LAB- 04 Introduction to Packet Analysis and Network Reconnaissance

By:- Faraz Ahmed

Part 1- Packet Analysis Investigation

Q1. **URL Redirection Attack**- A URL Redirection Attack is a type of attack where attackers basically trick a user into clicking some false and malicious links which will forward them to a phishing or malware-laden sites. So, basically it happens when a vulnerable link or web application redirects a user to an external, malicious site of unknown source.

Example:- When a user is fooled to click a malicious link http://micronotsoftoffice.com which according to him/her looks legit and it redirects him/her to a malicious website.

Q2. **Remote Code Execution (RCE)**- Remote Code Execution occurs when an attacker basically executes an arbitrary code on that user's machine or on a server. Attackers operate from a remote location and can affect the full system of that user.

Example:- When an attacker uploads a malicious PHP file of shell.php that contains some arbitrary commands to run.

Q3. **SQL Injection**- SQL Injection is a type of attack where an attacker injects a malicious SQL query codes inside the backend database of a website to manipulate it and gain access to some unauthorized data.

Example:- When an attacker enters 'or''-' into the input of login page which will help him/her to bypass user authentication.

Q4. **Cross-Site Scripting (XSS)**- Cross-Site Scripting is a type of attack where an attacker takes advantage of a vulnerability to inject some malicious JavaScript code into that web page which when accessed or viewed by other users can lead to session hijacking or malware transfer.

Example:- Typing <script>alert('Hacked');</script> in the comments of the website can cause every user's browser to execute it.

Q5. **Cross-Site Request Forgery (CSRF)**- Cross-Site Request Forgery basically tricks an already authenticated user into performing some suspicious activities which an attacker then takes advantage of that user's active user session. Because of this, its also called "one-click attack" or "session riding".

Example:- An attacker sends a malicious link in a victim which triggers a "POST" request so when victim logged in, their email is swiftly change into attacker's email.

Q6. **Authentication Bypass**- Authentication Bypass happens when am attacker can access some unauthorized and restricted areas without properly authenticating or providing valid credentials which can be achieved by performing some malicious activities.

Example:- By modifying the URL parameters of web page to gain some high privilege without logging in properly.

Q7. **Remote File Inclusion (RFI) and Local File Inclusion (LFI)**- The server in which attacker remotely executes remote code execution is called Remote File Inclusion whereas the server where a local file

(which is already present there) will allow execution on some code execution is called as Local File Inclusion.

Q1. How much money did the attacker at 10.10.10.66 steal from Tara's online banking account?

Ans1. The attacker stole $504 from Tara's online banking account which is highlighted in Figure 1.

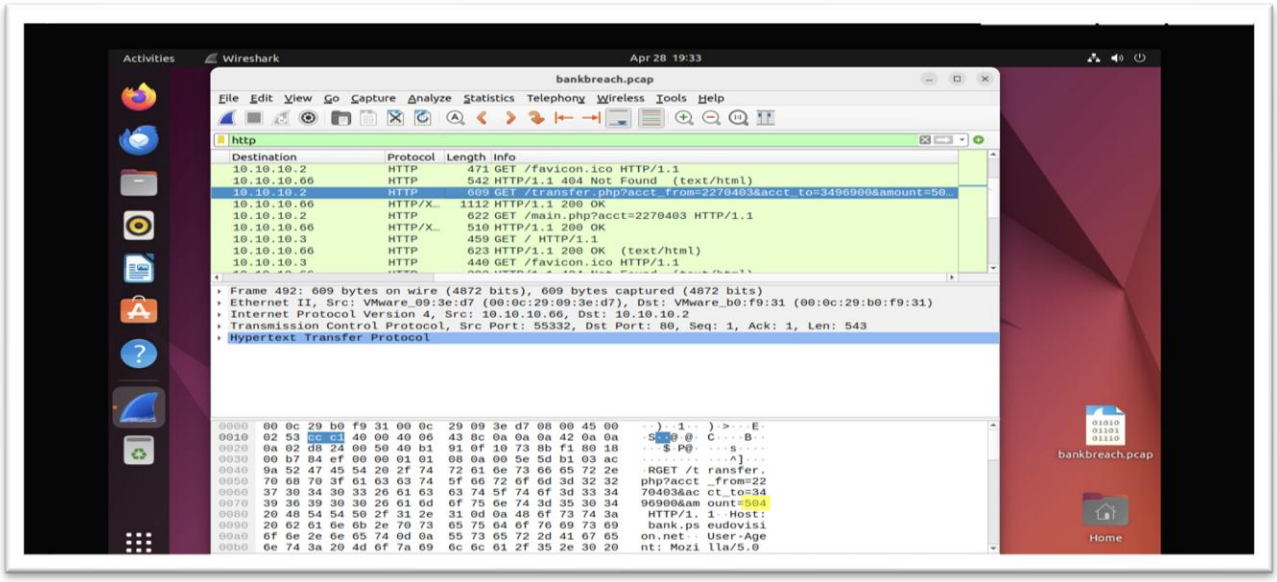

Figure 1: Screenshot of attacker stealing $504 from Tara's banking account.

Q2. How much money does Vincent have in his online bank account?

Ans2. Vincent has $560 in his online bank account as highlighted in Figure 2.

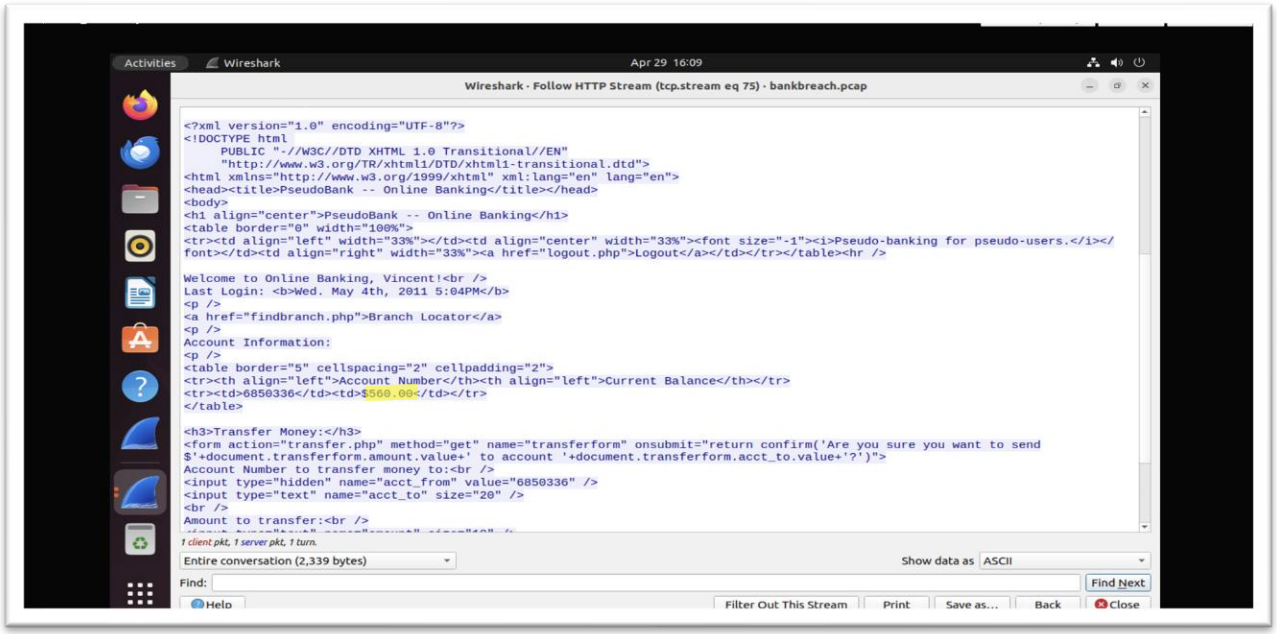

Figure 2: Screenshot of Vincent bank balance which is $560.

Q3. Which of the users has the highest account balance at PseudoBank?

Ans3. Stephen is the one with the highest balance with “58,392.10” in his account balance at PseudoBank as highlighted in Figure 3.

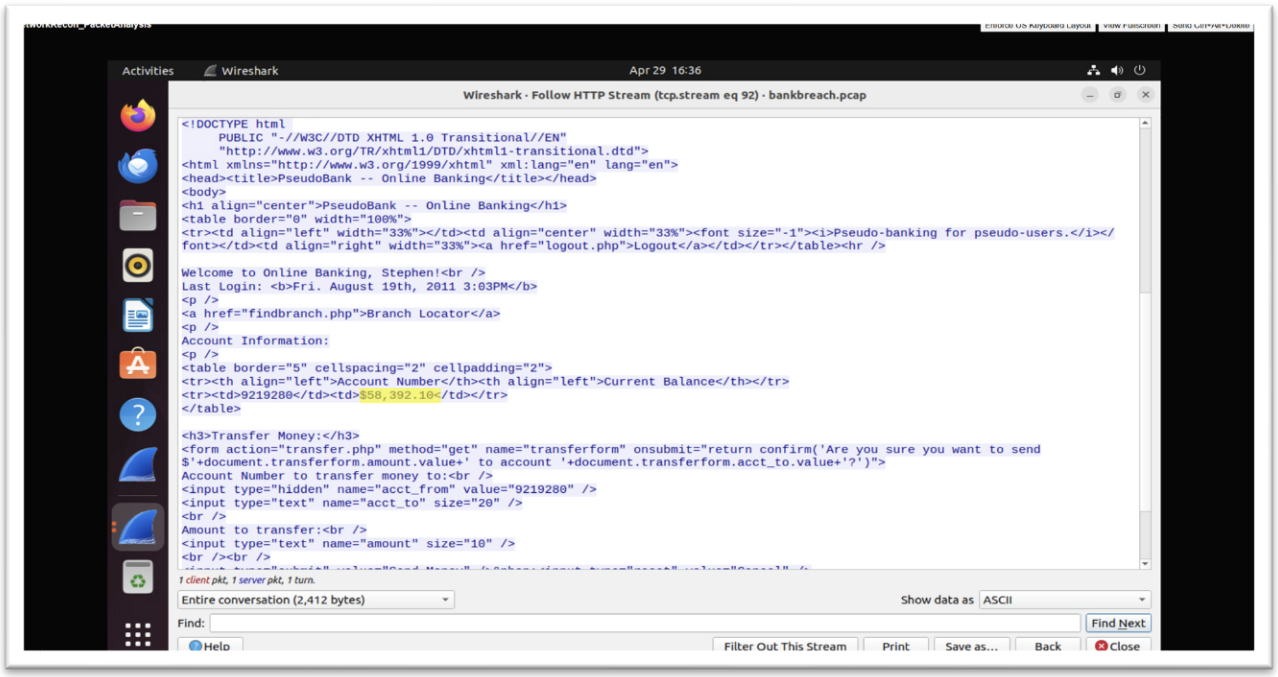

Figure 3: Screenshot of Stephen’s account balance of $58,392.10 at PseudoBank.

Q4. When was the last time that Tara logged on to her online bank account?

Ans4. The last time when Tara logged on to her online bank account was Monday, August 22nd, 2011 at 12:18PM as highlighted in Figure 4.

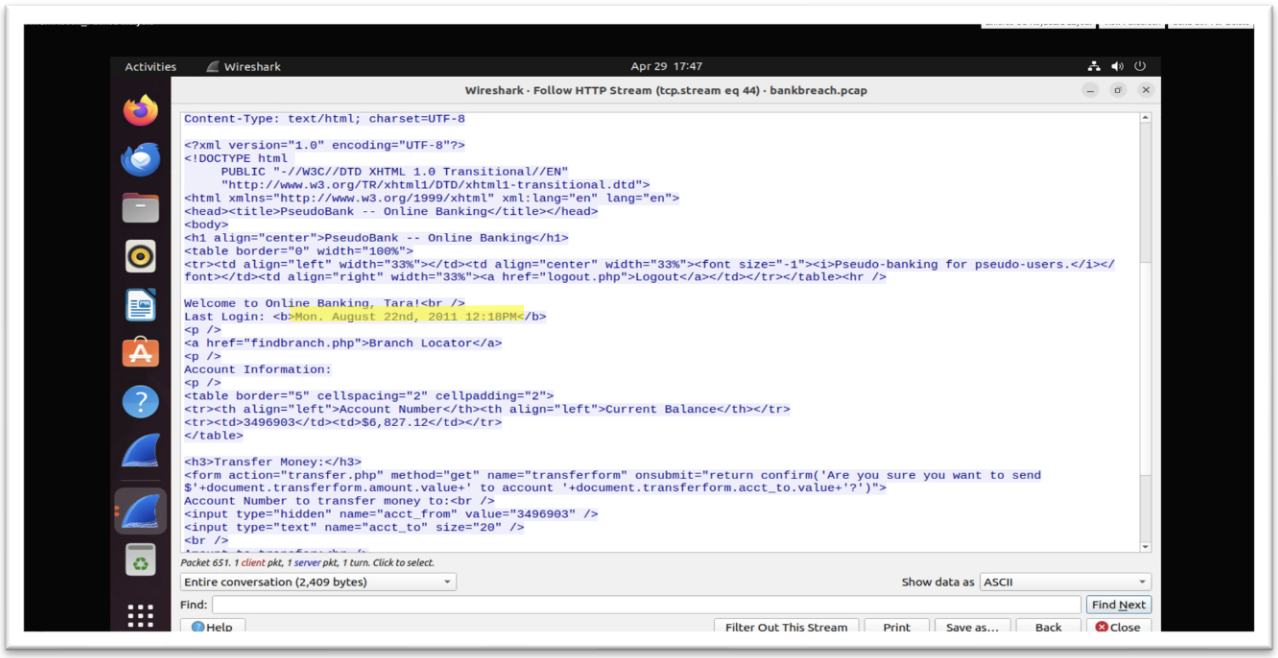

Figure 4: Screenshot of last time when Tara logged in her account.

Q5. Which IP address did the user at 10.10.10.11 ping using the web form on wireless.pseudovision.net?

Ans5. IP address is 10.10.10.3 which was pinged by user 10.10.10.11 as highlighted in Figure 5.

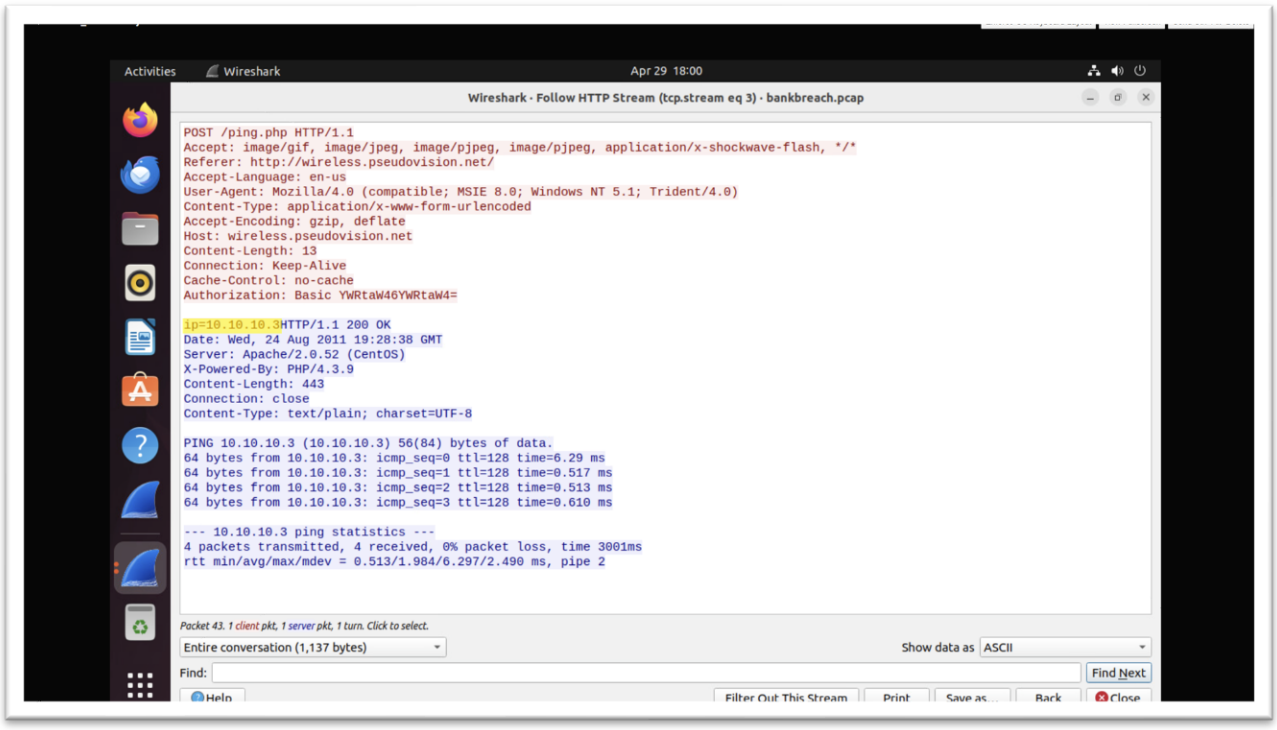

Figure 5: Screenshot of ip-10.10.10.3 which was pinged by user 10.10.10.11.

Executive Summary

PseudoBank basically faced a planned and coordinated cyberattack which originated from the external IP address of 10.10.10.66 and the attacker executed a Local File Inclusion (LFI) vulnerability on bob.pseudovision.net which can give them access and allow them to permit sensitive source code and configuration files which will also include database usernames and passwords.

So, what happened is that the attacker accessed source.php using LFI attack (packet 1164) which basically reveals Bob's data password. Then attacker used that same credential to intercept login requests and access user accounts. Then he/she used those accounts to extract main.php and transfer.php for some sensitive data such as user information, money balance and transfer. So, using all of that information, attacker targeted some users like Tara and enter $504 for unauthenticated transfer. Hence, attacker used unencrypted HTTP traffic to get user credentials, then LFI allowed to get direct access to source.php and then that give attacker enough sensitive data and credential to perform malicious activity in the system.

Here are some of my recommendations to mitigate this attack:-

a. Enforce HTTPS across whole network and systems which will increase overall security.
b. Enforce least privilege policy to all essential accounts and sensitive data.
c. There should be regular log monitoring and alert systems to detect some malicious activity into the systems.
d. Apply strict firewall rules to stop any external attacks.
e. Apply harden PHP web applications by disabling any type of external inclusion.

Part 2 – Network Scanning and Reconnaissance

- First, we will check the IP address of the VM by using “ip address” as highlighted in Figure 6.

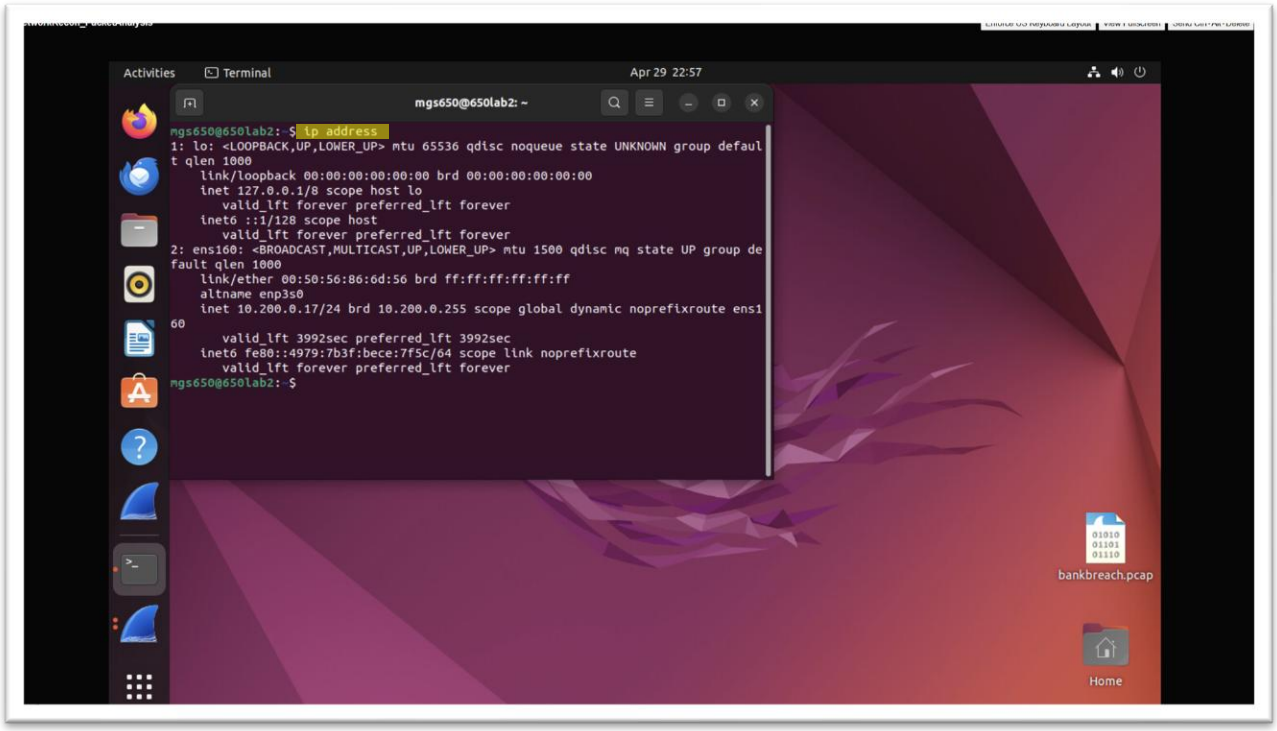

Figure 6: Screenshot of “ip address” to find out IP address of the VM.

- Then we can type “Zenmap” in terminal to open Zenmap as shown below.

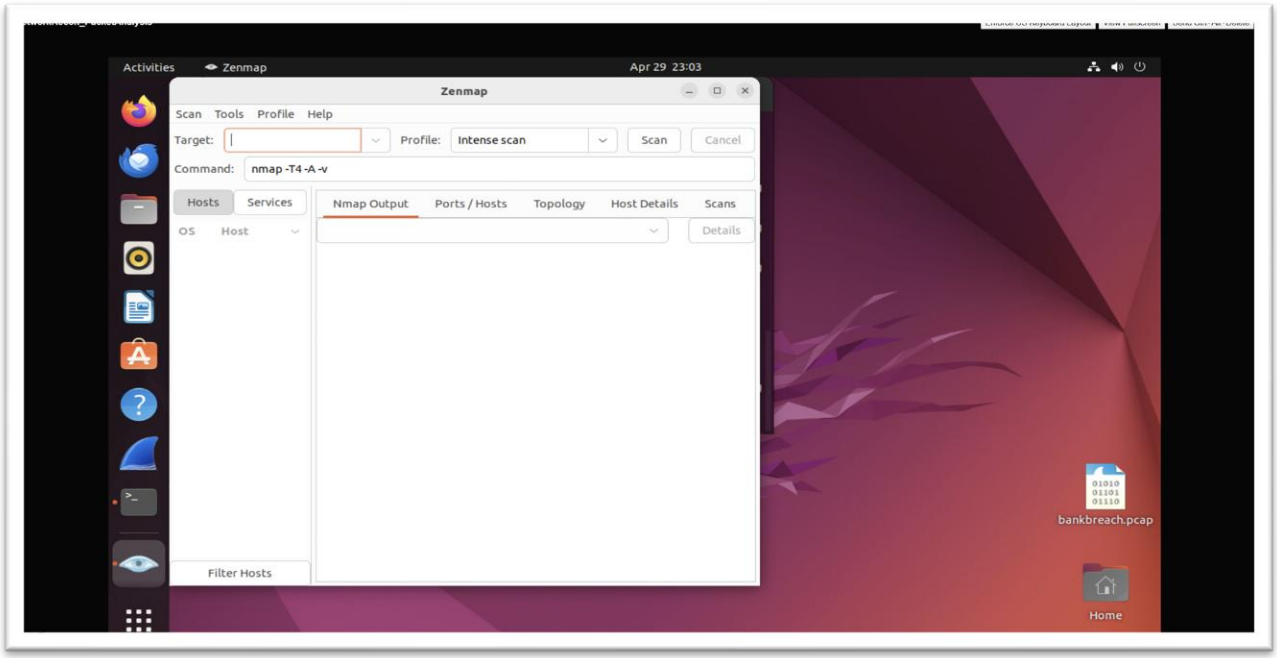

Figure 7: Screenshot of “Zenmap” tab.

- We input IP address 192.168.252.1 in the target box then select Quick scan in profile. We can note the command which is “nmap -T4 -F 192.168.252.1” as appears and the result is shown in Figure 8.

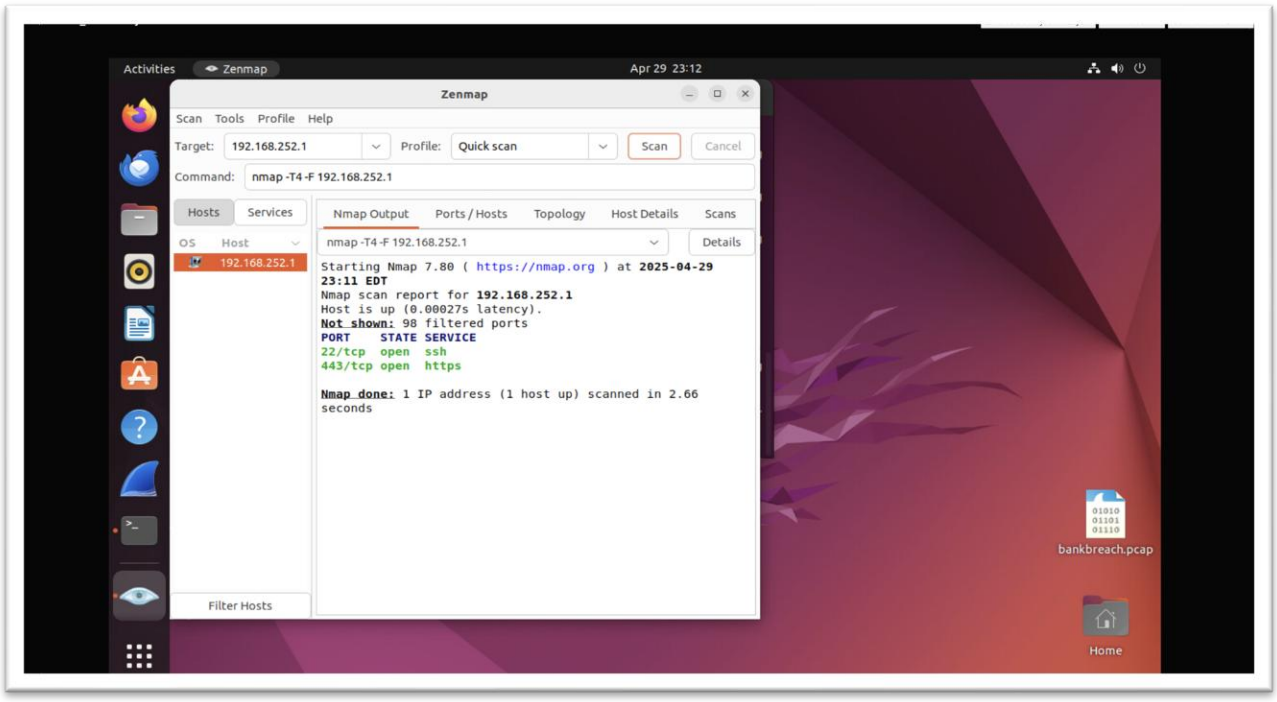

Figure 8: Screenshot of result from command “nmap -T4 -F 192.168.252.1”.

- Then we perform scan with target of 192.168.252.0/24 and select ping scan in profile which makes “nmap -sn 192.168.252.0/24” appears in Command and the result is as shown in Figure 9.

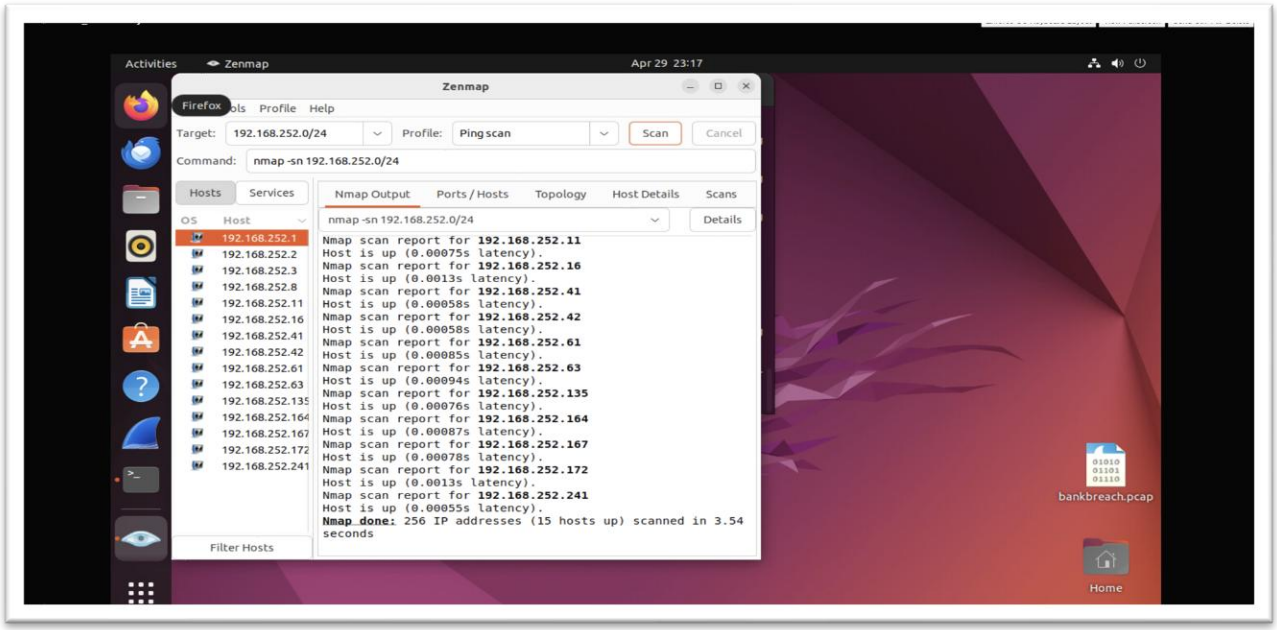

Figure 9: Screenshot of result from command “nmap -sn 192.168.252.0/24”.

- Then we enter 192.168.252.0/24 in target and select Intense scan in profile so we can also note “nmap -T4 -A -v 192.168.252.0/24” is there in command as observed in Figure 10 where we can note output from “Nmap Output”.

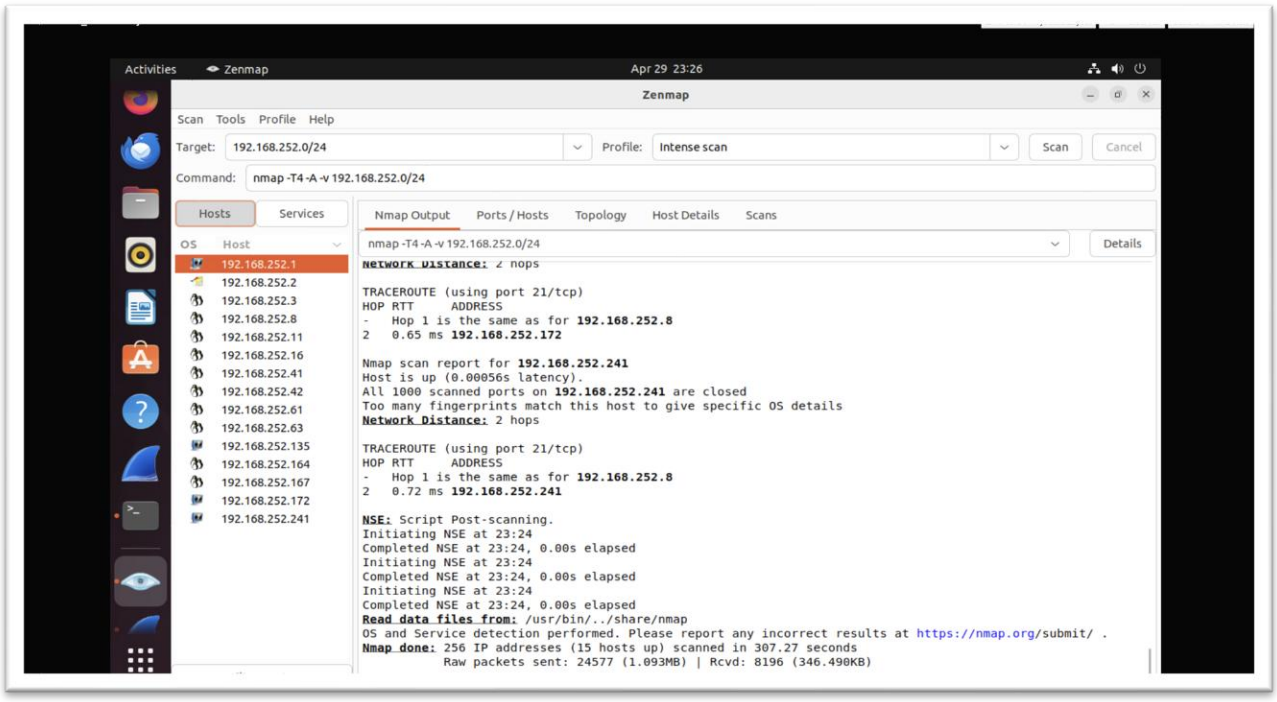

Figure 10: Screenshot of “Nmap Output” in nmap -T4 -A -v 192.168.252.0/24 in command.

- Here is output for “Ports/Hosts” for the same command used above (seen in Figure 11).

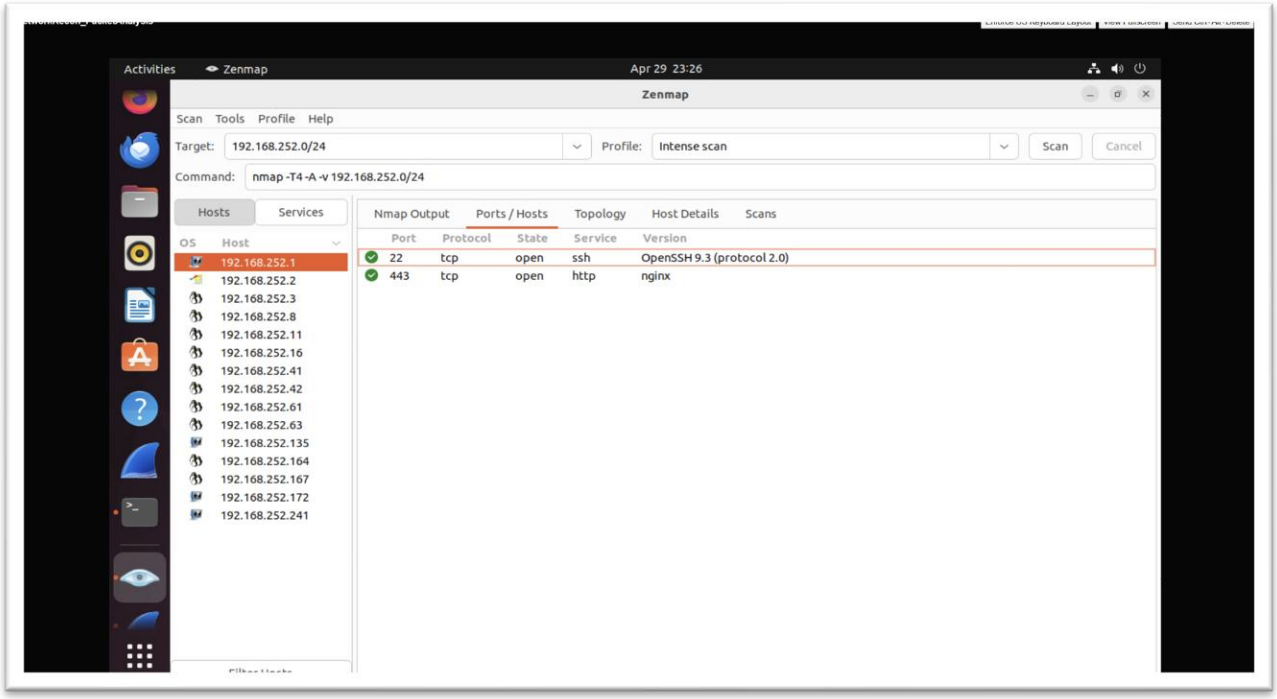

Figure 11: Screenshot of “Ports/Hosts” in nmap -T4 -A -v 192.168.252.0/24 in command.

- Here is output for “Topology” for the same command used above (seen in Figure 12).

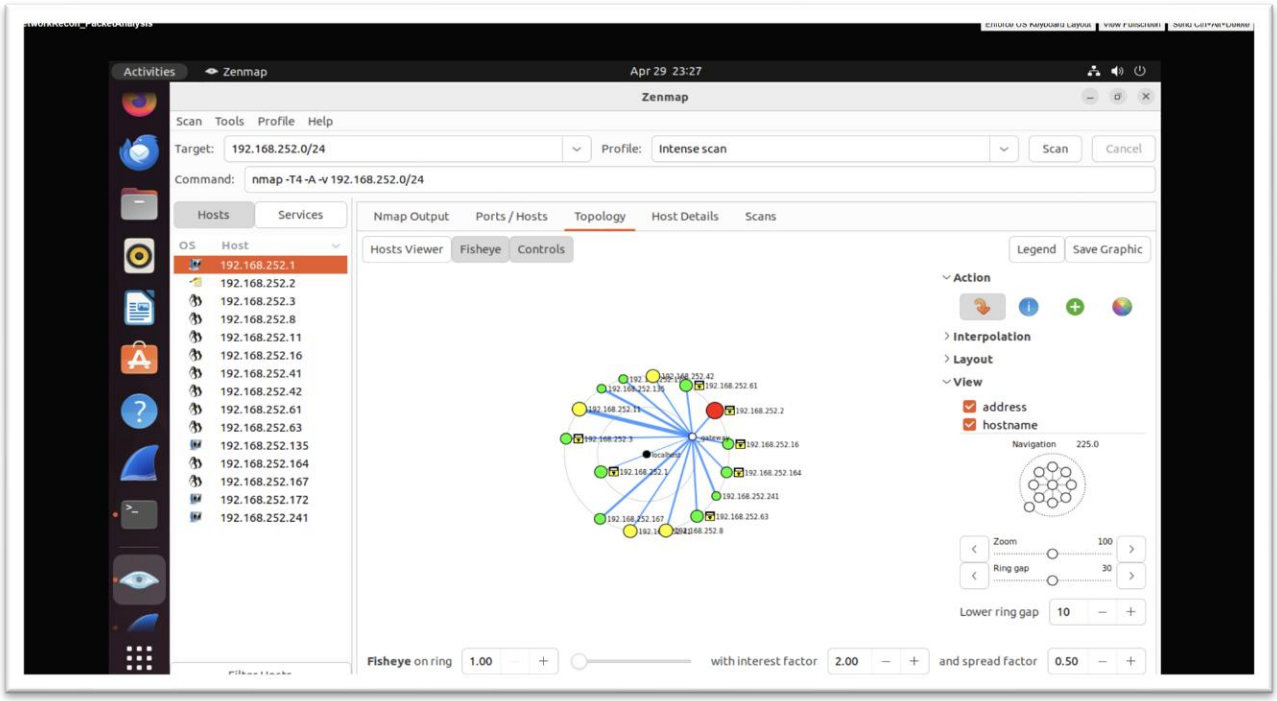

Figure 12: Screenshot of “Topology” in nmap -T4 -A -v 192.168.252.0/24 in command.

- Now, we input 192.168.252.0/24 in target and in command enter “nmap -sS -T4 192.168.252.0/24” which we can observe in Figure 13.

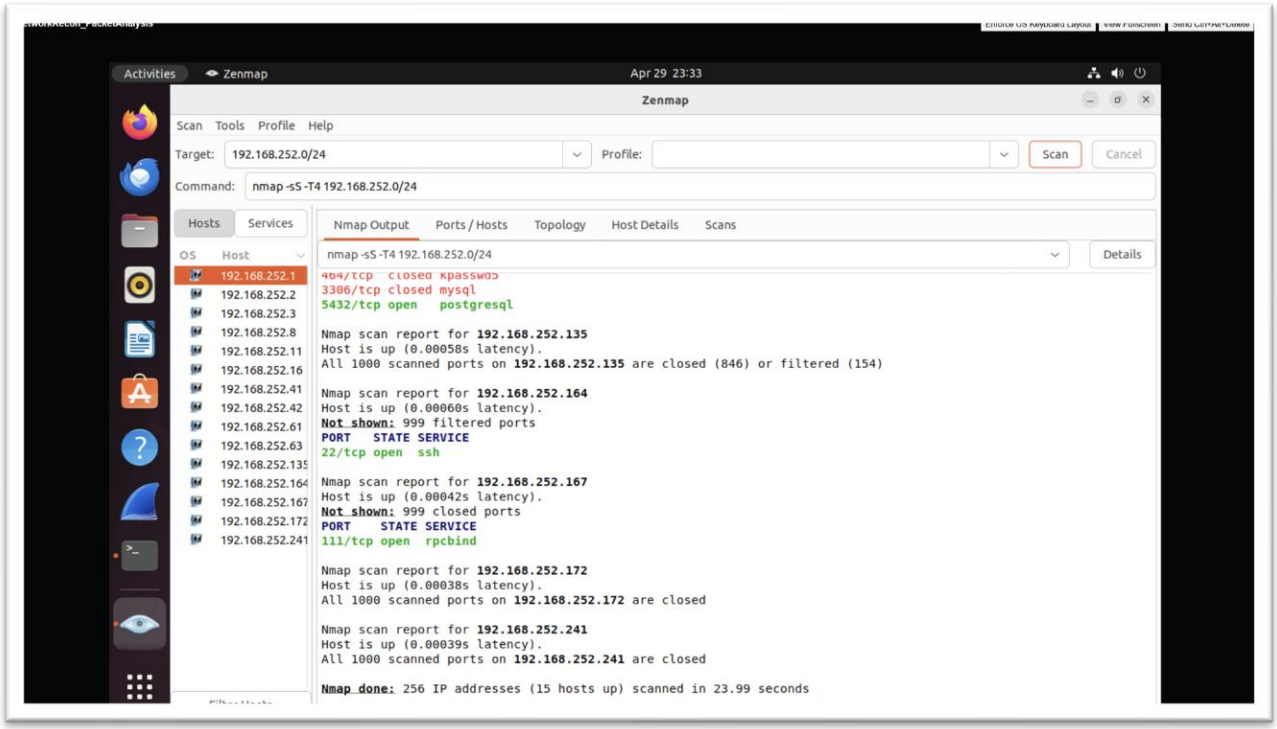

Figure 13: Screenshot of result from command “nmap -sS -T4 192.168.252.0/24”.

- Finally, we will input 192.168.252.42 in target and select- Intense scan in profile which will give us “nmap -T4 -A -v 192.168.252.42 in command as observed in Figure 14,15 and 16.

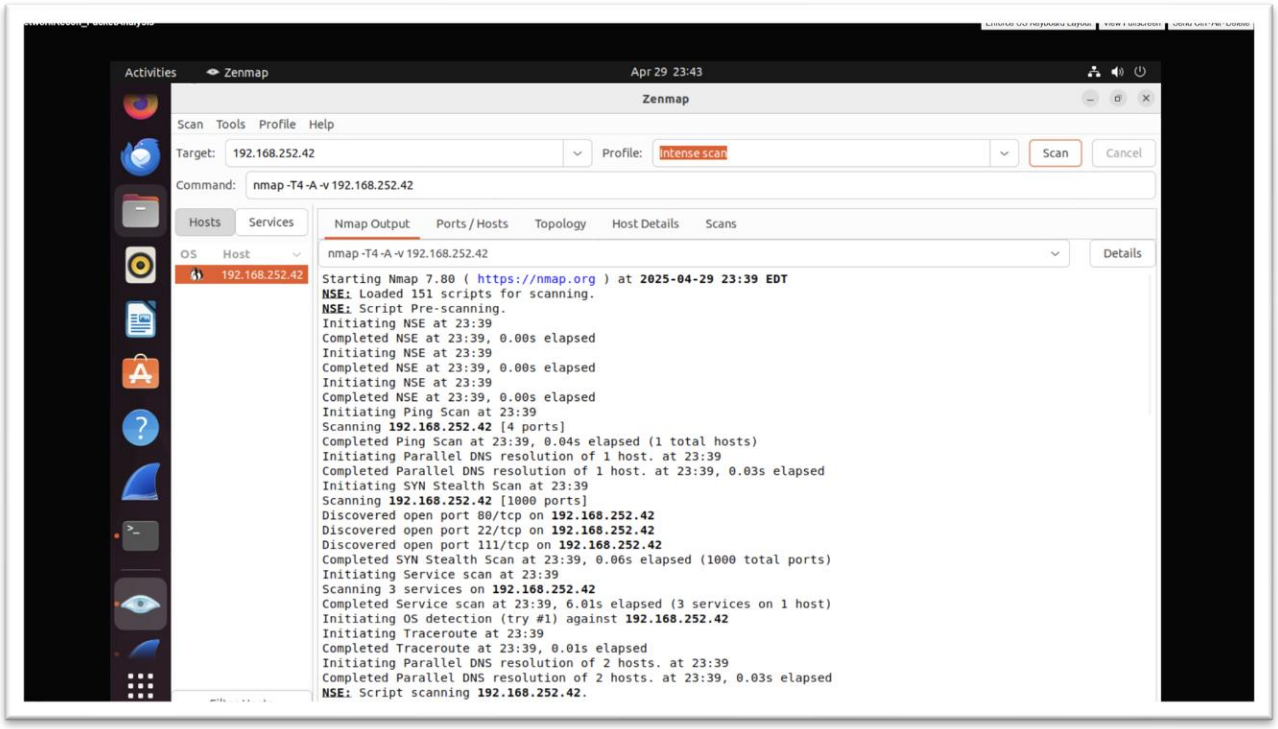

Figure 14: Screenshot of result from command “nmap -T4 -A -v 192.168.252.42”.

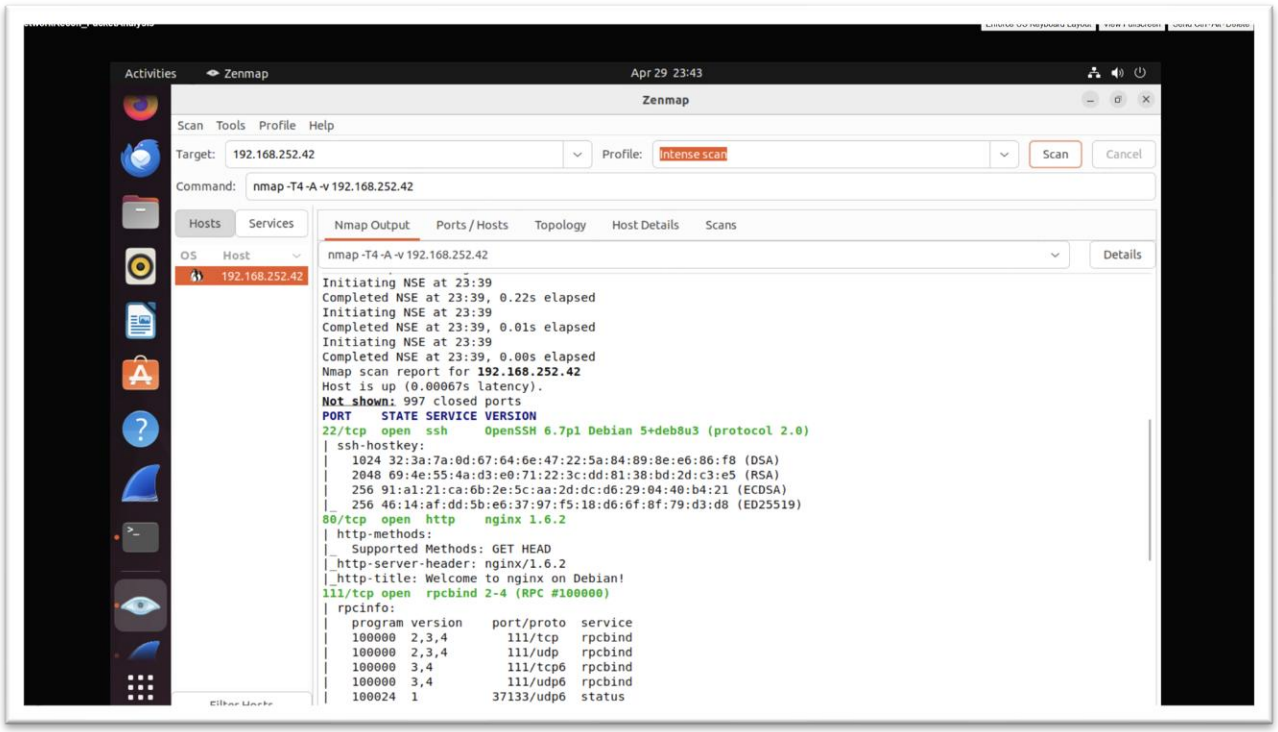

Figure 15: Screenshot of result from command “nmap -T4 -A -v 192.168.252.42”.

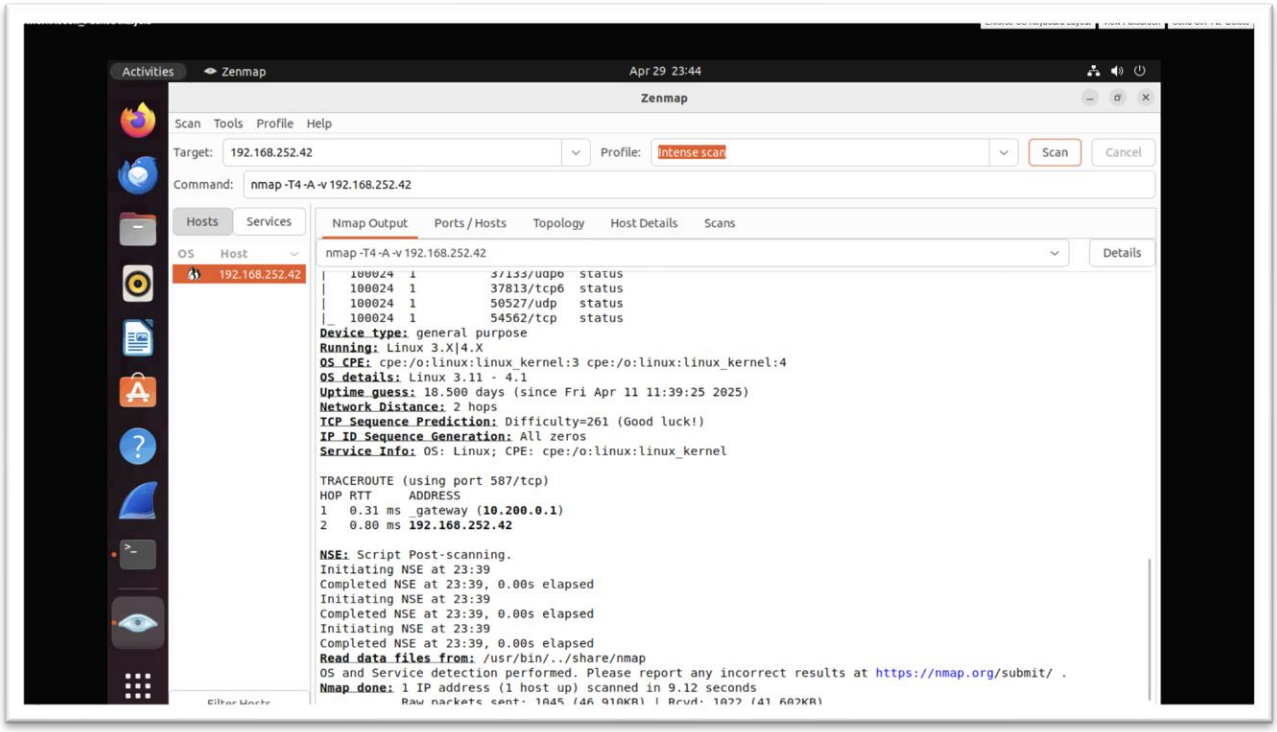

Figure 16: Screenshot of result from command “nmap -T4 -A -v 192.168.252.42”.