Exploitation Project

Table of Contents

Exploitation 2
Risk Analysis of the System 9
1.Apache 2.4.41 (Root Directory Listing Vulnerability) 10
2. Outdated Vim Version (v 8.1) 11
3. Libre Office (End of life version Installed) 12
4. File history enabled: 13
5. Old Operating System (Ubuntu 20.04.4 LTS) 14
6. Mozilla Thunderbird (Version 78.14) 16
7. Infected Mozilla Firefox 17
8. Password Never Expires 18
9 Privilege Escalation 19
10 Automatic Software Execution (Using Removable Media) 21
11 Connectivity Checking Vulnerability 22
12. Longer Screen Display Timeout 23
13 No Hard disk encryption 24
14 Insecure Bash History 25
15 Transmission Version 2.94 (Use After Free Vulnerability) 27
16 Old Python Version (3.8.10) 28
17. SELinux not Installed 29
18 Cups Service Vulnerability 30
19 No BIOS Password 31
20.Insecured Root Permissions 32
References 33

Exploitation

To begin with, I used netdiscover to find the “punisher” on my network and I found that the IP address of the punisher is 192.168.1.5. Here is the screenshot:

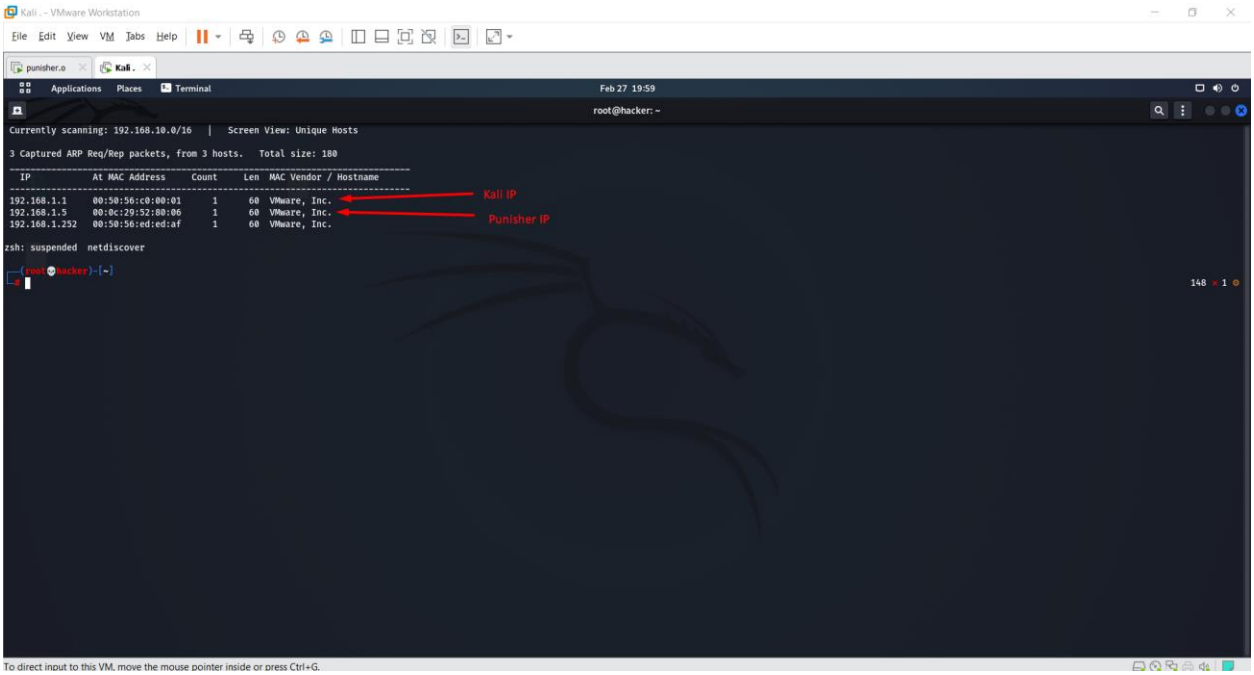
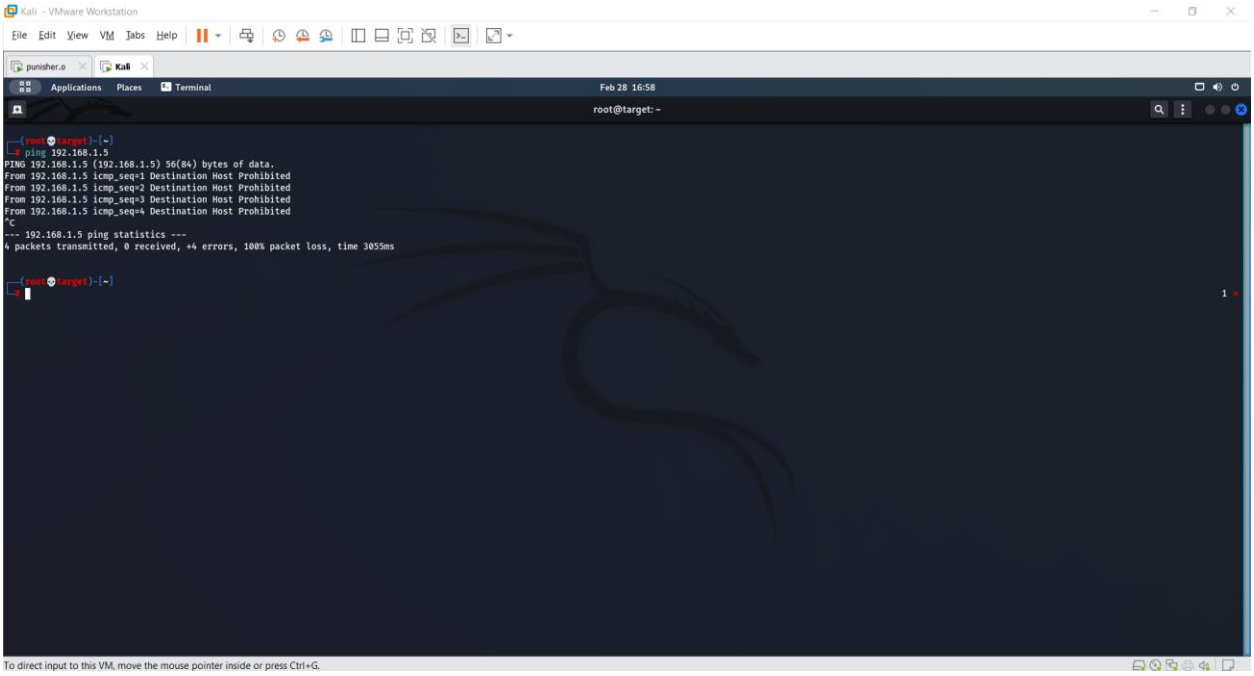


Figure 1: Punisher Discovery

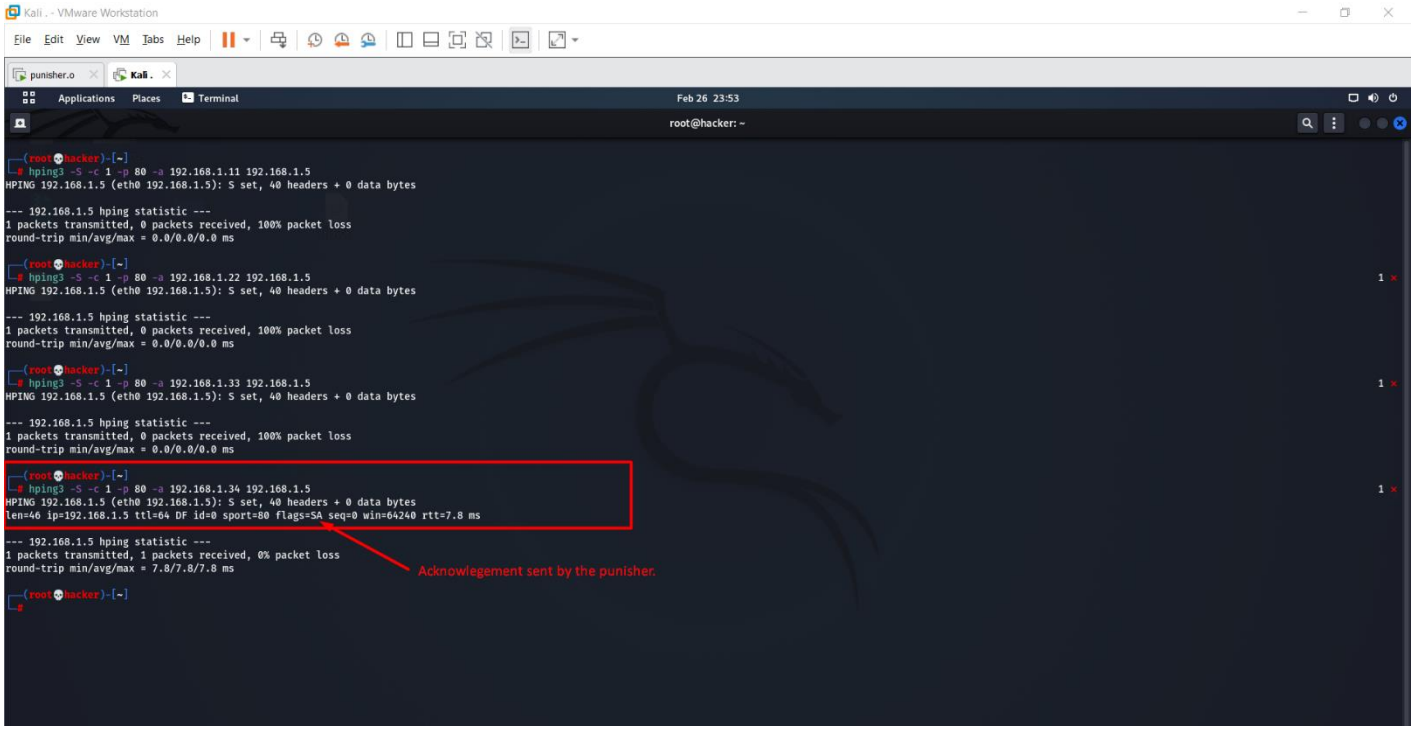
After that I tried to ping the machine, but it was showing “HOST PROHIBITED”. Below is the screenshot attached:



From this part I came to know that definitely a firewall is restricting the Ping. So, a quick thought about spoofing the IP address came to my mind and I used the following command

```
hping3 -S -c -p 80 192.168.1.34 192.168.1.5(Punisher IP)
```

Using the hping3 I sent a SYN packet to the Punisher on port 80 using the IP addresses 192.168.1.X (X=2,3,4,5…….252). Finally, after making some unsuccessful syn request's, IP 192.168.1.34 got acknowledgement from the punisher see the screenshot attached below:



Acknowledgement for connection by punisher (By spoofing IP 192.168.1.34)

Throughout the whole process I was taking Wireshark into use in order see the packets sent by spoofed IP's travelling across the network.

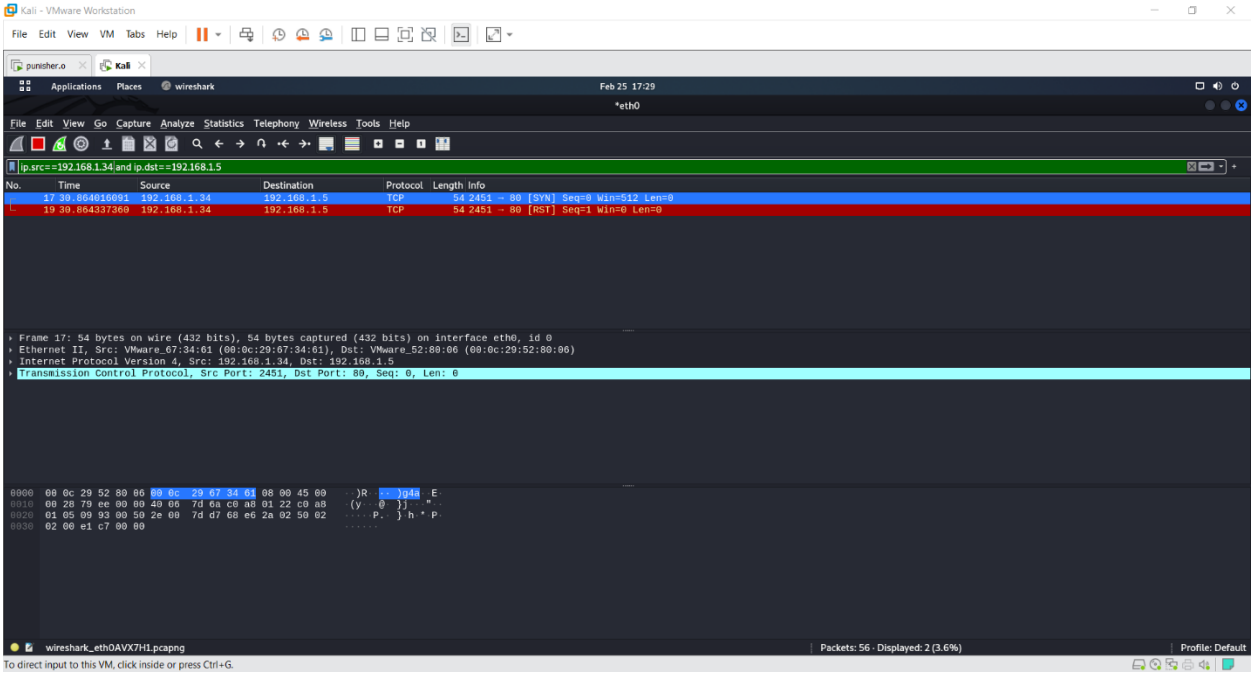
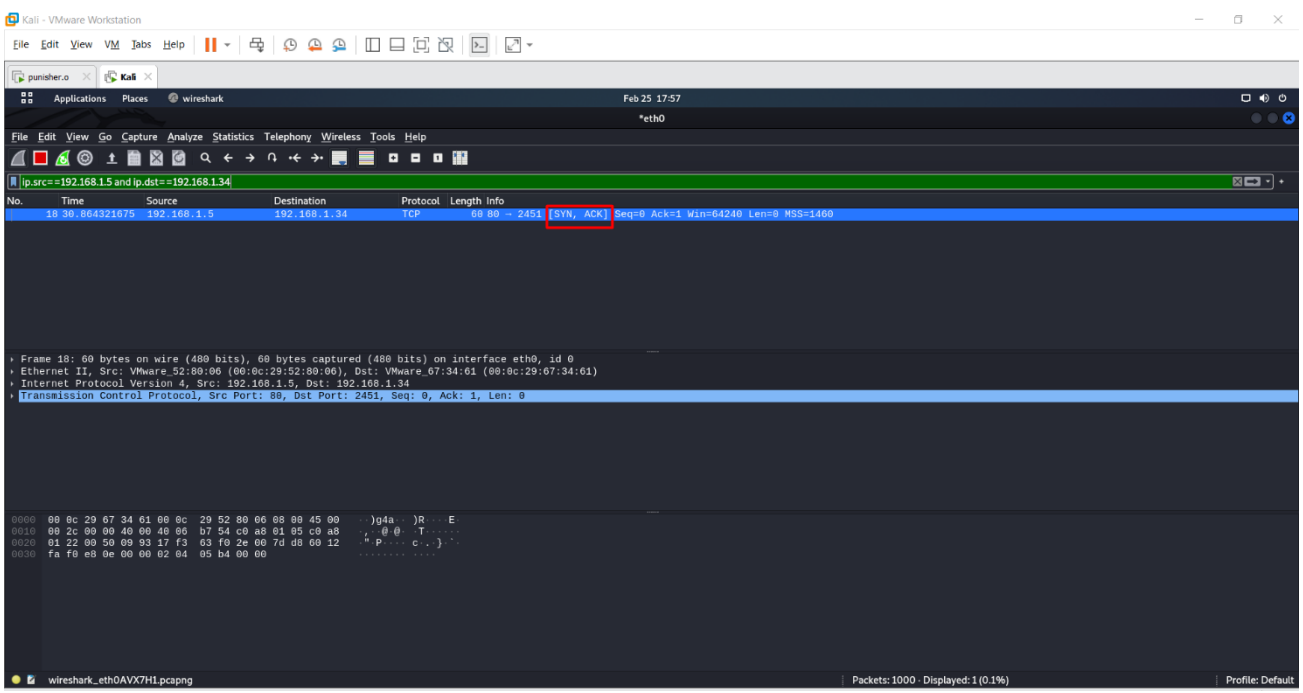


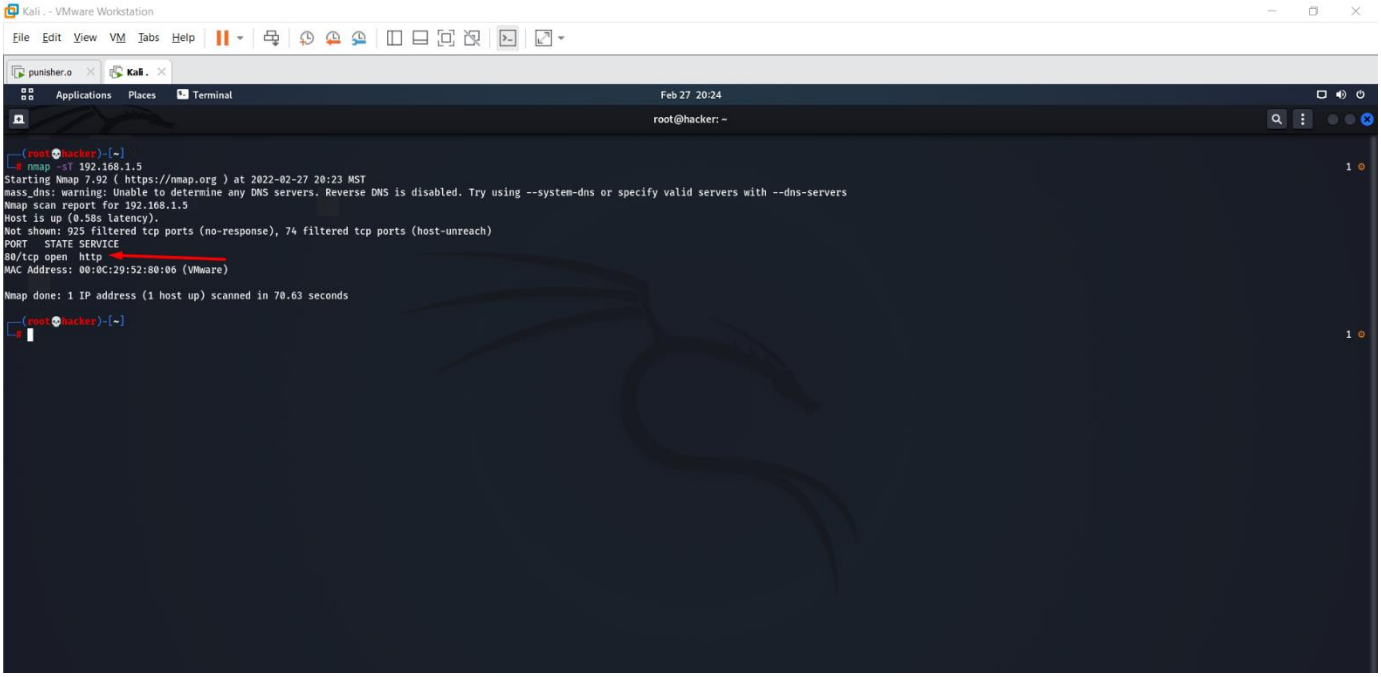
Figure 2: SYN request being sent by the spoofed IP

Here I have used the command IP.src==192.168.1.5 and IP.dest==192.168.1.34. It is clearly visible that SYN, ACK is being sent by the target (Punisher). In other words, the acknowledgement of the connection is sent by punisher machine which confirms that 192.168.1.34 is the only IP which can pass through the firewall for port 80.

Here is the screenshot showing the acknowledgement of the connection from punisher.



Moving ahead I used the Nmap to search for open ports on the machine and I came to know that port 80 is open and http service is running on it.



So, Using the Mozilla Firefox I tried to access the web server. I typed in the IP address of the punisher (192.168.1.5) in the search bar and after hitting the enter key, the output was shocking! Actually, web server was having 2 files named "Danger.zIP" and “hitlist”. (Refer to the screenshot attached below)

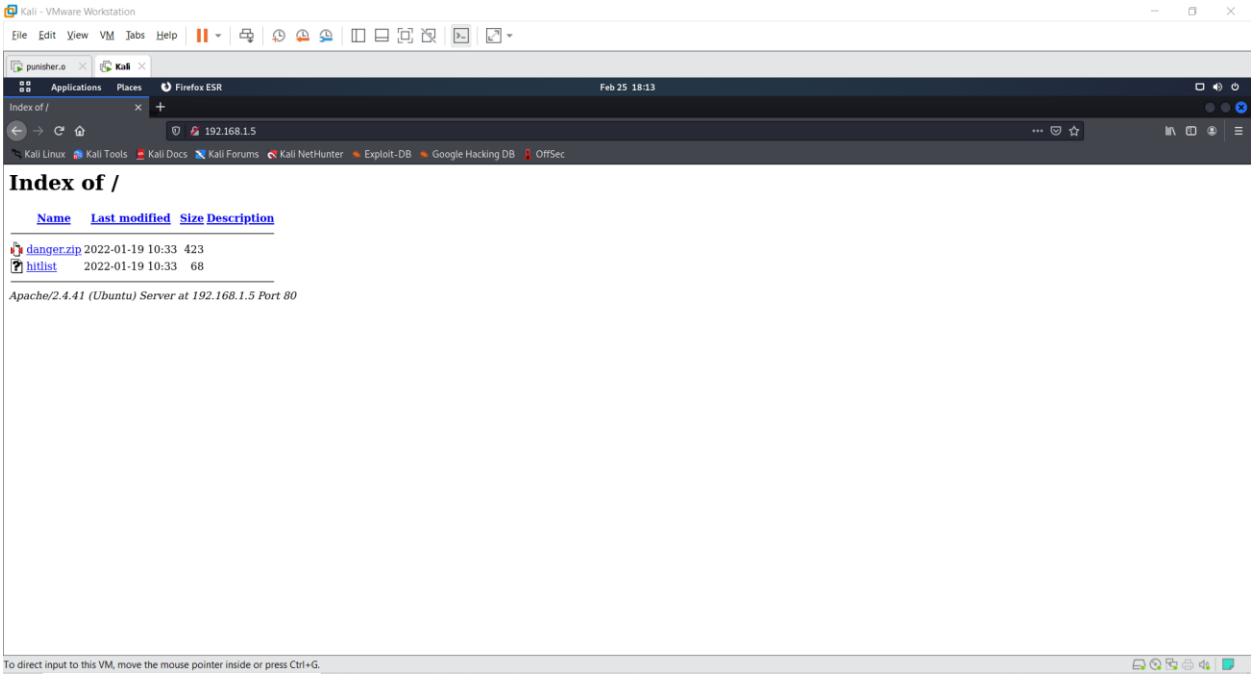


Figure 3: Directories listed on the server

I downloaded the danger.zIP in kali and it was containing confidential.txt. I tried to access it; however, it was password protected.

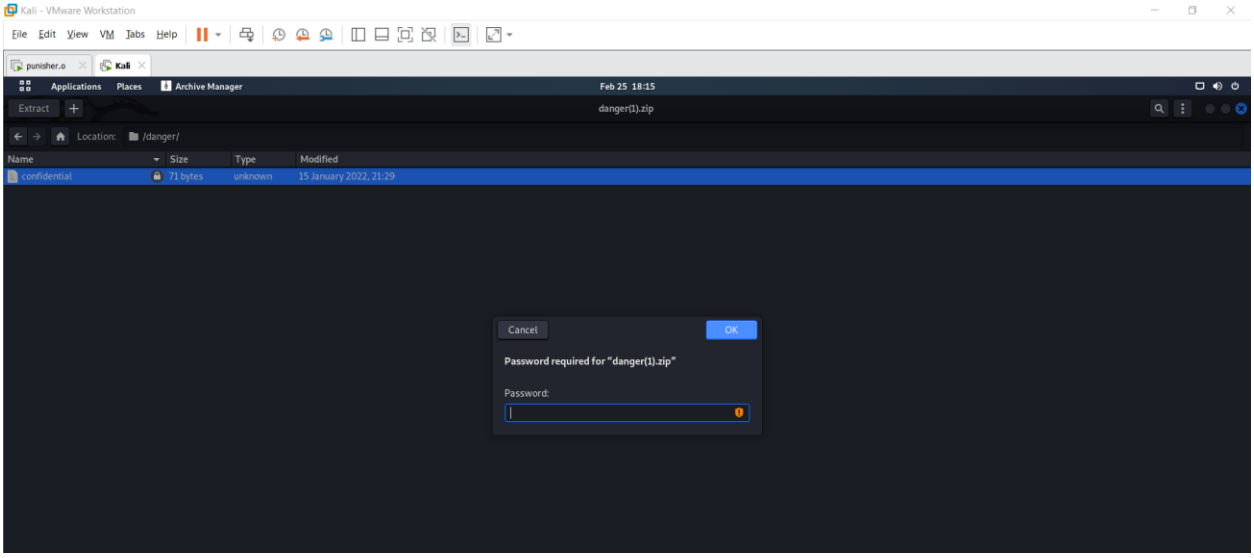


Figure 4: Password requested

Now, here was the beginning of another struggle to crack the password of the danger.zIP file. After making few unsuccessful guesses of the password for few minutes, I realized about the file "hitlist". It was having few words which could be the possible password and I was correct, and the password of the zIP file was one of the strings in the "hitlist" and password was "bubbles". (Refer to the screenshot below):

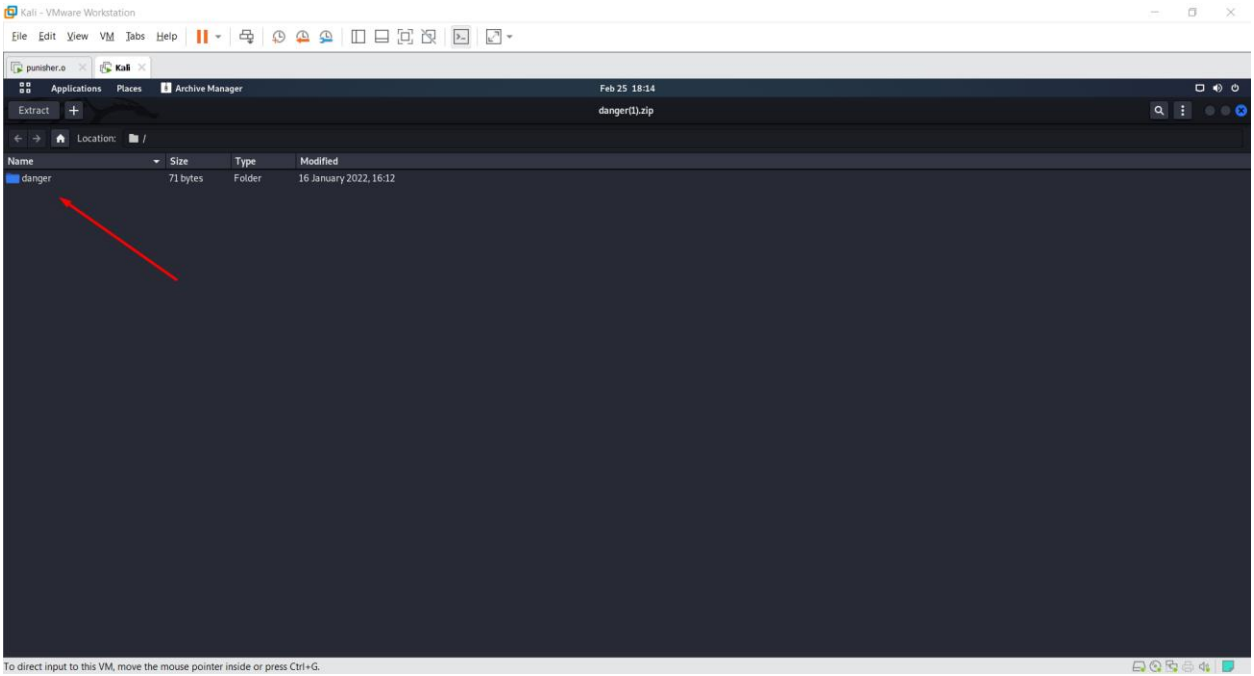


Figure 5: Danger.zIP file

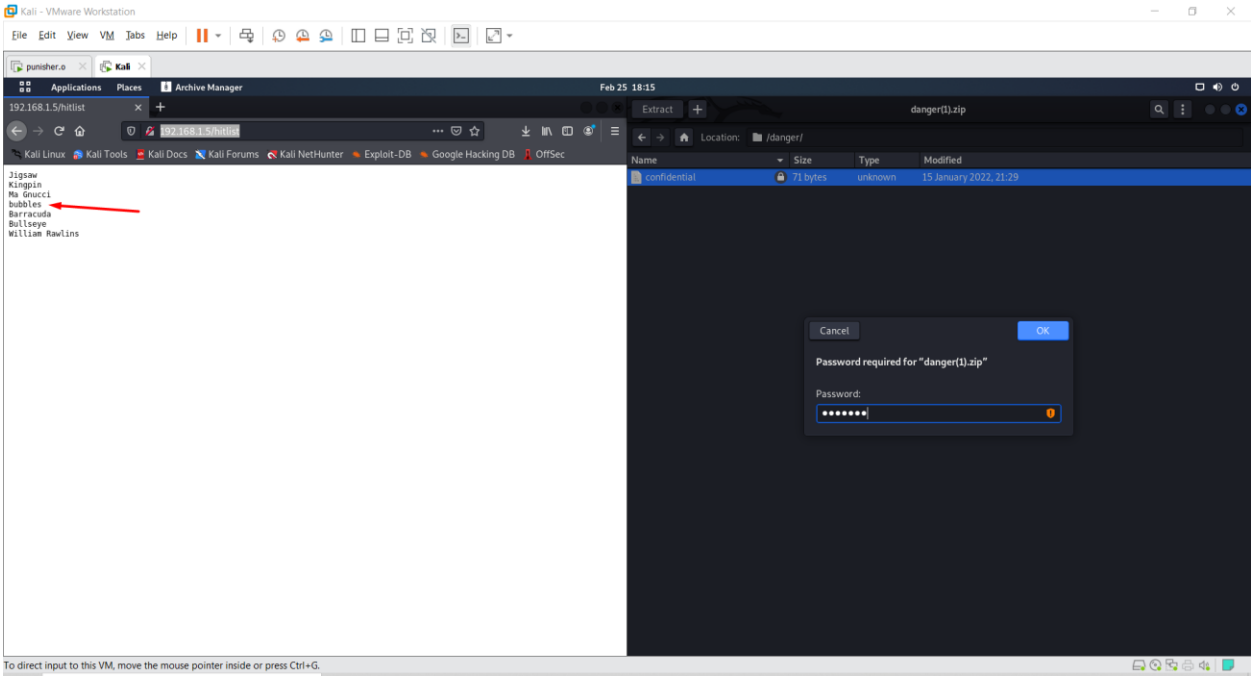


Figure 6: Password required for danger.zIP("bubbles")

After entering the password, output of the confidential.txt provided me with the login credentials of the Frankcastle. Here is the screenshot attached:

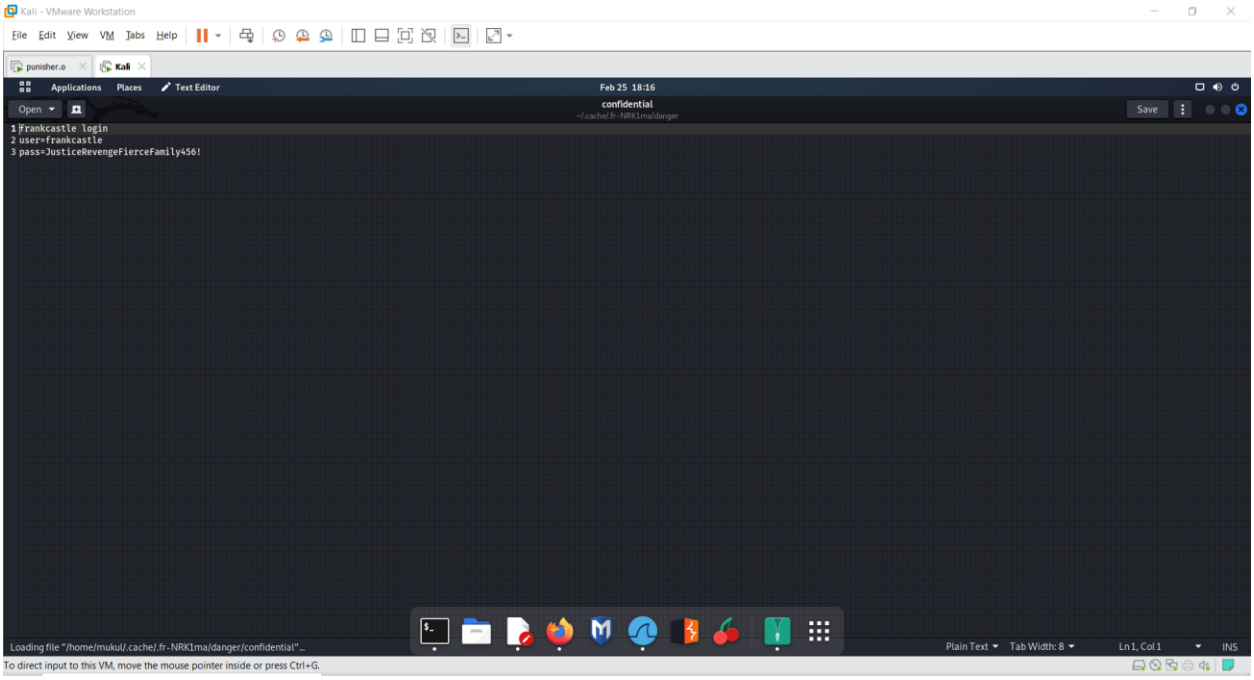


Figure 7: Login Credentials of Frankcastle

Proceeding further I logged into the machine using the Frankcastle credentials. Now I had to find the user.txt and the root txt. User txt was quite easy since it was present on the desktop of the Frankcastle. (Screenshot attached below)

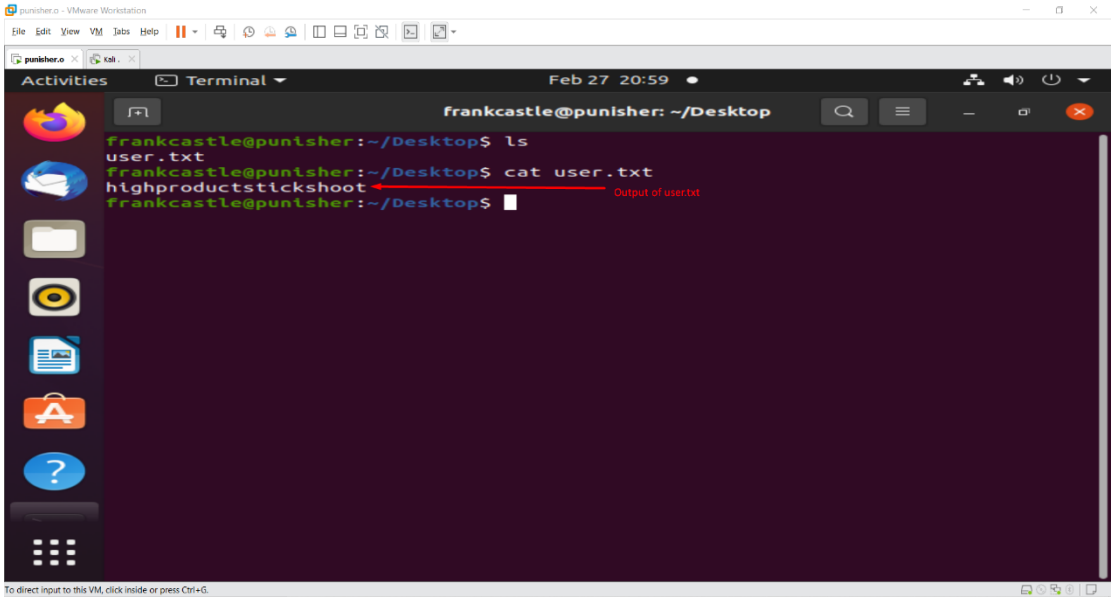


Figure 8: User .txt

However, talking about the root flag, It was quite simple but the logic behind this was quite interesting. Having a look at /etc/sudoers, provides the information that all of the users have root privileges. (Also, this can be seen as a very serious vulnerability because any newly added user on the machine can have access to the sensitive data.) Frankcastle is also not an exception and for entering the root privileges I simply provided the password of user "Frankcastle". Then I went to root desktop and found the root flag which can be clearly seen in the below given screenshots:

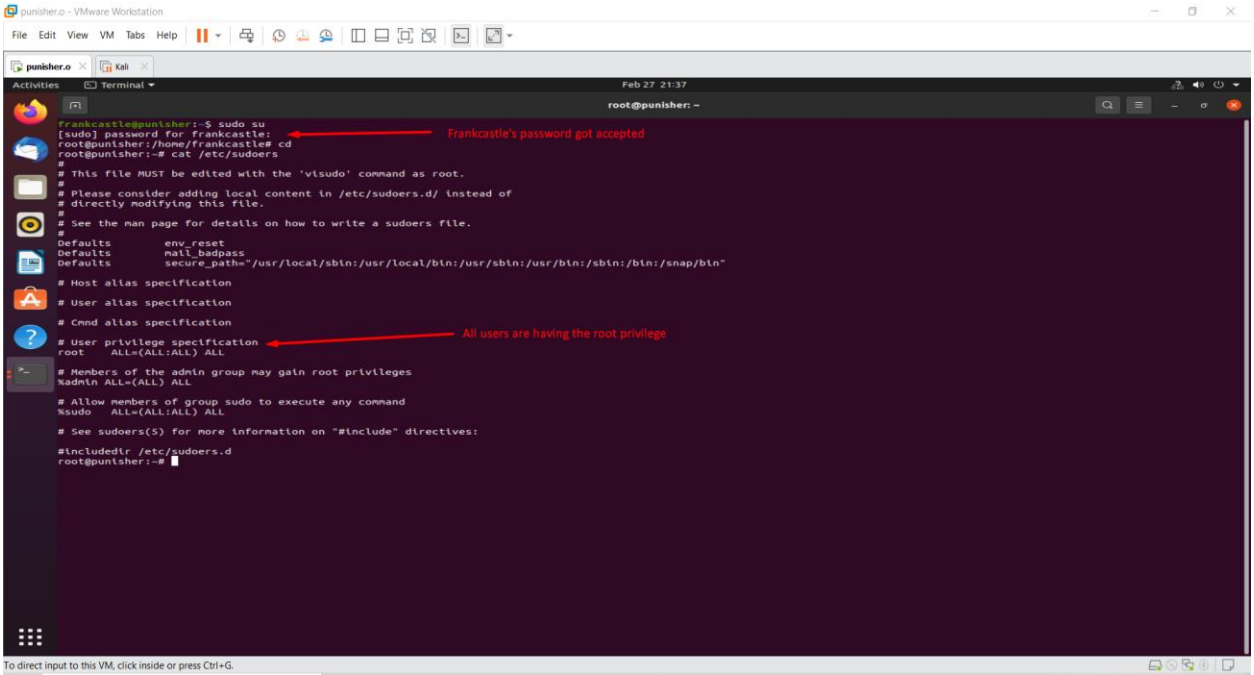


Figure 9: Output of /etc/sudoers file

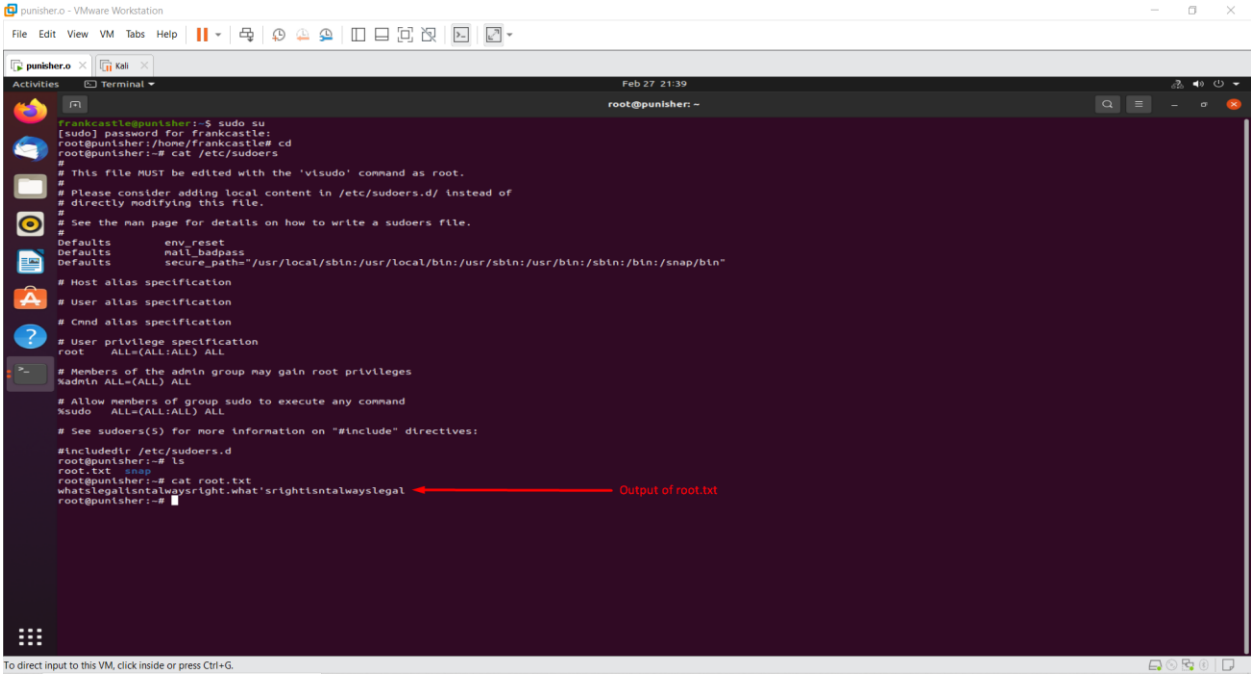


Figure 10: Root.txt

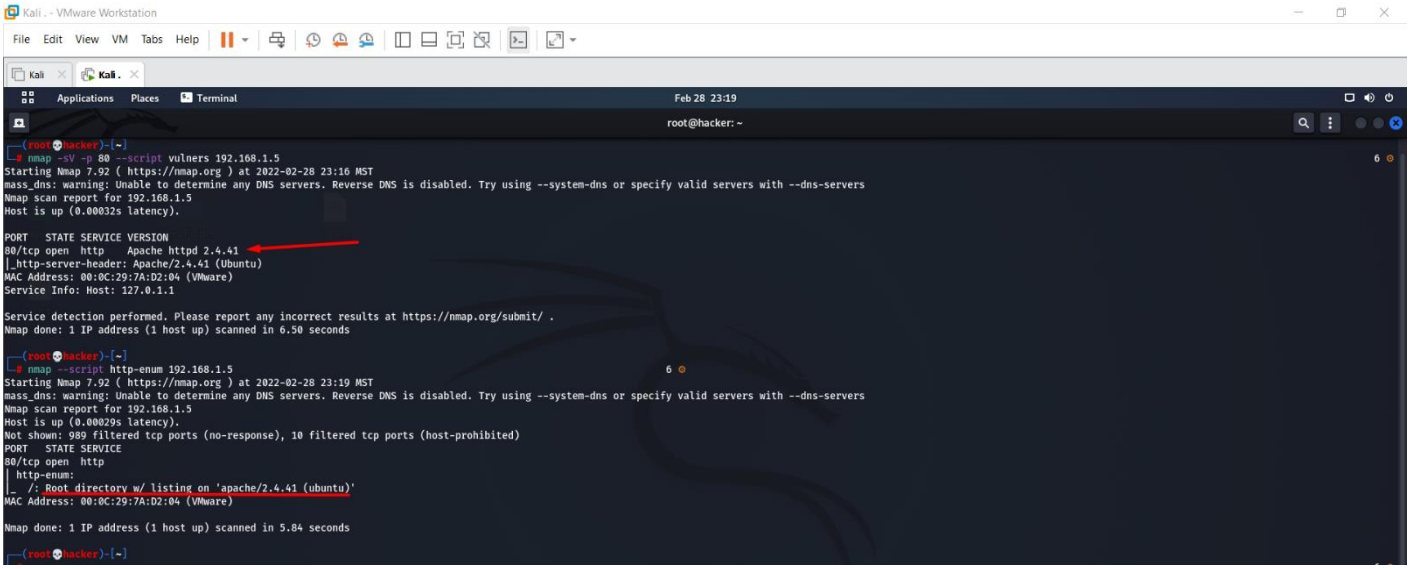
Risk Analysis of the System

After gaining the access to the system now it was time to explore the vulnerabilities which the punisher was having. I tried looking for OS Hardening techniques and also used minimal Nmap scrIPt to find out the vulnerabilities. Some of them are mentioned below: -

- nmap 192.168.1.5 --scrIPt=vulners.nse -sV
- nmap --scrIPt http-enum 192.168.1.5

Below is the list of 20 Vulnerabilities existing in punisher:

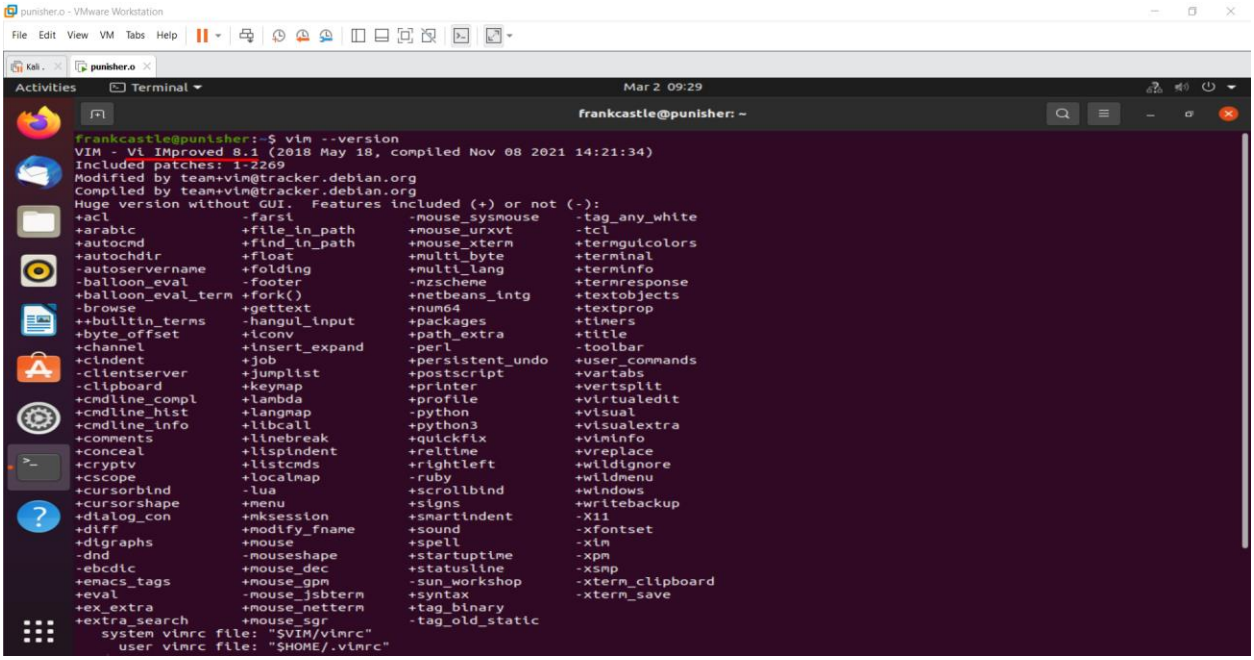
1.Apache 2.4.41 (Root Directory Listing Vulnerability)



When I run the “http-enum” scrIPt on the punisher then I came to know that it is having 2.4.41 version installed which is quite old and insecure in comparison to the latest Apache version 2.4.46. Having 2.4.41 version of Apache can lead to Root Directory listing. In other words, a hacker can basically have a look at the files (especially sensitive data residing in root directory) which are having much more sensitive information like passwords, server’s configuration files etc. If somehow hacker is able to look into the content of the root directory and it is not much secure, then chances of modifying the data like changing access rights of the users exists. This can result hacker in gaining the access to the web server. To put it in a nutshell, web server’s integrity and data security will be compromised.

This vulnerability can be fixed by updating the Apache server to the latest version (2.4.46). One can also disable the directory browser listing by changing the configuration file of the httpd and can simply add `Options All -Indexes` in the .htaccess file **[1]**. After making the changes then same file should be saved and uploaded.

2. Outdated Vim Version (v 8.1)



Latest version of Vim is 8.2 whereas machine is having the old version (v 8.1) of the Vim, which can have some serious consequences on the security of system. After doing some research on the internet I came to know that having an old version (including v8.1) of Vim can lead to the OS command injection. In OS command injection. [2]. OS command injection gives a user privilege (In our case it can be frank castle) to execute a malicious code in Vim. It was discovered that the main reason behind this vulnerability is a feature called “Modlines” [3]. Basically, Modlines allows the user to define a variable for a specified file. Adding to it, according to Common Vulnerability Score, this vulnerability is having a score of 5.3. Arminius [3] discovered this vulnerability and posted a proof of concept on the GitHub which also shows that chances of gaining the reverse shell access using this vulnerability is also possible.

Proof of concept:

https://github.com/numirias/security/blob/master/doc/2019-06-04_ace-vim-neovim.md [4]

To get rid of this vulnerability, “Modeline” feature of Vim can be turned off. In my opinion most effective solution will be upgrading to the latest Vim Version (V 8.2). Also, there are few updates available for the vim version 8.1 which can be downloaded from the official website of vim. Applying the upper mentioned fixes can have a significant impact on increasing the security of the system.

3. Libre Office (End of life version Installed)

Punisher is running a very old version (6.4.7.2) of LibreOffice. Moreover, an interesting thing to note here is 6.4.7.2 is now no longer supported and reached the end of life on 30 November,2020.

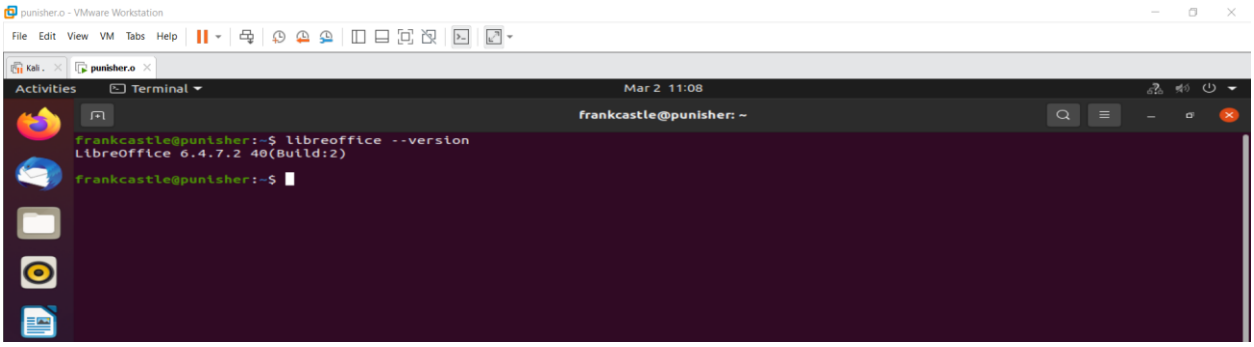
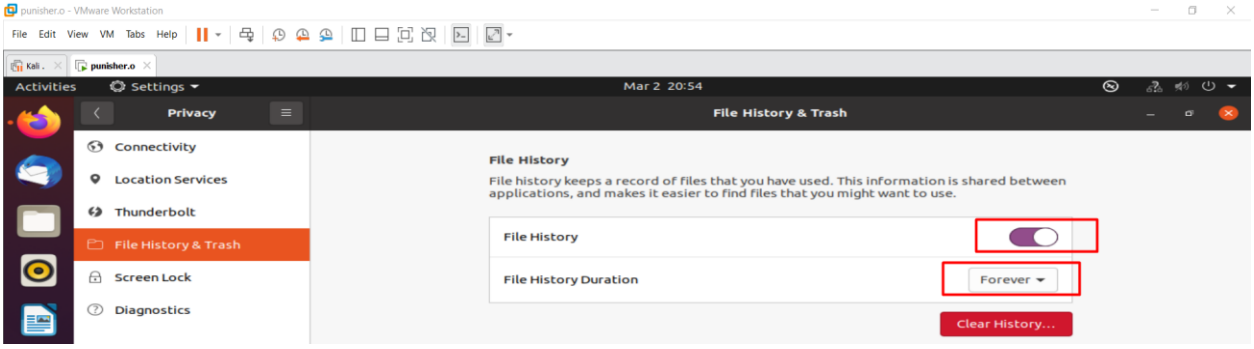


Figure 11: Version 6.4.7.2 Installed

Using an end-of-life LibreOffice can possess serious security threats to the operating system because no patches are now available from vendor. To be specific LibreOffice version 6.4.7.2 is vulnerable to CVE 2020-12801**[5].** This vulnerability revolves all around the encryption of a document. Moving further, LibreOffice Version 6.4.7.2 possess threat to the encryption of a file. In other words, if a user is working on an encrypted document in LibreOffice (v 6.4.7.2) and all of the sudden it shuts down then the file will be auto saved. There is no guarantee that the file format after recovering the file complies with the accepted ODF file format of LibreOffice. If it complies with the default ODF file format, then there is no threat to the document but if it doesn't then the document will be saved unencrypted. However, back in mind a user is assured that document is encrypted, and no one can access it but on the other hand if the system is compromised then attacker can easily access the so called "encrypted file”. This vulnerability can be avoided by installing the latest version of LibreOffice as it contains latest patches and is much more secure than any previous version of the application.

4. File history enabled:



Fourth vulnerability is that File History is turned on. This can have a detrimental impact on the overall security of the system. For example, if by any way hacker penetrates into the system and want to look for the files which have been lastly modified then he/she can easily do it by having a look at the file history. Moreover, another important thing to notice here is the “File History Duration”. It is set to forever which is even more dangerous because then hacker can see the file accessed since the machine was taken into use. This vulnerability can be mitigated by turning the file history off. If it is necessary to turn on the file history then the duration of the file history should be set to 1 or 7 days. If someday machine is hacked, and then hacker will not be able to have a look at the older file history (From beginning) instead few latest files will be visible in the history. In other words, hacker will have to spend a quality time with the machine to find out the files accessed a long ago.

5. Old Operating System (Ubuntu 20.04.4 LTS)

Punisher is running Ubuntu 20.04.3 LTS (Refer to the screenshots attached below) and in my opinion this is one of the biggest threats to the it because with this version of ubuntu several vulnerabilities are associated. I referred to ubuntu official website [5] to have look at the vulnerabilities associated with the same. Out of 100's of vulnerabilities here I am going to mention about 2 of them and they are listed below:

- GNU C Library vulnerability **[5]**: - This vulnerability revolves around the GNU C Library and most of them are just because of inappropriate handling of input functions. For example: - there is a feature called as "iconv" in GNU c library, responsible for conversion for a multibyte character [6] and it has been observed by security professionals that iconv was inappropriately dealing with the series of inputs. Adding to it just by utilizing this exploit hacker can cause the denial of service on the system thus impacting the machine. Appropriate packages of libc can be downloaded and installed in order to mitigate this issue.
- Denial of Service using php:**[5]** -In 20.04.3 version of ubuntu, chances of providing some arbitrary input to php can help an attacker to cause a denial-of-service attack. This vulnerability can be dealt with by installing few php package version available on official ubuntu website.

To be on the safer side, it is recommended to upgrade to Ubuntu 20.04.4 LTS. This will help in at least overcoming the vulnerabilities existing in the 20.04.3. Also, regular updates should be allowed.

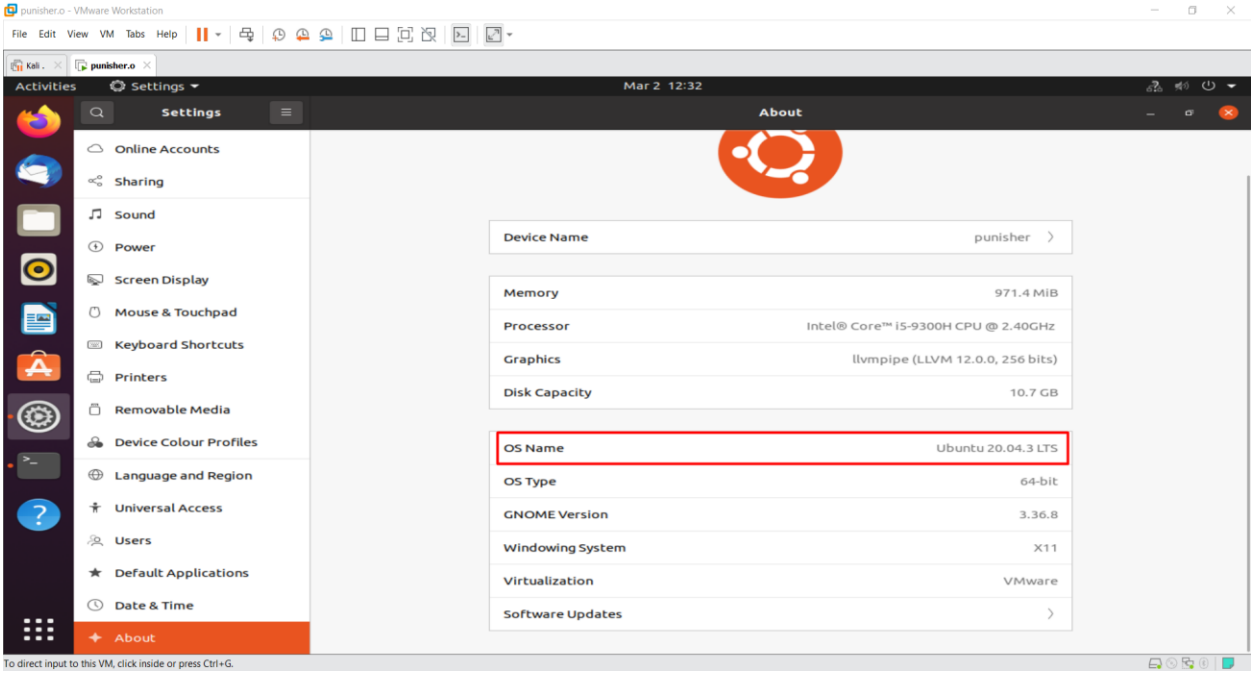
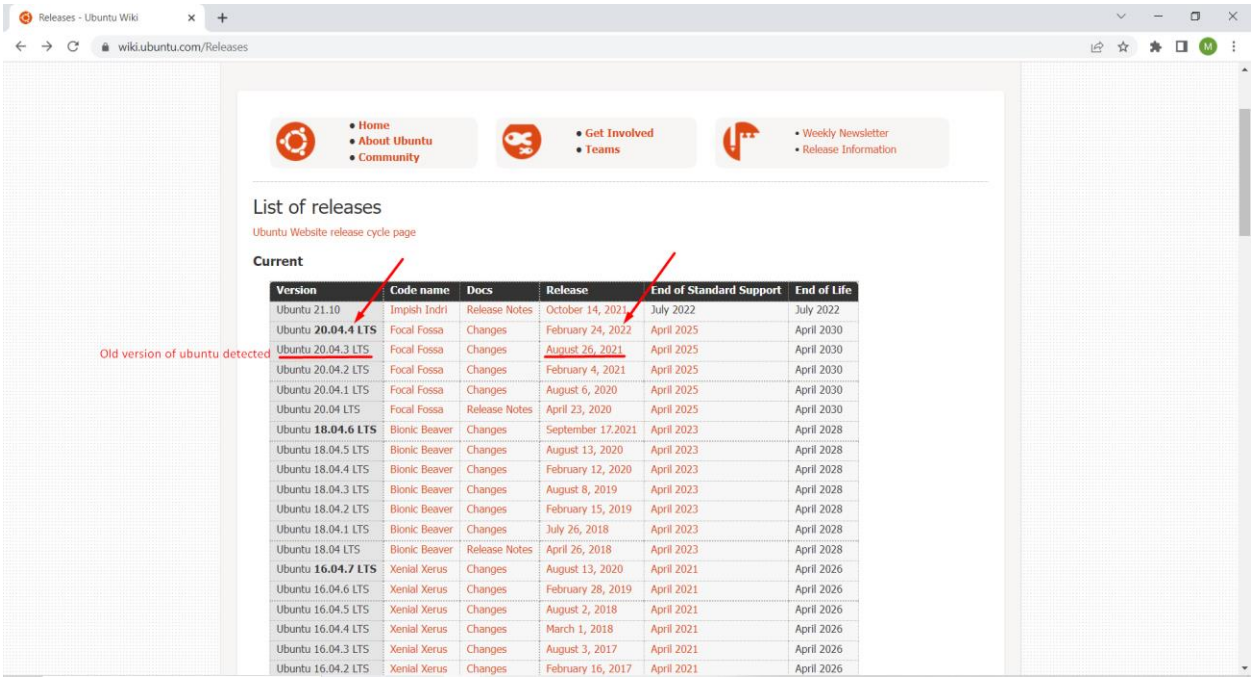


Figure 12: Ubuntu 20.04.3 LTS being used by punisher



Version	Code name	Docs	Release	End of Standard Support	End of Life
Ubuntu 21.10	Impish Indri	Release Notes	October 14, 2021	July 2022	July 2022
Ubuntu **20.04.4 LTS**	Focal Fossa	Changes	February 24, 2022	April 2025	April 2030
Ubuntu 20.04.3 LTS	Focal Fossa	Changes	August 26, 2021	April 2025	April 2030
Ubuntu 20.04.2 LTS	Focal Fossa	Changes	February 4, 2021	April 2025	April 2030
Ubuntu 20.04.1 LTS	Focal Fossa	Changes	August 6, 2020	April 2025	April 2030
Ubuntu 20.04 LTS	Focal Fossa	Release Notes	April 23, 2020	April 2025	April 2030
Ubuntu **18.04.6 LTS**	Bionic Beaver	Changes	September 17.2021	April 2023	April 2028
Ubuntu 18.04.5 LTS	Bionic Beaver	Changes	August 13, 2020	April 2023	April 2028
Ubuntu 18.04.4 LTS	Bionic Beaver	Changes	February 12, 2020	April 2023	April 2028
Ubuntu 18.04.3 LTS	Bionic Beaver	Changes	August 8, 2019	April 2023	April 2028
Ubuntu 18.04.2 LTS	Bionic Beaver	Changes	February 15, 2019	April 2023	April 2028
Ubuntu 18.04.1 LTS	Bionic Beaver	Changes	July 26, 2018	April 2023	April 2028
Ubuntu 18.04 LTS	Bionic Beaver	Release Notes	April 26, 2018	April 2023	April 2028
Ubuntu **16.04.7 LTS**	Xenial Xerus	Changes	August 13, 2020	April 2021	April 2026
Ubuntu 16.04.6 LTS	Xenial Xerus	Changes	February 28, 2019	April 2021	April 2026
Ubuntu 16.04.5 LTS	Xenial Xerus	Changes	August 2, 2018	April 2021	April 2026
Ubuntu 16.04.4 LTS	Xenial Xerus	Changes	March 1, 2018	April 2021	April 2026
Ubuntu 16.04.3 LTS	Xenial Xerus	Changes	August 3, 2017	April 2021	April 2026
Ubuntu 16.04.2 LTS	Xenial Xerus	Changes	February 16, 2017	April 2021	April 2026

Figure 13: Figure: -Old Version of Ubuntu

6. Mozilla Thunderbird (Version 78.14)

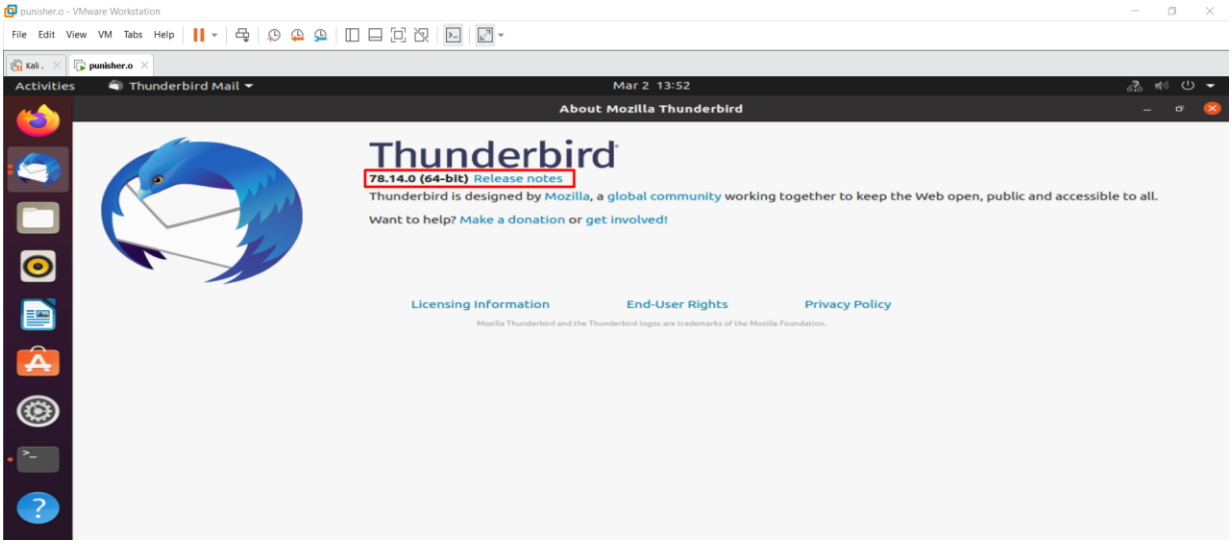


Figure 14: Thunderbird Version 78.14.0

A bit outdated version (v 78.14) of Thunderbird is installed which can lead to memory corruption. After brainstorming on internet, the conclusion came out to be that Thunderbird versions 78.13 and 91.1 are prone to memory corruption vulnerability (CVE 2021 38493). This vulnerability is having a score of 8.8 according to CVE. Basically, some minor changes in the memory were noticed by Mozilla Developers and at the end they reached out at a conclusion that an arbitrary code can be executed using this vulnerability. Also, other vulnerabilities are mentioned below:

- Bypassing the Restrictions: [12] This vulnerability is having a score of 7.7 according to CVE.In this vulnerability attacker try to fool the client by making the client install an extension of a browser. Most important thing here to note is that extension being installed by the client will be of a specific type and during the auto updation, the permission will be automatically granted to the extension. In this way hacker gets appropriate permission to access the files on the system.
- Lacking the alerts for Risky Processes: This vulnerability is quite common in the Thunderbird (v 78.14). What happens in this vulnerability is that when a user downloads a file (Modified by a hacker) and try to simply drag and drop it in a drive or on desktop then file changes to a malicious scrIPt and when unknowingly that the file contains a malicious scrIPt then system gets compromised. Now this situation could be avoided if Thunderbird automatically provided the user a warning regarding that malicious file.

A quick fix for all of the above-mentioned vulnerabilities will be updating to the latest version of Thunderbird which provides much security as against previous versions. Another approach can be installing more secure software like Spike, Outlook etc.

7. Infected Mozilla Firefox

Seventh vulnerability which I found is that Mozilla Firefox (version 96.0) is infected with CVE 2022-22743 and CVE 2022-22745.[8] Here is a brief about both of the vulnerabilities "-

- Full Screen Browser Window Spoofing (CVE 2022 22743): - This vulnerability relies on an iframe [8]. An Iframe is a document residing into another document into a website. When iframes are being used to go to another webpage's in a full screen mode then chances are there that tabs poisoned by attacker doesn't lets the user to escape from the full screen mode.

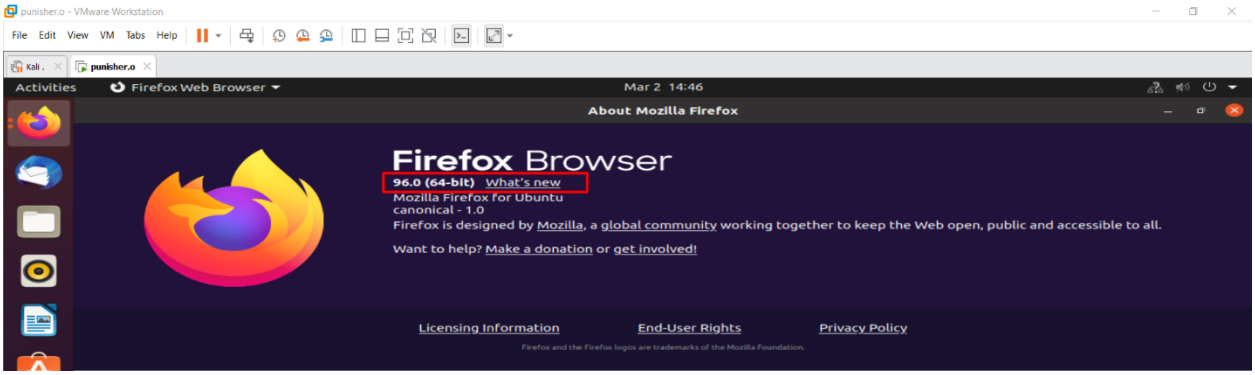


Figure 15: Firefox 96.08

- Security Policy Violation (CVE 2022-22745): -This vulnerability is all about playing with the frames of a URL. In simple words frame helps in presenting the content on the website irrespective of the containers [7]. Additionally, there is a policy called HTTP content security policy which is basically responsible for specifying the [6] primary URL having capability to frame the existing content and when this policy gets violated then a series of event can trigger thus resulting into a cross origin URL leak.

A solution to overcome this vulnerability can be updating the Firefox browser. By updating Mozilla latest patches will be installed which will help in reducing the risk to system to a significant extent. However, other web browsers having advanced security can also be considered.

8. Password Never Expires

Never expiring passwords for root and frankcastle are one of the biggest security threats. If by any chance password of either root or frankcastle is compromised then chances of accessing the sensitive information present in the system are much higher because for an unlimited period of time, hacker can easily exploit the machine but on the other hand if password is going to expire in X (20,30 etc.) days then hacker can only access the data for a limited period of time. Yes, it is true that 20-30 days is a huge time period for a hacker to exploit the system, but it is far better than leaving the machine accessible for an unspecified amount of time.

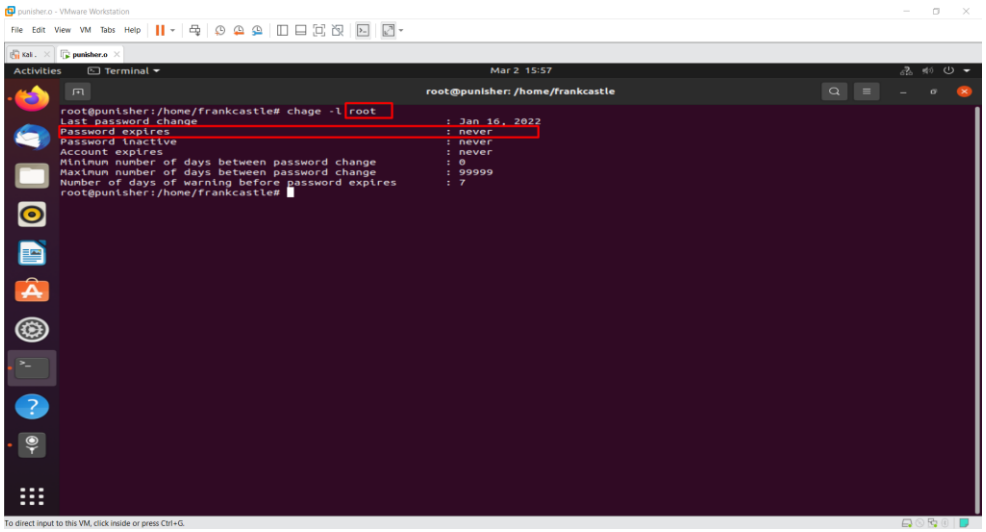


Figure 16: Password of root never expires

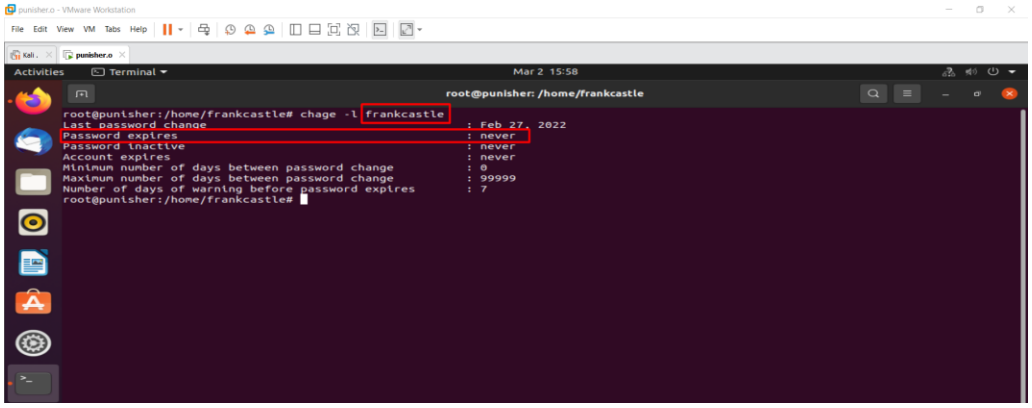


Figure 17: Password never expires for frankcastle

To fix this issue password expiry should be set on every user whether it is a root or whether it is frankcastle. Below given command can be used to specify the password expiry date:[9]

```
sudo chage -d YYYY-MM-DD Username    [9]
```

Moreover, if password complexity practice is followed then it will be cherry on the cake. For example, if a password consists of uppercase, lowercase, special characters, numbers etc then hacker is going to take a longer time to guess the password of a user. Whereas a simple password can be easily cracked.

9 Privilege Escalation

Running the `groups frankcastle` command, I came to know that frankcastle is a member of sudo group which look something is fishy. Being a member of sudo group frankcastle have the privilege to execute all command in the terminal. This vulnerability is also referred as CVE-2019-14287.Using a small word sudo attacker or any other user can bypass the security policy of the system and can modify the settings. Here thing is not that frankcastle is member of sudo, in fact point to note here is that what are other vulnerabilities which can be brought in by frankcastle.

For example, Frankcastle can

- Play with the passwords of users present
- Can setup a SSH connection
- Can open the vulnerable ports
- Change the dhcp configuration (if service is running)
- Download malicious software
- Play with the firewall configurations
- Can add another user's to sudo group and later on can use them

Here I have attached the screenshots showing the group to which frankcastle belongs and the output of nano /etc/sudoers:

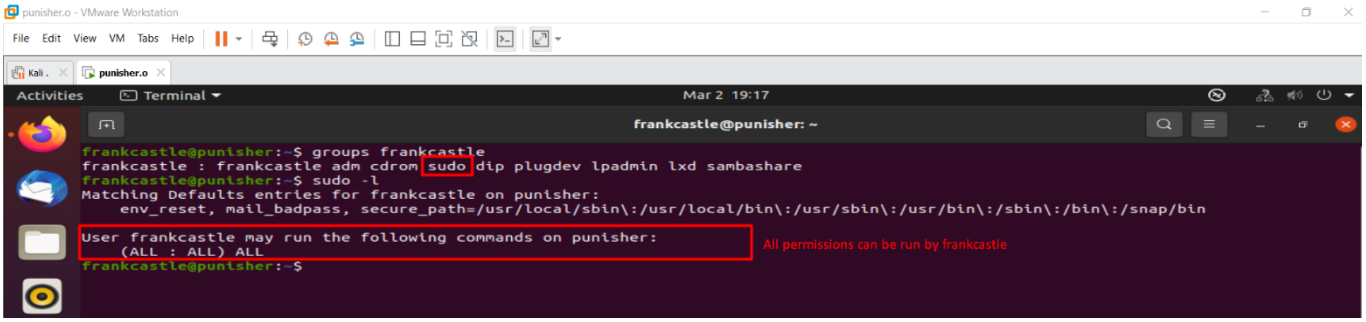


Figure 18: Groups frankcastle command-|

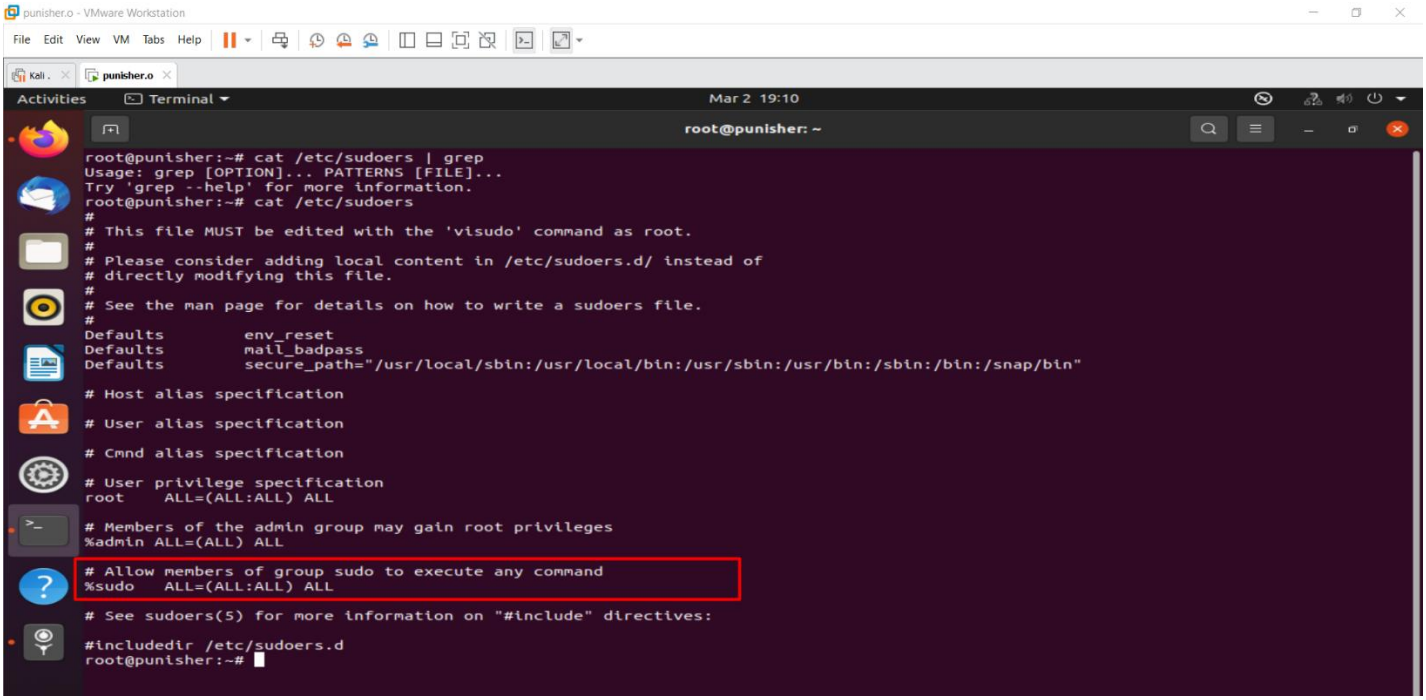


Figure 19: /etc/sudoers

To be on the safer side from this vulnerability, if the work environment doesn't require sudo usage then it will be better to remove the binaries of sudoedit.[13] and also can completely remove the sudo. On the other side, if it is a requirement to have sudo then the administrator can assign the permissions in sudo.conf file.

10 Automatic Software Execution (Using Removable Media)

Having a look at the removable media by navigating to settings in linux provides the confirmation that punisher is susceptible to Autorun Software vulnerability. In this vulnerability if an attacker inserts a removeable media (Most probably USB) into the machine and the USB is having a malicious software. Maybe there are chances the malicious software continues to run in the background and the user is unaware about the same. This can potentially lead to exposing the machine to other vulnerabilities as well. For example, if the malicious software allowed the attacker to restrict the permissions to certain files for the user etc. This type of attack can be considered as a zero-day attack **[17]** (an attack in which user comprehends something is wrong with the machine). It is worth it to mention here about the malicious code attack on the US government in 2008.**[18]** Basically, what happened was USB flash drive containing malicious software was inserted into one of the laptops of US army and the malicious code travelled across the network resulting into a software attack. To protect from this vulnerability, the "software" setting should be changed from "Run Software" to "Do Nothing". By doing so the chances of a software being executed will be minimal. Additionally, there is another option called as "Never prompt or start programs on media insertion" which should be ticked (Refer to Screenshot). This will also help in mitigating the same issue.

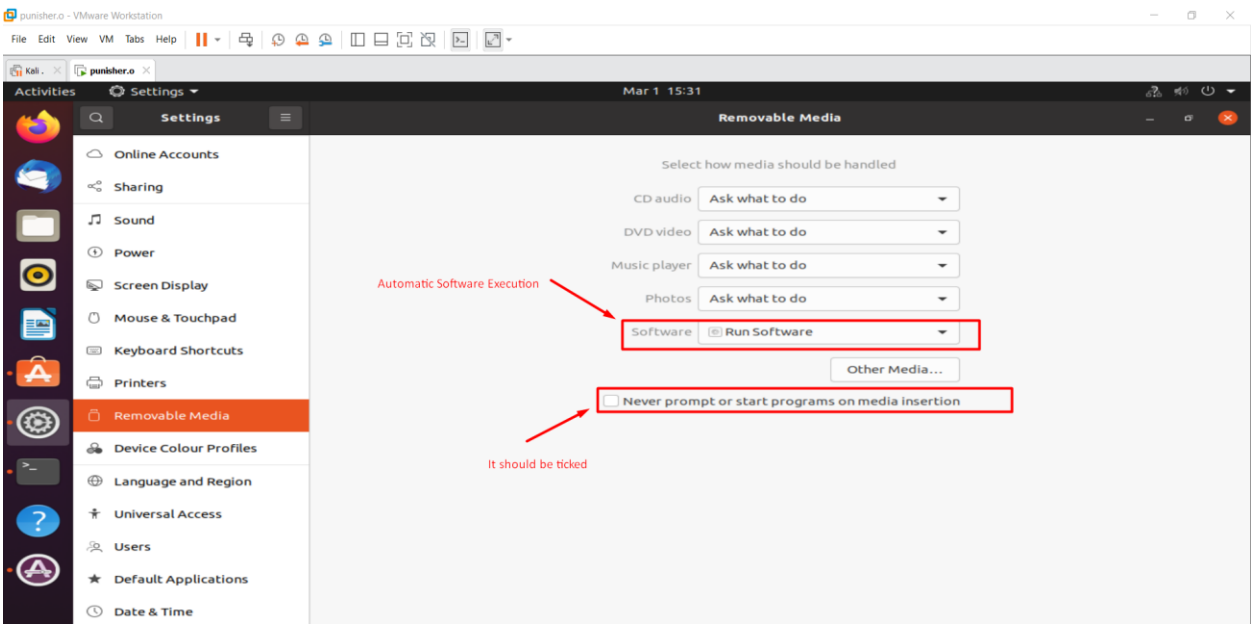
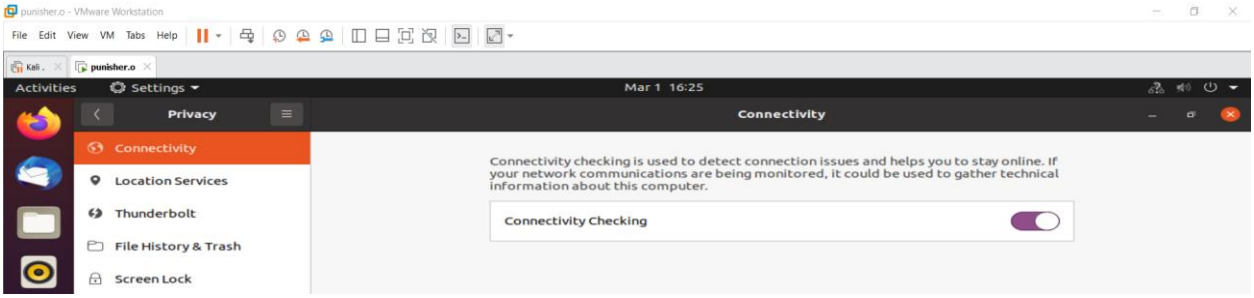


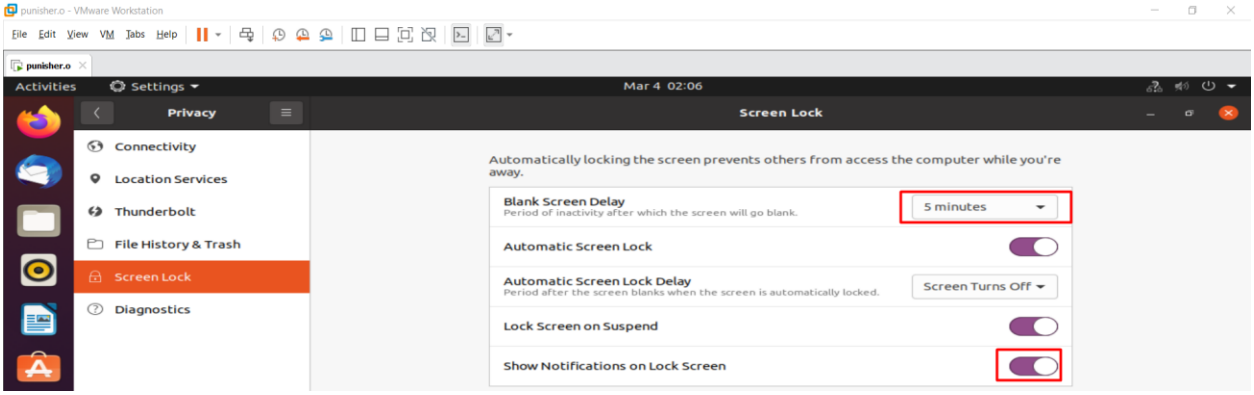
Figure 20: Automatic Software Execution

11 Connectivity Checking Vulnerability



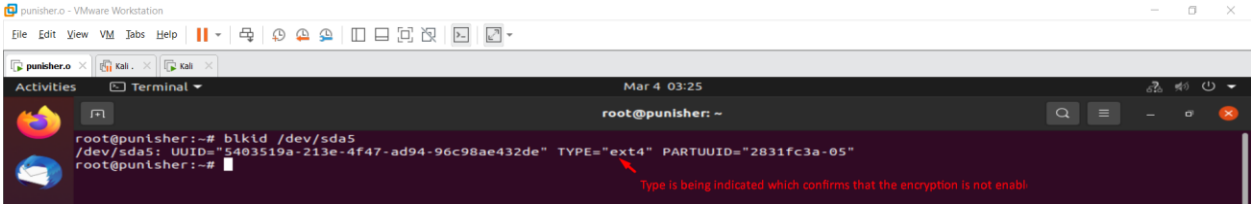
Another vulnerability which punisher have is Connectivity checking. This option allows the user or network technicians when a machine is not able to connect to the internet. On the other hand, hackers use this tool to have a look at the packets being sent by the target over the internet. This technique is sometime also referred as packet sniffing [19]. Using the packet sniffing technique and taking advantage of the “Connectivity checking " option (turned on), a hacker can be able to see which website a user is visiting, look at other sensitive information like (passwords etc.) and this as a result can led to sensitive information of the user being compromised. In order to get rid of this vulnerability a quick fix will be to simply turn off this feature. However, an advanced way can be taking a VPN into use [19]. Basically, VPN will use the encryption method while the user is surfing the websites and in this way a hacker will not be able to see which website etc a user is accessing.

12. Longer Screen Display Timeout



Another vulnerability which the punisher have is, an abnormal screen timeout specified (5 minutes (Refer to the screenshot attached)). According to me if a user goes away from the system (turned on) and a guy having bad intention is present at the spot then he/she can easily access the files available on the system or even run few commands on the terminal. However, if the owner of the system has already specified the screen timeout to a shorter span of time (like nearly 1 minute) then the chances of accessing the machine by somebody else (while the system is unattended) are negligible because after the screen goes blank then to access the system the user is required to enter the password. To fix this vulnerability the screen lockout (because of inactivity) should be reduced to nearly 1 or 2 minutes.

13 No Hard disk encryption



Out of 1000's of vulnerabilities, unencrypted hard drives is the most common vulnerability which is being possessed by many of the computers around the world. Punisher is also not an exception (Refer to the screenshot attached above). Having an unencrypted hard disk gives the attacker a privilege to have a look at the files and folders present on the system. Adding to it ,if a hard disk is encrypted it is obvious that a passphrase will be required to access the files and until or unless someone knows the password except the official user then chances of getting the sensitive files compromised are very less or even in the worst case scenario if an attacker wants to recover the data after deleting the disk then it is not possible because that data present in the disk before and after recovery will be encrypted [20] .One can have an encryption enabled on the disk and a strong passphrase(having a combination of uppercase,lowecase and symbols etc.) defined for accessing the encrypted hard disk.

14 Insecure Bash History

A feature called Bash history is responsible for collecting the commands supplied by the user. In punisher also bash history is on by default which is creating a severe loophole in the security of the device. Although most of the people debate that turning the bash history saves their time as they have to type very minimal,[15] however on the other side they are seen to enter the username and passwords in the bash terminal to access services like ssh [14] etc. Most of the time, passwords are supplied in a form of input which are also saved in the bash history. Here considering the fact that machine is in the hands of hacker somehow then having a look at bash history will easily provide attacker an edge. For example, if a user is trying to access SSH then he/she has to type:

```
Ssh username@hostIPaddress
```

And when bash history is accessed, it is going to reflect the same in the bash history. (Refer to the second screenshot below):

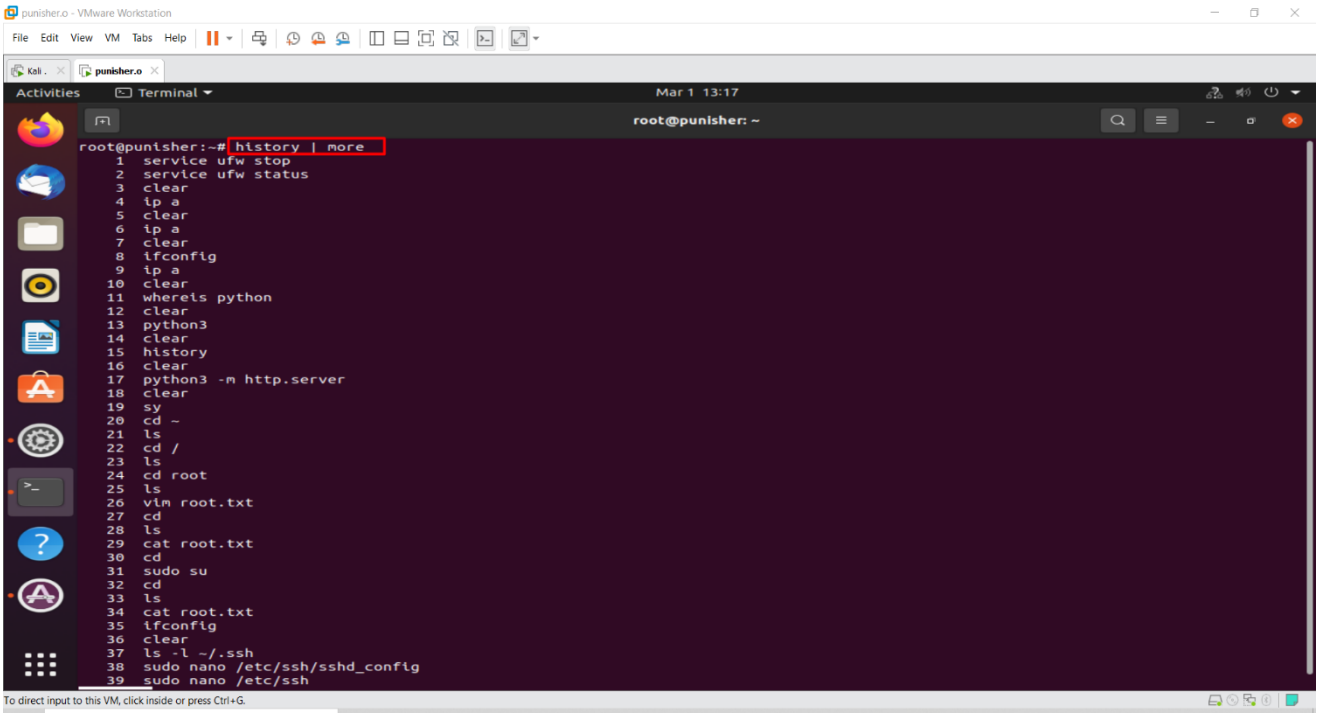


Figure 21: Command history | more showing previous commands entered

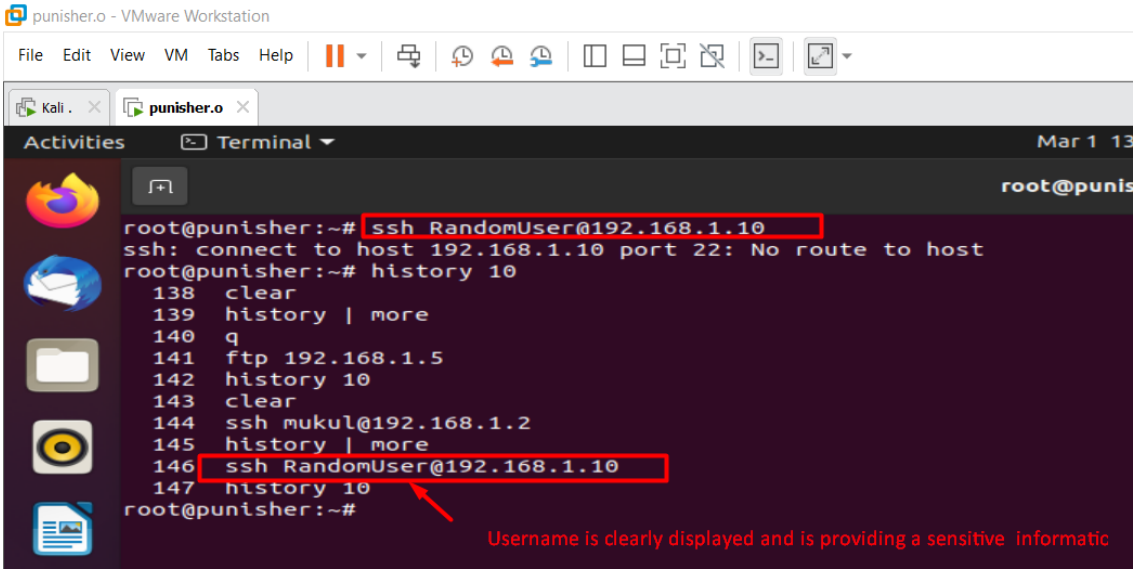


Figure 22: Username being reflected in the bash history

This vulnerability can be avoided by disabling the feature "bash history". To disable it "`echo 'set +o history '>> ~/. bashrc'`" [16] can be typed in the terminal. Also, another thing to keep in mind should be that after disabling bash history should be cleared by typing `history -c.` [16]

15 Transmission Version 2.94 (Use After Free Vulnerability)

Fifteenth vulnerability which machine is having is that it is using the transmission (Version 2.94) as against the latest transmission version 3.0.

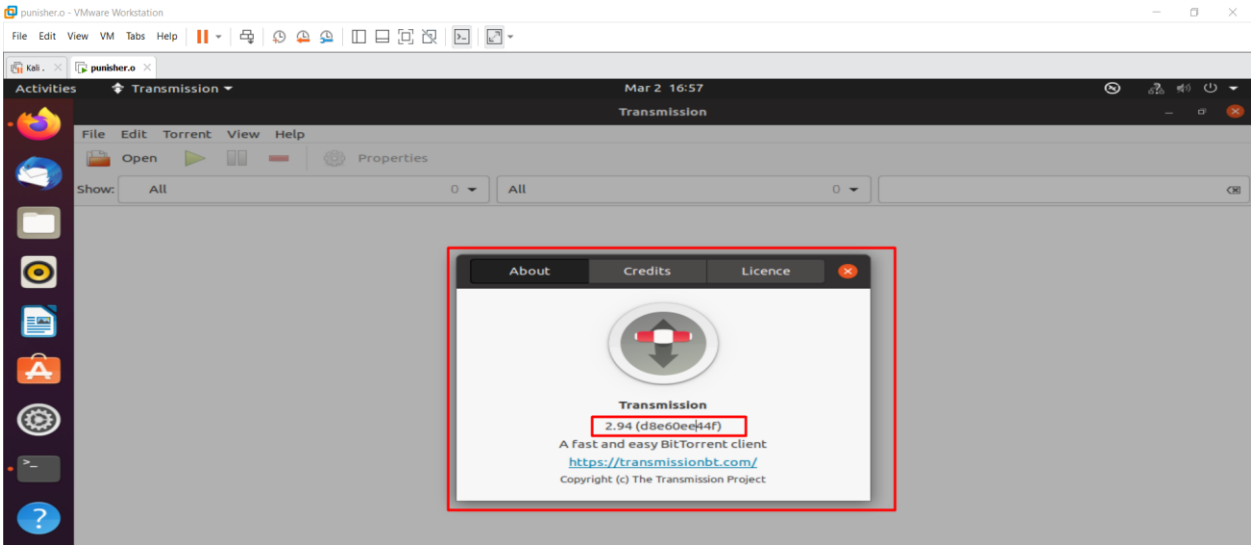


Figure 23: Old Version 2.94 Transmission Installed in punisher

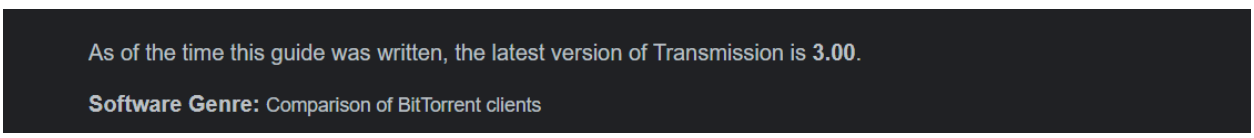


Figure 24: Latest version of transmission [11]

All in all, this attack relies on the "Use After Free"[10] error in transmission version 2.94. Usually when an application is closed in linux then memory is release but because of the presence of libtransmission/variant.c in transmission (V2.94), a significant portion of the memory remains in the use. Adding to it, hacker tries to fool the user by creating a fake .torrent file and if the user clicks on the file nothing is going to show on screen. According to user it can be a normal glitch but here starts the execution of attack. Even if the user closes the transmission application “use after free” error will let the torrent file run. Mostly such type of files is seen to consist malicious code and if the security parameter of the system is very limited then the probability of a taking over the system exists. An interesting fact about this vulnerability is that it is a kind of remote execution vulnerability. As per the recommendations of the cyber experts, it is better to upgrade to transmission version 3.0 because it comes up with the following features with enhanced security:

- Faster transmission rate in comparison to previous versions
- Limited user identity verification tries

16 Old Python Version (3.8.10)

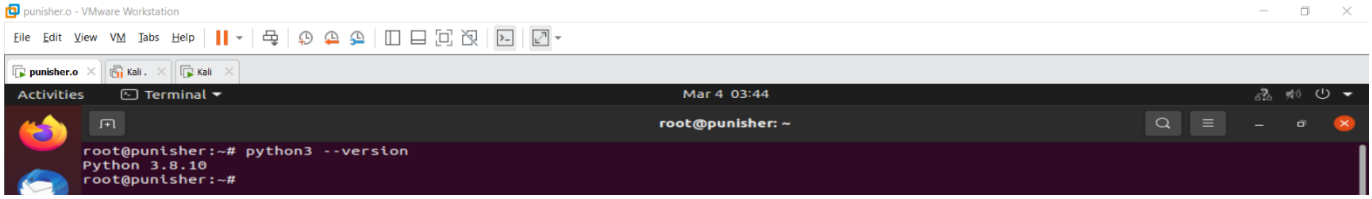


Figure 25: Python version 3.8.10

Punisher is running python version 3.8.10 but the latest version of the python is 3.10.0. Running the version 3.8.10 (Refer to the screenshot above) makes the machine vulnerable to code injection. Basically, a function called eval () is responsible behind this vulnerability. Eval function lets the user to have a look at the values of a python scrIPt. Adding to It if an attacker is capturing the packets being sent from the punisher, then being a man in the middle, hacker can inject the malicious code into the machine resulting in poisoning the target. This issue can be fixed by upgrading to the latest version of python.

17. SELinux not Installed

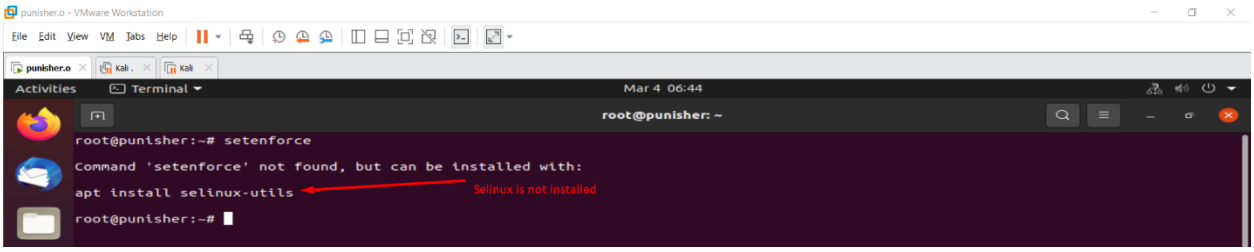


Figure 26: Selinux not installed

Having SELinux installed in the linux adds an extra layer of security to the machine. Unfortunately, punisher is not having SELinux installed which makes even more vulnerable. Basically, it is useful to allocate the permissions of access/modify the files among the different users. Talking about punisher since SELinux is not present here then chances of a user to have a squint on the sensitive and confidential files are higher. This in result can add to an information leak. Although it is true that sometime SELinux becomes an obstruction in regular usage of system, but it provides three different modes which kind of creates a filter of permissions on user. This filtering helps in making a secure linux environment. To fix this vulnerability, installation of SELinux should be done by using the following command and adequate mode (enforcing,permissive and disabled) should be choosed by editing the /etc/selinux/config [20]

```
sudo apt install selinux selinux-utils selinux-basics auditd audispd-plugins
[20]
```

18 Cups Service Vulnerability

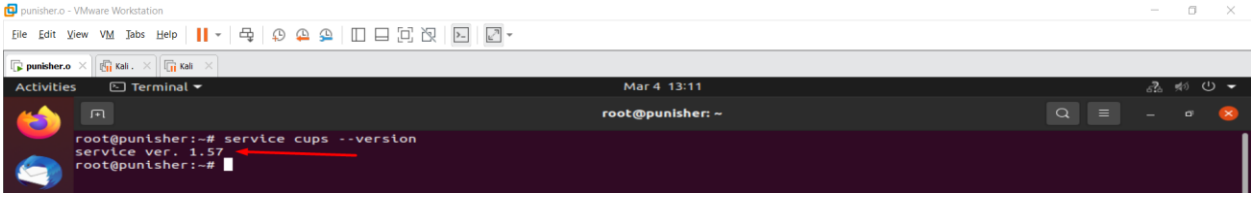


Figure 27: CUPS version

Cups also called as common Unix printing system provides extensive support to linux by tackling the printing service. However different version of CUPS are available and latest one is 2.3 but punisher is having cups version 1.5. With an old version thousands of vulnerabilities also arise along the time. Talking about the vulnerability (CVE 2015-1158(affects version below 2.0)) which this old version is possessing can be seen as a remote code execution vulnerability. Main reason behind the threat is add job function present in the cups service. Hacker tries to corrupt the data of a refence counted **[23]** string by manIPulating few jobs like (IPp_print_job). They are simply seen to swap the real configuration thus leading a way towards executing a malicious remote code attack. Above I have attached the screenshot of the CUPS version installed on punisher. To mitigate this vulnerability either one can download latest version of the cups service or can simply install the patches for the same version.

19 No BIOS Password

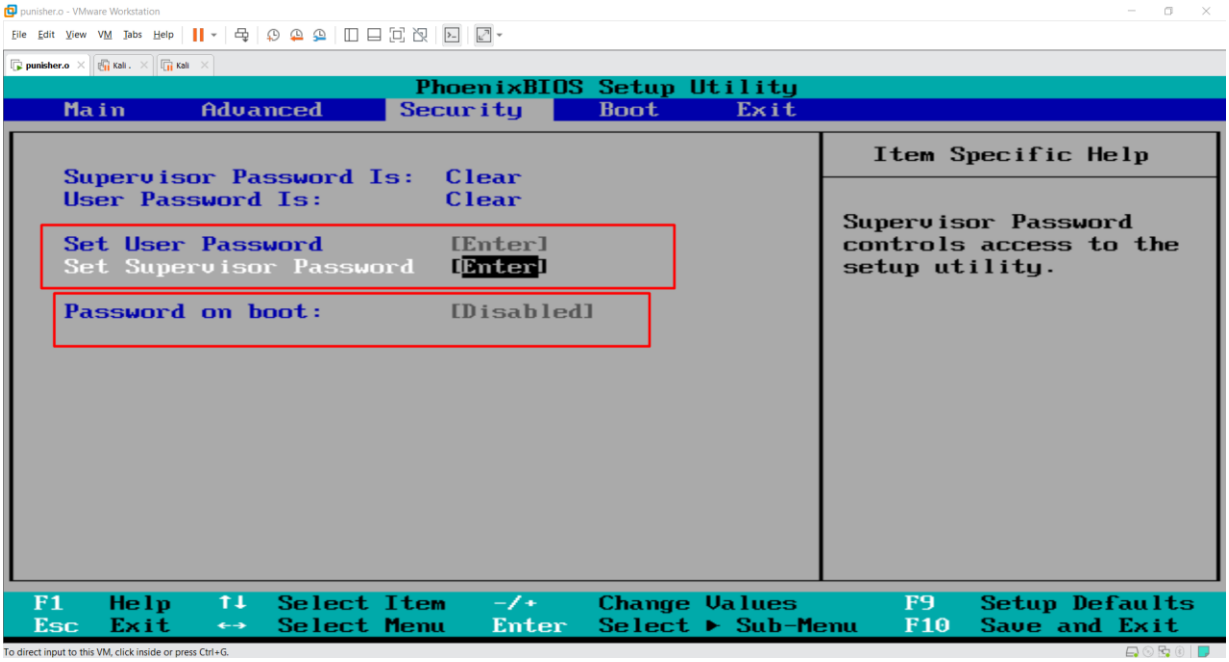


Figure 28: No BIOS password

Another vulnerability which punisher have is that it is not having a BIOS password set. BIOS loads before an operating system does and if a password is set to the BIOS then it will ask for the password before a user can boot into the operating system and start's using it.Most of the time this is seen to prevent any vulnerability attack to the system because even if attacker tries to format the whole system it is not even possible because there is no hardware resource accessible till the BIOS passphrase(which is not easily guessable) is entered. On the other hand, if no BIOS password is set and an attacker somehow cracks the usual password and logs into the machine then there are chances that below mentioned things can be performed on the machine: -

- Formatting or factory resetting machine
- Deleting or modifying the files on the machine
- Playing with the settings of the machine etc.

So, to fix this vulnerability a quick and simple solution will be to set a BIOS password. One important thing to note here is to provide a unique and bit complex password to mitigate any security risks.

20.Insecured Root Permissions

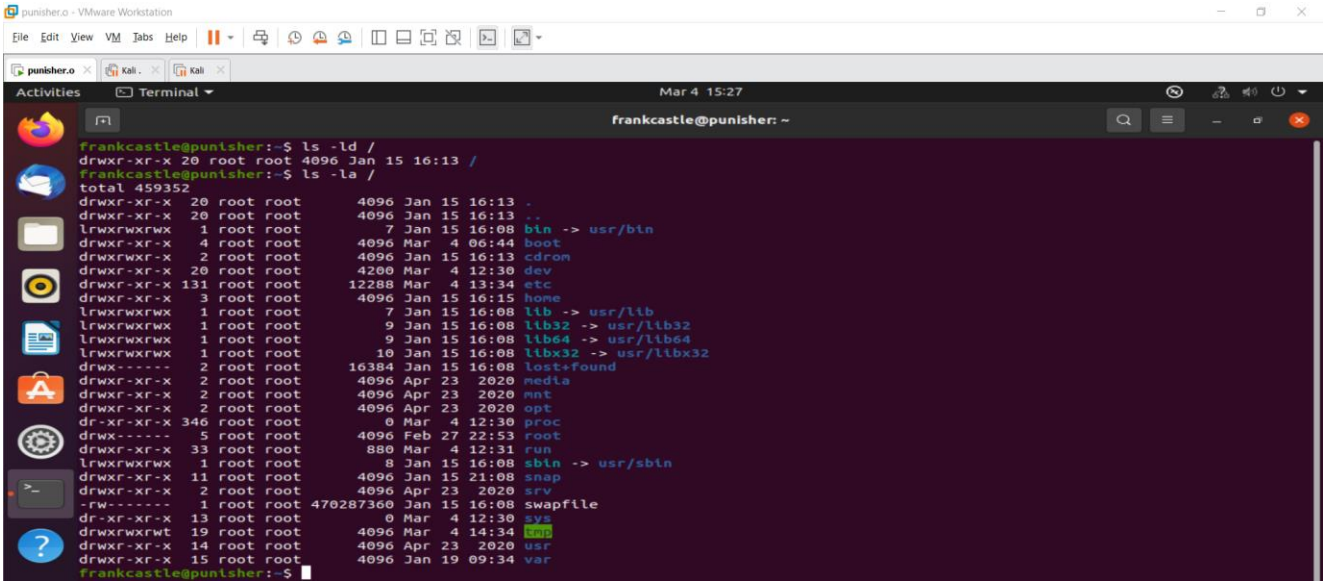


Figure 29: Inappropriate permissions on root director

Another issue with the punisher is that the root directory permissions are not as per the security standards. The permission it is having presently is drwxr-xr-x. Basically the (root user is having the permission to read, execute and write but group and other users can only execute and read). According to cyber experts, execute permission can easily be bypassed and a hacker can play with the root files. Also, attacker can use this against making the system more vulnerable. Other viewpoint of mine is also that if there are 2 administrators then only rwx permission should be assigned to them (so that they can make changes as per business need) for root directory while other users should not be able to even read it because other they don't have something to do with the root directory. So to protect against it read,write,execute permission should only be granted to the specific and trusted users.

References

[1] N. P. says: R. says: In reply to Raktim Micah says: September 6, M. says: and N. *, “Prevent directory browsing with .htaccess,” *WP Scholar*, 28-Aug-2015. [Online]. Available: https://wpscholar.com/blog/prevent-directory-browsing-with-htaccess/. [Accessed: 04-Mar-2022].

[2] “Vulnerability intelligence by cybersecurity help s.r.o.” [Online]. Available: https://www.cybersecurity-help.cz/. [Accessed: 05-Mar-2022].

[3] Unix-Ninja, unix-ninja : "Team Hashcat + defender of the realm + artist. CISSP, and Do you have questions about this article? Reach out on Twitter to ask!!, “Exploiting vim with CVE-2019-12735,” *unix*, 13-Jun-2019. [Online]. Available: https://www.unix-ninja.com/p/exploiting_vim_with_cve-2019-12735. [Accessed: 04-Mar-2022].

[4] Numirias, “Security/2019-06-04_ace-vim-neovim.md at master · numirias/security,” *GitHub*, 11-Jun-2019. [Online]. Available: https://github.com/numirias/security/blob/master/doc/2019-06-04_ace-vim-neovim.md. [Accessed: 04-Mar-2022].

[5] “Vulnerability details: CVE-2020-12801,” *CVE*. [Online]. Available: https://www.cvedetails.com/cve/CVE-2020-12801/. [Accessed: 04-Mar-2022].

[6] “CSP: Frame-ancestors - http: MDN,” *HTTP | MDN*. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-ancestors. [Accessed: 04-Mar-2022].

[7] “Frame (world wide web),” *WikIPedia*, 04-Feb-2022. [Online]. Available: https://en.wikIPedia.org/wiki/Frame_(World_Wide_Web). [Accessed: 04-Mar-2022].

[8] “Security vulnerabilities fixed in Firefox 96,” *Mozilla*. [Online]. Available: https://www.mozilla.org/en-US/security/advisories/mfsa2022-01/#CVE-2022-22742. [Accessed: 04-Mar-2022].

[9] İ. Baydan, “İsmail Baydan,” *LinuxTect*, 02-Feb-2021. [Online]. Available: https://linuxtect.com/linux-chage-command-change-password-expire-date/#:~:text=The%20chage%20command%20is%20used,be%20limited%20and%20changed%20periodically. [Accessed: 04-Mar-2022].

[10] “Vulnerability database,” *Vulnerability Intelligence by CyberSecurity Help s.r.o.* [Online]. Available: https://www.cybersecurity-help.cz/. [Accessed: 04-Mar-2022].

[11] K. S. Awaisi, “How to install transmission 3.00 BitTorrent client,” *Linux Hint*, 01-Jan-1968. [Online]. Available: https://linuxhint.com/transmission-bittorrent-client-linux/#:~:text=As%20of%20the%20time%20this,version%20of%20Transmission%20is%203.00. [Accessed: 04-Mar-2022].

[12] “Vulnerability intelligence by cybersecurity help s.r.o.” [Online]. Available: https://www.cybersecurity-help.cz/vdb/SB2022021114. [Accessed: 05-Mar-2022].

[13] Person, “Understanding sudo vulnerability CVE-2021-3156 & How Privilege Management for unix & linux can help,” *BeyondTrust*, 19-Feb-2021. [Online]. Available: https://www.beyondtrust.com/blog/entry/understanding-sudo-vulnerability-cve-2021-3156-and-how-privilege-management-for-unix-linux-can-protect-your-enterprise. [Accessed: 04-Mar-2022].

[14] “How to use SSH to connect to a remote server in linux or windows,” *Knowledge Base by phoenixNAP*, 07-Oct-2021. [Online]. Available: https://phoenixnap.com/kb/ssh-to-connect-to-remote-server-linux-or-windows. [Accessed: 04-Mar-2022].

[15] M. 11, F. 9, and F. 8, “Mitre ATT&CK vulnerability spotlight: Bash history,” *Infosec Resources*, 16-Oct-2020. [Online]. Available: https://resources.infosecinstitute.com/topic/mitre-attck-vulnerability-spotlight-bash-history/. [Accessed: 04-Mar-2022].

[16] Admin, “OS,” *The Geek Diary*. [Online]. Available: https://www.thegeekdiary.com/how-to-remove-disable-bash-shell-command-history-on-linux/. [Accessed: 04-Mar-2022].

[17] “What is a zero-day exploit?,” *FireEye*. [Online]. Available: https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html. [Accessed: 04-Mar-2022].

[18] “USB drop attacks: The danger of,” *RedTeam Security - 5200 Willson Rd. Suite 150, Edina, MN 55424*. [Online]. Available: https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives. [Accessed: 04-Mar-2022].

[19] “Packet sniffing. how bad guys spy on ... - whatismyIPaddress.” [Online]. Available: https://whatismyIPaddress.com/packet-sniffing. [Accessed: 05-Mar-2022].

[20] Kody, J. Masters, M. Roberts-Barter, TheDeliveryMan, ApeRock, S. Johnson, Occupytheweb, H.-D@d, J. McBradders, VoidX, R4d0n86, B. Eagle, A.-H. Ahmed, A. Suryawanshi, and S. Nicole, “How to scan for vulnerabilities on any website using Nikto,” *WonderHowTo*, 13-Mar-2019. [Online]. Available: https://null-byte.wonderhowto.com/how-to/scan-for-vulnerabilities-any-website-using-nikto-0151729/. [Accessed: 04-Mar-2022].

[21] “How to install selinux on ubuntu 18.04 | linode.” [Online]. Available: https://www.linode.com/docs/guides/how-to-install-selinux-on-ubuntu-18-04/. [Accessed: 05-Mar-2022].

[22] “HD wallpaper: Anarchy, computer, Hack, Hacker, hacking, internet, poster,” *HD wallpaper: anarchy, computer, hack, hacker, hacking, internet, poster | Wallpaper Flare*. [Online]. Available: https://www.wallpaperflare.com/anarchy-computer-hack-hacker-hacking-internet-poster-wallpaper-uodwl. [Accessed: 04-Mar-2022].

[23]“CVE-2015-1158,” *SUSE*. [Online]. Available: https://www.suse.com/security/cve/CVE-2015-1158.html. [Accessed: 04-Mar-2022].