

# PENETRATION TEST REPORT

Active  
Information  
Gathering



Prepared By:  
Gopi Gor

# **Table of Contents**

Executive Summary

Scope and Objectives

Methodology

Findings

Recommendations

Appendix

References

# 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

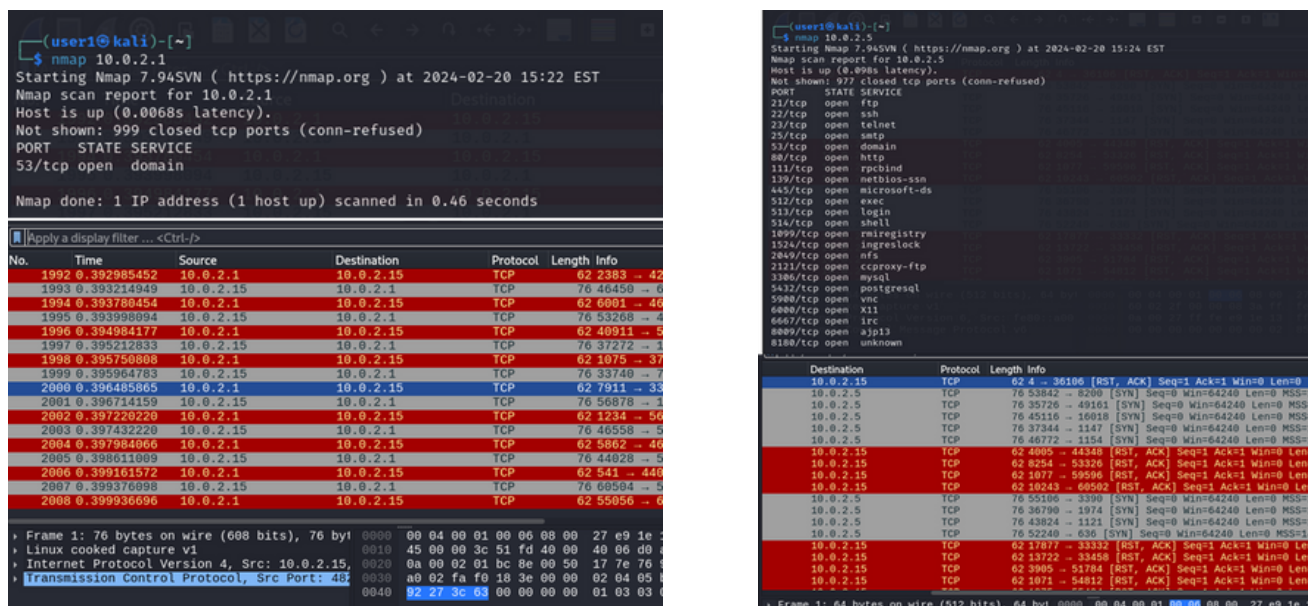


Fig. 1 & Fig. 2: Nmap and Wireshark on both servers

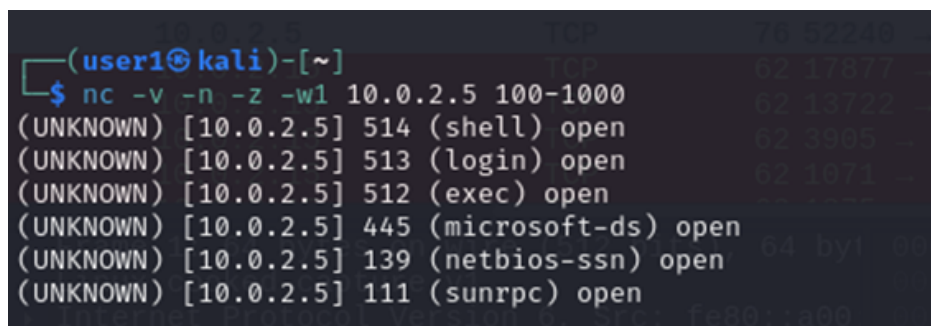


Fig. 3: Netcat scan on metasploit for ports 100-1000

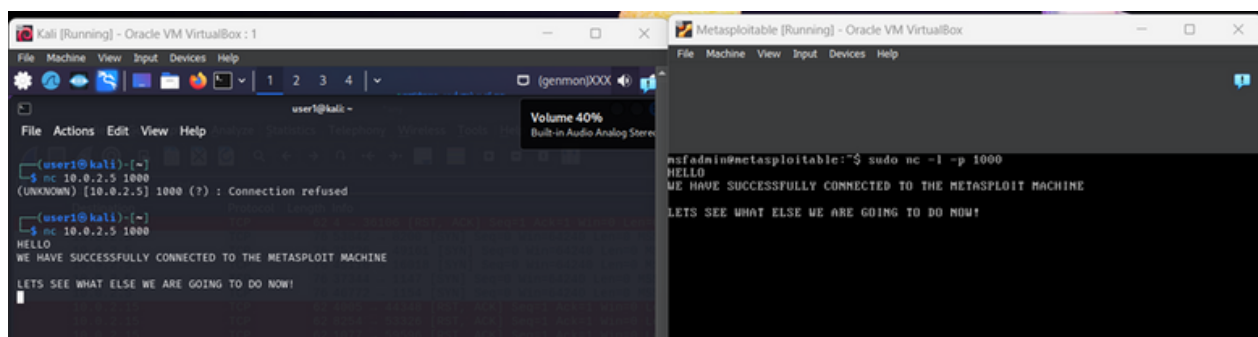


Fig. 4: Netcat connection with metasploit machine for remote shell



# Appendix

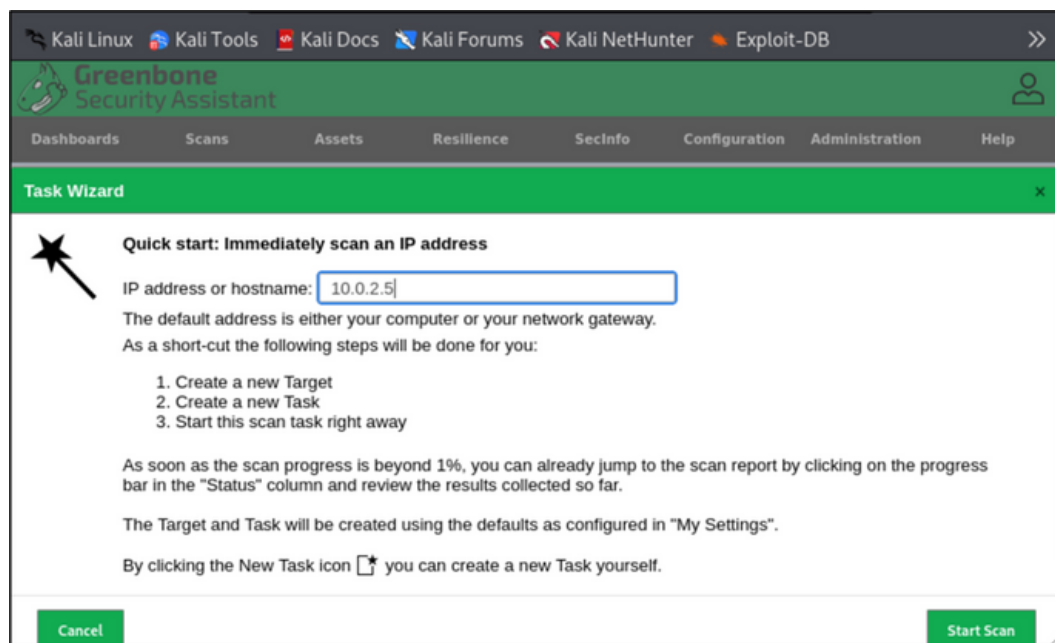


Fig. 5: OpenVAS scan page

CVE-2001-0645 CVE-2004-2357 CVE-2006-3451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4649 CVE-2016-4531 CVE-2018-15719	MySQL / MariaDB Default Credentials (MySQL Protocol)	1	1	9.8 (High)
CVE-2020-1938	Apache Tomcat AP RCE Vulnerability (Ghostcat)	1	1	9.8 (High)
CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability	1	2	9.8 (High)
CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	1	1	9.8 (High)
CVE-2016-7144	UnrealIRCd Authentication Spoofing Vulnerability	1	1	9.8 (High)
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2001-1594 CVE-2013-7404 CVE-2017-8218 CVE-2018-19063 CVE-2018-19064	FTP Brute Force Logins Reporting	1	2	7.8 (Medium)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP-CGI-based setups vulnerability when parsing query string parameters from php...	1	1	7.8 (Medium)

Fig. 5: OpenVAS scan for metasploit

Information	Results (9 of 42)	Hosts (2 of 2)	Ports (3 of 7)	Applications (0 of 0)	Operating Systems (2 of 1)	CVEs (5 of 5)	Closed CVEs (0 of 0)	TLS Certificates (1 of 1)	Error Messages (0 of 0)	User Tags (0)		
											<< 1 - 5 of 5 >>	
CVE	NVT						Hosts	Occurrences	Severity ▼			
CVE-1999-0503 CVE-1999-0504 CVE-1999-0505 CVE-1999-0506 CVE-2000-0222 CVE-2005-3595	SMB Brute Force Logins With Default Credentials						1	1	10.0 (High)			
CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)						1	1	9.8 (High)			
CVE-2013-2566 CVE-2015-2808 CVE-2015-4000	SSL/TLS: Report Weak Cipher Suites						1	1	5.9 (Medium)			
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection						1	1	4.3 (Medium)			
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure						1	1	2.5 (Low)			
Applied filter: apply_overrides=0 levels=html rows=100 min_qpd=70 first=1 sort=reverse=severity)												<< 1 - 5 of 5 >>

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](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>