Assignment 1 for CSE3220 – Computer Security
Network Data and Wireshark

Academic year 2023/2024

Abstract

In this practical assignment, you will take the role of an incident response team that is hired by a company called "QuantumBloc Innovations", a startup in the new field of *Quantum Blockchain technology*. The organization has just started growing and has not really thought about security before. You are asked to inspect their network traffic to see whether there are indications of the organization being compromised. After inspection, the company would also like you to critique their network topology and provide changes if needed.

1 Introduction

You have started a company specialized in network security and incident response. One day, you are approached by a new startup called "QuantumBloc Innovations" that is trying to do something with what they call a "quantum blockchain". They recently noticed that other startups are targeted in cyber-attacks, and fear that they can become a target as well. As they are a relatively new startup, the company has not yet thoroughly thought about security. The management team of QuantumBloc Innovations is worried about the situation and decided to hire you to investigate their network and provide them with recommendations on their network infrastructure.

This assignment concerns analyzing network data and writing recommendations to a management team that has limited technical knowledge and skills. Information that is relevant for this assignment can be found in:

- Lectures 1-5.
- Book chapters 1,8,9, and 22.

To work with network data, you can use any tool that is capable of opening and reading PCAP files. In the lecture we briefly showed "Wireshark", which we recommend to use for this assignment. You can get Wireshark from https://www.wireshark.org. Within this tool, you can view and filter network traffic. A cheat-sheet on how to use the different filtering options can be found here: https://cdn.comparitech.com/wp-content/uploads/2019/06/Wireshark-Cheat-Sheet-1.jpg.webp. A useful option is to right-click a packet and go to "Follow->TCP", which will show the entire TCP session.

For further questions or concerns please speak to one of the TAs, or ask your question in the discussion forum on Brightspace.

2 Assignment

In this section, the main tasks and questions you need to complete are presented. The assignment consists of three files:

1. The assignment document (this file)
2. A network diagram of the organization
3. A network capture file of a sample of organization traffic in PCAP format

The network topology as shown in the diagram is used by the organization. One employee (George) lives in another country and works from home. The rest of the employees work on-site. There is a wireless access point for personal devices, which is used by two employees, Luca and Aiden, to connect their personal device. The email server is running in the internal network and provides email services to all employees. The webserver is accessible to the outside world. The organization does not have their own DNS server. The firewall also acts as the VPN server, and therefore the VPN traffic is not captured.

You are directly connected to the main switch of the organization and receive a full copy of the data that travels between the main switch and the firewall.

2.1 Network analysis

The organization has noticed some weird behavior in the network and would like you to investigate. For every investigation, please identify whether something is wrong, and if so, provide a thorough description of (1) what is happening, (2) which indications you have for your conclusion, (3) potential causes of the compromise, (4) what the potential impact of the compromise is, and (5) what steps the company can take to potentially remediate the problem.

1. Aiden, one of the employees in the HR department, complains about problems with his work computer. He can use his web browser, but every time he opens a file, he receives a weird message.
2. The company has received a warning from the DNS provider that one of the devices in the organization tries to open a malicious domain. It is unclear which device is infected and how it became infected, but according to information found online it seems to originate from a new strain of IoT malware. Surprisingly, George had received this email as well.
3. The company has a suspicion that sensitive files are leaked to a competitor. It is unknown where this leak originates from.
4. As the new focus of the company is their security, management thinks it is good to specifically look at the IT department to make sure their systems are clean.

2.2 Revised network topology

Management would like to receive your professional recommendations on their way forward. Your task is to critique the network diagram and draw a new and more secure network topology. (The current diagram was drawn using www.draw.io, but you can use any tool you like). Please make sure that the diagram is easy to understand and does not need any additional information.

2.3 Letter to management

Next to the technical results of the analysis from 2.1, management would like to have a letter of **at maximum 1 A4** that explains in layman's terms what the state of the network is, and your recommendations. As management in organizations is usually not technical, it is your job to "translate" between technical and non-technical terms. You can structure this letter as if you were to write an email.

3 Deliverables

For this assignment, please provide the following documents:

- An analysis of the network data, including a timeline, detailing (1) what is happening, (2) which indications you have for your conclusion, (3) potential causes of the compromise, (4) what the potential impact of the compromise is, and (5) what steps the company can take to potentially remediate the problem. For all four analysis cases, clearly document the analysis and include visuals if necessary.
- A revised network diagram.
- A letter of maximum one A4 to management detailing the changes in the network topology and why they are important. The letter is intended to advise a **non-technical audience** (e.g. CEO).

4 Evaluation

This assignment is graded according to the following criteria:

- Analysis and interpretation of the network data (60%)
- Correctness and completeness of the revised network diagram (20%)
- Clarity and depth of the letter to management (20%)