Kalpa Publications in Computing

Volume 14, 2023, Pages 100–103

Proceedings of V XoveTIC Conference. XoveTIC 2022

Low-cost, scalable IoT technology for real-time streaming network auditing

Pedro Fernández-Arruti[1]*, Alejandro Mosteiro Vázquez[1]†, Carlos Dafonte[1]‡, and Francisco J. Nóvoa[1]§

CIGUS CITIC - Department of Computer Science and Information Technologies, University of A Coruña, Campus de Elviña s/n, A Coruña, 15071, Spain.

Abstract

Nowadays, the security of companies' assets and network infrastructure is very important for the proper development of their commercial activity. Large companies are capable of dealing with existing cyber threats, but small and medium-sized companies do not have the necessary budget. Existing security solutions are aimed at large companies, which can invest a lot of money in cybersecurity and have experts qualified of managing them. For this reason, we have created a network auditing tool capable of evaluating the security status of corporate networks and aimed at small and medium-sized companies. This allows us to obtain real time data through streaming techniques and, in addition, it is low cost, scalable, modular and easy to use, designed so that non-expert personnel can understand the security status of their company.

1 Introduction

The year 2020 has been a turning point in many areas of life due to the emergence of COVID-19. If we analyse this phenomenon in the field of cybersecurity, we can see that a large number of new cyber threats have been appearing and the number of attacks has greatly increased [3]. This is because the pandemic has forced many companies to adapt and build a new working infrastructure based on teleworking and the use of different network devices in order to access internal company resources from outside. This means greater exposure of company resources and, as a consequence, a greater number of threats to it.

Today, there are many security solutions that seek to mitigate these threats, but very few or practically none are focused on small and medium-sized companies (SMEs). Large companies have budgets large enough to hire expert staff or any of the existing cybersecurity tools. This does not happen in SMEs, which are not able to adapt due to the lack of targeted solutions.

*Formal analysis, data curation, software, hardware, research, resources, writing—original draft preparation, visualization and writing—review and editing

†Hardware, research, resources, visualization and writing—review and editing

‡Conceptualization, methodology, validation, supervision, writing—review and editing

§Conceptualization, methodology, validation, supervision, writing—review and editing

This project consists of the creation of a real-time network auditing system through the use of hardware devices created with the aim of analyzing the networks to which they are connected. These devices are responsible for carrying out an inventory of all network devices, identifying their vulnerabilities and, as a consequence, their level of criticality. In addition, they perform an analysis of nearby WiFi networks and send all the information to a central server, which works as a link and allows us to give persistence to the information and visualise it easily. This system is easy to use, low cost, scalable and modular, always aimed at SMEs, but perfectly functional in larger and more complex networks.

2 Related Work

Currently, if we look for solutions related to wired and wireless network audits, we can verify that there are very few tools that offer us the advantages we are looking for: ease of use through plug and play tools, low cost, and adaptability. Next, we name some projects that come close to what we are looking for:

First of all, Pwnagotchi is a project developed by Evilsocket (creator of Bettercap) with the aim of auditing wireless networks through a "friendly" interface. This tool is based on a Raspberry Pi Zero W board, but can be used with any other Raspberry Pi board [1]. On the other hand, there is the Wireless Attack Toolkit (WAT), a project that turns a Raspberry Pi into a security auditing system for different types of networks [2]. Finally, we can highlight Raspberry Pwn, which is an open source software created by the company Pwnie Express, aimed at detecting vulnerabilities in a network using a Raspberry [4].

3 Methods

The network auditing system of this project is based on the creation of custom-made and configured hardware devices to achieve our final objectives. These devices are the ones that we connect to the networks that we are going to audit and are responsible for carrying out the analysis tasks. To do this, they consist of the following components: a Raspberry Pi 4 Model B, a WiFi antenna, capable of performing wireless network analysis; a 3G module, which allows us to have Internet connection in cases where the agent is located in isolated subnets, a small fan to cool the system and a casing in which we can introduce all the previous components.

Thanks to these components, the devices are able to perform all the required functionalities. First of all, an in-depth analysis of the network assets is carried out. For this, a first passive analysis is executed, which allows us to capture all the multicast and broadcast traffic of the local area network. This functionality permits building the segment inventory, allowing the identification of all devices in it. On the other hand, we run an active analysis with which we perform device discovery tasks in order to discover possible hidden nodes (not identified in the previous phase). We also identify the operating system of each device, the state of its ports and the active services on them. Finally, we run a vulnerability analysis, which permits us to identify and classify all the existing vulnerabilities in the network equipment. This allows us to know the security status of each of the detected devices.

On the other hand, we carry out an analysis of the WiFi networks deployed in the geolocation of the audited company. With this we can detect WiFi Access Points and many of their characteristics.

4 Results

As a final result, we have managed to create a complete system capable of auditing corporate networks of different companies and sending and processing all the data in real time using streaming techniques. With this, we developed a web application that allows us to visualise all the data collected in an orderly and simple way.

Among the different functionalities of the web application, we can highlight the detailed visualisation of all the information collected in each network analysed. On the other hand, it automatically creates executive reports that summarise the security status of each company and displays different types of graphs that help to understand the data collected. In addition, from the web interface itself, we can modify the configurations of any sensor that we have deployed in the network of any company. Figure 1 shows an example of the web application, showing the result of a WiFi analysis.

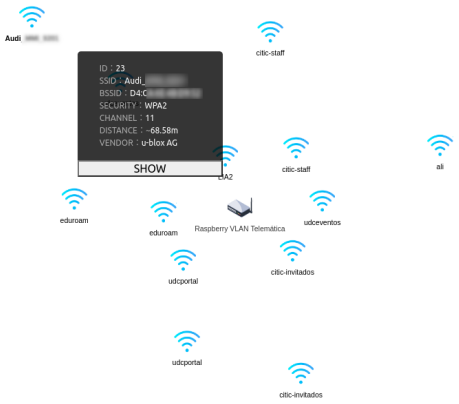

Figure 1: Web application: WiFi map

5 Discussion

Once this project has been put into practice, we can conclude that it is possible to create a corporate network auditing system oriented to SMEs, which is easy to understand and use, low cost and capable of adapting to organizations of different sizes.

As future work, we want to further improve the functionalities of our system, in order to obtain more information related to the security level of companies and their weaknesses.

6 Acknowledgments

This work made use of the infrastructures acquired with Grants provided by the State Research Agency (AEI) of the Spanish Government and the European Regional Development Fund (FEDER), through RTI2018-095076-B-C22, PID2019-111388GB-I00 and PID2021-122842OB-C22. We acknowledge support from CIGUS-CITIC, funded by Xunta de Galicia and the European Union (FEDER Galicia 2014-2020 Program) through Grant ED431G 2019/01; research consolidation Grant ED431B 2021/36; and scholarship from Xunta de Galicia and the European Union (European Social Fund - ESF) ED481A-2019/155.

References

[1] Evilsocket. Pwnagotchi. [online], 2022. Available at https://pwnagotchi.ai.

[2] Bryan "Crypt0s" Halfpap. Wireless attack toolkit. [online], 202. Available at https://sourceforge.net/projects/piwat/.

[3] Rajesh Kumar, Siddharth Sharma, Chirag Vachhani, and Nitish Yadav. What changed in the cyber-security after covid-19? *Computers & Security*, 120:102821, 2022.

[4] Pwnieexpress. Raspberry pwn. [online], 2022. Available at https://github.com/pwnieexpress/raspberry_pwn.