TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Edvin Ess 201739IVSB

Wireless LAN Security Vulnerabilities: A Case Study of IT College Network

Bachelor's thesis

Supervisor: Mohammad Tariq Meeran
PhD

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Edvin Ess 201739IVSB

Juhtmevaba kohtvõrgu turvahaavatavused: IT Kolledži võrgu juhtumiuuring

Bakalaureusetöö

Juhendaja: Mohammad Tariq Meeran
PhD

Tallinn 2023

Aim of the thesis

Wireless networks have become a standard for many businesses and enterprises nowadays. But the nature of wireless signals makes the networks more susceptible to exploitation. There are countless methods and attacks that hackers could use to identify vulnerabilities and exploit them in a wireless network.

The main goal of this thesis is to identify potential vulnerabilities in the IT College wireless network and to conduct penetration testing based on found vulnerabilities or common attack methods. The author will display how a potential malicious actor could approach attacking an open network taking the IT College wireless network as a case study, as well as underlining the importance of vulnerability assessment and penetration testing. If any vulnerabilities are found and testing proves to be successful, the author will explain the process of finding the vulnerability as well as propose possible security solutions to the found problems.

The author identifies various methods for identifying and conducting penetration tests based on existing work. Then a number of experiments are conducted in the live network. The experiments are divided into scanning of the network and penetration testing based on existing attack methods. The author performs 4 separate scans with 3 different tools and performs 4 different attacks on the live network.

Conclusions

The goal of this thesis was to see if any vulnerabilities could be found in the IT-College open Wi-Fi, what kind of impact they could have as well as how could the security be improved based on previous findings.

Over the course of the experiments and compilation of theoretical background, the author pointed out and practically applied different methods of how an attacker may try to exploit an open WLAN.

During the scanning and penetration testing part of the thesis, the author identified multiple vulnerabilities as well as other kinds of attacks that worked on the network. All of the identified vulnerabilities and attack methods were explained as well as shown how they could be exploited.

Throughout the experiments and analysis of the results the author explained, what kind of impact the vulnerabilities may have alongside proposing possible security measures that could be taken in order to minimize or mitigate the impact.