detection and Defence. Edited by E. Babulak. London: Intech Open.
10. Krieg, C. et al. (2013) Hardware malware. San Rafael, California (1537 Fourth Street, San Rafael, CA 94901 USA): Morgan & Claypool. Available at: <https://doi.org/10.2200/S00530ED1V01Y201308SPT006>.
11. Roman, S. (2002) Access database design and programming. 3rd ed. Sebastopol, Calif. ; O'Reilly.

ABBREVIATIONS:

P2P - peer to peer

DoS – Disk Operating System

WI-FI - Wireless Fidelity

OSI – Open Systems Interconnection.

Cyber Security Final

ORIGINALITY REPORT

8%

SIMILARITY INDEX

7%

INTERNET SOURCES

1%

PUBLICATIONS

4%

STUDENT PAPERS

PRIMARY SOURCES

1

cobhomepages.cob.isu.edu

Internet Source

1%

2

doria.fi

Internet Source

1%

3

www.igi-global.com

Internet Source

1%

4

Submitted to University of Alabama

Student Paper

1%

5

Submitted to University of Bedfordshire

Student Paper

1%

6

Submitted to Middlesex University

Student Paper

1%

7

Submitted to Western Governors University

Student Paper

1%

8

Submitted to Southampton Solent University

Student Paper

1%

9

Submitted to University of Maryland,
University College

Student Paper

<1%

10

rhinosec.fb.bg.ac.rs

Internet Source

<1 %

11

www.wowdetox.com

Internet Source

<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off