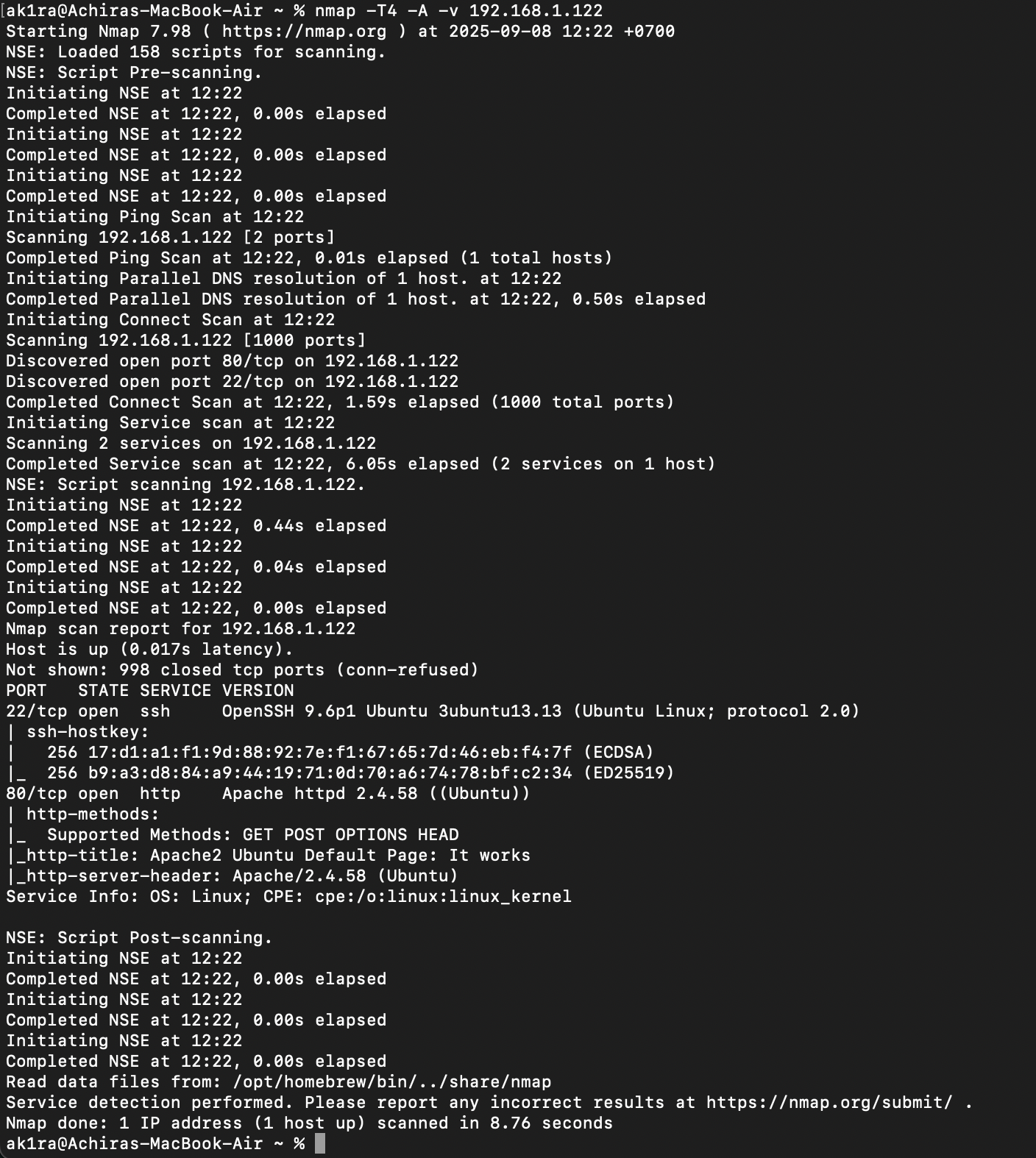
Act 3 : NetworkSecurity

Q1. Notice the open ports on all 3 devices (the attacker notebook, the target

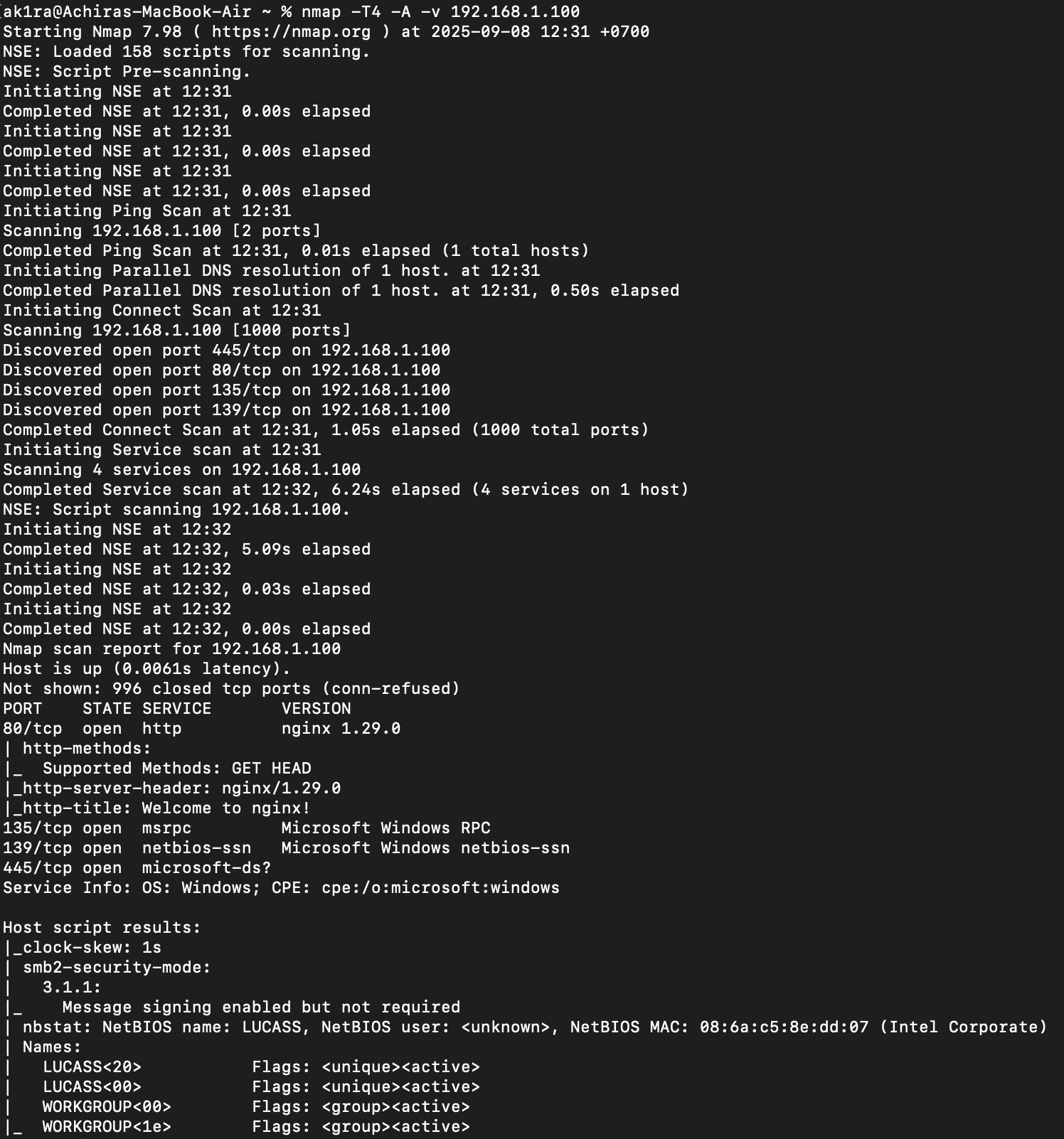
notebook, and the target Linux VM). Does anything look suspicious, i.e., some ports

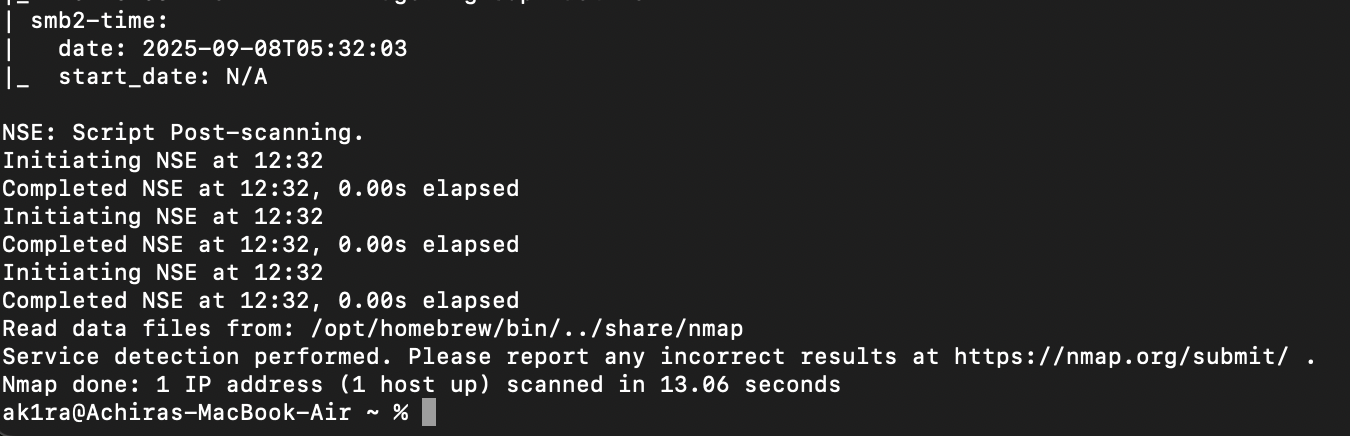
that you are not aware of that are open on the VM or on your notebooks?

VM : 

Not thing look suspicious, port 22 and 80 setting by us

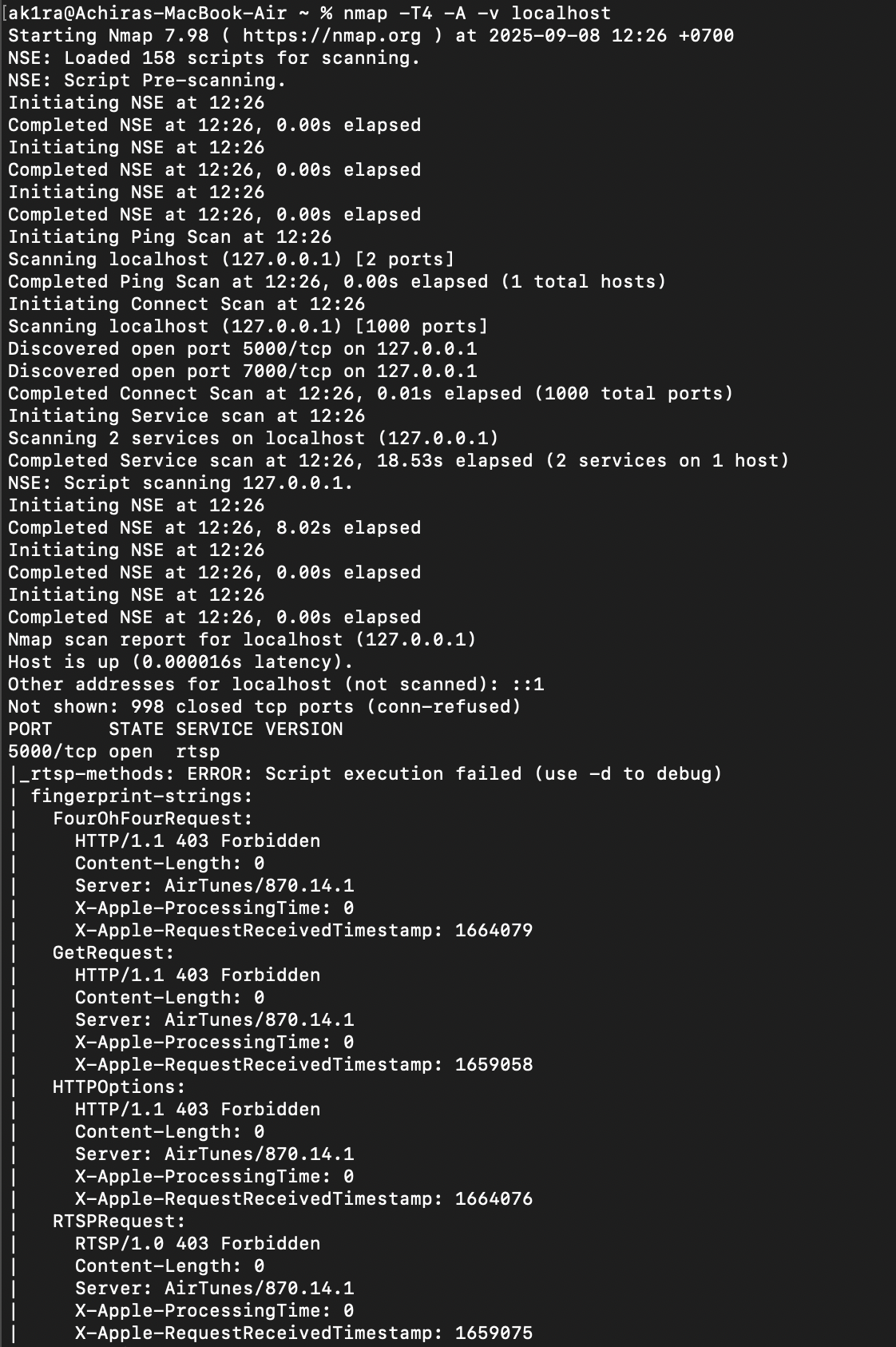
Target Notebook :

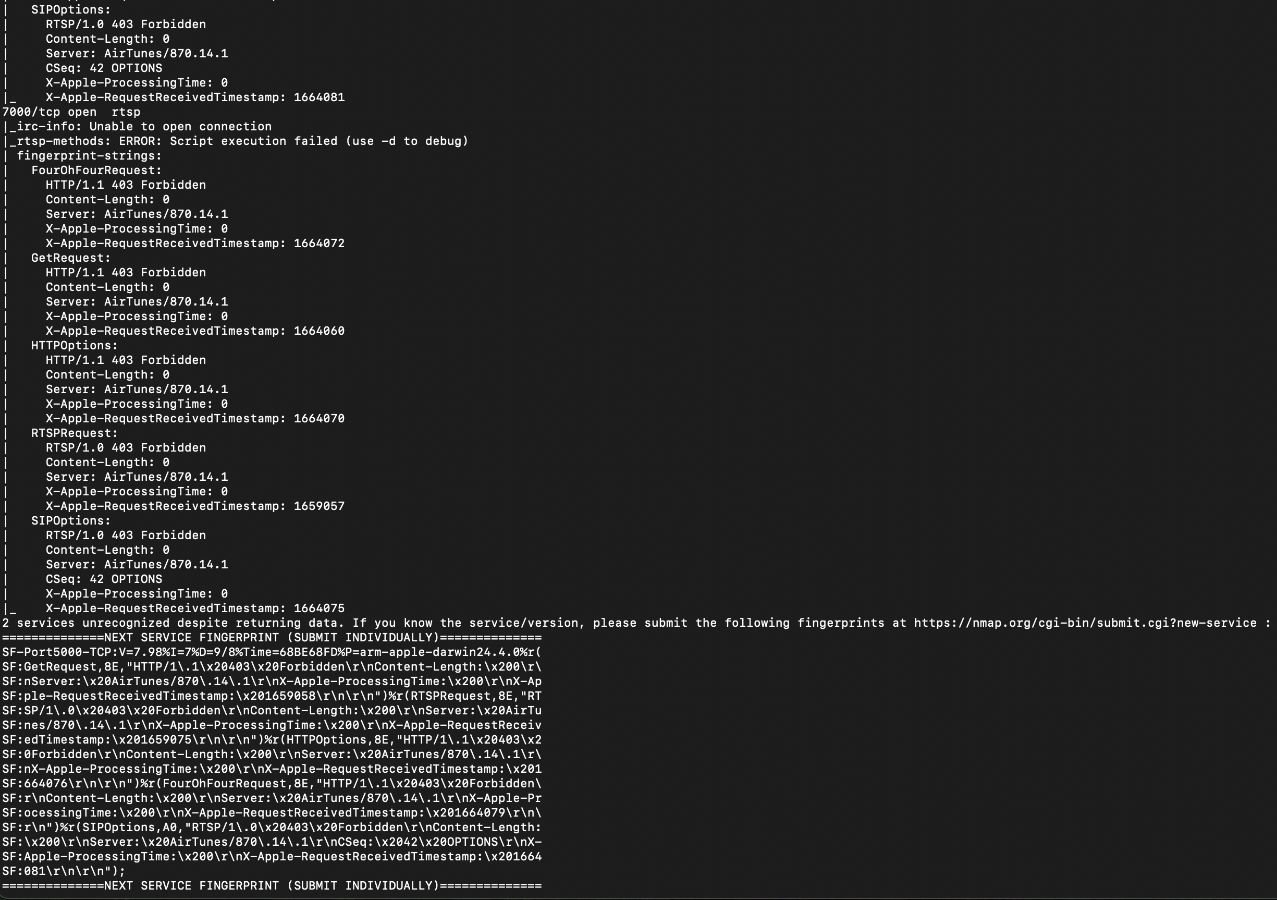




Only port 80 is suspicious because I open nginx, other like 445,135,139 is default of window

Attacker Notebook :







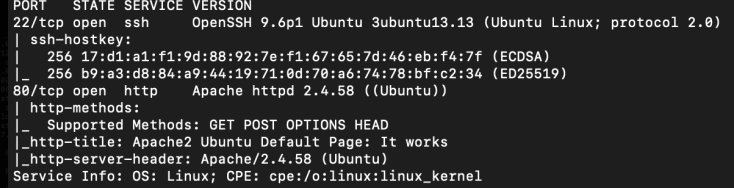
Nothing suspicious, port 5000 and 7000 is default of macOS

Q2. Look at the information provided by nmap about your OS's on all 3 devices. Is

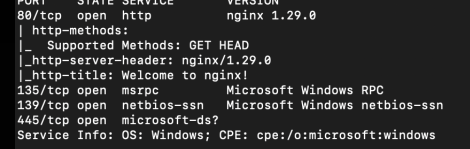
the information correct? Why is it or why is it not correct?

Ans : Its only provide two of them both of then are correct, which are

Linux of target VM :



Window of target notebook :



The one which is MacOS (attacker notebook) did not show.

Reason : namp using OS fingerprinting by sending specially crafted packet and analyzing how the target respond -> Nmap compares responses against its OS fingerprint database

And Linux VM responded a obvious fingerprint so easy so nmap, while Windows exposed multiple services -> which give much data easily identified as windows. The reason why MacOS did not show it might because it is localhost(which skip lot of step in network -> less data to identify), service not authenticate -> forbidden 403 so cant get response to analyze.

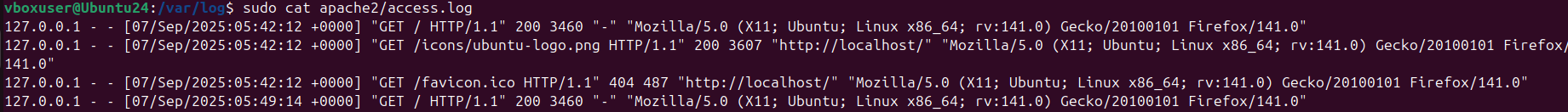
Q3. What do you think about the information you can get using nmap? Scary?

Ans : Scary a bit. So its easy for Hacker to identify which port is accessible. And might know our OS which can help hacker to plan how to hack our information

Q4. Look at the access.log file for the web server in your Linux VM. What IP

addresses do you see accessing the web server? Which devices do these IP addresses

belong to?



图片包含 背景图案

AI 生成的内容可能不正确。

127.0.0.1 : vm localhost

192.168.1.102 : attacker notebook (MacOS)

192.168.1.100 : target notebook (Windows)

Q5. Find the nmap scan in the web server log. Copy the lines from the log file that

were created because of the nmap scan.

图片包含 水, 女人, 站, 游戏机

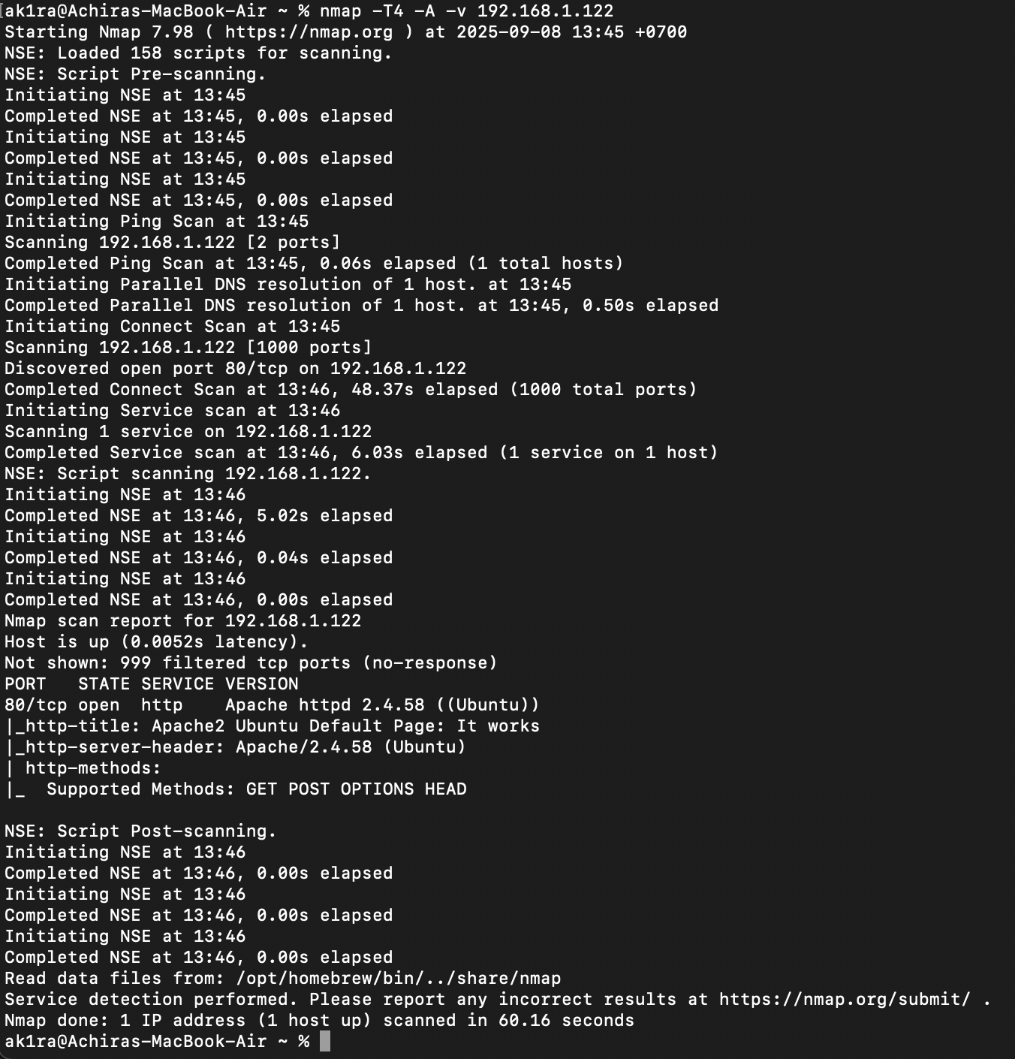
AI 生成的内容可能不正确。

Q6. After you successfully install your iptable rule(s), how do the reported results

from your new nmap scan compare to your previous scan before using iptables?

Look to see if OS detection, port open results, etc. have changed. Something(s) have

definitely changed.

Ans : 

Port open results changed : port 22/tcp gone as designed

Q7. Notice that nmap can still figure out you have Apache httpd running. Look at

the access.log file for the web server in your Linux VM. Are the logs the same as in

Part II?

Ans : same as part 2

图片包含 图形用户界面

AI 生成的内容可能不正确。

Q8. Explain whether or not you could prevent nmap from reaching the web server

while still allowing legitimate clients to get service. Will a firewall be sufficient for

this? Or do you need some other device? Please think critically about this.

Ans : Firewall is not sufficient, cuz it only work on packet-level rules (IP, port, protocol). They cannot tell whether a packet is from a real browser or from nmap.

Solution : use whitelist (for internal or allowed device) combined with Proxy/ CDN so scanner can only scan Proxy or CDN not the real device or server.

Q9. What are your firewall rules? Run iptables -L on your VM and enter the output

here.

Ans : 文本

AI 生成的内容可能不正确。

หมายเหตุ : ที่เห็นมี tcp anywhere 2 อัน เพราะผมพิมคำสั่งเหมือนกันสองรอบ มีผลเหมือนกับมีบรรทัดเดียว