WILLIAM & MARY
CHARTERED 1693

Computer Science

Applied Cybersecurity

Penetration Test Report

bentremblay38@gmail.com

Table of Contents

1.0 Applied Cybersecurity Penetration Test Report

1.1 Introduction

This penetration testing assessment was conducted as part of a cybersecurity take-home assignment designed to demonstrate practical offensive security skills learned throughout the course. The assessment targeted a Metasploitable virtual machine operating within an isolated lab environment intended for educational testing purposes. Testing activities included reconnaissance, vulnerability scanning, service enumeration, exploitation, and post-exploitation validation. Industry-standard tools such as Nmap, GVM, Metasploit Framework, and Netcat were utilized during the assessment process. The findings and methodologies documented throughout this report reflect both the vulnerabilities identified on the target system and the practical security risks associated with insecure or outdated services.

1.2 Objective

The objective of this assessment was to simulate the workflow and methodology of a real-world penetration test while demonstrating the technical knowledge developed throughout the course. The assessment aimed to identify vulnerable services exposed on the target host, validate publicly known vulnerabilities, and safely demonstrate the potential impact of successful exploitation. Particular focus was placed on demonstrating compromise of the confidentiality and integrity aspects of the CIA triad through unauthorized system access and disclosure of sensitive information. The testing process also emphasized the importance of structured reconnaissance, vulnerability analysis, and post-exploitation verification when conducting a professional security assessment. Ultimately, this project was intended to provide practical experience in both offensive security techniques and the documentation standards commonly used within professional penetration testing engagements. Implementing the recommendations outlined throughout this report would significantly strengthen the overall security posture of the target system by reducing exposure to known vulnerabilities, limiting unauthorized access opportunities, and improving the system's resilience against potential attacks.

2.0 Executive Summary

An internal penetration testing assessment was conducted against the target host 192.168.180.133 within an isolated lab environment using a Metasploitable virtual machine. The purpose of the assessment was to evaluate the security posture of the target system and demonstrate practical penetration testing methodologies through reconnaissance, vulnerability analysis, exploitation, and post-exploitation validation. Multiple industry-standard tools,

including Nmap, Greenbone Vulnerability Manager (GVM), Metasploit Framework, and Netcat, were utilized throughout the assessment process to identify and validate vulnerable services exposed on the target host.

The assessment identified several critical vulnerabilities associated with outdated and intentionally vulnerable services running on the system. Through successful exploitation of multiple remote code execution vulnerabilities, unauthorized access to the target machine was achieved without valid credentials. The testing demonstrated compromise of the confidentiality and integrity aspects of the CIA triad through remote shell access, privilege validation, and unauthorized disclosure of sensitive system information, including protected account and password hash data.

Three vulnerabilities were successfully exploited during testing: the vsftpd 2.3.4 backdoor vulnerability (CVE-2011-2523), the DistCC remote command execution vulnerability (CVE-2004-2687), and the UnrealIRCd backdoor vulnerability (CVE-2010-2075). Exploitation of these vulnerabilities demonstrated the ability of an attacker to gain elevated system access, execute arbitrary commands remotely, and access confidential system information. Additional high-risk vulnerabilities and insecure services were also identified during scanning and are discussed throughout this report.

If vulnerabilities of this nature were present within a production environment, a malicious actor could potentially gain unauthorized administrative access, access sensitive organizational data, establish persistence mechanisms, or pivot further into internal network infrastructure. The presence of outdated services and insecure configurations significantly increases the likelihood and potential impact of system compromise. Implementing the recommendations outlined throughout this report would significantly strengthen the overall security posture of the target system by reducing exposure to known vulnerabilities, limiting unauthorized access opportunities, and improving the system's resilience against potential attacks.

3.0 Scope and Methodology

3.1 Scope

The assessment was conducted against a single target host located at 192.168.180.133 within a controlled virtual lab environment. The target system was a Metasploitable virtual machine intentionally configured with vulnerable and outdated services for penetration testing and security training purposes. Testing activities focused on identifying exposed network services,

analyzing publicly known vulnerabilities, and validating the impact of successful exploitation through controlled penetration testing techniques. Exploitation efforts were performed in a limited and non-destructive manner, with post-exploitation activities focused primarily on demonstrating unauthorized access and disclosure of sensitive information as proof of vulnerability impact. The assessment was limited solely to the assigned target system and the services exposed by that host.

3.2 Methodologies

The assessment followed a structured penetration testing methodology designed to simulate the workflow of a real-world security assessment. Testing began with information gathering and service enumeration using Nmap and Greenbone Vulnerability Manager (GVM) in order to identify open ports, exposed services, software versions, and publicly known vulnerabilities associated with the target system. NSE vulnerability scripts and vulnerability scan results were then analyzed to identify high-risk services potentially susceptible to remote exploitation.

Following vulnerability identification, publicly documented vulnerabilities were validated and selectively exploited using both manual exploitation techniques and the Metasploit Framework. Exploitation activities focused on demonstrating unauthorized access, remote command execution, privilege validation, and disclosure of sensitive system information. Post-exploitation validation was performed using standard Linux system commands to verify privilege levels and confirm access to restricted files. Findings were then assessed based on the severity of the vulnerabilities, the level of access obtained, and the potential impact such vulnerabilities could have if present within a production environment.

4.0 Information Gathering

The initial phase of the assessment focused on information gathering and service enumeration against the target host located at 192.168.180.133. The objective of this phase was to identify exposed network services, determine software versions, and locate publicly known vulnerabilities associated with the discovered services. Enumeration activities were conducted using Nmap and Greenbone Vulnerability Manager (GVM), both of which provided valuable insight into the attack surface presented by the target system.

An Nmap scan was first conducted against all ports on the target host in order to identify active services and determine version information associated with each exposed service. Additional NSE vulnerability scripts were enabled during scanning to assist in identifying known vulnerabilities tied to detected software versions. The scan results revealed multiple outdated and intentionally vulnerable services commonly associated with the Metasploitable platform, including vulnerable FTP, IRC, SMB, database, and remote service configurations.

Following initial enumeration, a full vulnerability scan was conducted using Greenbone Vulnerability Manager (GVM). The scan identified numerous critical and high-risk vulnerabilities, including several remote code execution vulnerabilities associated with outdated services running on the target machine. Vulnerability scan results provided CVE references, severity ratings, affected services, and additional technical information used to guide later exploitation activities. Particular attention was given to services identified as vulnerable to unauthenticated remote command execution or unauthorized system access.

Analysis of the combined Nmap and GVM scan results led to the selection of several vulnerabilities for further validation and exploitation testing. Services identified as running vulnerable versions of vsftpd, DistCC, and UnrealIRCd were selected due to the presence of publicly documented remote exploitation vulnerabilities with a high potential impact. Additional vulnerabilities and insecure services discovered during this phase are discussed later in the report as part of the overall risk assessment

5. Vulnerabilities Exploited

This section documents the vulnerabilities that were successfully exploited during the penetration testing assessment. Each finding includes a description of the vulnerability, how it was identified during the information gathering and vulnerability discovery phase, the exploitation methodology used, the resulting impact on the target system, and recommendations for remediation. Successful exploitation of these vulnerabilities

demonstrated compromise of the confidentiality and integrity aspects of the CIA triad through unauthorized remote access and disclosure of sensitive system information. Screenshots and evidence collected throughout the assessment have been referenced within each subsection to support the findings and validate successful exploitation.

5.1 vsftpd 2.3.4 Backdoor Vulnerability (CVE-2011-2523)

The FTP service running on the target system was identified as vsftpd version 2.3.4. This version is known to contain a malicious backdoor vulnerability tracked as CVE-2011-2523. The vulnerability allows an attacker to trigger a hidden shell listener through a specially crafted username during FTP authentication, ultimately resulting in unauthenticated remote root access to the affected system.

Initial reconnaissance and vulnerability scanning identified that the target host exposed an FTP service running vsftpd 2.3.4. The vulnerability was detected through both GVM vulnerability scanning and Nmap NSE vulnerability scripts.

Critical (CVSS: 9.8)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability - Active Check
Summary vsftpd is prone to a backdoor vulnerability.
Quality of Detection (QoD): 99%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution:
Solution type: VendorFix
The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.

Affected Software/OS
vsftpd 2.3.4 source packages downloaded between 20110630 and 20110703 are affected.

Vulnerability Insight
The tainted source package contains a backdoor which opens a shell on port 6200/tcp.

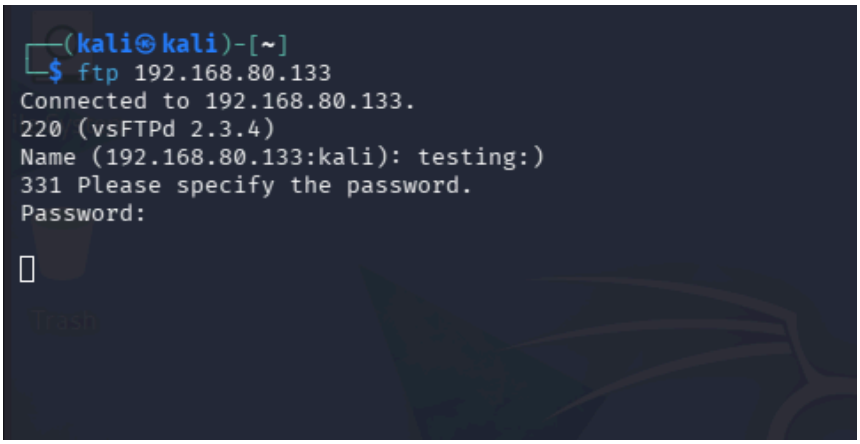
Vulnerability Detection Method
Details: vsftpd Compromised Source Packages Backdoor Vulnerability - Active Check
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: 2026-02-18T05:57:21Z

References
cve: CVE-2011-2523
url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backd
↪oored.html
url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bi
↪d/48539/

Exploitation Process:

To manually exploit the vulnerability without relying on Metasploit, an FTP connection was established to the target host. During authentication, a username containing the string ':) ' was supplied, triggering the hidden backdoor functionality within the vulnerable service. Once triggered, the service opened a shell listener on TCP port 6200.

A Netcat connection was then established to the newly opened listener, successfully providing remote root shell access to the target system.

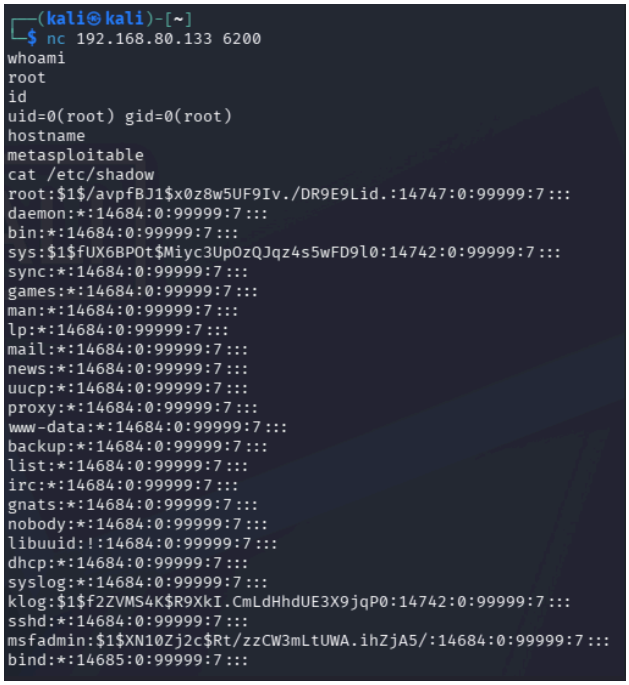


Post-Exploitation Process:

A Netcat connection was then established to the newly opened listener, successfully providing remote root shell access to the target system.

Following successful exploitation, commands such as whoami and id were executed to verify that root-level access had been obtained. To demonstrate unauthorized disclosure of sensitive information, the /etc/shadow file was accessed. This file contains protected password hash information that should only be accessible by privileged users.

Access to this file demonstrated successful compromise of system confidentiality and integrity through unauthorized disclosure of credential-related information.



Impact:

Successful exploitation of this vulnerability allows unauthenticated attackers to obtain remote root access to the affected system. An attacker could leverage this level of access to steal sensitive information, modify system configurations, establish persistence mechanisms, or pivot further into the internal network environment.

Recommended Actions:

The vulnerable vsftpd 2.3.4 service should be immediately removed or upgraded to a secure and supported version that is not affected by the backdoor vulnerability. FTP services should not be publicly exposed unless absolutely necessary, and any required file transfer functionality should instead utilize secure alternatives such as SFTP or SCP. Firewall rules should be implemented to restrict unauthorized access to file transfer services, and systems should be regularly patched to ensure outdated software versions are not present within the environment. Additionally, organizations should implement continuous vulnerability scanning and service auditing procedures to identify unsupported or maliciously modified software before exploitation occurs.

5.2 DistCC Remote Code Execution (CVE-2004-2687)

Severity: critical

The target system was identified as running a vulnerable DistCC service susceptible to remote command execution vulnerabilities tracked under CVE-2004-2687. DistCC is a distributed compilation service that, when improperly exposed, may allow remote attackers to execute arbitrary commands on the target host without authorization.

The DistCC vulnerability was identified during vulnerability scanning performed with GVM. Scan results indicated that the DistCC service was exposed and vulnerable to remote command execution attacks.

Critical (CVSS: 9.3)

NVT: DistCC RCE Vulnerability (CVE-2004-2687)

Summary
DistCC is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
It was possible to execute the "id" command.
Result: uid=1(daemon) gid=1(daemon)

Impact
DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

Solution:
Solution type: VendorFix
Vendor updates are available. Please see the references for more information.
For more information about DistCC's security see the references.

Vulnerability Insight
DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

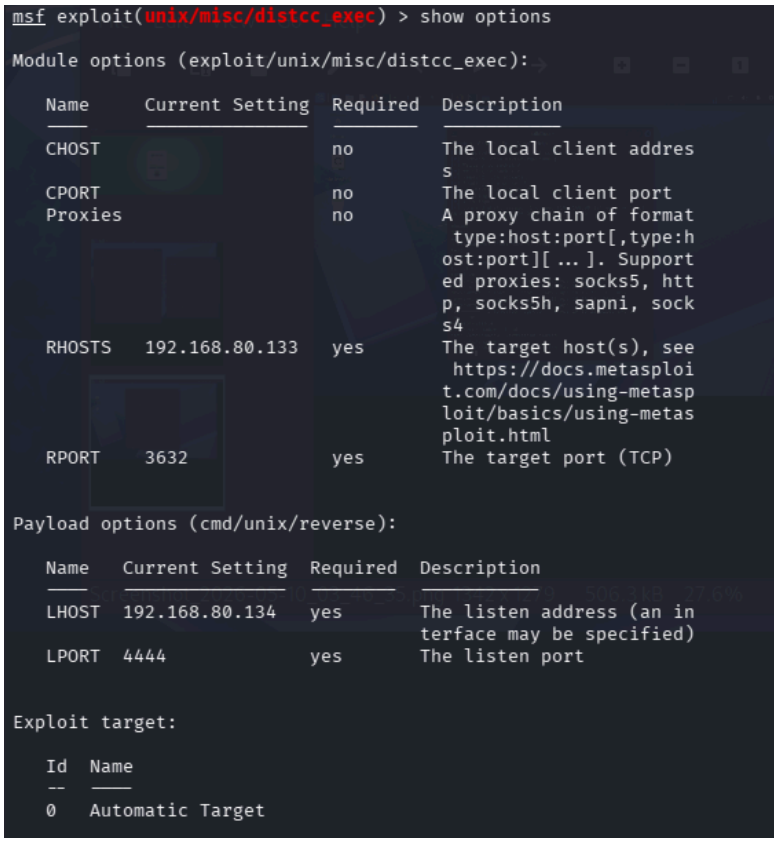
Vulnerability Detection Method
Details: DistCC RCE Vulnerability (CVE-2004-2687)
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: 2022-07-07T10:16:06Z

References
cve: CVE-2004-2687
url: https://distcc.github.io/security.html
url: https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80
↪/archives/bugtraq/2005-03/0183.html
dfn-cert: DFN-CERT-2019-0381

Exploitation Process:
The vulnerability was exploited using Metasploit Framework.

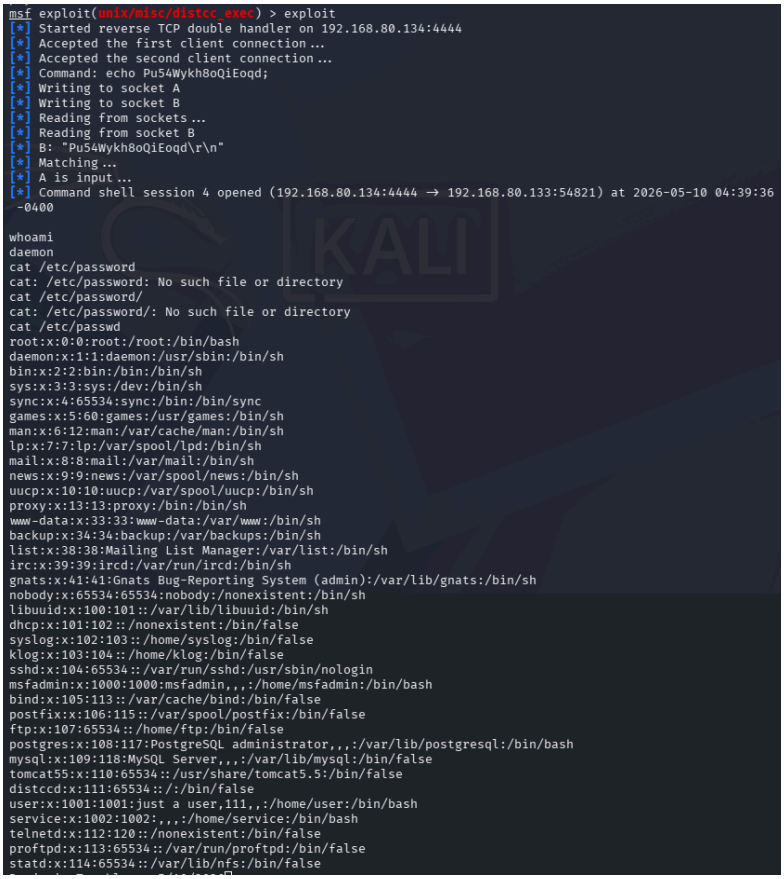
Metasploit Framework module: exploit/unix/misc/distcc_exe
Payload utilized: cmd/unix/reverse

After configuring the required target and payload options within Metasploit, the exploit was executed successfully, resulting in unauthorized remote command execution access on the target system.



Post-Exploitation Process:

To demonstrate unauthorized access to local system information, the /etc/passwd file was accessed following successful exploitation. This confirmed the ability to retrieve local account information from the compromised host without authorization.



Impact:

An attacker successfully exploiting this vulnerability could remotely execute arbitrary commands against the affected system. This may allow attackers to enumerate local users, deploy malicious software, escalate privileges, or move laterally throughout an internal network environment.

Recommended Actions:

The DistCC service should be disabled entirely if distributed compilation functionality is not operationally required. If the service must remain enabled, access should be strictly restricted to trusted internal hosts through firewall rules and network segmentation controls. The affected software should be updated to a secure and supported version that is not vulnerable to remote command execution attacks. Organizations should also implement least-privilege principles to limit the potential impact of service compromise and continuously monitor exposed services for unauthorized access attempts or suspicious activity.

5.3 UnrealIRCd Backdoor Exploitation (CVE-2010-2075)

Severity: critical

The target system was identified as running a vulnerable version of UnrealIRCd containing a malicious backdoor vulnerability tracked as CVE-2010-2075. The vulnerability originated from a compromised software distribution and allows remote attackers to execute arbitrary commands on the target system. The UnrealIRCd vulnerability was identified through GVM vulnerability scanning during the reconnaissance and vulnerability analysis phase of the assessment.

High (CVSS: 7.5)

NVT: UnrealIRCd Backdoor

Product detection result
cpe:/a:unrealircd:unrealircd:3.2.8.1
Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)

Summary
Detection of backdoor in UnrealIRCd.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:
Solution type: VendorFix
Install latest version of unrealircd and check signatures of software you're installing.

Affected Software/OS
The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.

Vulnerability Insight
Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.

Vulnerability Detection Method
Details: UnrealIRCd Backdoor
OID:1.3.6.1.4.1.25623.1.0.80111
Version used: 2025-03-21T05:38:29Z

Product Detection Result
Product: cpe:/a:unrealircd:unrealircd:3.2.8.1
Method: UnrealIRCd Detection
OID: 1.3.6.1.4.1.25623.1.0.809884)

References
cve: CVE-2010-2075
url: http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt
url: http://seclists.org/fulldisclosure/2010/Jun/277
url: http://www.securityfocus.com/bid/40820

Exploitation Process

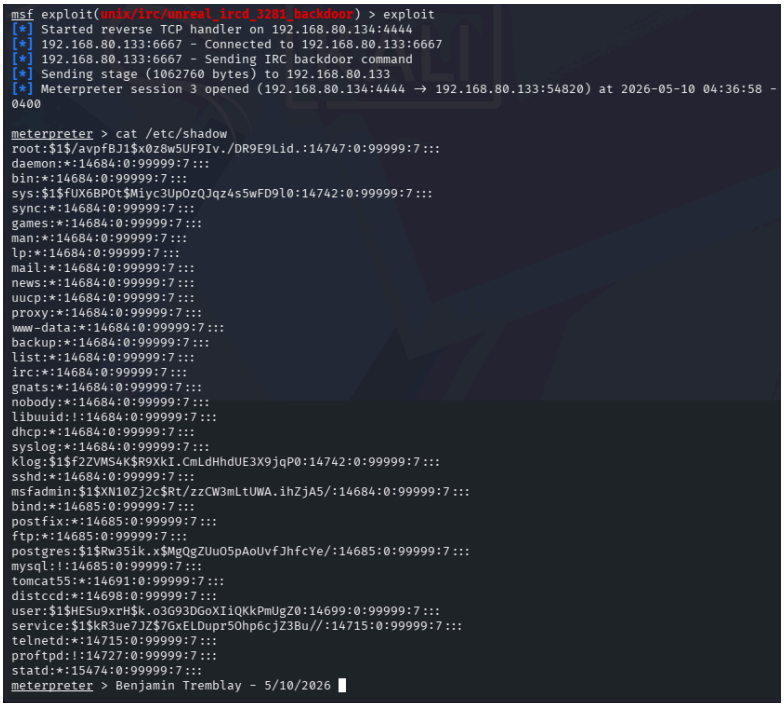
The vulnerability was exploited using the Metasploit Framework

Module: exploit/unix/irc/unreal_ircd_3281_backdoor
Payload: cmd/linux/http/x86/meterpreter/reverse_tcp

After configuring the appropriate exploit options within Metasploit, the exploit was executed successfully and established a Meterpreter session with the target system.

Post-Exploitation Process:

Following successful exploitation, sensitive system information was accessed through the /etc/shadow file in order to demonstrate unauthorized disclosure of credential-related data.



Impact:

Successful exploitation of this vulnerability could allow attackers to remotely execute commands, install persistence mechanisms, compromise sensitive data, and obtain long-term unauthorized access to affected systems.

Recommended Actions:

The compromised UnrealIRCd installation should be immediately removed and replaced with a secure and verified version obtained directly from trusted sources. Any systems running unsupported or legacy IRC services should be reviewed to determine whether the service is still operationally necessary, and unnecessary services should be permanently disabled. External exposure of IRC-related services should be restricted through firewall and access control policies to reduce attack surface exposure. Additionally, organizations should implement software integrity verification procedures, patch management policies, and regular vulnerability assessments to ensure maliciously modified or outdated software is not deployed within production environments.

6.0 Additional Identified Vulnerabilities

In addition to the vulnerabilities successfully exploited during the penetration testing assessment, multiple additional security weaknesses were identified throughout the target environment during reconnaissance and vulnerability scanning activities. While these

vulnerabilities were not directly exploited as part of this assessment, many of them could still provide attackers with unauthorized access, remote code execution capabilities, credential compromise opportunities, or avenues for lateral movement within a network environment. The vulnerabilities below have been organized from highest to lowest assessed risk based on a combination of exploitability, likelihood of abuse, potential business impact, and the severity of consequences that could result from successful exploitation. Particular emphasis was placed on vulnerabilities capable of resulting in remote code execution, authentication bypass, credential disclosure, or full system compromise.

Active Listener on Port 1524

Severity: Critical

Details:

An active listener was identified on TCP port 1524, commonly associated with intentionally backdoored or unauthorized services. Attackers may leverage the listener to obtain unauthorized shell access to the system.

Recommended Actions:

Disable the service immediately, identify the associated process, and investigate the system for indicators of compromise.

vsftpd 2.3.4 Backdoor (CVE-2011-2523)

Severity: Critical

Details:

The FTP service was identified as running a backdoored version of vsftpd vulnerable to unauthenticated remote root access. Successful exploitation provides attackers with immediate root-level control of the affected system without valid credentials.

Recommended Actions:

Remove the vulnerable vsftpd installation immediately and replace it with a secure and supported alternative.

UnrealIRCd Backdoor (CVE-2010-2075)

Severity: Critical

Details:

The installed UnrealIRCd service contained a malicious backdoor vulnerability permitting arbitrary remote command execution. Successful exploitation could allow attackers to gain unauthorized access, install persistence mechanisms, or fully compromise the affected host.

Recommended Actions:

Remove the compromised UnrealIRCd installation immediately and replace it with a verified secure version.

Samba Username Map Script Vulnerability

Severity: Critical

Details:

The Samba service was identified as vulnerable to the Username Map Script remote command execution vulnerability. Successful exploitation could allow unauthenticated attackers to execute arbitrary commands remotely and fully compromise the affected system.

Recommended Actions:

Update Samba immediately, disable vulnerable script functionality, and restrict SMB exposure to trusted hosts only.

DistCC Remote Code Execution (CVE-2004-2687)

Severity: Critical

Details:

The DistCC service was identified as vulnerable to unauthenticated remote command execution attacks capable of allowing attackers to execute arbitrary commands and potentially fully compromise the affected system.

Recommended Actions:

Disable DistCC entirely unless operationally required and restrict service exposure through firewall controls.

Ingreslock Backdoor

Severity: Critical

Details:

The target system was identified as containing the Ingreslock backdoor service. Backdoor services may provide attackers with unauthorized access while bypassing normal authentication controls.

Recommended Actions:

Remove the backdoor service immediately and investigate the system for additional unauthorized modifications or compromise indicators.

Apache Tomcat AJP Remote Code Execution (Ghostcat)

Severity: Critical

Details:

The Apache Tomcat AJP service was identified as vulnerable to the Ghostcat vulnerability. Successful exploitation may allow attackers to read sensitive files or execute arbitrary code remotely through the AJP connector.

Recommended Actions:

Disable unused AJP connectors, restrict network exposure, and apply vendor security patches immediately.

Distributed Ruby Remote Code Execution Vulnerabilities

Severity: Critical

Details:

The Distributed Ruby service was identified as vulnerable to remote code execution attacks capable of allowing attackers to execute arbitrary commands remotely and potentially fully compromise the system.

Recommended Actions:

Disable Distributed Ruby services if unnecessary and update vulnerable Ruby components immediately.

Java RMI Server Insecure Default Configuration

Severity: High

Details:

The Java RMI service was identified as operating with insecure default configurations vulnerable to remote code execution attacks. Attackers may remotely execute arbitrary Java code on the target system.

Recommended Actions:

Restrict RMI exposure, disable unnecessary RMI services, and apply secure configuration controls.

PostgreSQL Vulnerability

Severity: Critical

Details:

The PostgreSQL service was identified as vulnerable to insecure configurations or potential privilege abuse conditions. Attackers may gain unauthorized database access, escalate privileges, or execute commands against the underlying system.

Recommended Actions:

Secure PostgreSQL configurations, restrict external exposure, and enforce strong authentication controls immediately.

MySQL / MariaDB Default Credentials

Severity: High

Details:

The database service appeared vulnerable to authentication using default or weak credentials. Successful access could expose sensitive application or system data stored within the database environment.

Recommended Actions:

Remove default credentials immediately and enforce strong password policies for all database accounts.

Rlogin Passwordless Login

Severity: High

Details:

The target system appeared to permit passwordless authentication through insecure Rlogin trust relationships. This may allow attackers to obtain unauthorized remote access without valid credentials.

Recommended Actions:

Disable passwordless trust relationships and remove legacy Rlogin services entirely.

FTP Brute Force Login / Default Credentials

Severity: High

Details:

The FTP service appeared vulnerable to brute-force authentication attacks or the use of default credentials. Weak authentication controls could allow attackers to gain unauthorized access to file transfer services and sensitive data.

Recommended Actions:

Disable anonymous FTP access, remove default credentials, enforce strong password policies, and implement account lockout protections.

VNC Brute Force Login

Severity: High

Details:

The VNC service was identified as potentially vulnerable to brute-force login attempts. Successful compromise of VNC credentials may provide attackers with remote graphical access to the affected system.

Recommended Actions:

Restrict VNC access to trusted hosts, enforce strong passwords, and disable the service entirely if unnecessary.

TWiki 4.2.4 Multiple Vulnerabilities

Severity: High

Details:

The installed TWiki application was identified as vulnerable to multiple cross-site scripting and command execution vulnerabilities. Successful exploitation may allow attackers to execute arbitrary commands or compromise application users.

Recommended Actions:

Upgrade TWiki to a supported and patched version or remove the application entirely if unnecessary.

PHP 5.3.13 / 5.4.x Multiple Vulnerabilities

Severity: High

Details:

The target system was identified as running outdated PHP versions containing multiple publicly known vulnerabilities. Vulnerable PHP environments may allow attackers to compromise web applications or execute arbitrary code.

Recommended Actions:

Upgrade PHP to a currently supported version receiving active security updates.

EasyPHP Webserver < 12.1 Multiple Vulnerabilities

Severity: High

Details:

The EasyPHP web server installation was identified as vulnerable to multiple publicly known security issues. Attackers may exploit vulnerable components to compromise hosted applications or gain unauthorized access to the system.

Recommended Actions:

Upgrade EasyPHP to a supported version or replace unsupported web server software entirely.

SSL/TLS OpenSSL CCS Injection Vulnerability

Severity: High

Details:

The target system was identified as vulnerable to the OpenSSL CCS Injection vulnerability affecting SSL/TLS communications. Successful exploitation could allow attackers performing man-in-the-middle attacks to weaken encryption protections or intercept sensitive communications.

Recommended Actions:

Update OpenSSL to a patched version and disable vulnerable SSL/TLS configurations.

Operating System End-of-Life Detection

Severity: Medium

Details:

The target operating system was identified as unsupported or end-of-life software no longer receiving security updates. Unsupported operating systems remain vulnerable to publicly known exploits and lack vendor patch support.

Recommended Actions:

Upgrade the affected operating system to a currently supported and actively maintained version.

Test HTTP Dangerous Methods Enabled

Severity: Medium

Details:

The web server was identified as permitting dangerous HTTP methods such as PUT, DELETE, or TRACE. Improperly secured HTTP methods may allow attackers to upload malicious content, alter server files, or perform web-based attacks against hosted applications.

Recommended Actions:

Disable unnecessary HTTP methods and configure the web server to permit only required request types.

Rlogin Service Running

Severity: Medium

Details:

The target system was identified as running the Rlogin service, an insecure legacy remote access protocol lacking encryption protections. Use of Rlogin may allow attackers to intercept authentication traffic or abuse trust relationships for unauthorized access.

Recommended Actions:

Disable the Rlogin service and replace it with encrypted remote access protocols such as SSH.

Rexec Service Running

Severity: Medium

Details:

The Rexec service was identified as enabled on the target system. Rexec is an outdated remote execution protocol that transmits authentication credentials in plaintext and does not provide secure communications. Attackers capable of intercepting network traffic may obtain credentials or remotely execute commands against the affected system.

Recommended Actions:

Disable the Rexec service entirely and replace legacy remote administration protocols with secure alternatives such as SSH.

7.0 Recommendations

The assessment identified multiple critical vulnerabilities associated with outdated services, insecure configurations, exposed backdoors, and legacy remote access protocols. Immediate remediation efforts should prioritize vulnerabilities capable of providing unauthenticated remote access or remote code execution, including the active listener on port 1524, the vsftpd backdoor vulnerability, UnrealIRCd backdoor services, Samba remote command execution vulnerabilities, and DistCC remote code execution exposure. Unsupported and end-of-life software should be upgraded or removed entirely to reduce exposure to publicly known exploits, while unnecessary services such as Rlogin, Rexec, insecure FTP configurations, and exposed remote administration services should be disabled. Organizations should also implement centralized patch management procedures, continuous vulnerability scanning, network segmentation, least-privilege access controls, and firewall restrictions to limit attack surface exposure and reduce opportunities for lateral movement throughout the environment. Implementing the recommendations outlined throughout this report would significantly strengthen the overall security posture of the target system by reducing exposure to known vulnerabilities, limiting unauthorized access opportunities, and improving resilience against future attacks.

8.0 Conclusion

This penetration testing assessment successfully demonstrated the presence and impact of multiple critical vulnerabilities affecting the target system. Through reconnaissance, vulnerability analysis, exploitation, and post-exploitation validation activities, unauthorized access to sensitive system information was obtained and compromise of the confidentiality and integrity aspects of the CIA triad was demonstrated. The assessment highlighted the severe risks associated with outdated software, insecure configurations, exposed backdoors, and unsupported legacy services. Several vulnerabilities identified during testing were capable of providing attackers with remote code execution, unauthorized administrative access, or disclosure of sensitive credential-related information. Overall, the findings of this assessment emphasize the importance of proper patch management, secure system configuration, service hardening, and continuous security monitoring in maintaining a secure operating environment.