Packet Capturing

Khubaib Farah

Vincent Nguyen

Table of contents

1. Introduction
2. Risk Analysis: Physical
3. Risk Analysis: Virtual
4. Ways to fix risks
5. Etc.
6. Bibliography
7. Introduction

The purpose of the project is to learn how to perform packet capturing and understand how it works. As we continue this project, we will understand and learn how security correlates with packet capturing.

1. Risk Analysis: Physical

Find proof of security compromises such as a strewn USB, written password, open and logged in computers unsupervised, etc.

1. Risk Analysis: Virtual

Utilizing different tools, perform packet capturing, etc. to find weak points in networks and other sources connected through Bluetooth, internet, etc. Utilize kali linux.

1. First understand what is a security risk assessment.  
   Answer three important questions:

* What are your organization’s critical information technology assets — that is, the data whose loss or exposure would have a major impact on your business operations? [8]
* What are the key business processes that utilize or require this information?[8]
* What threats could affect the ability of those business functions to operate?[8]

It is best to understand the underlying intention of these questions and process the information from observational methods such as being a spectator and witnessing risks that can be seen just from being in a 3rd person position. Utilization of the risk analysis chart can assist in this process.

1. Ways to fix risks
2. Etc.
3. Bibliography

[1] Siteadmin, “Capture passwords using wireshark,” *InfosecMatter*, 17-Nov-2021. [Online]. Available: <https://www.infosecmatter.com/capture-passwords-using-wireshark/>. [Accessed: 05-Nov-2022].

[2] “Kali tools: Kali linux tools,” *Kali Linux*, 14-Jul-2022. [Online]. Available: https://www.kali.org/tools/. [Accessed: 05-Nov-2022].

[3] R. Sharpe, E. Warnicke, and U. Lamping, “Wireshark User's Guide,” *Wireshark user's guide*. [Online]. Available: https://www.wireshark.org/docs/wsug\_html\_chunked/. [Accessed: 05-Nov-2022].

[4] Siteadmin, “Capture passwords using wireshark,” *InfosecMatter*, 17-Nov-2021. [Online]. Available: https://www.infosecmatter.com/capture-passwords-using-wireshark/. [Accessed: 05-Nov-2022].

[5] “What is wireshark and how to use it: Cybersecurity: Comptia,” *Default*. [Online]. Available: https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it. [Accessed: 05-Nov-2022].

[6] “Wireshark: Kali linux tools,” *Kali Linux*, 05-Aug-2022. [Online]. Available: https://www.kali.org/tools/wireshark/. [Accessed: 05-Nov-2022].

[7] “Kali docs: Kali Linux Documentation,” *Kali Linux*, 25-Jul-2022. [Online]. Available: https://www.kali.org/docs/. [Accessed: 05-Nov-2022].

[8] I. Sotnikov, “How to perform it risk assessment,” *How to Perform IT Security Risk Assessment*, 16-Jan-2018. [Online]. Available: https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/. [Accessed: 07-Nov-2022].