PENETRATION TEST REPORT

Active Information Gathering

Prepared By:

Gopi Gor

Table of Contents

Executive Summary

Active Information Gathering is the technique used to gather information about any target, such as open ports, services running, versions of services and vulnerabilities and risks involved for the business.

This information-gathering technique is different from passive reconnaissance, where we get both positive and negative implications on the business. Positive impacts on the business could be a competitive advantage and higher security. Similarly, the negative effects could be security risks, reputational damage and ethical concerns. Additionally, open ports can be passages for attackers who are waiting to enter a network to cause major damage to a business.

Scope and Objectives

The scope of this document is to perform active reconnaissance or active information gathering on 2 targets as part of lab setup. The report will cover network infrastructure details like open ports, services, vulnerabilities and recommendations.

The specific objectives of this report are:

- Active recon - Metasploitable 2
- Active recon - Windows 7 Vulnerable
- Identify open ports and services.
- Run remote shell to execute commands.
- Identify vulnerabilities and risks.
- Provide recommendations to improve security.

Methodology

This section discusses the methodology and tools used to conduct the penetration test on active recon. The IP addresses of the devices used are below:

- Kali - 10.0.2.15
- Metasploitable 2 - 10.0.2.5
- Windows 7 - 10.0.2.1

1. **Scripting**: a basic **ping.sh** script was created to use bash scripting.
2. **NMAP**: This was used to scan the targets and get info on the open ports, states and services. We also used Wireshark to check packets information. **nmap <target-addr>**
3. **Netcat:** This was used to check services in ports, and then to connect to remote shell and interact with the ports.
4. **OpenVAS:** Finally, this was used to run a scan on the target to identify vulnerabilities and easily view and prioritize them.

Findings

The findings gave a lot of information on both the servers. The findings have been listed below.

- For the Windows Server, we found one open port (53) running the domain service in tcp.
- Similarly, for the Metasploitable, we found almost 23 open ports running tcp services.
- Through the wireshark observations, we could notice that all closed ports had a RST, ACK flag set.
- A netcat command to enable listening ports, could connect to that specific port via the Kali VM to run remote commands, by easily connecting to the shell. This shows that once we get access to the server, one line on the CLI can allow complete remote access.
- Finally, when we run the OpenVAS scan for both the targets, we found a list of vulnerabilities, which if used by an actual attacker could be exploited on each server via the open ports and services.

Recommendations

In the findings, we came across multiple known vulnerabilities and their CVE's with a description of their severities. Here are a few recommendations to overcome these weaknesses:

1. The CVE's should be resolved from order of highest severity, occurrences and priority.
2. Accounts that have been compromised due to brute force or spoofing , should be completely removed, or passwords changed.
3. For servers like MS SQL or Apache, all the recent patches should be made.
4. For encryption methods, the weak ciphers and encryption methods can be completely discontinued, followed by updating and upgrading the current versions.
5. For any kind of backdoor or open disclosure, the open ports running services that are not required shut be completed closed.

Appendix

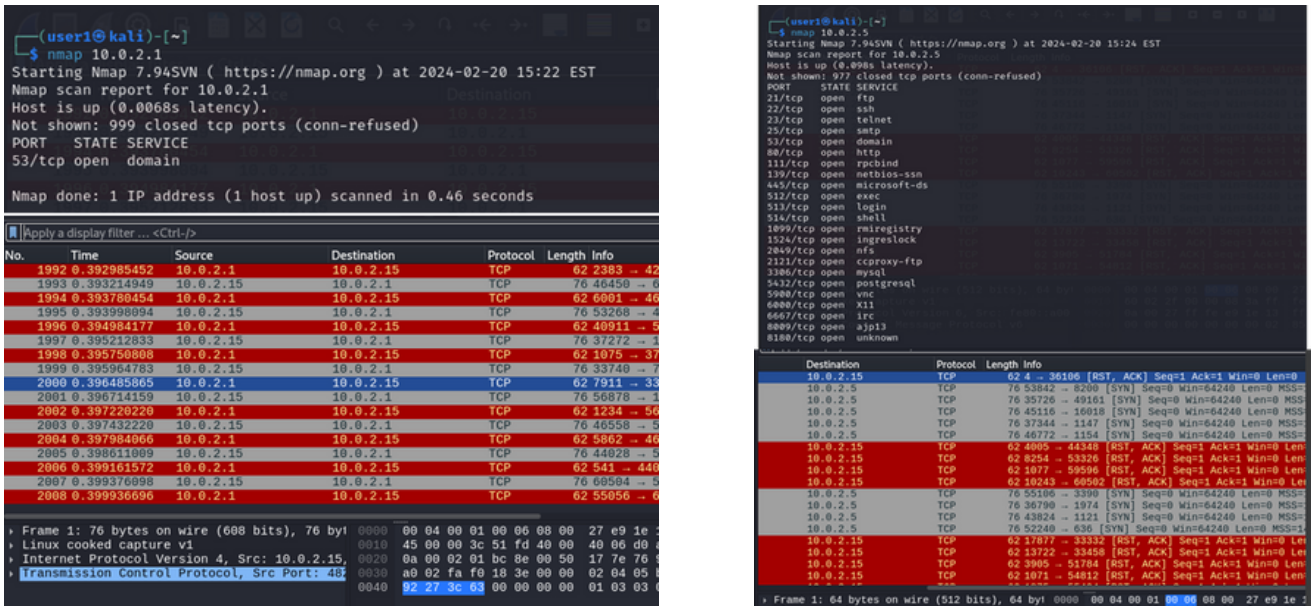

Fig. 1 & Fig. 2: Nmap and Wireshark on both servers

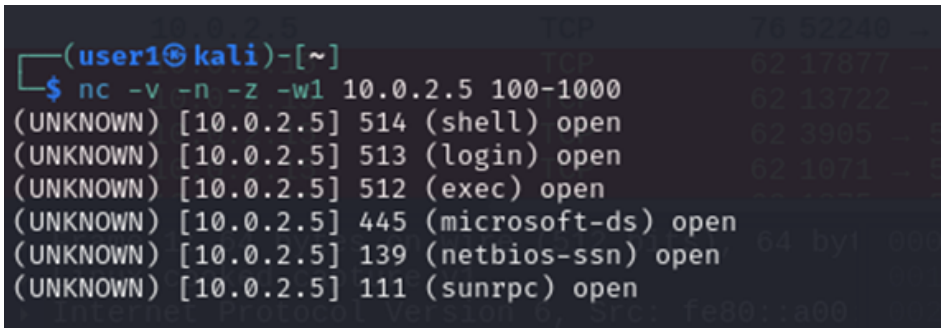

Fig. 3: Netcat scan on metasploit for ports 100-1000

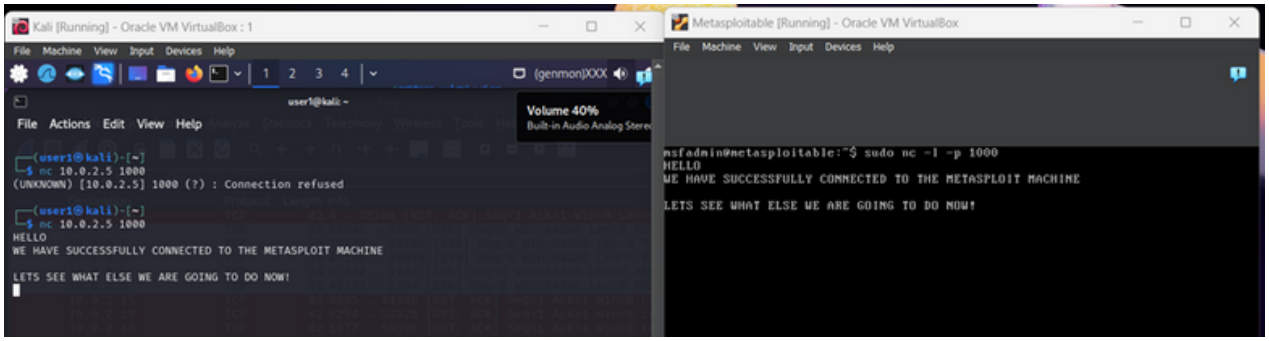

Fig. 4: Netcat connection with metasploit machine for remote shell

Appendix

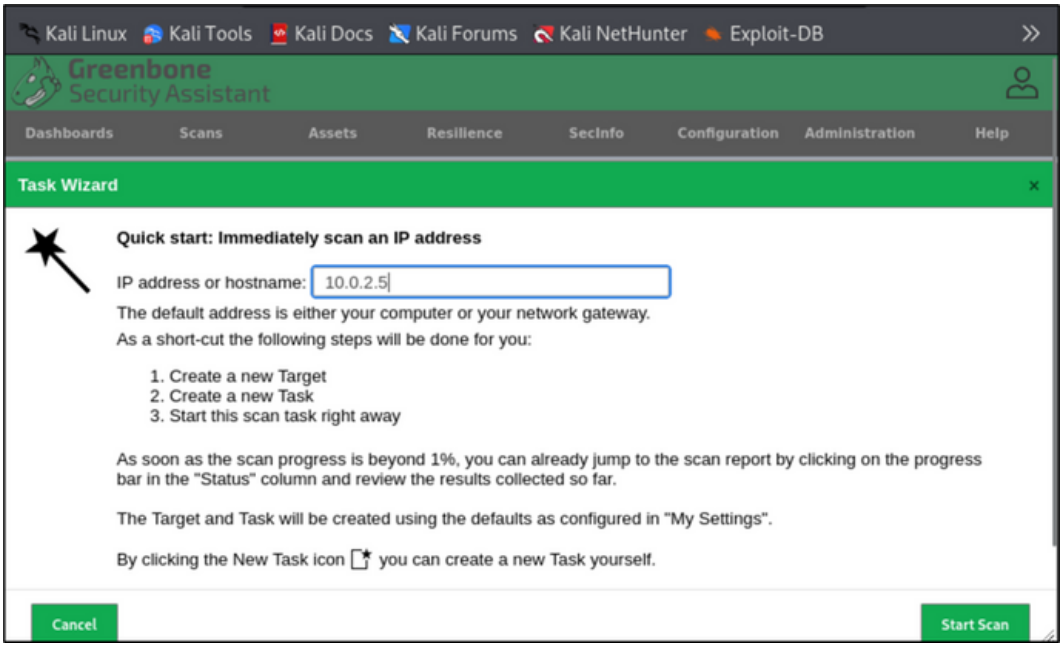

Fig. 5: OpenVAS scan page

Fig. 5: OpenVAS scan for metasploit

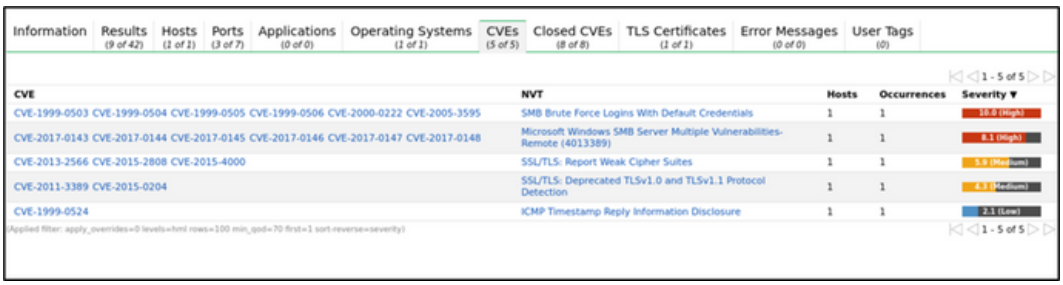

Fig. 5: OpenVAS scan for windows

References

1. https://www.tenable.com/plugins/nessus/61696
2. https://www.tenable.com/blog/cve-2020-1938-ghostcat-apache-tomcat-ajp-file-readinclusion-vulnerability-cnvd-2020-10487#:~:text=Solution,-Patch%20availability
3. https://forum.greenbone.net/t/no-scan-list-no-port-lists-after-build-of-20-08/6360
4. https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_SSL_TLS_Ciphers_Insufficient_Transport_Layer_Protection
5. https://www.upguard.com/blog/weak-ssl