Εργασία 1

Κωνσταντίνος Γαρείος - inf2021036

December 2024

1 A. INITIAL ACCESS

1.1 A1: Enumeration

1) The first step is always to perform host discovery. For this reason, use nmap to discover the IP address of the target VM using the correct flags for Ping Sweep. Write the command you used.

Ans:
Using the Kali linux VM, we first try to find the Network prefix that we'll use for the host discovery. Using 'ip a' I derive from Kali's private ip address that the prefix to use is (inet:172.16.48.0/24)

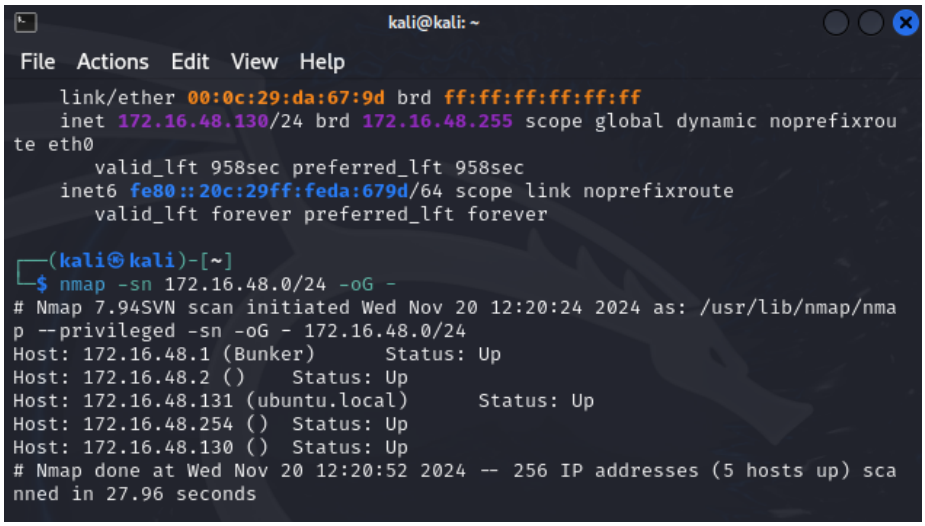

Figure 1: We can conclude from our nmap PingSweep that (ubuntu.local)'s private ip address corresponds to 172.16.48.131

2) Use now nmap to identify open ports (port scanning) based on the IP address you discovered in question 1. Execute nmap with and without -F flag. What is the nuance between those? What is the usage of the -F flag? Now execute nmap with and without -n flag. What did you discover? What is the usage of -n flag?
Also write all open ports that you found.

Ans:
The -F flag stands for 'fast' and scans only the top 100 ports, reducing scan time.

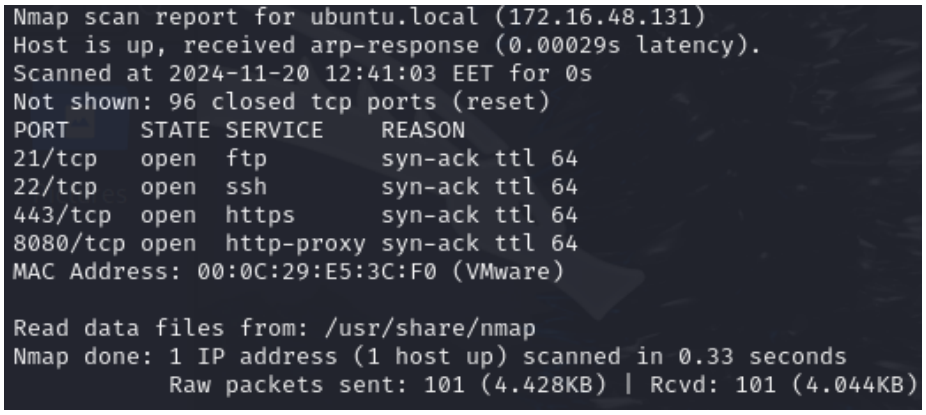

Figure 2: nmap -F on the Ubuntu machine finds 4 open tcp ports

The -n flag skips DNS resolution, which reduces running time and can prevent misconfiguration bugs during DNS resolutions. In this instance there are no noticeable difference to using this flag. In nmap scans where we don't have the hostname of the device verified, we wouldn't want to use this flag, since that process is entirely skipped.

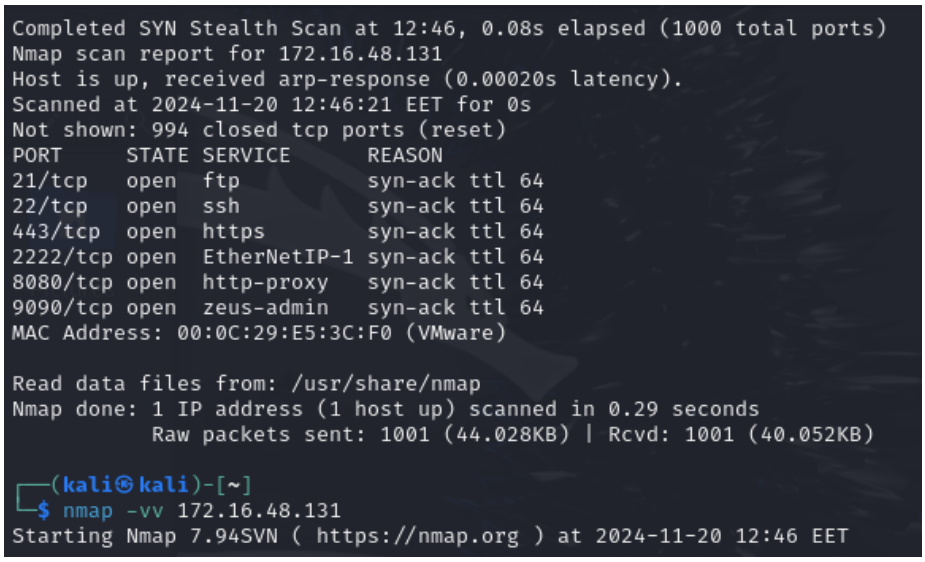

Figure 3: The open top 1000 ports of the nmap scan results are: 21/ftp, 22/ssh, 443/https, 2222/EtherNetIP-1, 8080/http-proxy, 9090/zeus-admin

3) What is the use of -Pn flag of nmap?. Would you use -Pn in host discovery (question 1) or port scanning (question 2)?

Ans:
The -Pn flag is used in port scanning. If a firewall is configured to not respond to the ICMP ping that nmap normally performs during host discovery, the -Pn flag is recommended. It will skip the host discovery process and may find open ports that would otherwise appear down because of the firewall.

4) Perform now service enumeration but scan only the open ports found in question 2. You should use a specific flag of nmap. Write down which services you discovered running.

Ans:

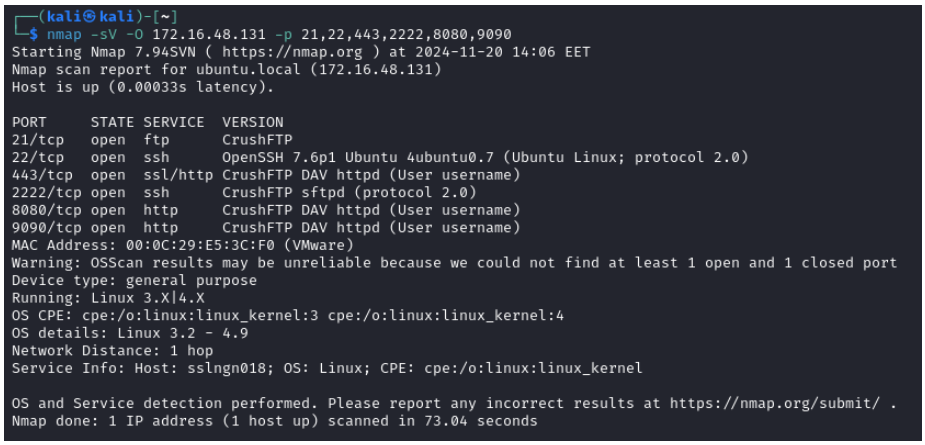

Figure 4: The services running are CrushFTP and OpenSSH, ports are specified.

5) Run now nmap to discover the running services and their version using the flag -sC and the operating system (use -O). What is the difference between -sC and -sV flag? Use also the flag -T4. What is the usage of this flag?

Ans:
The -T4 flag refers to the Timing Template 4; the default one being -T3. T4 makes the scan slightly sloppier and faster. The -sV flag only detects the service version of the port, whereas the -sV flag does a full nmap default script scan, providing more information about each port.

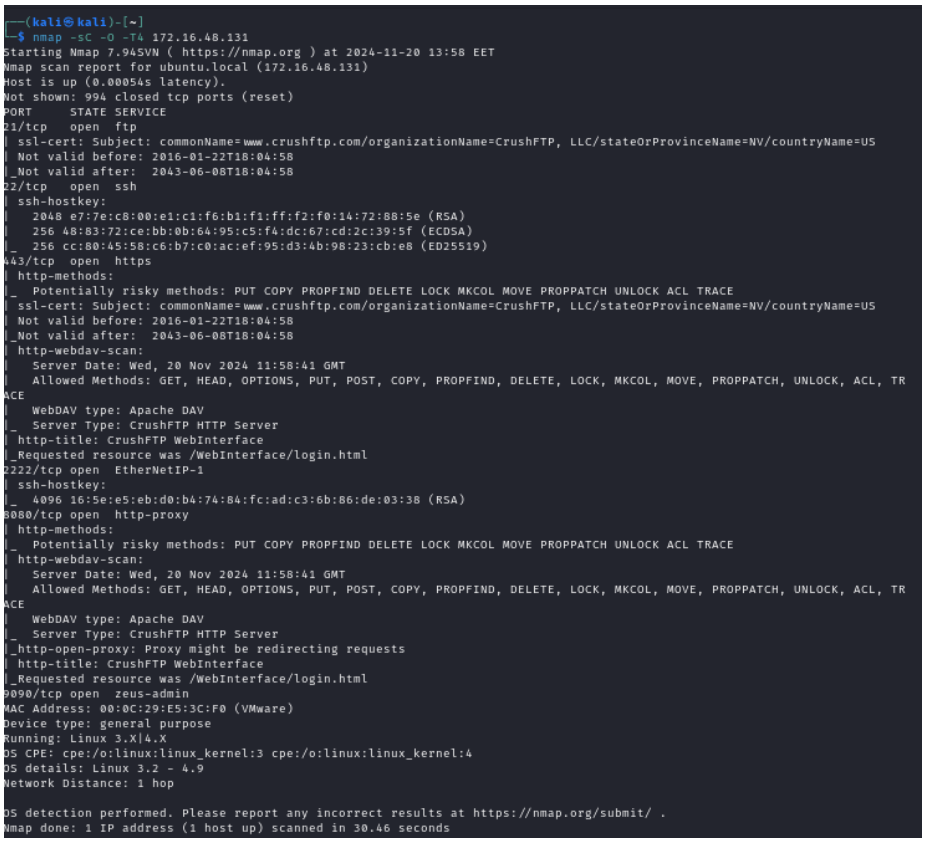

Figure 5: Many more details are now identified

1.2 A2: Vulnerability assessment

6) Run nmap with an appropriate flag to perform vulnerability assessment (nmap is not recommend for this step, see extra question at the end).
Did nmap discover vulnerabilities with a CVE?

Ans:
Running the command: nmap -vv -sV -O –script=vuln 172.16.48.131 -p 21,22,443,2222,8080,9090 I got Slowloris DOS attack (CVE-2007-6750), phpmyadmin subform Parameter Traversal Local File Inclusion (CVE-2005-3299), LiteSpeed Web Server Source Code Disclosure (CVE-2010-2333) and a long list of vulners exploits for OpenSSH:

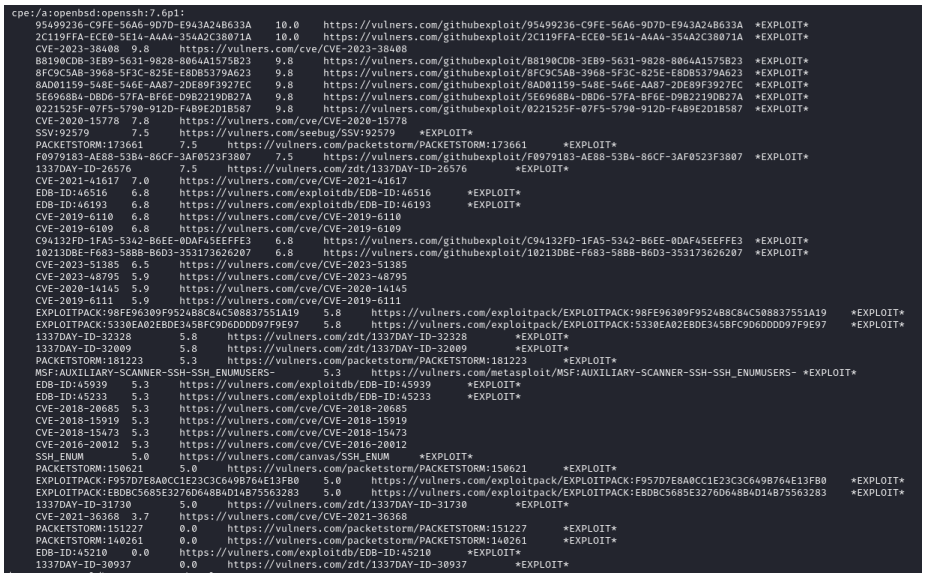

Figure 6: OpenSSH vulners list

1.3 A3: Exploitation

7) We have noted in the beginning of the exercise that a recent CVE will be utilized for exploitation. nmap did its best but none of the vulnerabilities found in question 6 are useful for initial access and they are also not recent. We have to perform manual testing. One specific service stands out! Google and find whether this service had vulnerabilities in the past. Now we will use Metasploit to exploit this service as it has the required exploit module. Run msfconsole and search using the name of the service, setup the required options and run the exploit. It is important to understand that the impact of this vulnerability is information disclosure of arbitrary files not RCE! Using the exploit, read a file in the system that includes the usernames of all users. Write the exploit that was successful (i.e., the Metasploit path of the exploit) and the CVE number.
What is the name (category) this vulnerability?

Ans:
The CrushFTP service has a 9.8 CSS Critical vulnerability that is recent that allows for unauthorized arbitrary file reads. On the metasploit path: Auxiliary/gather/crushftp_fileread_cve_2024_4040

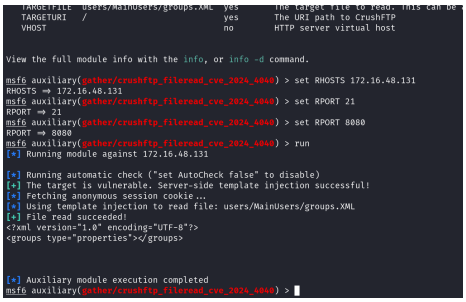

Figure 7: I set the ip address of the ubuntu machine and port 8080, as that is the web application using crushFTP

8) What are our privileges when we are reading the system files?

Ans:
They are root privileges, since we can read any file on the host, such as /etc/shadow

Figure 8: results of setting TARGETFILE = /etc/shadow

9) There are two users in the system, one of them has left a hint for you in her Desktop. Find the file with the hint and proceed with the instructions to achieve initial access. An important remark here is that you are strongly advised to search and use an appropriate Metasploit auxiliary modu le, because meterpeter will help you later for the privilege escalation (you can use an external tool for initial access, but then you will have to convert it to a meterpreter manually). Write down the Metasploit auxiliary module path.

Ans:
Using the CrushFTP exploit, I can read the hint file in notaroot's Desktop. By setting the TARGETFILE to "home/notaroot/Desktop/hint"

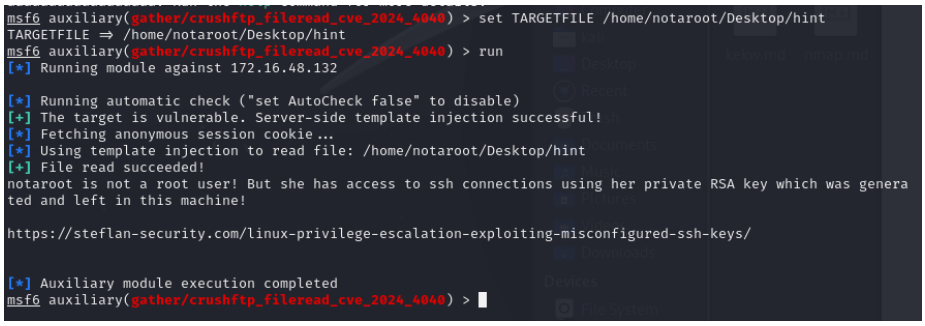

Figure 9: I proceed to read the Webpage that is linked

After reading the webpage's content, I set the TARGETFILE to where the ssh key should be stored and export the contents to some local file on my kali machine, for later use.

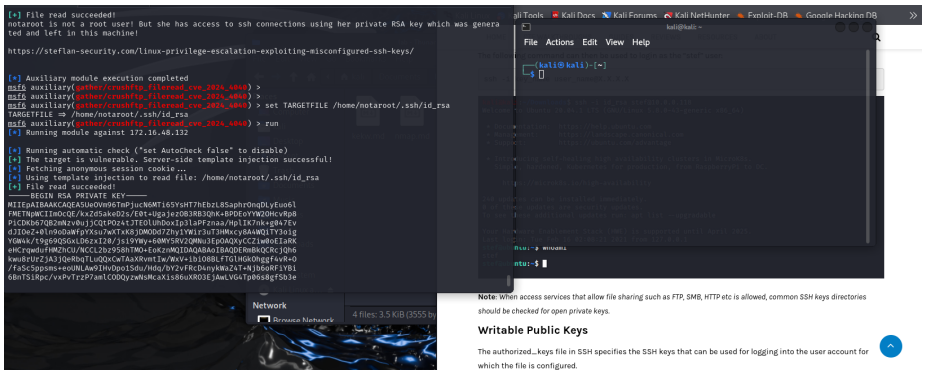

Figure 10: TARGETFILE: /home/notaroot/.ssh/id_rsa

By using the ssh_login_pubkey module of metasploit. I set the ssh KEY_PATH to the file I previously stored, set USERNAME notaroot and RHOSTS to the ubuntu machine's ipv4 and execute the attack successfully.

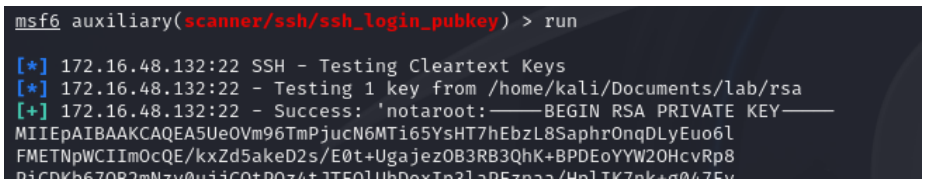

Figure 11: Success!

10) Your opened shell for initial access from step 9 is not a meterpreter shell. Metasploit can automatically upgrade a non-meterpreter shell to a meterpreter shell.

To achieve this, background the shell and upgrade it to meterpreter using sessions -u 1 (where 1 should be your session id number). Do you have meterpreter access now?

Ans:
Using the -u flag, I upgraded the shell to meterpreter.

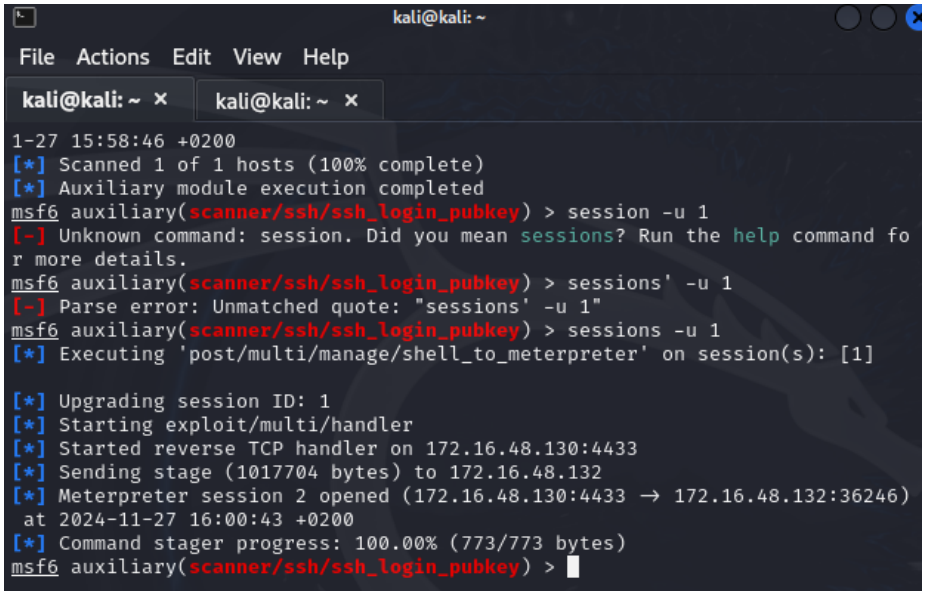

Figure 12: Upgraded to meterpreter

2 B POST EXPLOITATION

2.1 B1. Enumeration

11) Now you should have at least one meterpreter session. What is the current directory of the opened meterpreter session? Execute the meterpreter command systeminfo to identify the target machine.

Ans:
Using the command 'pwd' I can see that meterpreter is in the home directory of notaroot.

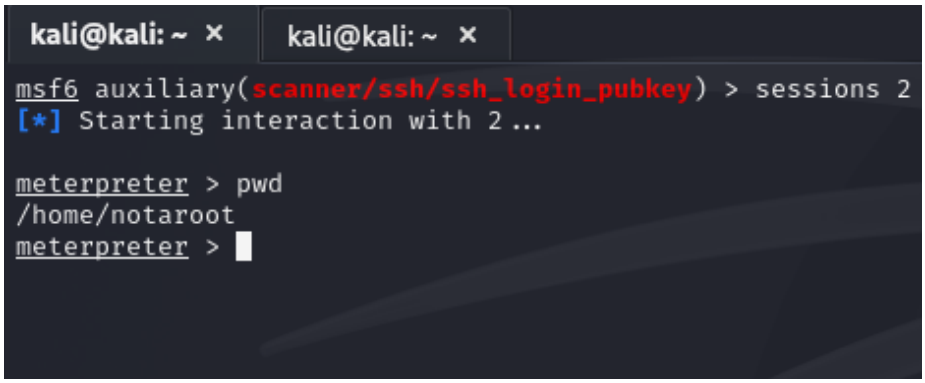

Figure 13: pwd: /home/notaroot

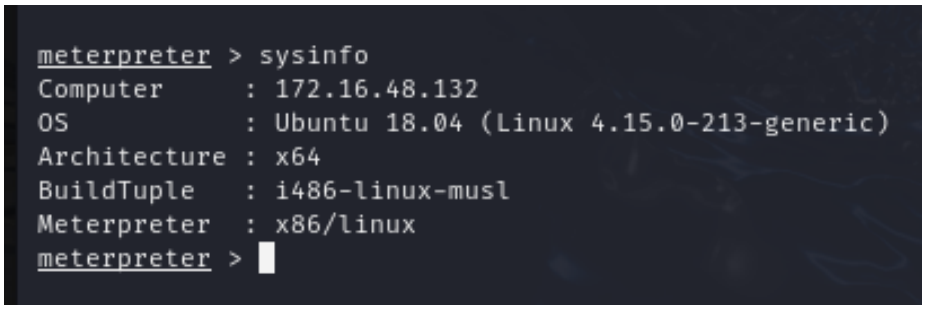

Figure 14: sysinfo

2.2 B2. Privilege escalation

12) Time for privilege escalation. Background the meterpreter shell and use the Metasploit suggester (post/multi/recon/local_exploit_suggester) to find potential exploits for privilege escalation. If you succeeded in gaining root rights, write the exploit path that you used.

Ans:
By setting SESSION 1 as background, I run the suggester successfully.

Figure 15: I can see 6 potential attacks

Eventually, after running some of the attacks, I land on pwnkit_lpe_pkexec, which provides me with root access:

Figure 16: module: exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec getuid: root

13) Upload a text file in the desktop of the ergasia user.
Write the meterpreter command that you used.

Ans:

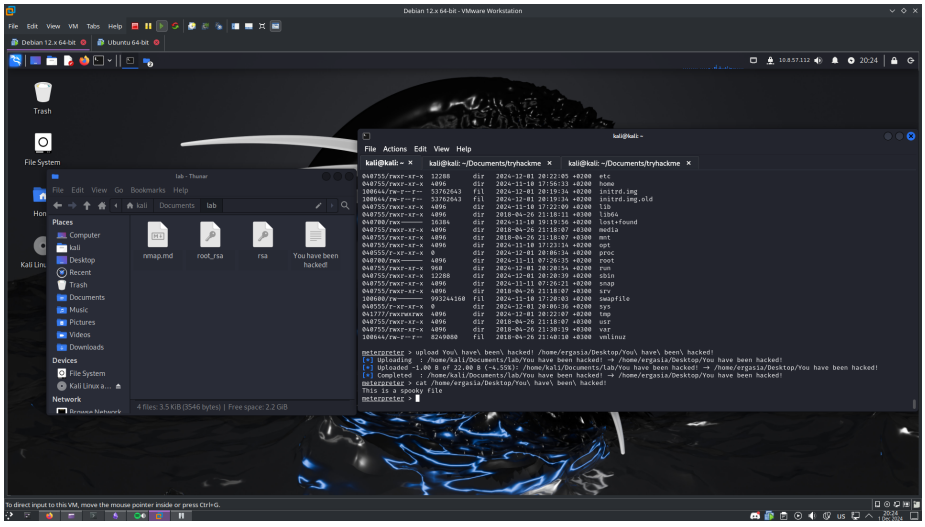

Figure 17: Uploading the file: /home/ergasia/Desktop/You have been hacked!