J103563

by ABDELRAHMAN ABDELWAHAB

Submission date: 06-Apr-2023 02:57PM (UTC+0100)
Submission ID: 201635226
File name: J103563_948676_359176442.docx (8.28M)
Word count: 5162
Character count: 27557

Assignment One

Penetration testing report requested by Chester Business Ltd (CBL)

Table of Contents

Section (1) Executive Summary

1. Background:

The purpose of the tests done in the executive report was to measure and outline possible vulnerabilities and exploitation, besides evaluating the risk profile of the company. The following table will be used as a way of defining the technical terms that are going to be used in the subsequent parts of the executive summary.

Terminology	Definition
HTTP vs HTTPS	The way of transferring data across the web, the difference between them is that HTTPS is encrypted and secured so if the protocol was intercepted by hackers the data will not be revealed (Chai et al., 2021)
SSH	A service allowing for remote connection with the devices of the company.
The target IP address	The company IP address is 10.0.2.15
The host IP address	The machine, which was used to exploit the company system, its IP address is 10.0.2.4
Physical vulnerability	**Tail gating**: can occur when someone without authority can get physically into a restricted area and obtain sensitive data (McAfee, 2022).
	Piggy backing: when an intruder is moving closely without being noticed behind an authorized employee into a restricted area, or the intruder can disguise as a mail clerk (McAfee, 2022).
	Key loggers: they can be either a hardware or a software intended to monitor what is being typed in the computer and send these data remotely to the hacker, for instance, it can be a USB device (V, 2021)
Exploitation	Techniques of compromising systems through the identified vulnerabilities (Engebretson , 2013).
Dictionary attack	It is a file which is composed of commonly used passwords which are used by automated tools to attempt login into a particular target (Engebretson , 2013).
Brute force attack	It is a technique used by automated tools to produce all the probable combined forms of letter in alphabetical order until it reaches the correct password (Engebretson , 2013)
Root privilege	It means giving the user an administrative authority over the system to be able to modify and compromise the system in the desired way (Spacey, 2018).
Directory listing	It is a kind of vulnerabilities when private directories or files in the website are publicly accessible as it usually contain sensitive data (Viimeksi, 2021)
Public and private keys	They are pair of credentials which cannot be used to login unless both are obtained by the user, for instance one key decipher the other key (Jackson, 2022).
Social engineering attack	A method of cyberattacks which relies on human psychology by their curiosity against security protocols, for instance, opening an email or using unidentified USB drives "Baiting" (Rosencrane et al., 2021).

Table 1. *Technical terminologies definitions.*

Some of the terms here are not relevant for the Executives. Definitions should only focus on the terms used in the executive summary

2. Overall posture:

In the exploitation phase four tools were used and they have achieved their purpose except one tool and the intent of using it was to obtain Peter and Debian passwords, for instance, the dictionary attacks did not work which mean the passwords are strong to some extent, however if the tool is given enough time it can brute force and obtain the password and this could take days or even months. The reasons why the tests were successful are the SSH open port, using easy passwords by Mr. James on the webpage and the SSH service, besides being able to gain root privilege remotely.

You should also include an explanation of the ranking

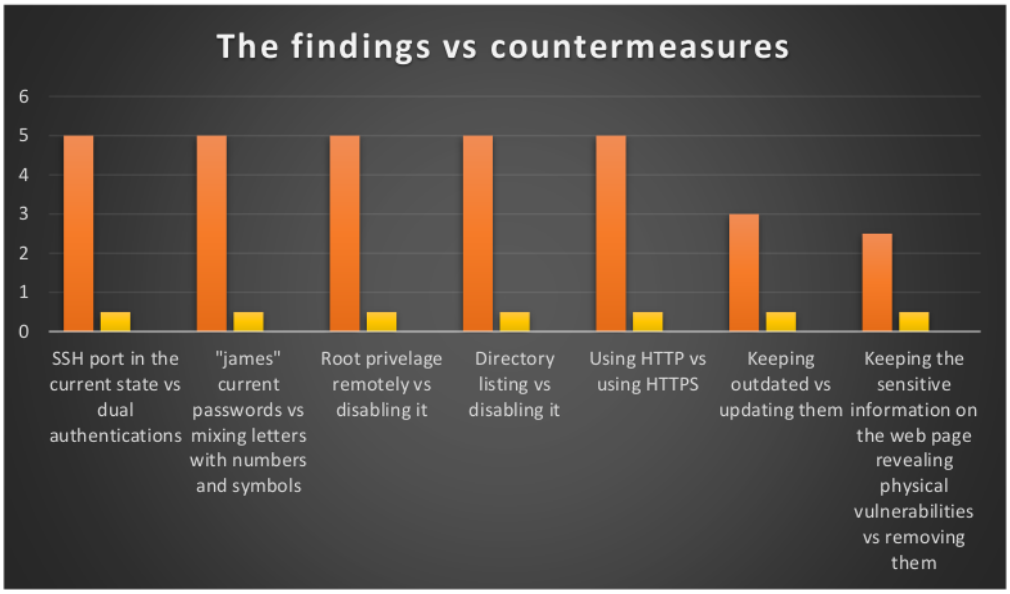
3. Risk profile:

The risk profile can be defined as high, since the credentials of the head of IT Mr. James were obtained both on the WordPress login page and on the SSH, besides being able to upload a payload and infiltrate the communications, critical here extend from obtaining Mr. James credentials to obtaining all the data of the customers since the company database is

centralized in Chester. Hence, moderate risk could have been selected if the issue was only about vulnerable outdated services which were discovered in the report as well. Low could have been the case if the remaining issues are only about social engineering possible threats which will be explained in the following subsections since the employees can be educated to deal with it.

4. General findings:

Label The following bar chart represents the main possible risks in red color vs its countermeasures in yellow in an interval between 0 – 5 where 5 is the highest risk and 0 is the lowest, in security there is nothing impossible so an absolute zero was not taken into consideration. Vague



Bar chart. *Representing the findings vs countermeasures.*

5. Recommendation summary:

It can be reiterated that after finding these vulnerabilities and exploiting some of them, it could be advisable to follow the recently published criteria mentioned by (Miller, 2022). Thus, it suggests using public and private keys for accessing SSH service because to some extent they can be resistant to brute force attacks, disabling the remote root privilege and using dial authentication ways of login.

Additionally, it is also advisable to adjust the WordPress login page to take a limited number of wrong credentials entries then it sends an alert to the IT team, besides using HTTPS protocol to encrypt and secure the data. It is worth mentioning that while the main web page of the target was introducing the services the company provides, it revealed two dangerous pieces of information.

The first one is that they let out their conference room to external organizations meetings, and this could lead to tail gating, piggy backing, or key loggers since meetings of different external companies and the company assets itself run on the same network. In addition, intruders may unplug anything and cause denial of service. The second one is that the web page mentions that they do not have an offsite backup center and their assets are in their facility in Chester, and it is advised to do decentralization of data. *Good*

Likewise, the About page has revealed that the company allows employees to bring their own devices and connect it to the company network, besides allowing analysts to use external storage devices to store and transfer data which could be

taken as an advantage by attackers to use keyloggers. Moreover, revealing the operating system's versions, and the services running for example SSH. However, the most serious piece of information mentioned was that they do not perform security checks on individuals before attending their meetings and the justification is that they are wearing ID, which could be easily replicated or stolen.

6. Strategic roadmap

The short-term plan advisable would be to change Mr. James credentials into strong passwords composed of letters, numbers, and symbols, besides disabling the remote root privilege settings. In addition to applying SSH dual authentications login. On the other hand, the long-term plan would involve using HTTPS protocol, educating the employees including the security staff about social engineering attacks and perform checks in every gap between the meetings to check if there is any key logger connected to a desktop computer. Moreover, establishing a backup database, by other means it is recommended to work on decentralization of the company data.

Section (2) Technical report

1. Engagement:

The engagement phase is crucial as it will emphasize first on details about the company, for example its history, target customers, speciality, and the operation headquarters (Khawaja, 2018). In addition, it involves discussions with the company to decide what are the desired outcomes of the test, and what triggered them to decide to do it in the first place. For instance, are they using legacy devices which are prone to attacks? (Weidman, 2014).

Additionally, it should emphasize on how far the testing shall go and what is allowed and what is limited, for example the specific IP address or ports allowed to be tested. Moreover, the nature of the testing whether it is just vulnerability scan or it can extend to exploitation which can affect the status of the service; the amount of time on which their services might go down during the scanning process should be also taken into consideration because it might lead to financial loss (Weidman, 2014).

In illustration, a signed consent for performing these tests is essential because it makes the process legal and authorised and it should involve third parties as well in case the company is not the primary owner of the service (Weidman, 2014). Nevertheless, communication ways of reaching out the company to inform them of severe vulnerabilities should be agreed upon, besides ensuring the confidentiality of any data (Weidman, 2014). According to Khawaja (2018), hiring an advocate could be one of the secure measures to take during this stage to ensure that the upcoming stages and the signed contract are legal.

You have correctly identified engagement considerations. However, you should go beyond what should be considered and provide specifics

2. Information gathering:

2.1 Light weight scanning

According to (Engebretson , 2013), information gathering is concerned with collecting publicly available information and by getting more information about the target, the next steps will be easier to accomplish. The phase began by connecting the host and the target on one NAT network of IP address 10.0.2.0, where the target IP address is 10.0.2.15 and the penetration tester machine is 10.0.2.4. Accordingly, Nmap light weight scanning was done to identify the target IP address and the open ports that were revealed are port 22 serving as SSH protocol, and port 80 which serve as HTTP protocol. What can be iterated is that the target is a web server, and this information is shown in Figure 1.

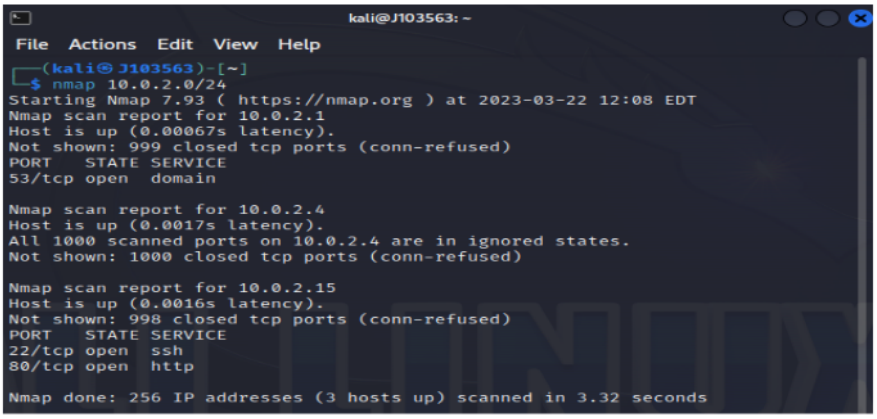


Figure 1. *Nmap light weight scanning.*

Similarly, Nmap SYN scan was made to double check the target IP address using MAC address, besides confirming the open ports, as mentioned by Weidman (2014), Nmap will wait for the synchronization acknowledgement if a particular port is open, and this was explained in Figure 2.

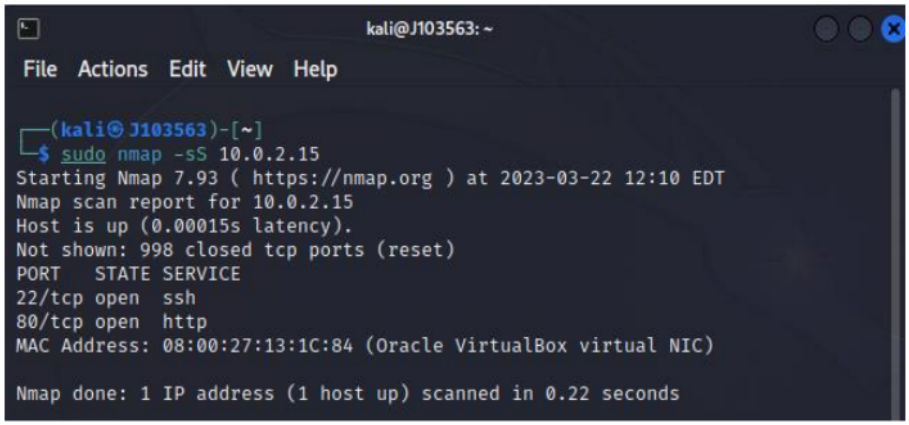


Figure 2. *Nmap SYN scan*

To ensure that the target is reachable and communicating, a ping command was launched as shown in Figure 3, and this is used according to Muniz et al. (2013), to ensure that the target is alive, and there were responses meaning that the target is responding and the ICMP request is not restricted.

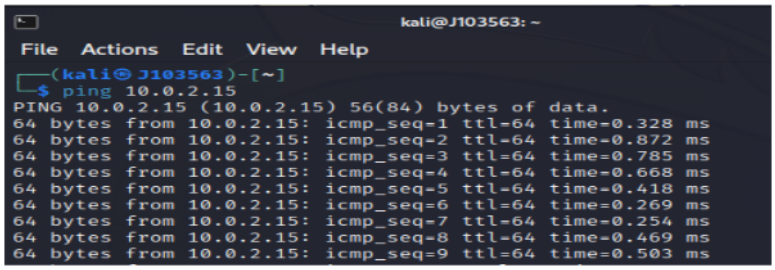
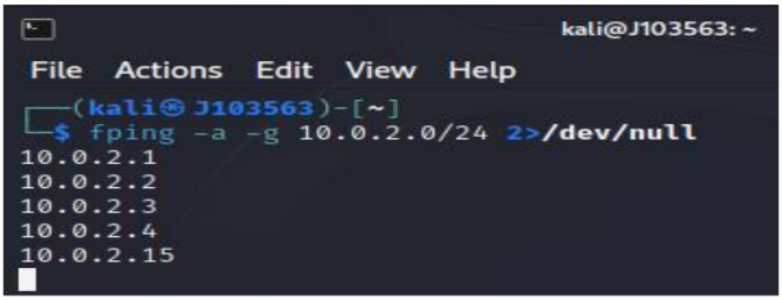


Figure 3. *Ensuring the target is reachable.*

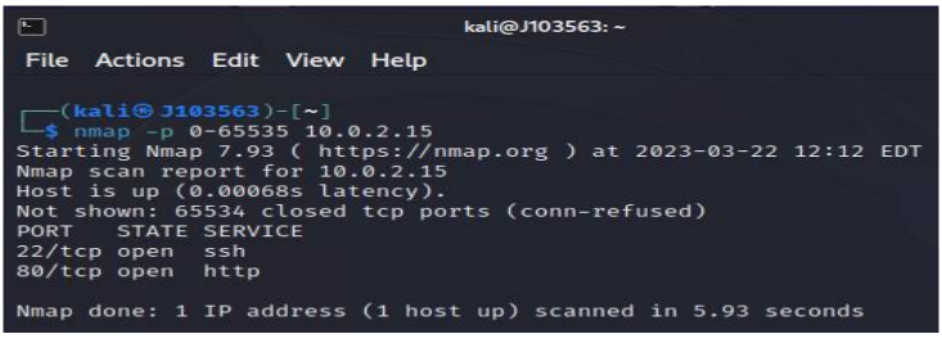
Afterwards, fping command was used as it is capable of pinging only the reachable IP addresses in the network by using the -a option (Muniz et al., 2013). It was done to collaborate with the previous findings as shown in Figure 4.



This is unnecessary since you have already identified the target IP address

Figure 4. *Collaborating ping command findings*

However, after ensuring that the target is communicating, another Nmap command was made to check the rest of the possible open ports because by default Nmap only checks the most common one thousands TCP ports, the result as shown in Figure 5 has revealed that there are no more open TCP ports beyond what was discovered previously.



Very good

Figure 5. *Searching for TCP open ports beyond the one thousand default port.*

Comparatively, since the previous Nmap tests were considered TCP scans and do not cover UDP ports, so SU command was launched to cover them as well (Weidman, 2014) . The results show in Figure 6, that there are not any open UDP ports at the time being, but this was not the case in the following phase. Similarly, the scan was launched to cover all the possible 65,535 ports.

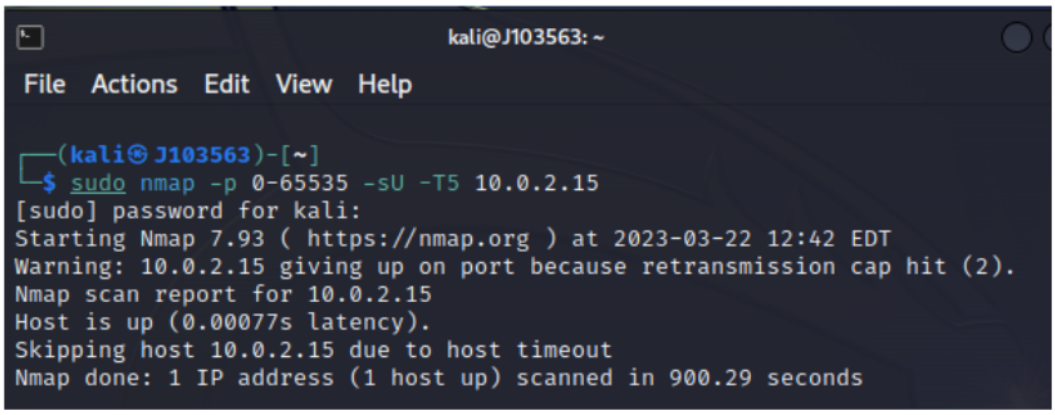


Figure 6. *Searching for open UDP ports*

Then the website pages were examined, and it was beneficial to identify how the target is referring to the username and password fields as mentioned in Figure 7, besides where the login page redirects to, which was revealed to be wp-admin page, and these findings could be used in the following phases. Additionally, there was an attempt to access the URL mentioned in the figure, but it was protected.

Furthermore, by checking the login page, when inputting a wrong username, the response should not be specifying which credential is wrong because this will decrease the projected time for hackers to crack the specified credential. Perhaps, after doing the exploitation phase it was revealed that this specification was not true and it might have been left this way to misdirect hackers.

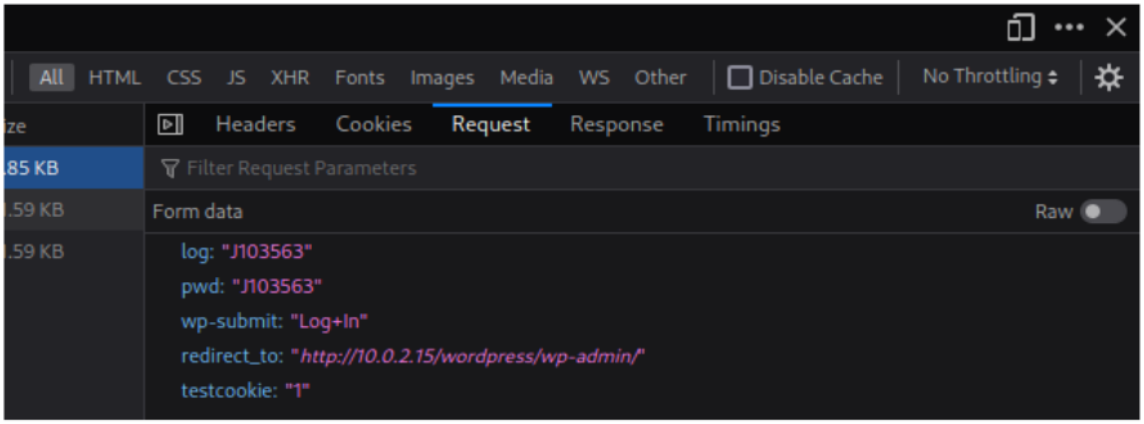


Figure 7. *How the server identifies the username and password.*

Afterwards, packet analyzers were used starting by Burp suite as shown in Figure 8 and by connecting the target and the host machine via a proxy, the findings reveal that the web server is reachable because it returns 200 status code.

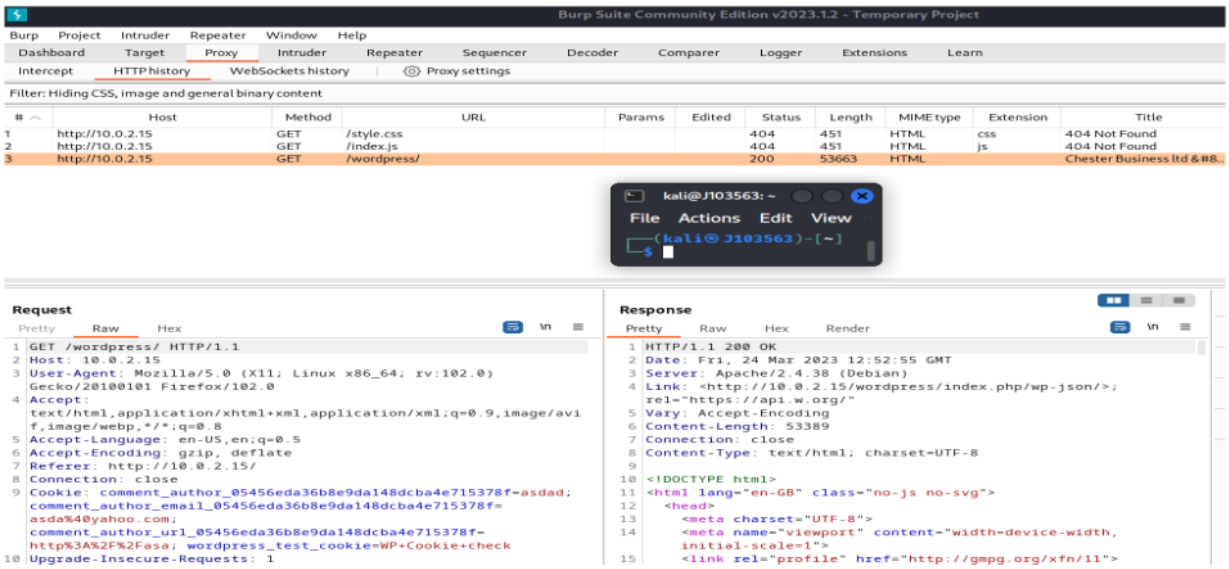


Figure 8. *Analysing the packet using Burp suite*

Similarly, Wireshark was used to analyse the packets at Ethernet interface level, and as shown in Figure 9, the TCP 3-way handshake was achieved at port 80, as mentioned earlier the target IP address is 10.0.2.15.

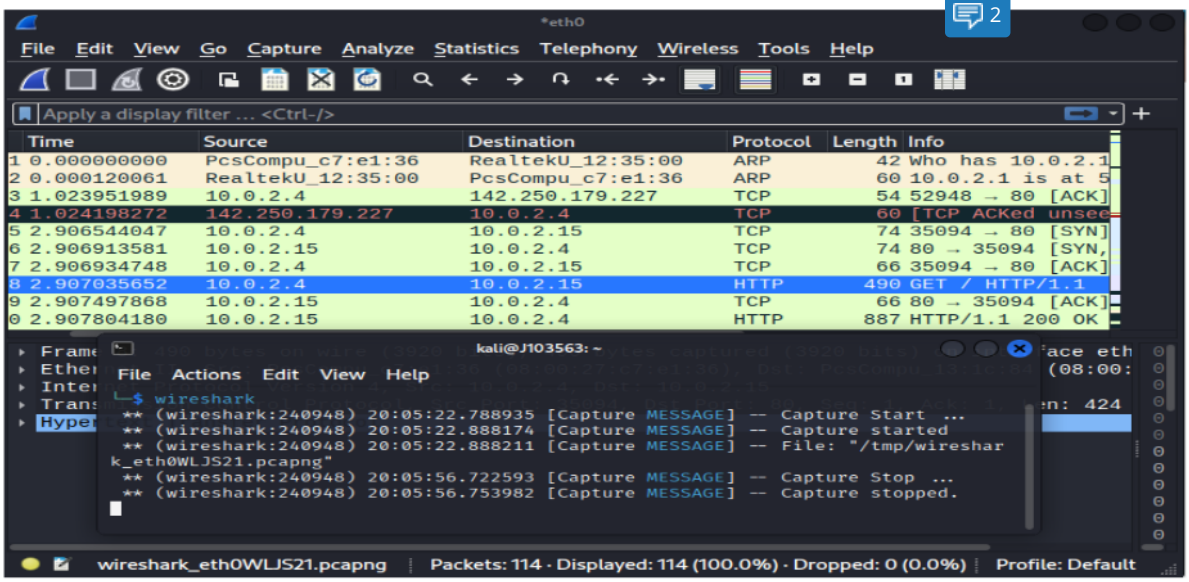


Figure 9. *The TCP 3-way handshake*

Additionally, as shown in Figure 10, the set value of Synchronization flag is on set mode which can be used to craft a Christmas tree attack and as Engebretson (2013) mentions, this type of attack is rarely achievable if the synchronization and acknowledgement flags are not on set mode

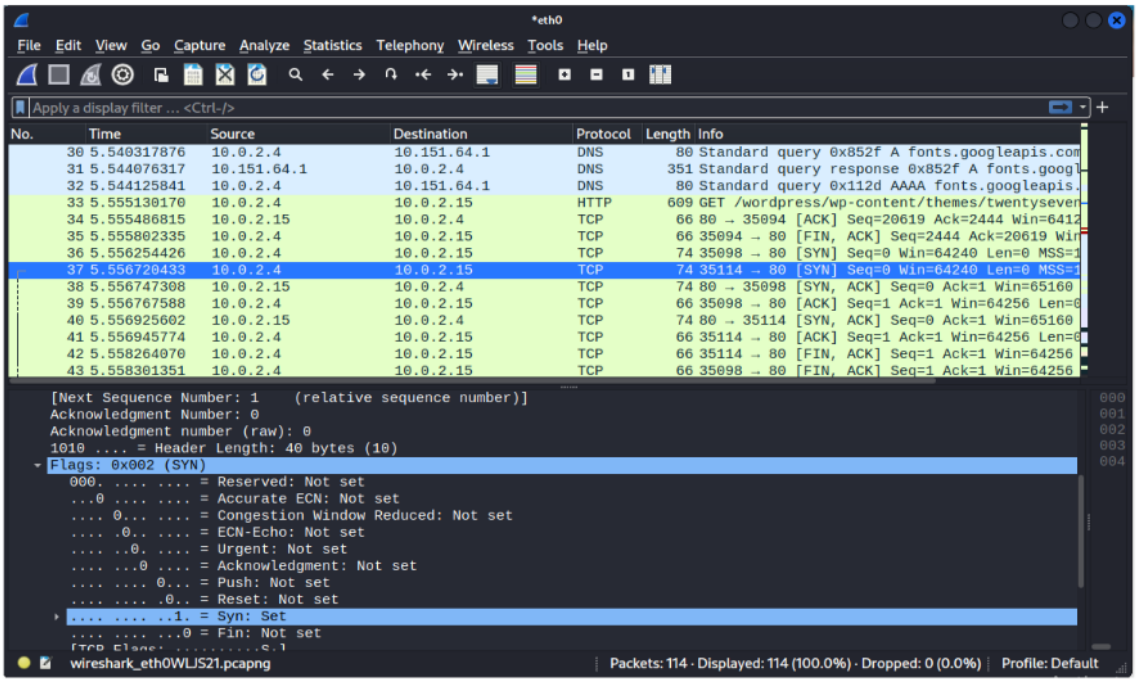


Figure 10. *The Syn flag is in set mode.*

Moreover, by following the stream of the HTTP it reveals the version of the server on which the target is running as demonstrated in Figure 11.

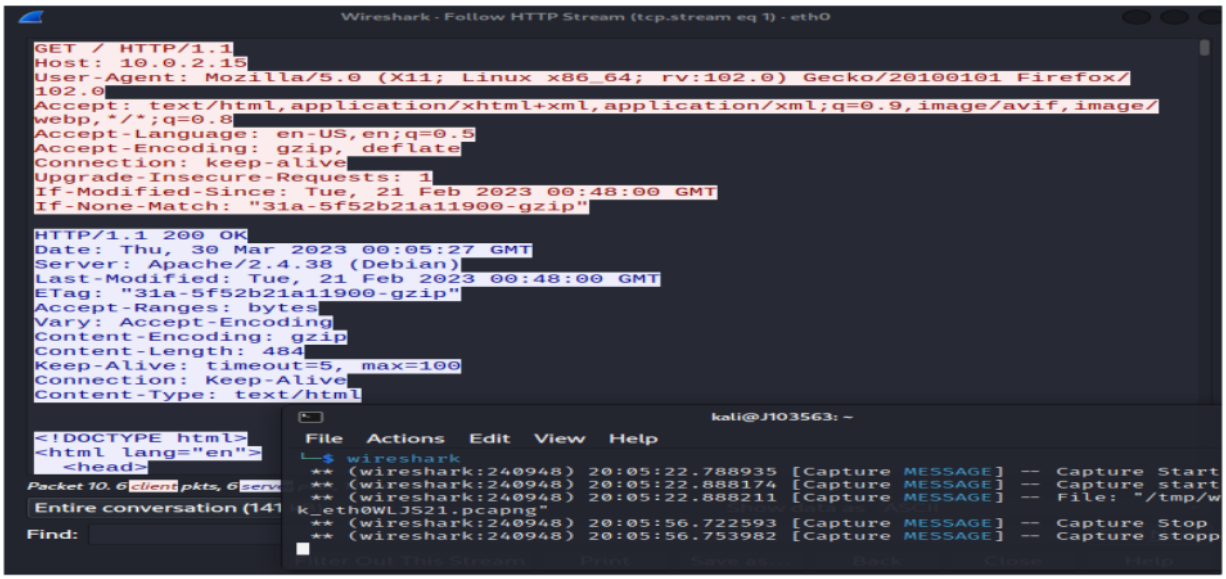


Figure 11. *HTTP stream*

2.2 Foot-printing and scanning (heavy scanning)

Afterwards, aggressive scans were used beginning with Nmap heavy scan or version scan covering all the 65,535 possible ports as mentioned in Figure 12, which is according to Weidman (2014), is used to check the services versions of the open ports in the target system as an attempt of researching about their possible vulnerabilities in the following phase. Additionally, adding the -O option was in order identify the type and version of the operating system running on the target (Engebretson , 2013).

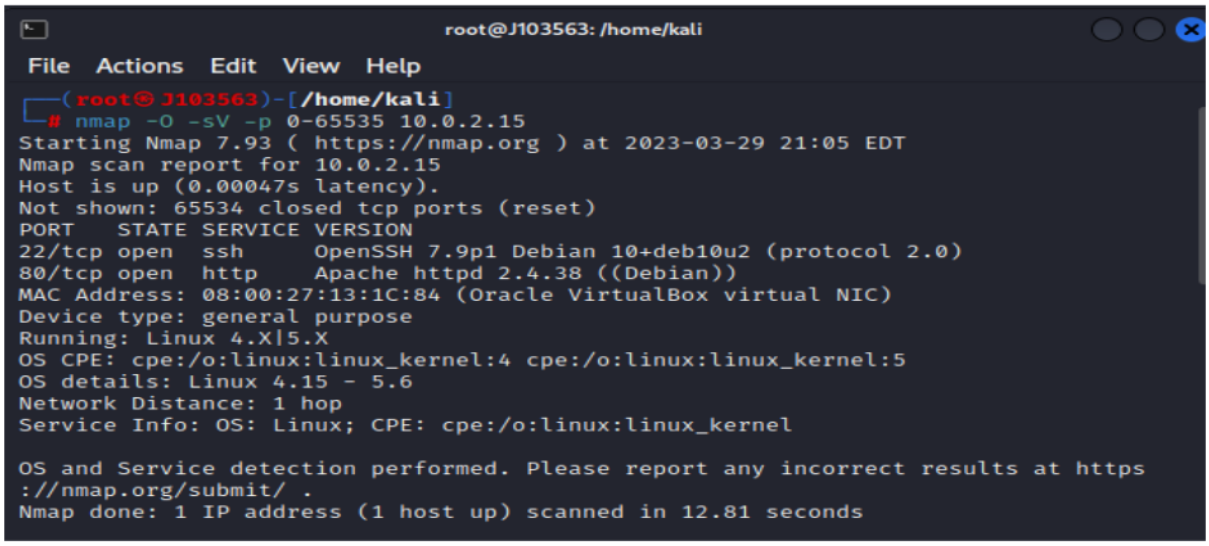


Figure 12. *Nmap TCP heavy scan*

A null scan was inspired from Engebretson (2013), as it is mentioned that in some cases the TCP scans might not show some open ports because the firewall can ignore synchronisation packets, so the test was made as shown in Figure 13, and it was revealed that there are no other open ports apart from those which were discovered earlier.

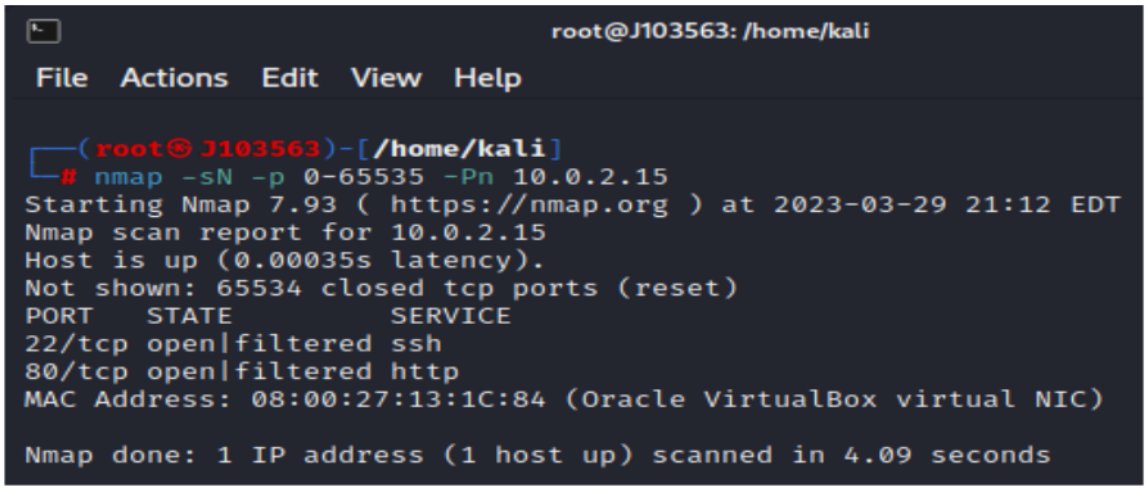


Figure 13. *Nmap null scan*

Furthermore, an aggressive UDP scan covering all the 65,535 possible port was done and it counteracts the prementioned UDP test because it reveals that there are two open ports as mentioned in Figure 14, this is due to the sV option in nmap allowing for double checking on the interactions with the target since UDP is not a connection communication as the case in TCP.

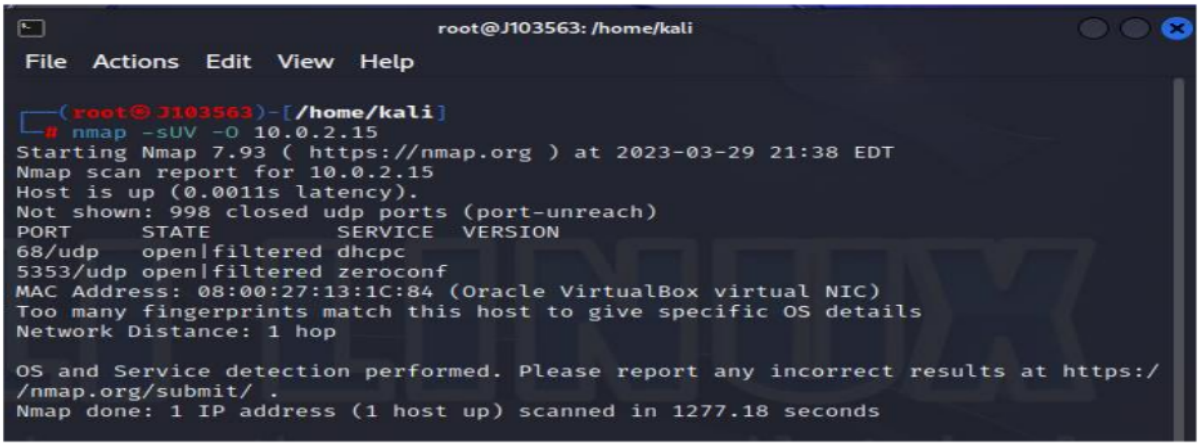


Figure 14. *Aggressive UDP scan*

Consequently, by further research it was found that port 68 is used to assign IP addresses to the devices running in the network from DHCP (Droms, 1997). While port 5353 runs multicast DNS service used to share various services across the network according to the Multicast DNS organization; its points of vulnerability will be discussed in the vulnerability sub section.

Ok

As shown in Figure 15, Burp suite was used again to intercept the packets and because the server uses HTTP protocol which is not encrypted, the username and password J103563 were visible and intercepted. The ability of intercepting could also allow hackers to cause denial of service by dropping requests. However, the interception done by Burp suite to the GET requests of the forget password page will be used in the phase of vulnerability assessment for SQL injection.

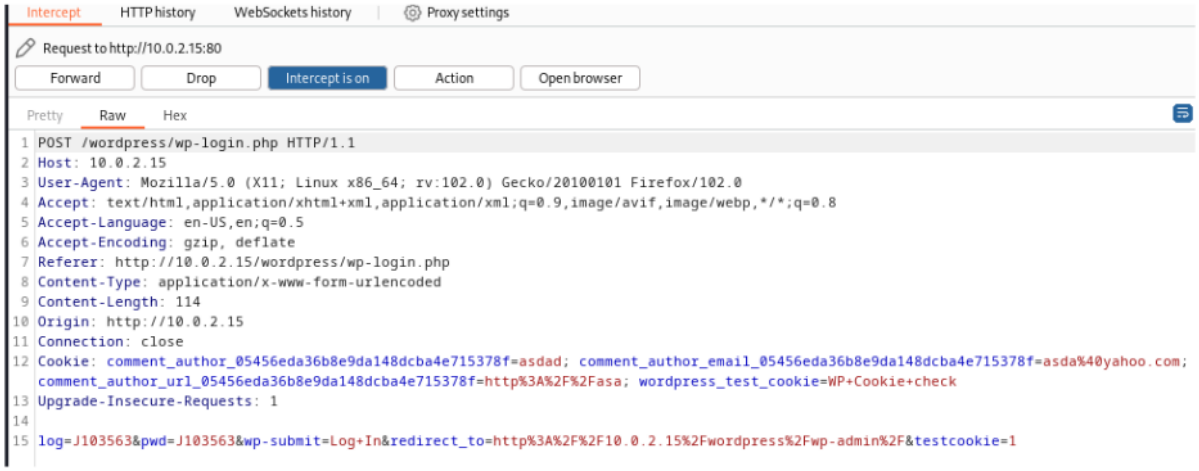


Figure 15. *intercepting the login credentials.*

Accordingly, as shown in Figure 16 and 17, by changing the request method of the login page into GET request method using Burp suite options and copying the URL this will be made use of in the vulnerability phase.

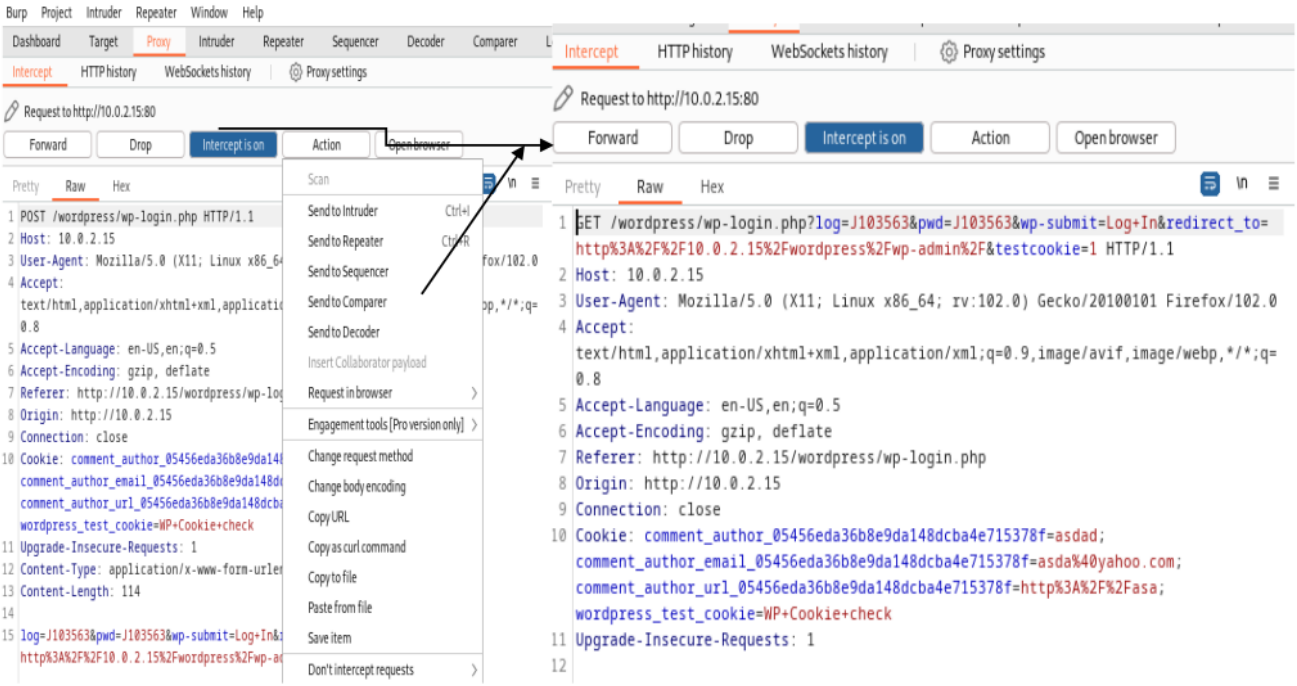


Figure 16,17. *Changing the POST request into a GET request.*

As mentioned earlier while demonstrating Wireshark, the target might be vulnerable to Christmas tree attacks so while using sX flag which is responsible for starting the Christmas tree scan, there was an attempt to do that and see how the server reacts which is shown in Figure 18, and it resulted in setting on the urgent, push and fin flags.

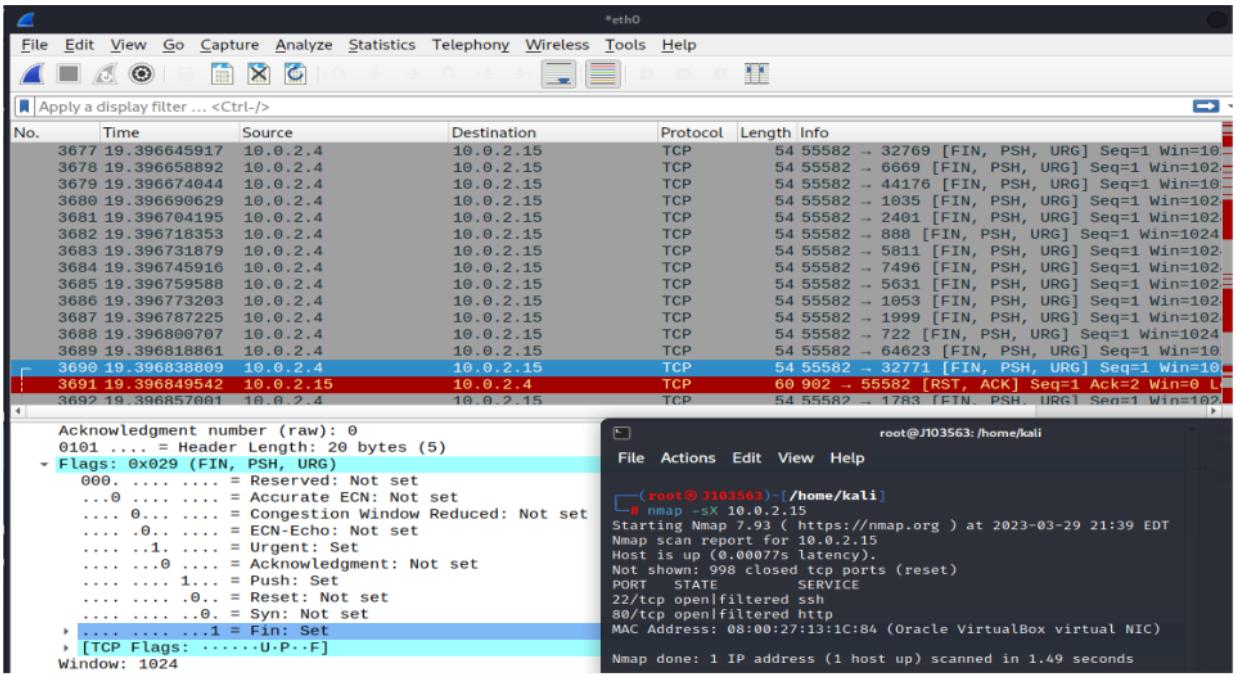


Figure 18. *Christmas tree attack*

Then as shown in Figure 19, the target replied by Acknowledgment then it closed the communication, but afterwards the interaction was still going on, but the bright side is that the server did not reboot, shut down or reveal sensitive information.

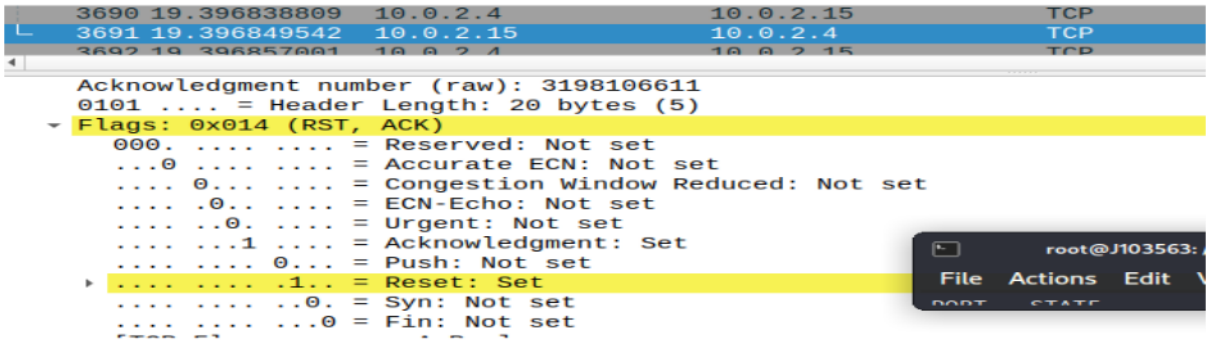


Figure 19. *The target closed the connection and was not affected by denial of service.*

At the end of the information gathering phase the following table was used to summarize additional findings.

Figure	Observation	Comment
1	TCP port 53 is open in router	It belongs to DNS.
1	Port 80 is open running HTTP	It means that the target is a web server (Weidman, 2014)
1	Port 22 is open running SSH service	Could be a possible path of exploitation
7	The user identifies the username as “log”, and the password as “pwd”	Could be used in the vulnerability assessment
7	The login page redirects to the admin page.	Admin page is hidden
9	The server uses HTTP	Not secure, not encrypted
11,12	Target is running on Apache server version 2.4.38 Debian	This version is vulnerable to request smuggling attack (CVE-2023-25690, 2023)
12	SSH version open SSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)	
12	OS running is Linux 4.15 – 5.6	The exact version will be identified in the following phases.

Table 2. *Information gathering additional findings.*

Good

3 Vulnerability assessment

WPScan was one of the essential tools to be used because the target is a webserver running on WordPress platform, and according to Kashyap et al. (2021), WPScan was created to check WordPress based websites for vulnerabilities. As mentioned in Figure 20, it was able to detect that xmlrpc is enabled which is regarded as a vulnerability as mentioned by (Goldshlager, 2018), and could lead to denial of service.

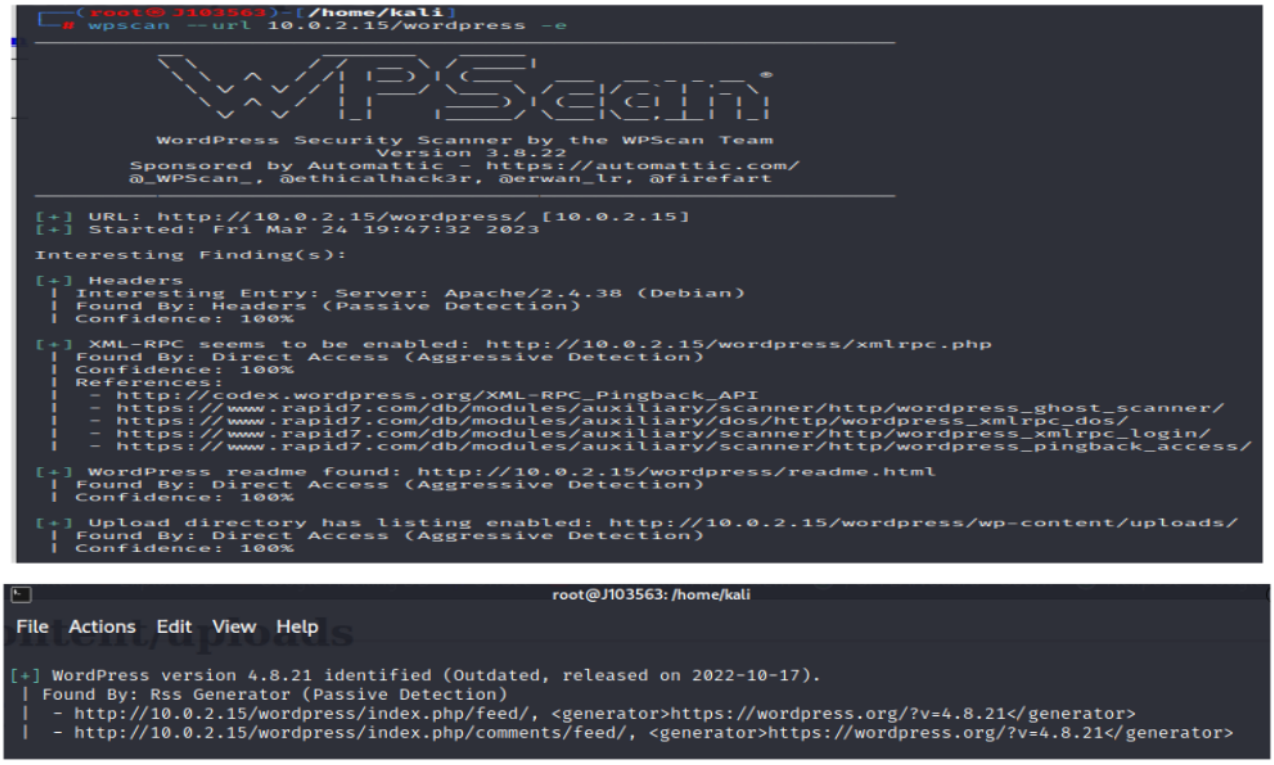


Figure 20. *WPScan checking for vulnerabilities.*

Additionally, the upload directory listing was discovered, and it is accessible as mentioned in Figure 21, and this could allow attackers to see sensitive files. WPScan has also discovered that the WordPress version is outdated.

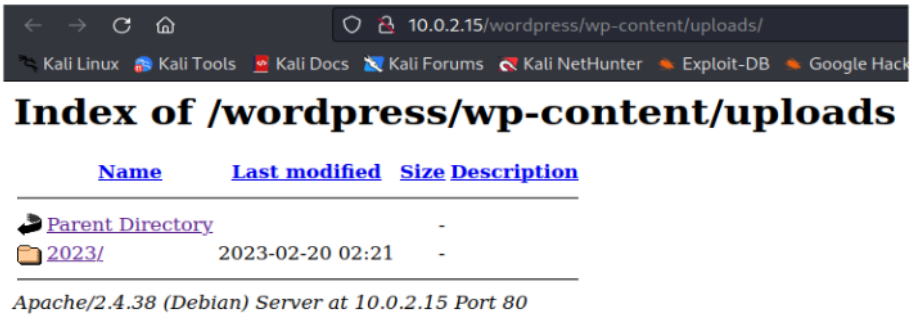


Figure 21. *Upload directory is publicly accessible.*

Consequently, by adding the vp and the api-tokens options to look for vulnerability plugins and bugs, WPScan was successful in finding a vulnerability, which could lead to denial-of-service attack according to (Haworth, 2022).

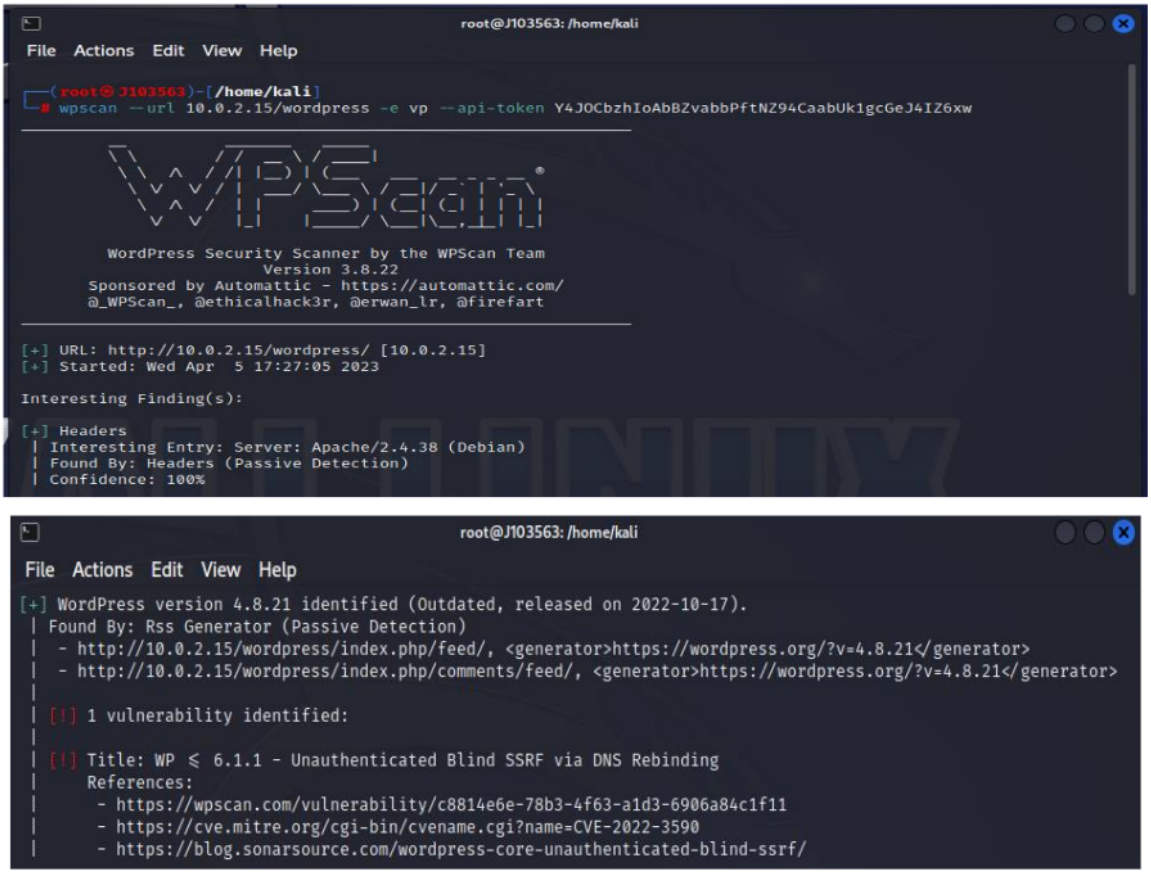


Figure 22. *SSRF vulnerability*

Good

Afterwards, Nmap script was used as demonstrated in Figure 23, the command has shown that admin, index.php and info.php directories are publicly accessible and not hidden which is regarded as a vulnerability and intruders can access sensitive files and information according to (CWE-548, 2006).

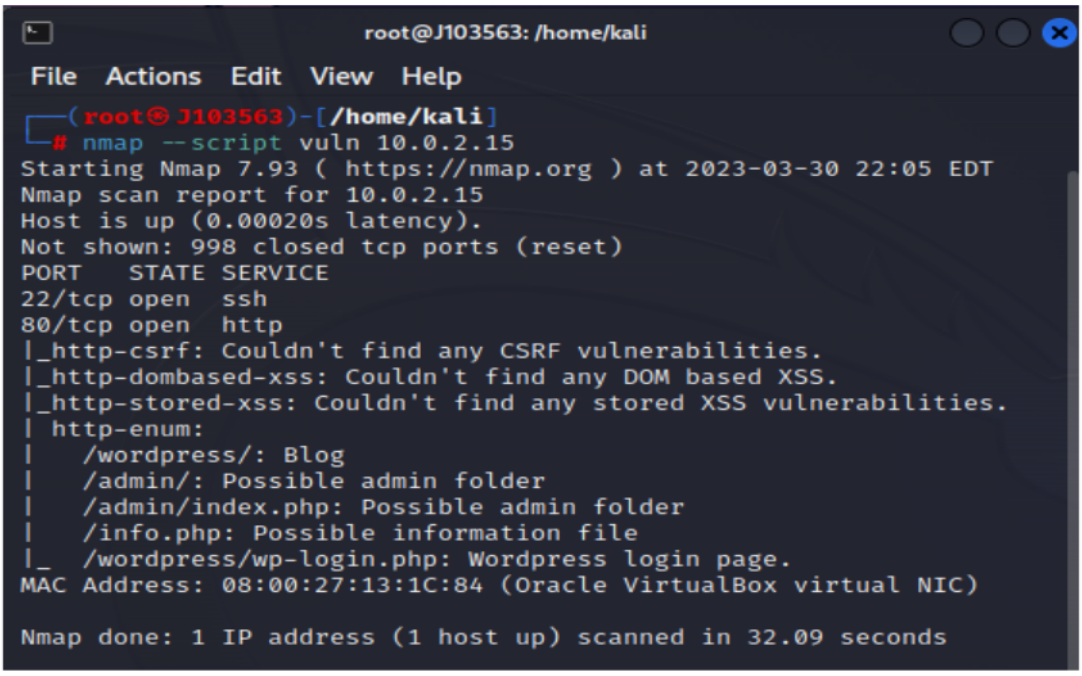


Figure 23. *Nmap script demonstration*

Additionally, by increasing the aggressiveness of the test by adding the sV option, it has shown that the Sshtranger things bugs were found in port 22 which are regarded by CVSS3 as a medium risk. On the other hand, in port 80 there were severe vulnerabilities because of the outdated version of HTTP server, according to CVE, for instance HTTP configurations are vulnerable and attackers can make use of that and send loads of requests leading to denial of service. As well as CVSS3 ranks port 80 vulnerability by 9.8 out of 10 which allows intruders to cross IP authentications because the HTTP out-of-date version lacks the ability of sending x forwarded headers as shown in Figure 24.

Good

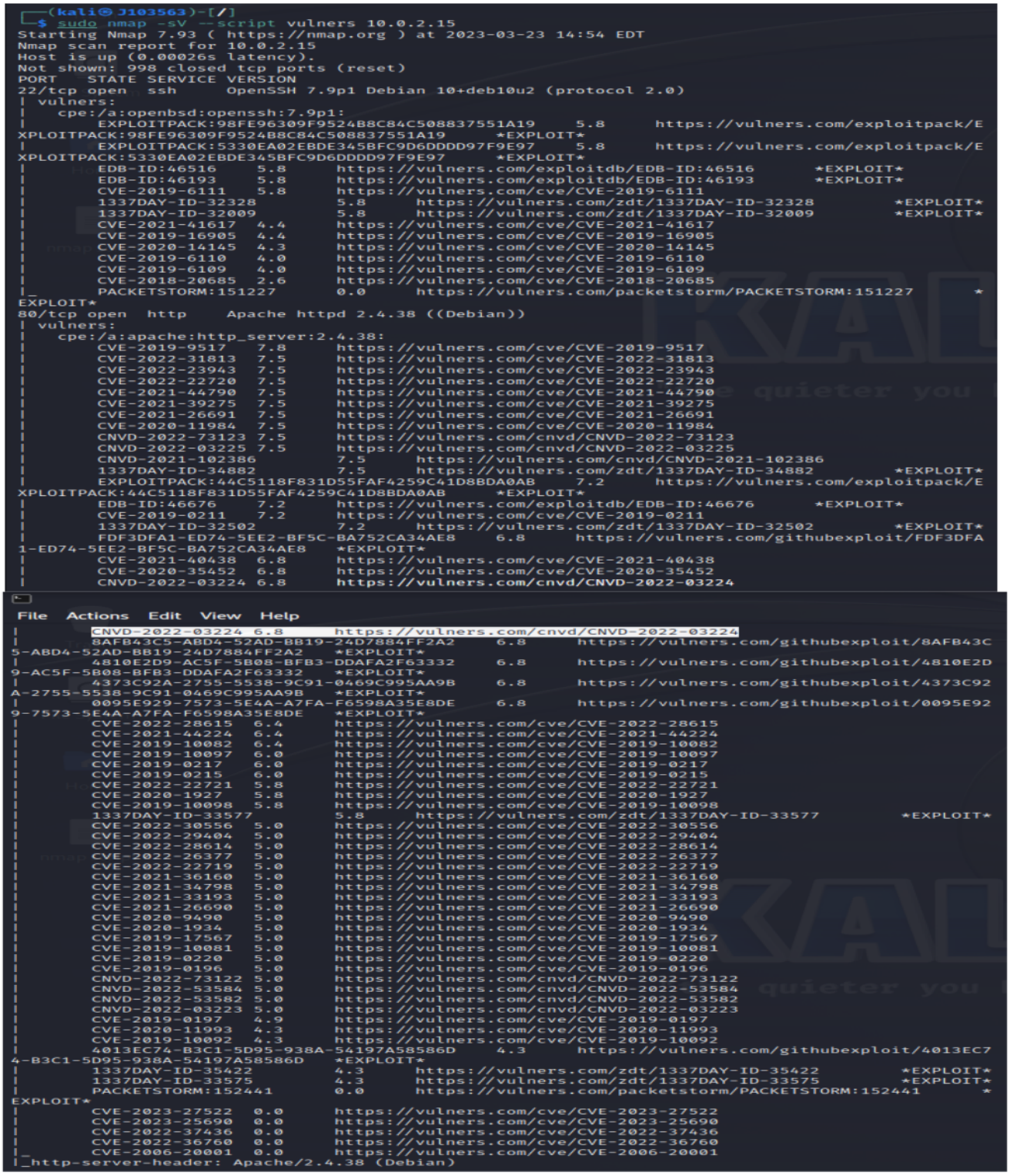


Figure 24. *Nmap script aggressive scan*

Nikto was used because as mentioned by Weidman (2014), it is able to check outdated services and vulnerable files, as Figure 25 shows, the x-content type header is not set and according to (OWASP 2017-A6, 2017), this could lead to Cross Site Script attacks. Moreover, the website is misconfigured in regard to the clickjacking which might be taken into advantage of intruders so users may not assume they are clicking on something irrelevant to the webpage (Dhawan, 2008).

The server runs Apache version 2.4.38 which is outdated and further reading in vulnerability intelligence search engine reveals that the Apache 2.4 to 2.4.38 has various vulnerabilities, for instance the client certificate verification can grant access to restricted configurations. Nikto has also revealed that uploads directory index is browsable, and it highlighted the possibility of revealing sensitive data, and as mentioned earlier by (CWE-548, 2006), it is a vulnerability and could lead to data breach.

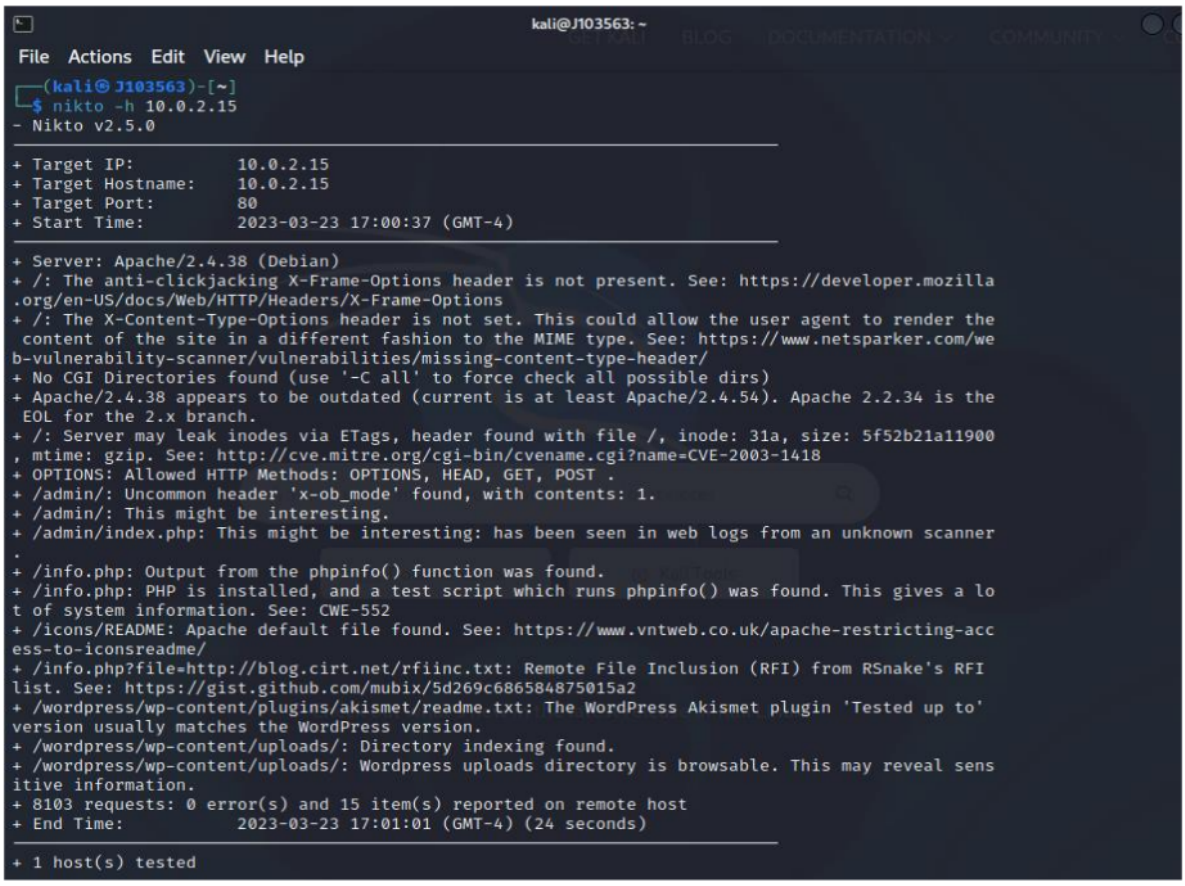


Figure 25. *Nikto scan*

Afterwards, go buster was used to look for directories by using dirb dictionary lists, it has shown the availability of the previously discovered directories as mentioned in Figure 26.

Good

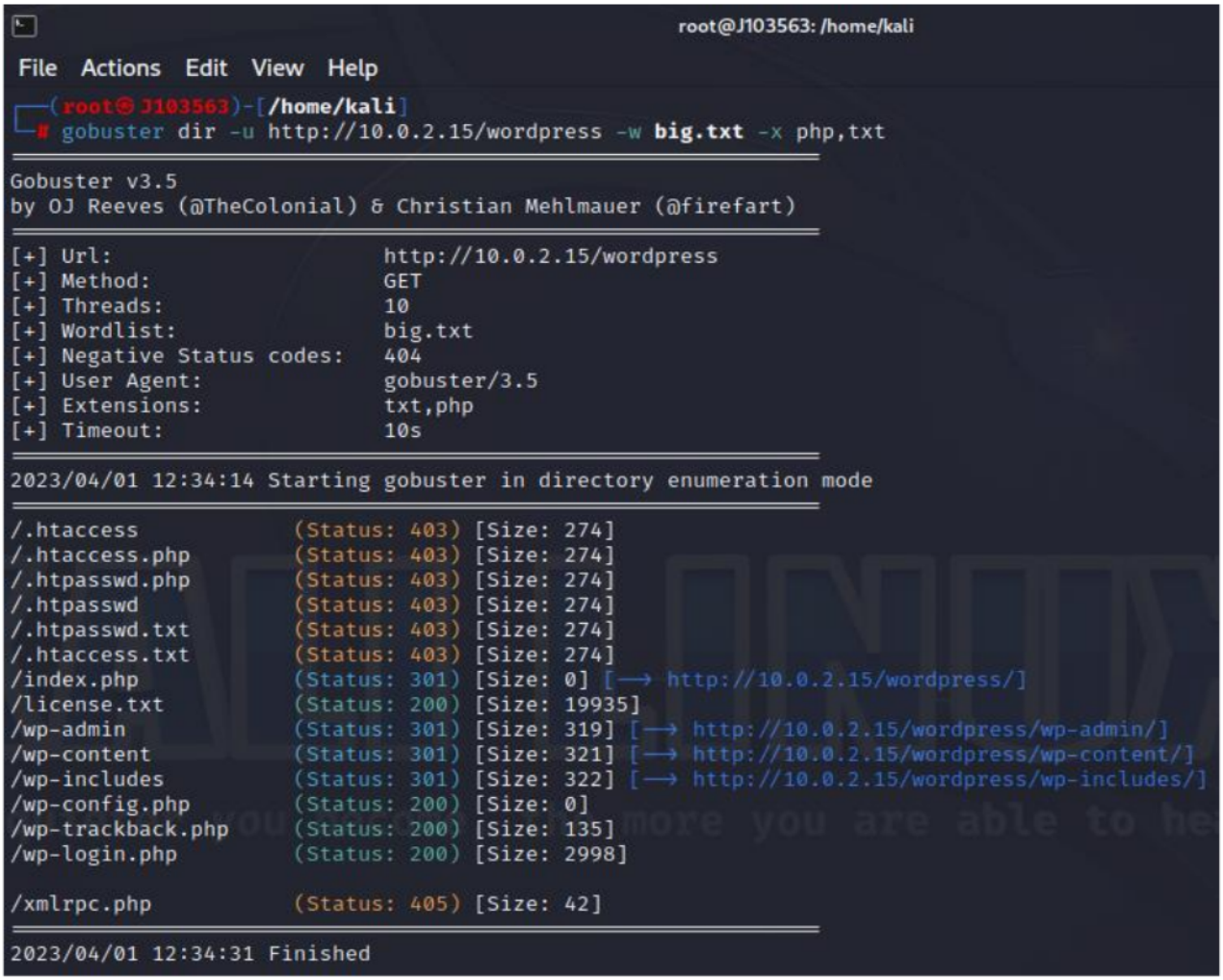


Figure 26. *Using go buster to look for directories.*

In order to collaborate the findings Dir buster was used as well with a different dictionary list as mentioned in Figure 27, and it was able to find variety of accessible directories which are considered to be vulnerabilities such as: Downloads and various admin directories

As mentioned earlier, how the credentials are referred to in the server database is beneficial, so this was made use of by searching in each admin directory file using the word "pwd" in Mozilla browser to find anything related but it was not successful. However, the presence of these files is still regarded as a vulnerability because it will be mentioned in the following phase that WPScan used one of the admin directories to look for a username and it was successful.

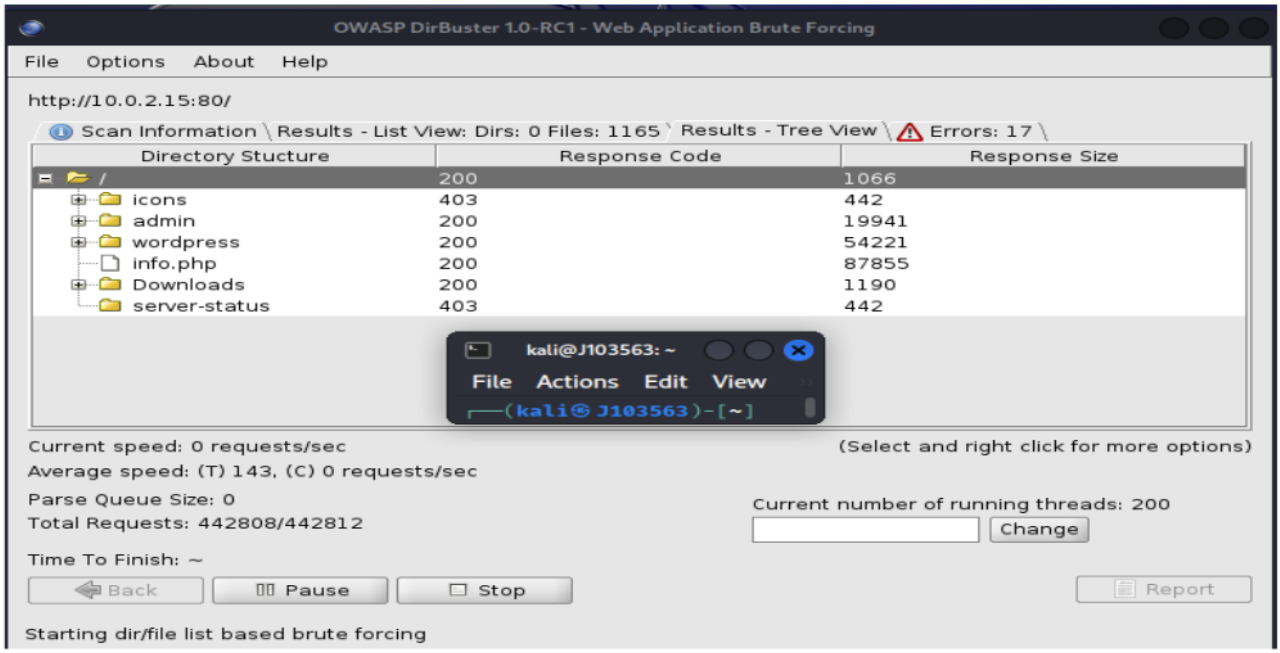


Figure 27. *Dir buster directory listing*

However, by the help of intercepting the packets in information gathering stage using Burp suite and changing the POST request of the login page into a GET request, besides trying to infiltrate the forget password page, SQL map tool was used as an attempt to find vulnerabilities, but as shown in Figure 28 and 29 it was not able to find any.

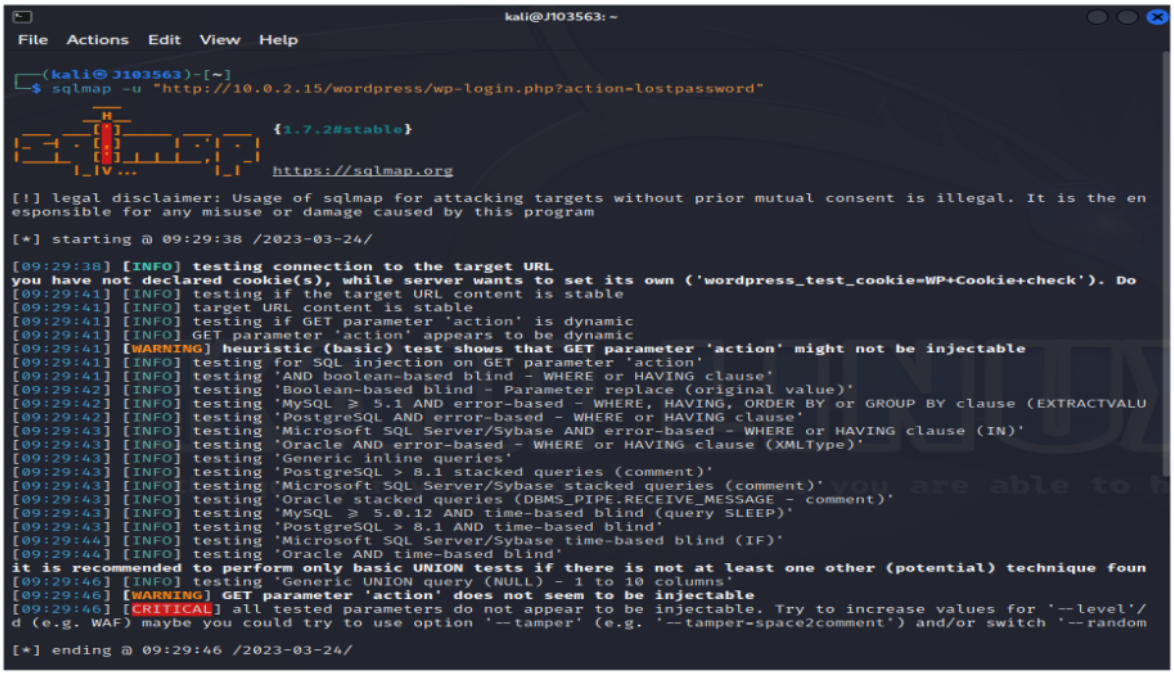


Figure 28. *An attempt to find sql injection vulnerabilities in the lost password page.*

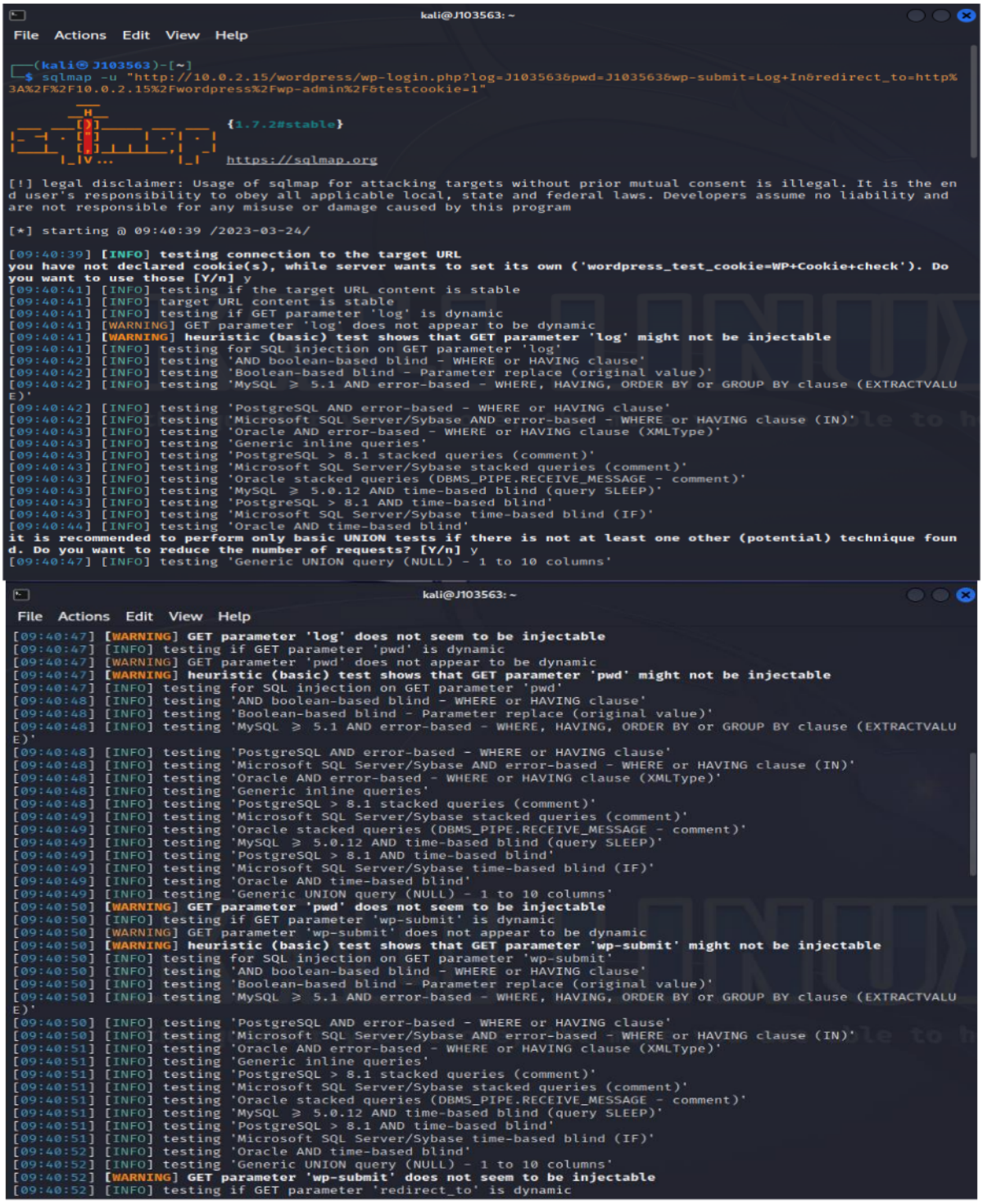


Figure 29. *An attempt to find sql injection vulnerabilities in the login page.*

Then, Nessus vulnerability scan automated tool was used to search for additional vulnerabilities. As shown in Figure 30 Nessus has not found serious vulnerabilities but it has provided some sort of security information, besides collaborating the findings on the previous phases in terms of open ports and services running and their versions.

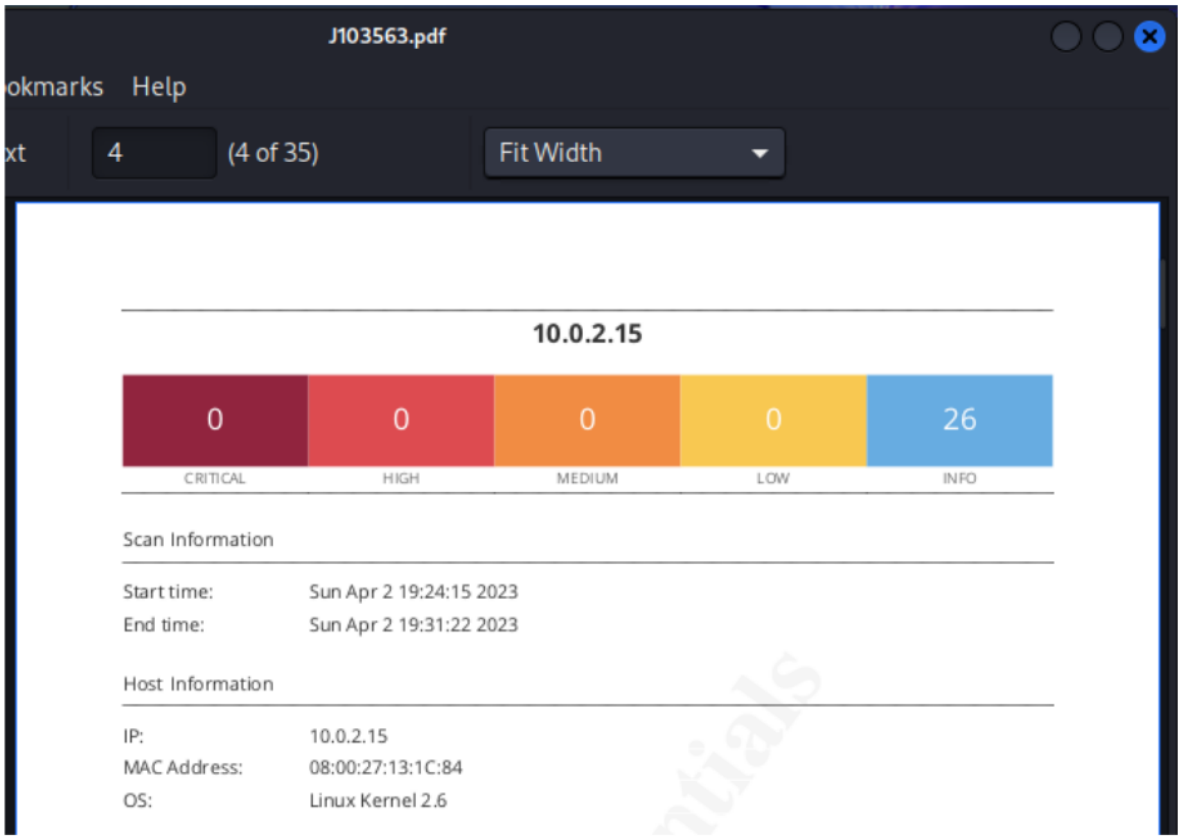


Figure 30. *Nessus automated tool report*.

Regarding the prementioned UDP open ports, and according to (Crawley, 2017), port 5353 running multicast DNS service could lead to denial of service if hackers send floods of request to bring the system down, and it is advised to disable it. At the end of the information gathering phase the following table was used to summarize additional findings.

Tool	Observation	Comment
WPScan	The WordPress version is 4.8.21	Outdated, released in 2022/10
Nmap script	Port 80 vulnerabilities	-HTTP configurations are vulnerable to denial of service, for instance the intruder can send loads of requests leading to excessive CPU usage (CVE-2019-9517, 2019).
		According to CVE-2022-31813 (2022), the Apache versions released before 2.4.53 are vulnerable to bypassing of the IP address verifications.
Nikto	Has found admin, phpinfo pages publicly accessible	Collaboration of the findings
Nikto	10.0.2.15/wordpress/wp-content/uploads/: Directory indexing found	Could be a possible way of exploitation
Manual	There was attempts of performing sql	The attempts did not succeed in showing SQL vulnerabilities

A very good attempt, using a wide range of relevant tools. It's good to see contextualised discussions on some of the identified vulnerabilities

SQL injection	injection in the login page, for example by using apostrophes to alter the webpage code.	
Cross-site scripting	There were attempts of performing cross-site scripting on the search label by entering phrases inside <p>, and <u>.	The attempts did not prove that the website is vulnerable to cross-site scripting.

Table 3. *vulnerability assessment additional findings.*

4 Exploitation and post exploitation

Firstly, WPScan was used again and the -e -u options were used to enumerate usernames, and WPScan was able to find one user who is "james" as shown in Figure 31.

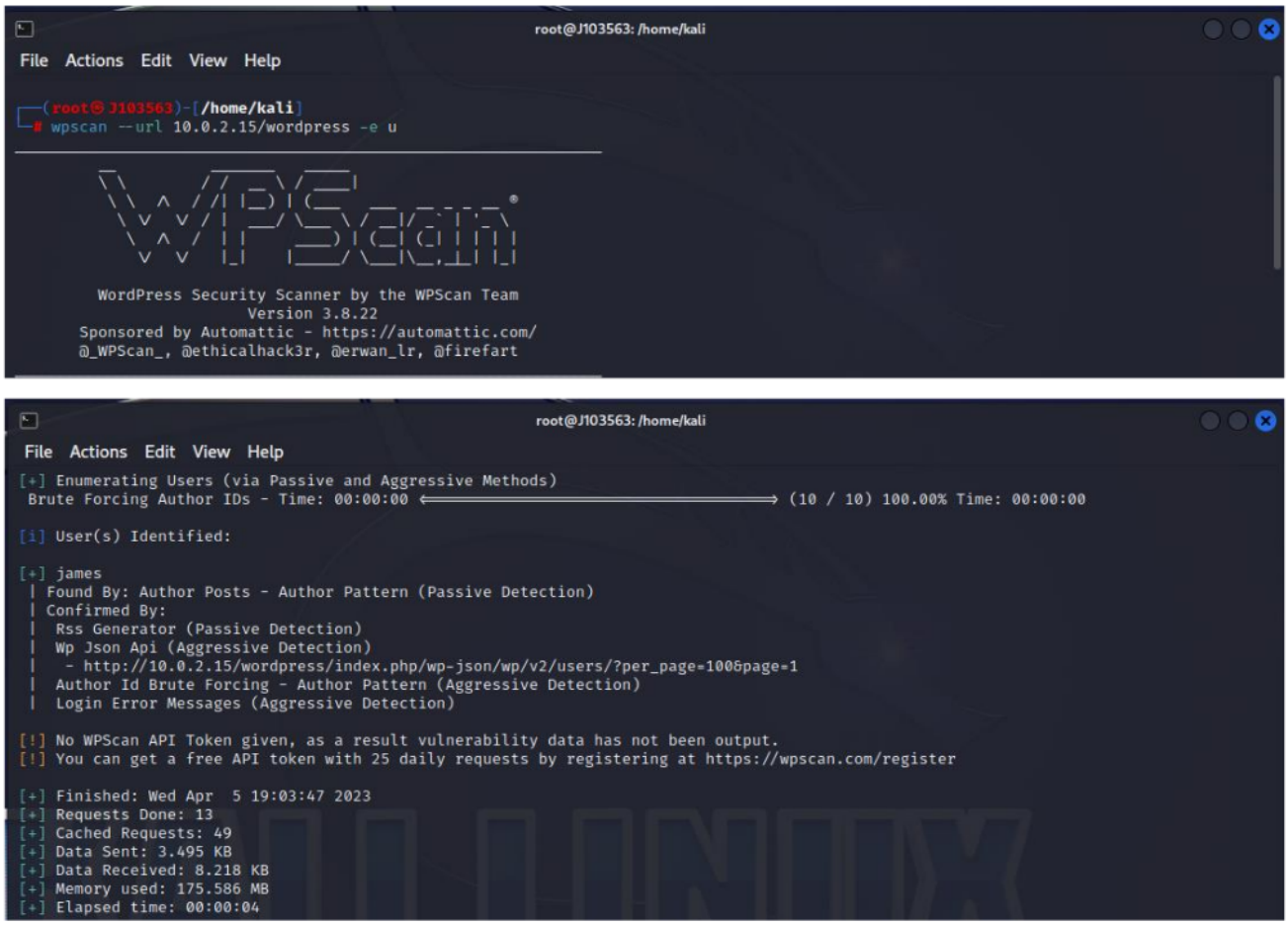


Figure 31. *Identifying a username*

Good

In brief, the reason behind WPScan was able to discover this username is because wp-json directory is accessible and shows the username publicly as shown in Figure 32.

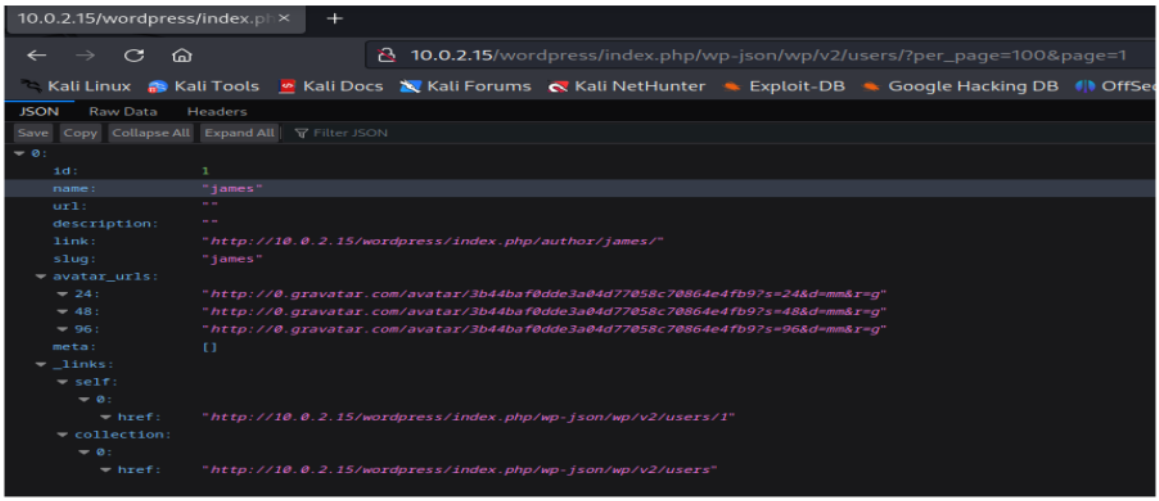


Figure 32. *how did WPScan find the username*

Additionally, WPScan was used again to find the password using a wordlist called “common” of dirb tool, and a password matching the user “james” was found which is “password” as demonstrated in Figure 33.

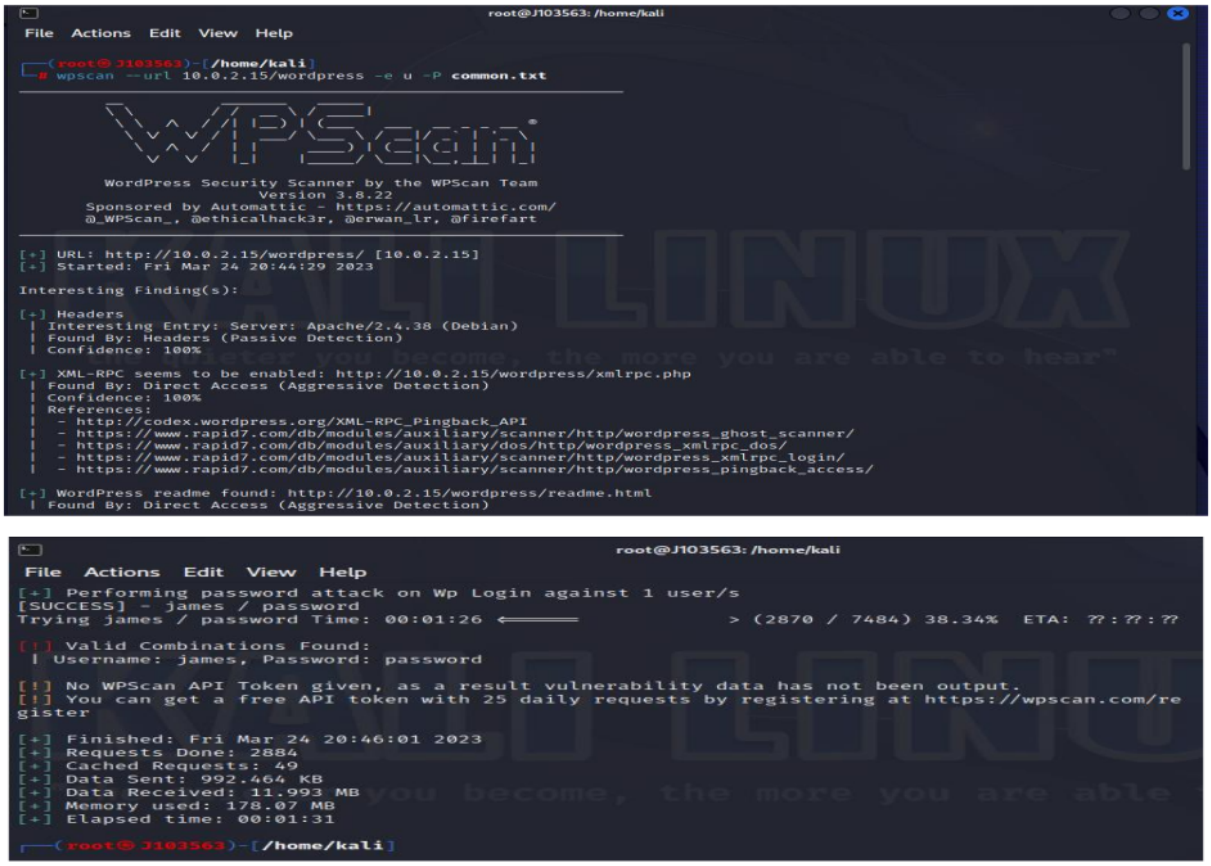


Figure 33. *WPscan password dictionary attack*

Consequently, by using the obtained credentials to login, the users list was found, it was ensured that these credentials belong to Mr. James, the head of IT, and the media files were obtained as well as shown in Figure 34

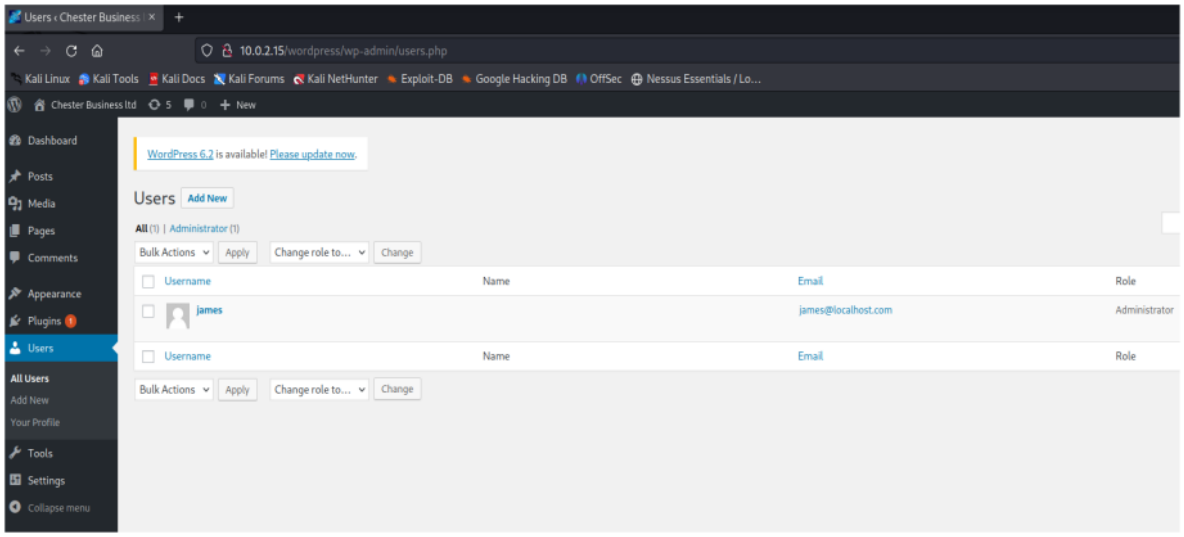


Figure 34. *Using the obtained credentials to login*

Good

Similarly, Hydra was used in order to attack SSH service using a dictionary list called "john", the attack was successful, and it was revealed that the password of the user "james" is "qwerty"

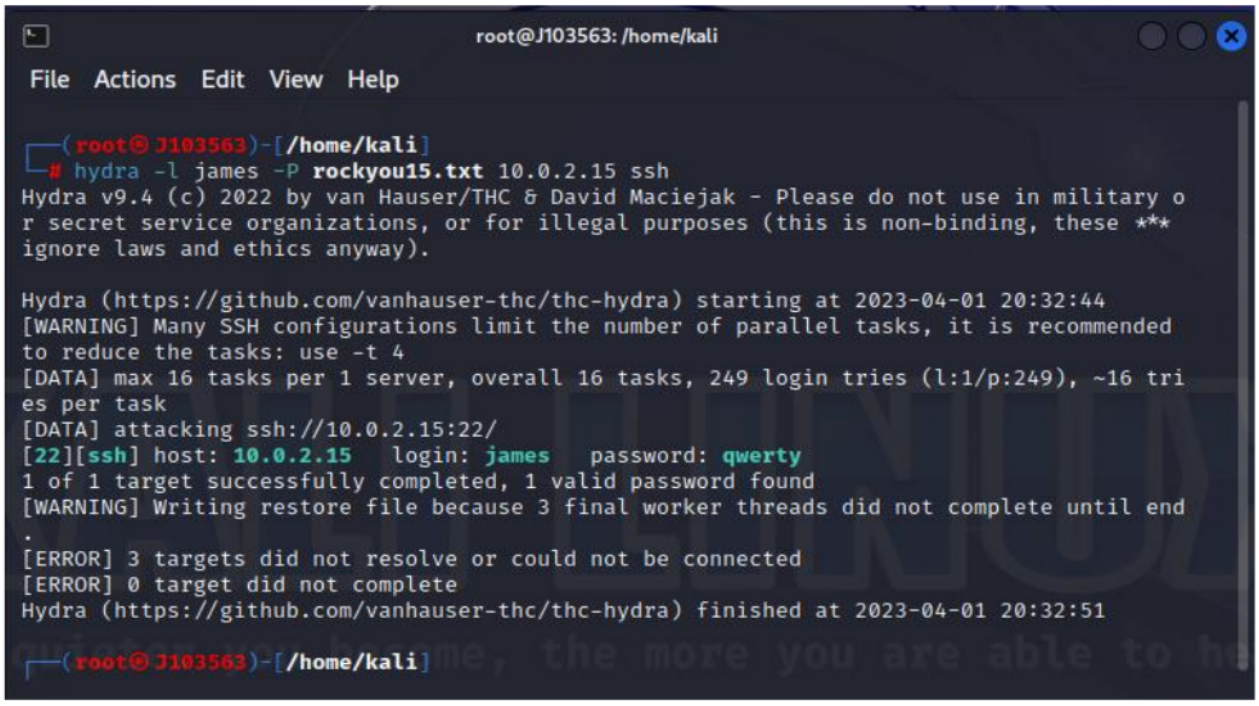


Figure 35. *Successful Hydra password dictionary attack*

By making use of the obtained password, SSH remote connection was established, and it was extended to root privileges as well. By changing the current directory, and going back to the home directory, there was another finding that there is another user with the name peter, and debian which might be a user or common login credentials for the employees as shown in Figure 36.

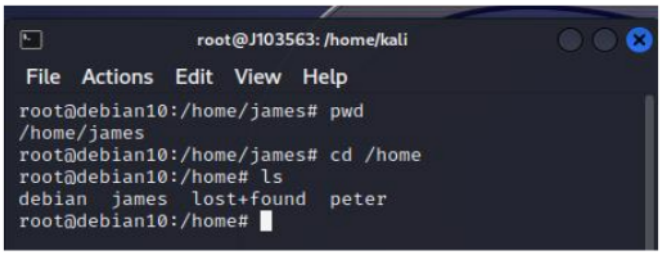


Figure 36. *Two other users were discovered by accessing "james" remotely via SSH.*

Good

Moreover, the command ls with the flag -a was used in "james" folder to look for the hidden files as mentioned in Figure 37, and this was also done in the other 2 users' folder but there were not sensitive files.

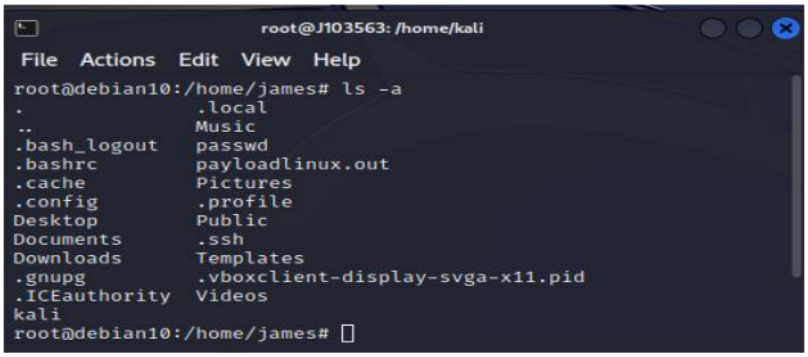


Figure 37. *List command*

Accordingly, there was also a successful attempt of downloading the password and shadow files located in the target machine remotely while being connected through SSH as illustrated in Figure 38.

Figure 38. *Copying the password file.*

However, while attempting to download the shadow file, the permission to do that was denied, but since the root privileges login was obtained, it was possible to change the permission as shown in Figure 39 and 40.

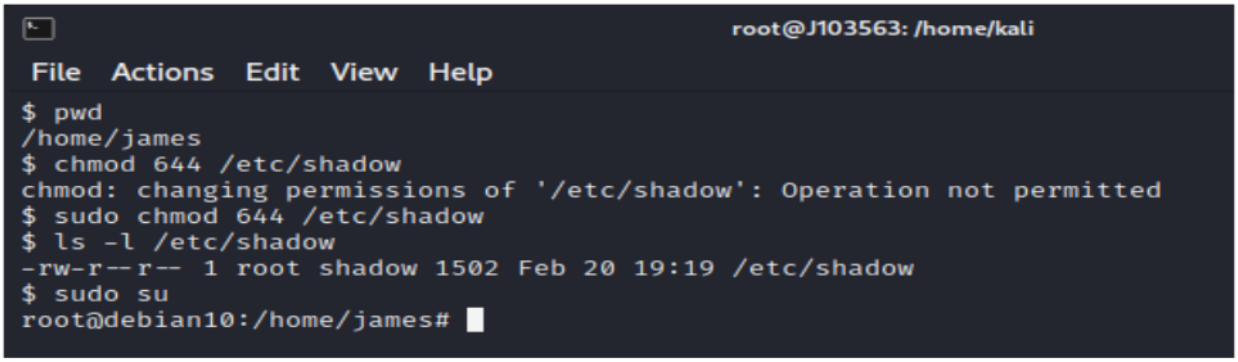


Figure 39. *Changing the permission of shadow file.*

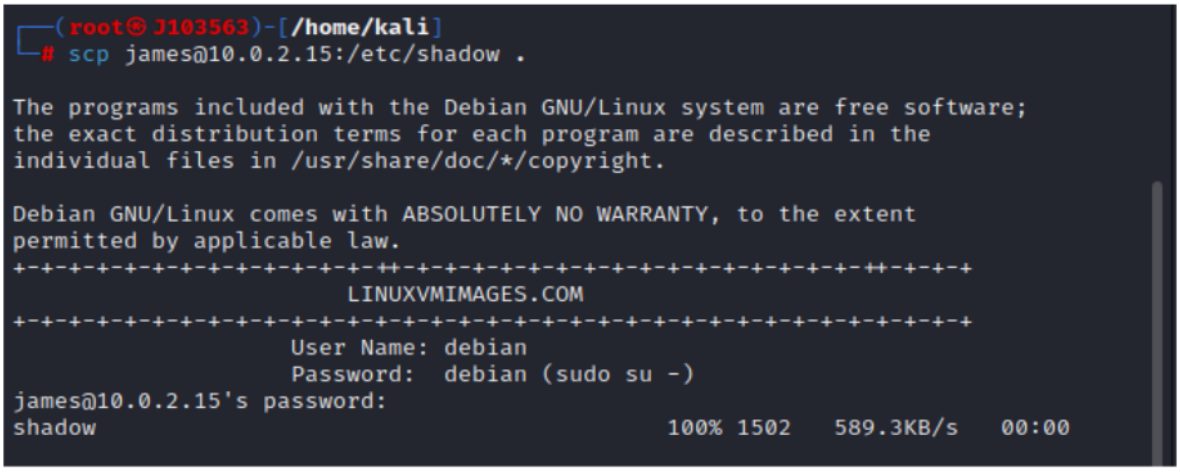


Figure 40. *Copying the shadow file*

As a result, John the ripper tool was used to decrypt the passwords file obtained from the target machine, but as shown in Figure 41 before doing that the files had to be un-shadowed to be usable by the tool.

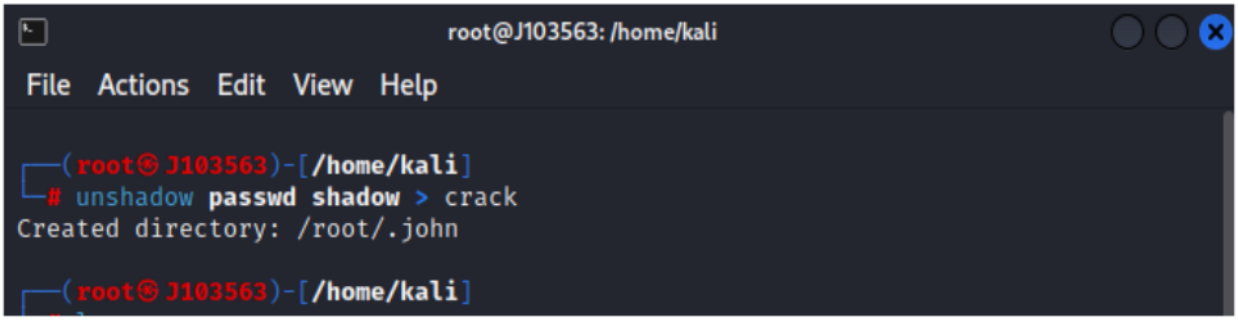


Figure 41. *unshadowing the sensitive files*

However, it is suggested that the passwords are strong enough since various dictionary list were used one of them was "rockyoulist", besides brute forcing attack, but the passwords were not obtained as shown in Figure 42 and 43.

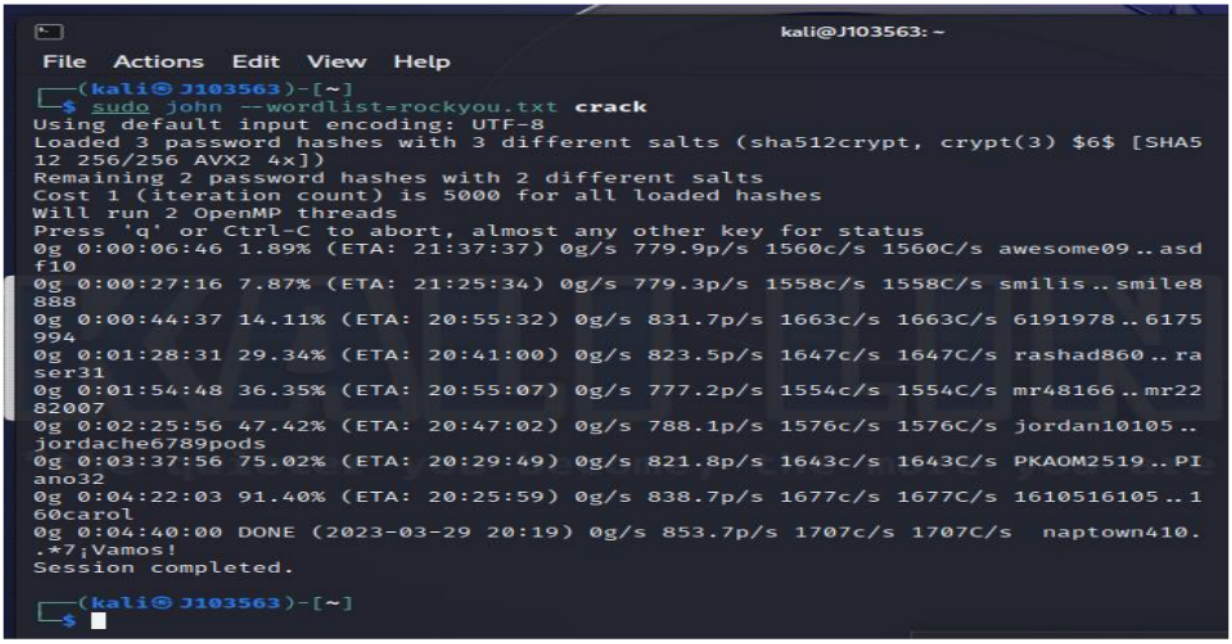


Figure 42. *John the ripper dictionary attack*

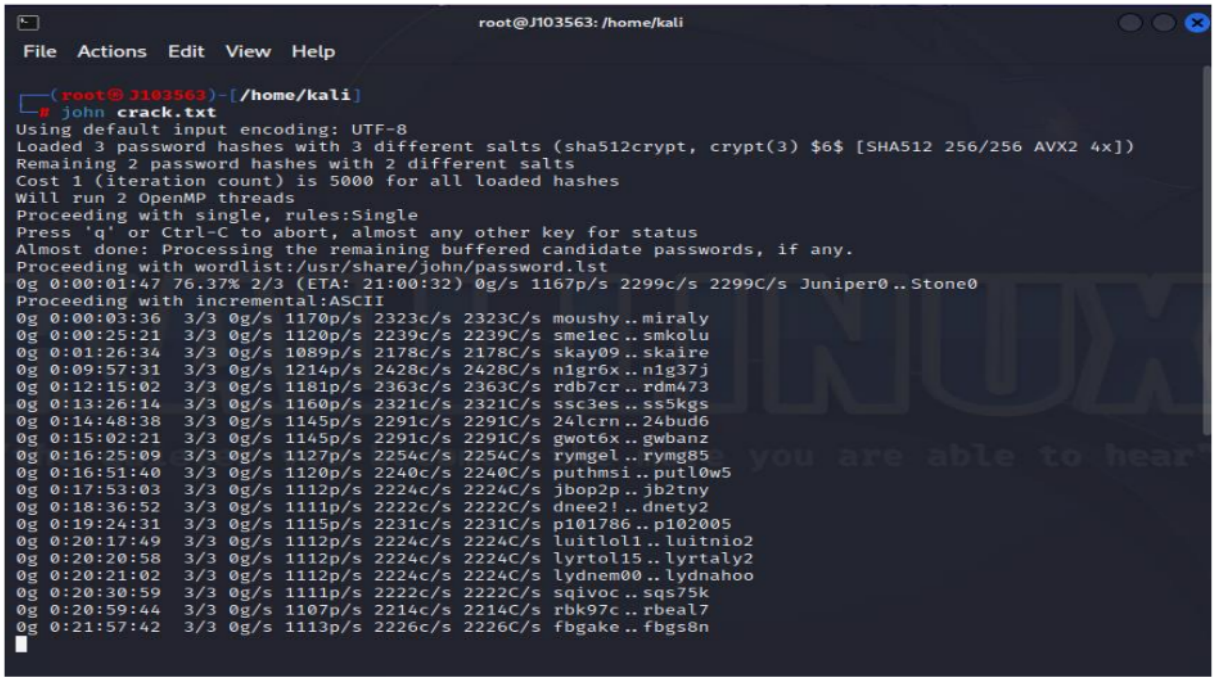


Figure 43. *John the ripper brute force attack*

Afterwards, as demonstrated in Figure 44, a backdoor metapreter attack was performed using metapreter reverse TCP which was preferred over bind TCP because it can bypass firewall, so a payload was made, and it was made executable as well, then it was uploaded successfully on the target machine.

Figure 44. *Reverse TCP attack*

Then Metasploit was used to create a handler as shown in Figure 45 which is responsible for listening to the communication going on the target machine.

Figure 45. *Using a handler*.

Good

As shown in Figure 46, when the payload is executed on the left side command, the right-side command starts listening to the target.

Figure 46. *Payload demonstration*

By using the command sysinfo it is possible to identify the exact version of the operating system which was revealed in Figure 47.

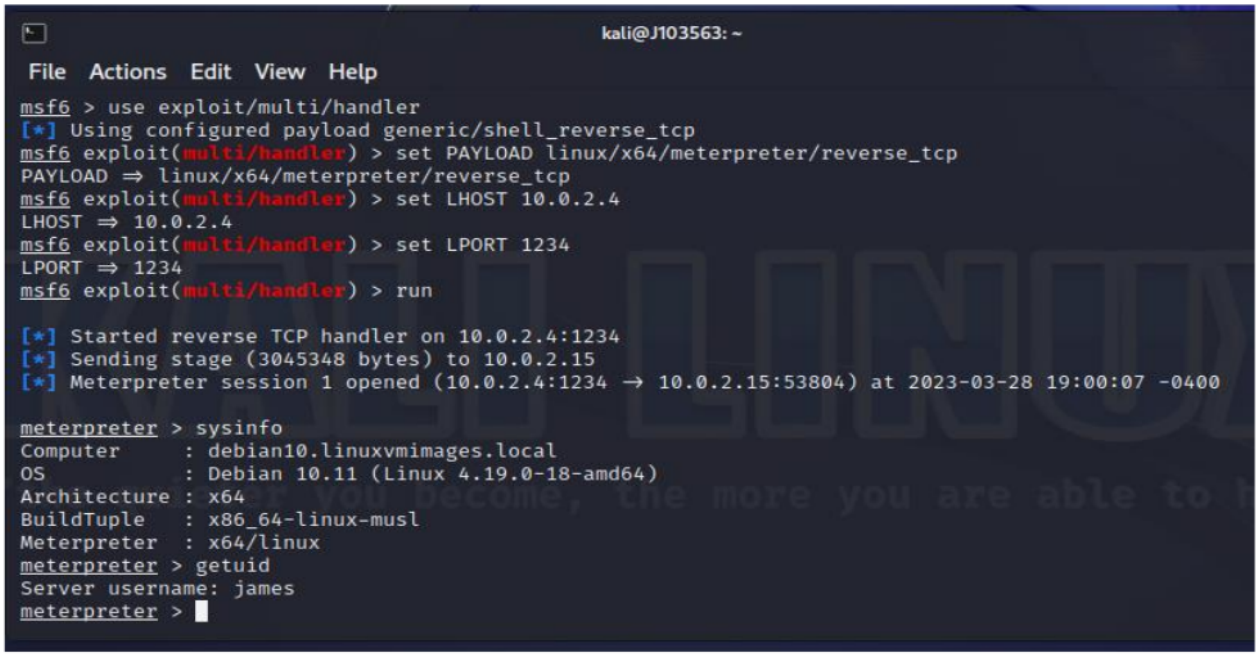


Figure 47. *The operating system exact version*

Excellent

5 Risk / exposure

After all the previous tests and stages were done, it can be said that the company is at a high risk based on the following listing:

- Mr. James passwords were obtained in the WordPress page and the SSH service.
- Root privilege is allowed after login via the SSH service, which was used to permissions.
- A reverse TCP was installed on the target machine, and it is working properly.
- The website visitors are in danger of social engineering attacks by allowing a comment to be posted on the website with a malicious link which will be visible to the users.
- The full users list is available on the webpage.
- It is just a matter of time for peter and Debian passwords to be obtained as well by brute forcing attacks.
- Since the data is centralized and head of IT passwords are easy to detect, there is a highly possibility of data breach.

6 Conclusion

To summarize, it can be reiterated that careful measures were taken to deliver the executive summary part in a simplified language for the company board, and it is advised to take action as soon as possible. However, the technical report was made in a technical language showing the bugs and the vulnerabilities of the company system, and it is of high importance for the company IT team to act quickly as well and work on the vulnerabilities which were exploited successfully in the previous subsection.

3.References

Chai, W., & Ferguson, K. (2021). HTTP (Hypertext Transfer Protocol). *Whatls.com*. https://www.techtarget.com/whatis/definition/HTTP-Hypertext-Transfer-Protocol

Crawley, S. (2017). Multicast DNS (mDNS) vulnerability. *QRIS CLOUD*. https://support.qriscloud.org.au/hc/en-us/articles/115002714663-Multicast-DNS-mDNS-vulnerability

CVE-2023-25690. (2023). *CVE*. https://www.cve.org/CVERecord?id=CVE-2023-25690

CWE-548. (2006). *Common Weakness Enumeration*. https://cwe.mitre.org/data/definitions/548.html

Dhawan, M. (2008). Beware, clickjackers on the prowl. *India Times*. https://web.archive.org/web/20090724155021/http://infotech.indiatimes.com/quickiearticleshow/3543527.cms

Droms, R. (1997). Dynamic Host Configuration Protocol. *RFC*.https://www.rfc-editor.org/rfc/rfc2131#section-2.2

Engebretson , P. (2013). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy 2nd Edition*. Syngress.

Goldshlager, N. (2018). Wordpress XMLRPC DoS. *Rapid7 Vulnerability & Exploit Database*. https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

Haworth, J. (2022). Six-year-old blind SSRF vulnerability in WordPress Core feature could enable DDoS attacks. *The Daily Swig*. https://portswigger.net/daily-swig/six-year-old-blind-ssrf-vulnerability-in-wordpress-core-feature-could-enable-ddos-attacks

Jackson, A. (2022). What Is the Difference Between a Public Key and a Private Key? *Venafi*. https://venafi.com/blog/what-difference-between-public-key-and-private-key/

Kashyap, K., Noor, A., Saraswat, R., & Sharma, V. K. (2021). Learning of Penetration Testing Using Open Source Tools for Beginner. *International Journal of Advances in Engineering and Management (IJAEM). 3(12) p1287-1305*. https://doi.org/10.35629/5252-031212871305

Mamilla, S. R. (2021). *A Study of Penetration Testing Processes and Tools.* Electronic Theses, Projects, and Dissertations.

McAfee. (2022). What Are Tailgating Attacks and How to Protect Yourself From Them. *McAfee*. https://www.mcafee.com/blogs/internet-security/what-are-tailgating-attacks/#:~:text=Tailgating%20is%20a%20type%20of,even%20install%20malware%20on%20computers.

Miller, M. (2022). SSH Key Management Overview & 10 Best Practices. *Beyond Trust*. https://www.beyondtrust.com/blog/entry/ssh-key-management-overview-6-best-practices

Muniz, J., & Lakhani, A. (2013). *Web Penetration Testing with Kali Linux.* Packt Publishing.

OWASP 2017-A6. (2017). *Beagle Security*. https://beaglesecurity.com/blog/vulnerability/x-content-type-options-header-cannot-be-recognized.html

Rosencrance, L., & Bacon, M. (2021). What is social engineering? *TechTarget*. https://www.techtarget.com/searchsecurity/definition/social-engineering

Spacey, J. (2018). What is Root Access. *Simplicable*. https://simplicable.com/IT/root-access

V, E. (2021). What is Keylogger? How Does It Work? *Cyber Security News*. https://cybersecuritynews.com/keylogger/

Viimeksi, P. (2021). Directory indexing attacks. *IBM*. https://www.ibm.com/docs/fi/snips/4.6.0?topic=categories-directory-indexing-attacks

Weidman, G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking.* No Starch Press.

J103563

ORIGINALITY REPORT

9%	6%	1%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Chester College of Higher Education Student Paper	1%
2	louisdl.louislibraries.org Internet Source	1%
3	Submitted to Lincoln College, Lincolnshire Student Paper	1%
4	Submitted to Southern New Hampshire University - Continuing Education Student Paper	1%
5	Submitted to Olivet Nazarene University Student Paper	<1%
6	Submitted to american-intercontinental-university Student Paper	<1%
7	Submitted to Georgetown University Student Paper	<1%
8	Submitted to Kaplan College Student Paper	<1%

9	Submitted to Bournemouth University Student Paper	<1 %
10	Submitted to RDI Distance Learning Student Paper	<1 %
11	Mohammad Ali A. Hammoudeh, Ali Alobaid, Ali Alwabli, Faris Alabdulmunim. "The Study on Assessment of Security Web Applications", International Journal of Interactive Mobile Technologies (iJIM), 2021 Publication	<1 %
12	Submitted to Purdue University Student Paper	<1 %
13	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1 %
14	Submitted to Staffordshire University Student Paper	<1 %
15	www.go-que.com Internet Source	<1 %
16	Submitted to Bury College Student Paper	<1 %
17	Submitted to University of Bedfordshire Student Paper	<1 %
18	www.unfantasmaenelsistema.com Internet Source	<1 %

19	www.mirrorservice.org Internet Source	<1 %
20	www.yumpu.com Internet Source	<1 %
21	dergipark.org.tr Internet Source	<1 %
22	jultika.oulu.fi Internet Source	<1 %
23	www.0x1ceb00da.net Internet Source	<1 %
24	www.igi-global.com Internet Source	<1 %
25	www.thinkmind.org Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

J103563

GRADEMARK REPORT

FINAL GRADE

76/100

GENERAL COMMENTS

Instructor

Engagement -- 2/5

Info. Gathering & Scanning -- 15/20

Vulnerability Assessment -- 19/25

Exploitation -- 18/20

Overall quality -- 22/30

Total: 76/100

PAGE 1

PAGE 2

PAGE 3

Comment 1

The scope is just a standalone PC and not the entire company

Text Comment. Some of the terms here are not relevant for the Executives. Definitions should only focus on the terms used in the executive summary

Text Comment. You should also include an explanation of the ranking

PAGE 4

QM

Label

It is a good practice to label tables (Table x) and figures/images (Figure x) and then refer to them in your discussion appropriately. In this way, instead of saying "From the table above", you can say "From Table x" or "From Table x above".

QM

Vague

Unclear:
When making a point in one of your body paragraphs, one of the most common mistakes is

to not offer enough details. A paragraph without much detail will seem vague and sketchy. A paper is always strengthened when your claims are as specific as possible, The more detailed evidence you offer, the more reference points your reader will have. Remember that you are communicating your argument to a reader who has only your description to go by. Someone who reads your essay will not automatically know what you mean to express, so you have to supply details, to show the reader what you mean, not just tell him or her.

Text Comment. Good

PAGE 5

Text Comment. You have correctly identified engagement considerations. However, you should go beyond what should be considered and provide specifics

PAGE 6

PAGE 7

Text Comment. This is unnecessary since you have already identified the target IP address

Text Comment. Very good

PAGE 8

PAGE 9

Comment 2

OK, but what's the relevance of this?

Comment 3

You would need more than one flag for a Christmas attack

PAGE 10

PAGE 11

Text Comment. Ok

PAGE 12

PAGE 13

PAGE 14

Text Comment. Good

PAGE 15

Text Comment. Good

PAGE 16

Text Comment. Good

PAGE 17

PAGE 18

Text Comment. Good

PAGE 19

PAGE 20

PAGE 21

PAGE 22

Text Comment. A very good attempt, using a wide range of relevant tools. It's good to see contextualised discussions on some of the identified vulnerabilities

PAGE 23

Text Comment. Good

PAGE 24

PAGE 25

Text Comment. Good

PAGE 26

Text Comment. Good

PAGE 27

PAGE 28

PAGE 29

Text Comment. Good

PAGE 30

Text Comment. Excellent

PAGE 31

PAGE 32

KNOWLEDGE	Distinction
Demonstration of knowledge and understanding of subject matter, tailoring of discussion to case study and coverage	
DISTINCTION	Extensive subject knowledge, thorough coverage of topic, focused use of detail and examples. Excellent understanding of case study.
MERIT	Breadth and depth of coverage, accurate and relevant in detail. Well tailored to case study.
PASS (STRONG)	Content generally relevant and accurate, most central issues identified; basic knowledge sound but may be patchy.
PASS (THRESHOLD)	Fairly basic knowledge, limited consistency of depth and accuracy of detail; not all aspects addressed, some omissions.
FAIL	Contains very slight detail; content may be thin or irrelevant; issues poorly identified.
FAIL	Knowledge base extremely weak; content almost entirely irrelevant or erroneous.

COGNITIVE	Distinction
Clarity of discussion, coherency, perception, articulation of views, thoughtful interpretation	
DISTINCTION	Excellent perception, critical insight and interpretation. Very good depth and breadth of critical analysis; sustained, thorough questioning informed by theory.
MERIT	Perceptive, thoughtful interpretation. Consistent development of critical analysis and articulation of views; coherently presented.
PASS (STRONG)	Sound explanation; this may be partly descriptive and factual; ideas tend to be stated rather than developed. Some attempt at critical analysis using theory; may be limited and lack consistency or conviction.
PASS (THRESHOLD)	Some interpretation or insight; may be largely descriptive, or superficial; over-reliance on narrative. Some evidence of rationale; minimal attempt to examine strengths and weaknesses of an argument
FAIL	Little attempt to interpret material, or merely descriptive; explanations may be muddled at times. Limited breadth and depth of analysis, inadequate critical skills; shallow and superficial.
FAIL	Any attempt at discussion limited to personal view; no discernible insight. Isolated statements indicating lack of thought

PRACTICAL	Distinction
Technical understanding and use of materials. Breadth and depth of material, academic writing, formatting and strength of argument.	

DISTINCTION	Thorough technical understanding and judgement; excellent level of competence in use of materials and appropriate application of working processes and techniques.
MERIT	Accurate technical understanding and judgement; good level of competence in use of materials and appropriate application of working processes and techniques.
PASS (STRONG)	Mostly accurate technical understanding and judgement; satisfactory level of competence in use of materials and appropriate application of working processes and techniques.
PASS (THRESHOLD)	Adequate though only partially accurate technical understanding and judgement; adequate level of competence in use of materials and application of working processes and techniques.
FAIL	Slight technical understanding and judgement, with inaccuracies; lack of competence in use of materials and erroneous application of working processes and techniques.
FAIL	Almost no technical understanding or judgement; serious incompetence in use of materials and erroneous application of working processes and techniques.

COMMUNICATION — Merit

Presentation, vocabulary and style, spelling and punctuation

DISTINCTION	Near perfect spelling, punctuation, punctuation, presentation and syntax.
MERIT	High standard of accuracy in spelling, punctuation, punctuation, presentation and syntax.
PASS (STRONG)	Overall competence in spelling, punctuation, punctuation, presentation and syntax, although there may be some errors
PASS (THRESHOLD)	Inaccuracies in spelling, punctuation, presentation and syntax do not usually interfere with meaning
FAIL	Many errors in spelling, punctuation, presentation and syntax
FAIL	Many serious errors of even basic spelling, punctuation, presentation and syntax.

REFERENCING — Merit

DISTINCTION	All sources acknowledged and accurately presented
MERIT	Sources acknowledged and accurately presented
PASS (STRONG)	Sources acknowledged and referencing mostly accurate
PASS (THRESHOLD)	Sources acknowledged; references not always correctly cited/presented
FAIL	Referencing incomplete or inaccurate

FAIL	Referencing inaccurate or absent