Securing Your Home Network: A Guide to Parrot OS Tools

Author: Luis Raúl Ortiz-Serrano
Advisor: Dr. Alfredo Cruz
Electric & Computer Engineering and Computer Science

Abstract

This master's project explores the world of ethical hacking, highlighting its importance in protecting home systems from cyber threats and examining the role of ethical hacking in contemporary cybersecurity practices through the use of five Important tools. The project aims to deepen understanding of these tools, systems, and principles by immersing participants in a real-world home scenario, fostering a culture of prevention and response, and improving students' understanding of cybersecurity in a domestic context. By integrating ethical hacking exercises into education, the project equips students with basic skills and knowledge to mitigate modern threats, strengthening personal data protection and system integrity, and contributing to the field of cybersecurity while fostering a more professional and vigilant student community. The purpose is to effectively navigate the ever-evolving landscape of cybersecurity.

Introduction

Pentesting is a cybersecurity technique that involves simulating attacks on computer systems to find vulnerabilities, also known as ethical hacking or white hat hacking. The goal of pentesting is to expose security vulnerabilities and improve information security. The project presents a real domestic pentest laboratory as a unique opportunity to test and improve ethical hacking skills, using the Parrot OS operating system as a robust and versatile platform for penetration testing. Accompanied by 5 tools used in this environment, are Nmap, Wireshark, Bettercap, Burp Suite, and Metasploit.

Background

The emergence of smart devices and the proliferation of internet connectivity have transformed the modern household into a complex networked environment. With the advent of smart TVs, home assistants, security cameras, and devices, homes are now more connected than ever before. This interconnectedness brings convenience and efficiency but also introduces new challenges and vulnerabilities in terms of cybersecurity. In response to this evolving landscape, the concept of a home network laboratory has gained traction among cybersecurity professionals, researchers, and enthusiasts. A home network laboratory is a simulated or real-world environment within a household setting, specifically designed for testing, experimenting, and analyzing various aspects of network security and device interactions. These laboratories typically consist of a variety of networked devices, such as routers, switches, computers, smartphones, devices, and network-attached storage devices. These devices are interconnected to simulate a typical home network environment, complete with wired and wireless connections. Additionally, specialized software tools and platforms may be deployed to monitor network traffic, detect vulnerabilities, and assess security posture.

Problem

The security of home networks and devices is a major concern due to the lack of awareness about security best practices and the proliferation of vulnerabilities in insecure devices. Homeowners lack the tools and resources to understand and protect their home networks against emerging cyber threats. The lack of training and expertise in cybersecurity among home users contributes to the exposure of sensitive personal data to security risks.

Methodology

VirtualBox [1] is a free and open-source virtualization product developed by Oracle Corporation. It's a software application that allows users to create and run virtual machines on their computers First of all, make sure you have VirtualBox installed on your computer. See Figure 1

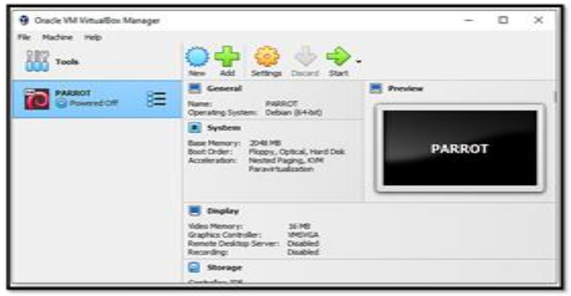

Figure 1 Install Parrot OS with VirtualBox

Parrot is a security-oriented OS. [2] It comes with a wide range of security tools for various purposes, such as penetration testing, forensics, and general security assessments. See Figure 2

Figure 2 Desktop Parrot OS

After the installation of Parrot OS as a virtual machine, the security assessment of the home network begins using five hacking tools. We start with network recognition. For this will use NMAP to obtain information about available devices and services. Once the information about the network has been collected, the network traffic is analyzed.

In this phase, Wireshark [3] is used to capture and analyze network traffic, detect patterns and anomalies, and identify the devices and services that are generating the traffic. This allows us to identify possible vulnerabilities. Then an attack simulation is an important part of security assessment. In this phase, will use Bettercap to simulate attacks against the network and evaluate the network response.

Vulnerability assessment is another important step in security assessment. In this phase, tools such as Burp Suite and Metasploit are used to assess vulnerabilities in web applications and network services. Possible vulnerabilities are identified in security configurations and devices and services connected to the network.

After assessing vulnerabilities, the overall network security can be assessed. In this phase, factors such as authentication, authorization, encryption, and firewall, among others, are considered. Possible improvements are identified to improve network security.

Results and Discussion

First, scan the network with Nmap to detect connected devices and open ports using the nmap -sS 192.168.1.0/24 command. Next, I use Wireshark to capture and analyze network traffic.

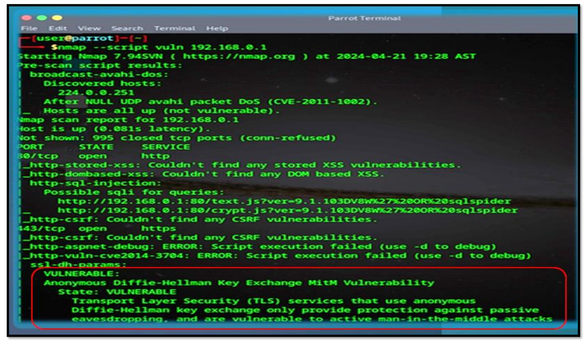

Figure 3 Nmap vulnerable

Performed an internal penetration test on the home network using Bettercap, taking a systematic approach to evaluating its security. Used Bettercap to execute ARP spoofing attacks and other exploits, enabling proactive identification and remediation of security risks.

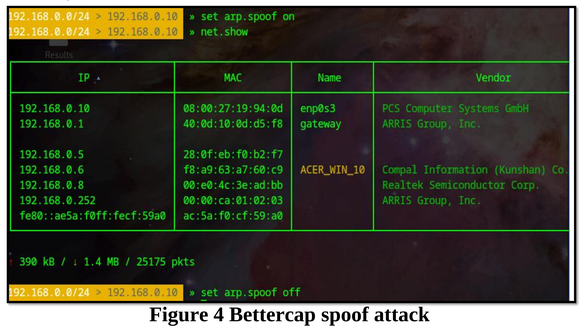

Figure 4 Bettercap spoof attack

Metasploit Meterpreter Figure 5 represents the exploitation that was successful and access to the compromised system is obtained, you can navigate through the directories of the hacked machine to explore its structure and content.

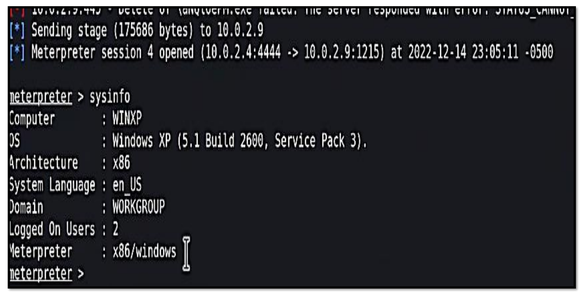

Figure 5 Metasploit Meterpreter

Simulating a cybersecurity exercise in a home environment helps with detailed testing of security measures and incident response capabilities. In essence, conducting cybersecurity exercises in a home environment using ethical hacking tools is a proactive measure to improve cybersecurity proficiency and strengthen digital defenses.

Conclusions

Through practical learning, students enhance their skills and comprehension of real-world cyber threats. By engaging in cybersecurity exercises, students not only reinforce their theoretical knowledge but also gain hands-on experience in identifying vulnerabilities, managing risks, and responding to security incidents. This experiential learning cultivates confidence among students as they navigate the complexities of cybersecurity. The conclusion asserts that these exercises serve as a valuable platform for students to explore diverse topics, tools, and techniques within the cybersecurity domain, including penetration testing, vulnerability assessment, incident response, and digital forensics. By expanding their understanding of cybersecurity and fostering a culture of hands-on learning, students are equipped to adapt to the evolving digital landscape and pursue lifelong learning and innovation in the field. Ultimately, cybersecurity exercises play a crucial role in educating students, providing them with the practical skills, knowledge, and experience necessary to succeed in addressing the challenges of an increasingly digitized world.

Future Work

The project should cover a wider range of topics beyond the basics, including network security, cryptography, secure coding, incident response, and regulatory compliance. This helps students gain a more well-rounded understanding of the field. Exposing students to a variety of tools used in vulnerability assessment, intrusion detection, log analysis, threat intelligence, etc., equips them with a broader skillset and the ability to choose the right tool for the job. Integrating practical scenarios like simulated cyberattacks, incident response, and red/blue team exercises allows students to apply their theoretical knowledge and develop practical skills in a safe environment.

Acknowledgements

As I reflect on my journey in my studies, I am deeply grateful to Dr. Alfredo Cruz for his invaluable guidance and expertise, which have been instrumental in helping me overcome the challenges of completing my master's degree. His wisdom has been a constant source of inspiration and support during my graduate studies.

References

[1] Filipsson, F. (January 23, 2024). What is VirtualBox? A Complete Guide to Virtualization. Redresscompliance.com https://redresscompliance.com/what-is-virtualbox-a-complete-guide-to-virtualization/

[2] Kingsland University. (2024). What Are the Best Linux Distros for Cybersecurity Students? kingslanduniversity.com https://kingslanduniversity.com/best-linux-distros-cybersecurity

[3] Terrell, K. (2024). What is Wireshark? Techtarget.com https://www.techtarget.com/whatis/definition/Wireshark