Система за практическо обучение по киберсигурност чрез симулация на атаки от тип “penetration testing”

Ons Chebel, Галина Иванова, Павел Златаров

(резюме)

A System for Practical Cybersecurity Education Through Simulation of Penetration Testing Attacks

Ons Chebel, Galina Ivanova, Pavel Zlatarov

(summary)

Abstract:

In a world where data is more vulnerable than ever and where it is becoming harder to protect it, it is crucial to teach students about the risks and attacks that may occur and what they can do to prevent the exploitation of various security vulnerabilities. In this paper, a digital lab for simulation, consisting of virtual machines with three different operating systems is presented. A Kali Linux machine is used to simulate attacks against an intentionally vulnerable environment (Metasploitable 2), and a standard user environment (Windows 10). This will allow the observation of the differences in the defense strategies of each one.

Advantages of the presented solution include the fact that it bridges the gap between theoretical education and practice, giving students the opportunity to better grasp the concept of different vulnerabilities and risks of attacks. Potential challenges, such as the high technical requirements, are also discussed.

Keywords: cybersecurity, digital transformation, virtual laboratory, penetration testing, vulnerability assessment, operating systems, network security, defense strategies.

For contacts: Ons Chebel, Computer Science Engineering student, University of Carthage, National Engineering School of Carthage, Erasmus student in University of Ruse, ons.chebel@enicar.ucar.tn

INTRODUCTION

Technology has made major advancements in recent years, and despite the many benefits it provides, humanity is also facing a whole new set of challenges, especially regarding data and its security [1]. This is an important reason why it is crucial now to protect data, teach engineering students good cybersecurity practices, and provide regular training for teaching professionals to keep them aware of current trends.

One of the best ways to demonstrate the importance of cybersecurity is to perform controlled attacks and observe how systems react to them [2,3]. This is where we can see the power of penetration testing, a concept in which various tools are used to observe how attackers take advantage of systems’ vulnerabilities and what kind of attacks they can perform on said systems, especially if outdated software is used or many unnecessary ports are left open [4].

IMPLEMENTATION OF THE VIRTUAL LAB

The aim of this virtual lab is to solidify the knowledge that students acquire in other academic subjects, such as computer networks and communication, and to develop a practical understanding of how attacks are carried out and what vulnerabilities attackers take advantage of. The main learning objectives are to demonstrate host identification, port scanning, service enumeration, exploit selection,

and the verification of successful or failed attacks in a controlled environment. In an era where new technologies are emerging rapidly, it is crucial to educate future engineers on how to protect data, as data is extremely valuable.

In this project, Oracle VirtualBox, a hypervisor, was used to create the virtual environment and run all the operating systems on one machine.

The following operating systems were used in this implementation:

- Kali Linux as the attacker;
- Metasploitable as the vulnerable target;
- Windows 10 as a more robust target and a practical alternative since it is one of the most widely used operating systems.

All of these operating systems were placed in an internal network, called “Security”, with the Windows 10 firewall disabled. The virtual environment is isolated and used only for educational purposes.

The first step of this virtual lab is to identify the IP configuration of each system. Therefore, we use the command *ifconfig* for Metasploitable 2, *ipconfig* for Windows 10 and *ip a* for Kali Linux.

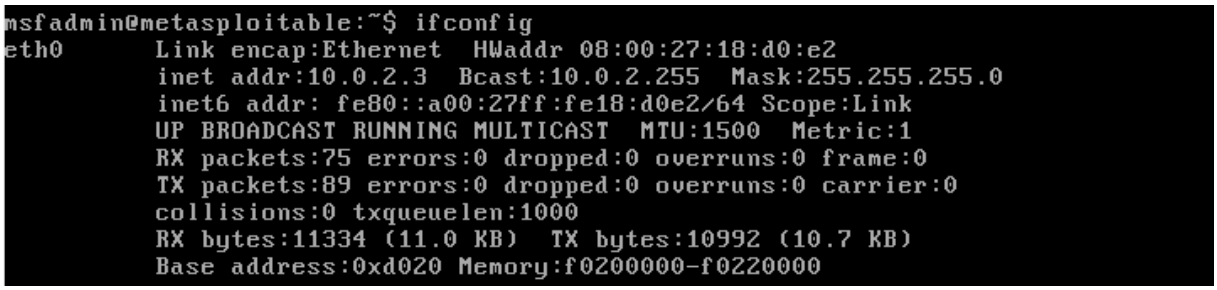

Fig. 1. IP configuration of Metasploitable 2

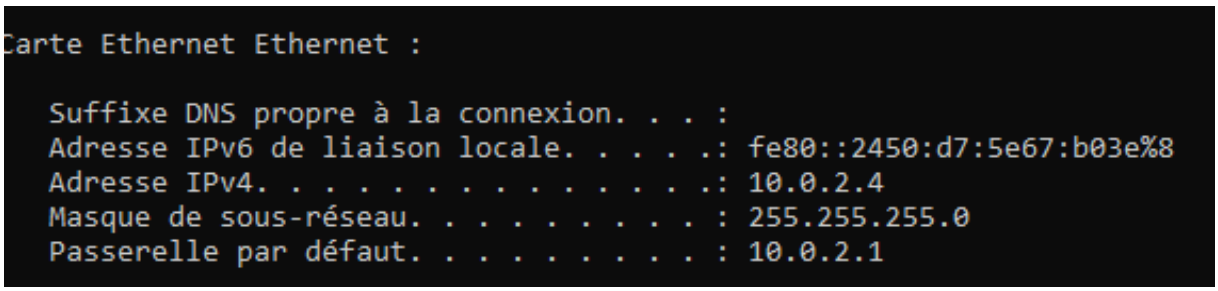

Fig. 2. IP configuration of Windows 10

Fig. 3. IP configuration of Kali Linux

The next step consists of scanning the open ports on both target systems from Kali Linux using the nmap command with the -sV option, which detects service versions. The results show that Metasploitable 2 exposes a much larger number of potentially vulnerable services compared to Windows 10. The results of the scans for each operating system are shown in Fig. 4 and Fig. 5.

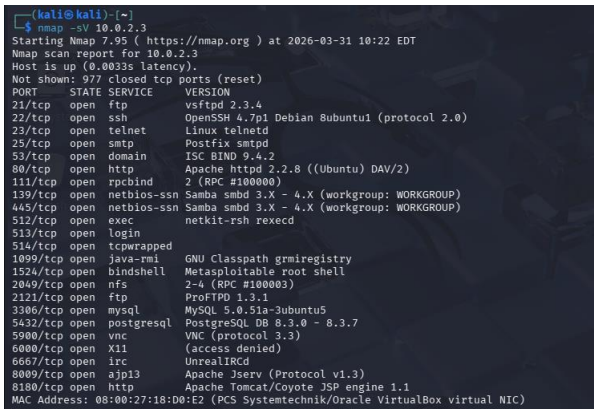

Fig. 4. Open ports on Metasploitable 2

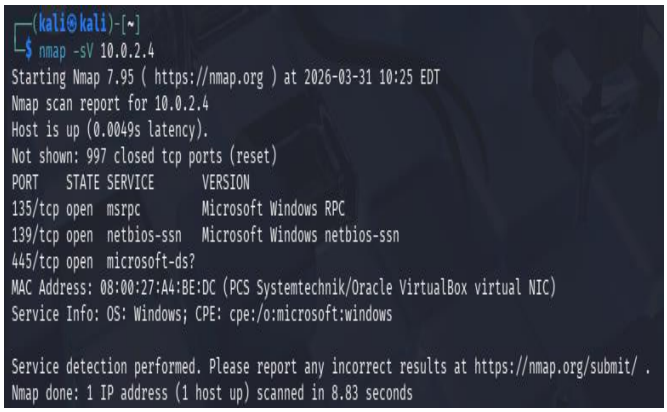

Fig. 5. Open ports on Windows 10

The next step demonstrates exploitation using Metasploit [5], a widely used testing framework for identifying, exploiting, and validating vulnerabilities in computer systems. In this example, port 21, used by the FTP service, is targeted on Metasploitable 2. The Metasploit Framework is started with the msfconsole command, after which the exploit/unix/ftp/vsftpd_backdoor module is selected. The target IP address is then configured using set RHOSTS 10.0.2.3, and the attack is started with the exploit command. After successful exploitation (Fig. 6 and Fig. 7), commands such as whoami, hostname, and ifconfig can be used to verify access to the compromised system. The result shows that access has been gained with root privileges. This demonstrates the importance of disabling unnecessary services, closing unused ports, and avoiding outdated vulnerable software.

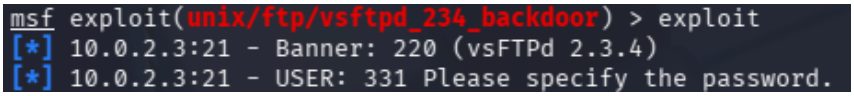

Fig. 6. Exploitation of Metasploitable 2 via the vsftpd_234_backdoor exploit

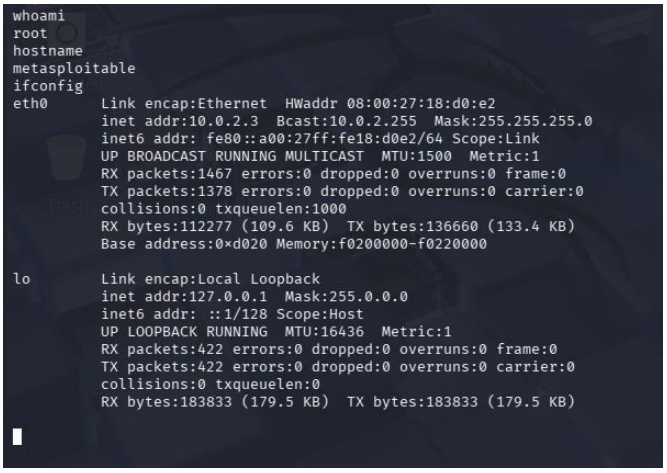

Fig. 7. Successful exploitation of Metasploitable 2

When the same exploit is executed against the Windows 10 target by changing the target IP address to 10.0.2.4, the attack fails, as shown in Fig. 8, since the selected exploit is specific to the vulnerable FTP service on Metasploitable 2.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.4
RHOSTS ⇒ 10.0.2.4
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] 10.0.2.4:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refuse
d by the remote host (10.0.2.4:21).
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

Fig. 8. Failed attack on Windows 10

SURVEY

The virtual lab was presented to a group of Bulgarian students in order to evaluate its perceived usefulness as an educational demonstration. The survey included questions about students' prior awareness of how quickly an outdated system could be compromised, why the attack failed against the modern Windows 10 system, what personal cybersecurity habit they would change after the demonstration, and why digital transformation without software updates can be dangerous. The results suggest that the demonstration helped students connect the simulated attack with practical cybersecurity behavior. Most respondents correctly identified that the attack against the Windows 10 system failed because of the firewall and closed ports, while their open-ended answers mentioned stronger passwords, regular software updates, avoiding unsafe third-party downloads, and controlling open ports. This indicates that the virtual lab can support not only technical understanding of penetration testing steps, but also awareness of everyday cybersecurity practices.

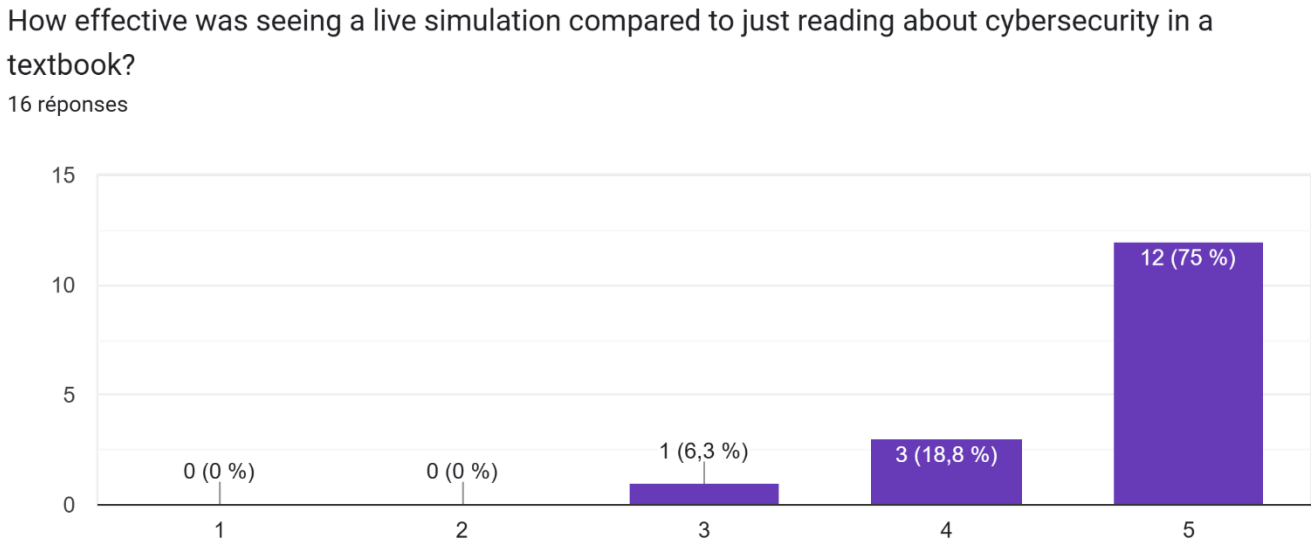

Fig. 9. Student responses regarding the perceived usefulness of the simulation

CONCLUSION

In conclusion, the presented simulation demonstrates the importance of raising cybersecurity awareness and teaching students how to protect information systems. The proposed virtual lab provides a practical way to demonstrate attacks, vulnerabilities, and basic defensive considerations in a controlled environment. By allowing students to observe the attack process directly and understand the role of

open services, outdated software, and system configuration, such exercises can support traditional lectures and create a more engaging learning experience.

REFERENCES

1. Hilario, E., Azam, S., Sundaram, J., et al. (2024). Generative AI for pentesting: The good, the bad, the ugly. International Journal of Information Security, 23, 2075–2097. https://doi.org/10.1007/s10207-024-00835-x

2. Justice, C., & Vyas, R. (2017, June). Cybersecurity education: RunLabs rapidly create virtualized labs based on a simple configuration file. Paper presented at the 2017 ASEE Annual Conference & Exposition, Columbus, Ohio. https://doi.org/10.18260/1-2--28098

3. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Kuzminykh, I., & Mersni, A. (2022). Development of virtual laboratories and innovative cybersecurity courses for distance learning. CEUR Workshop Proceedings, 3188, 98–107. https://ceur-ws.org/Vol-3188/paper10.pdf

4. Valea, O., & Oprişa, C. (2020). Towards pentesting automation using the Metasploit framework. In 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP) (pp. 171–178). IEEE. https://doi.org/10.1109/ICCP51029.2020.9266234

5. Kennedy, D., O’Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The penetration tester’s guide. No Starch Press.