KIba

KIba is a vulnerable machine of the tryhackme platform.

LInk: https://tryhackme.com/room/kiba
Goal: Find the user and root flags.
Report by: Martin Martinez

Intro:

On this machine we have to solve a series of fairly simple questions, plus we will use linux capabilities to escalate privileges.

Enumeration

As always, to know what I'm dealing with I like to send an ICMP packet to the victim machine and based on the TTL determine its operating system.

ping -c 1 10.10.78.80 > os-ping-discover.txt

```
┌──(kali㉿kali)-[~/TryHackMe/kiba]
└─$ cat os-ping-discover.txt
PING 10.10.78.80 (10.10.78.80) 56(84) bytes of data.
64 bytes from 10.10.78.80: icmp_seq=1 ttl=61 time=186 ms

--- 10.10.78.80 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 185.753/185.753/185.753/0.000 ms
```

The TTL should be 64 and therefore it is a Linux machine but the TTL decreases as the connection goes through some intermediary nodes.

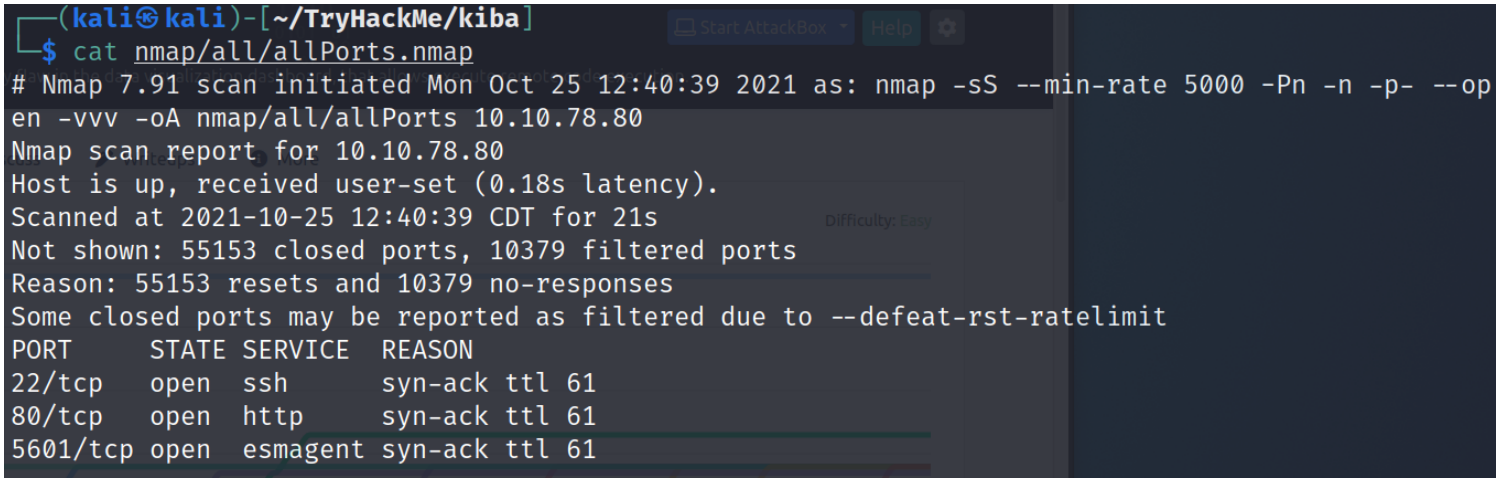
To know the available ports of the machine I like to divide this phase in two:

→ One to get all the open ports as quickly as possible.
→ Another one to concentrate on those ports and get more information.

All Ports

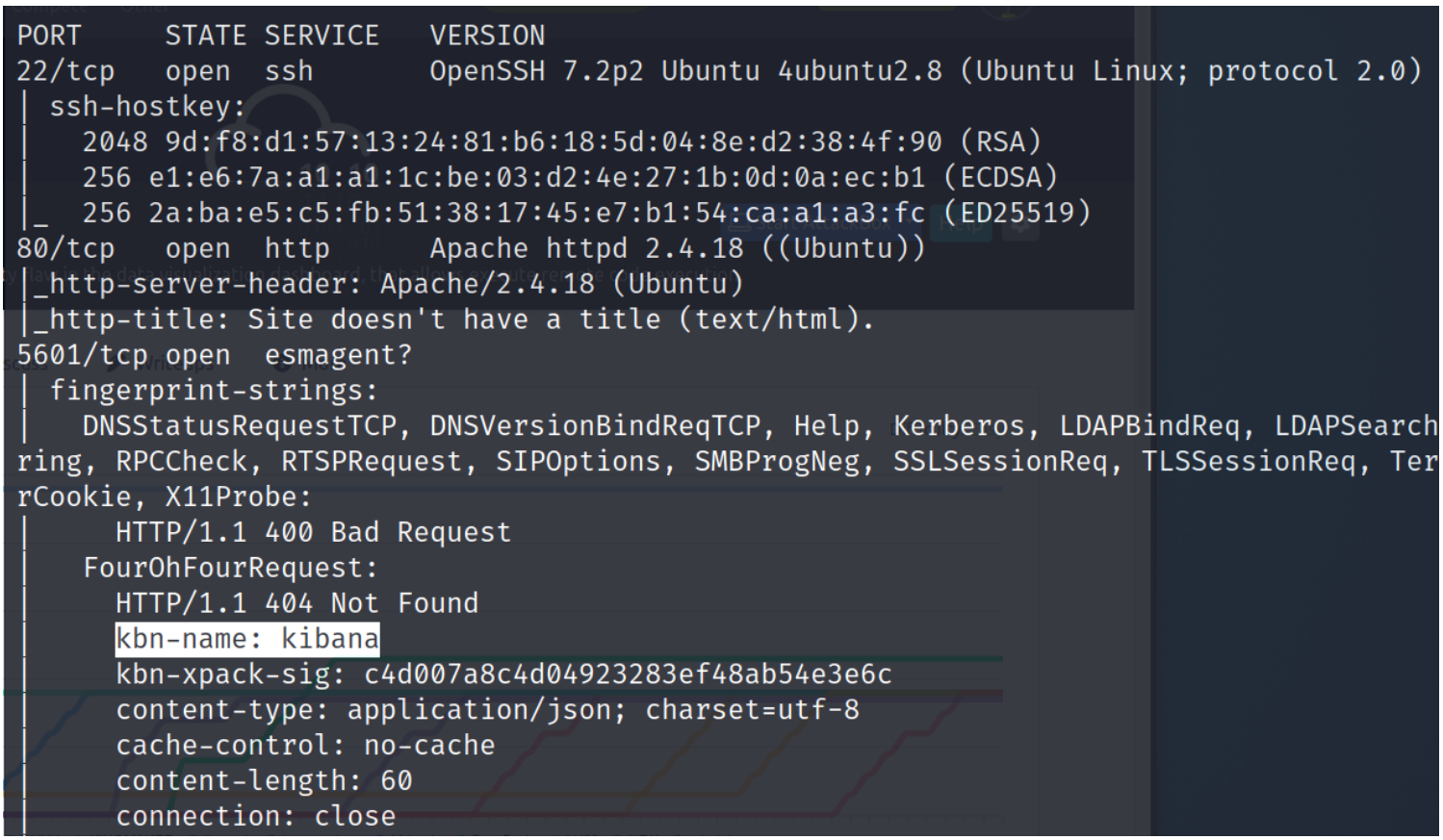
In the first scan I like to do it as fast as possible, without getting too much information as this will be done in the next scan, and it also saves me a lot of time.

nmap -sS --min-rate 5000 -Pn -n 10.10.78.80 -p- --open -vvv -oA nmap/all/allPorts



Now that I know which ports are 100% open I can focus on them and get more information with the following scan.

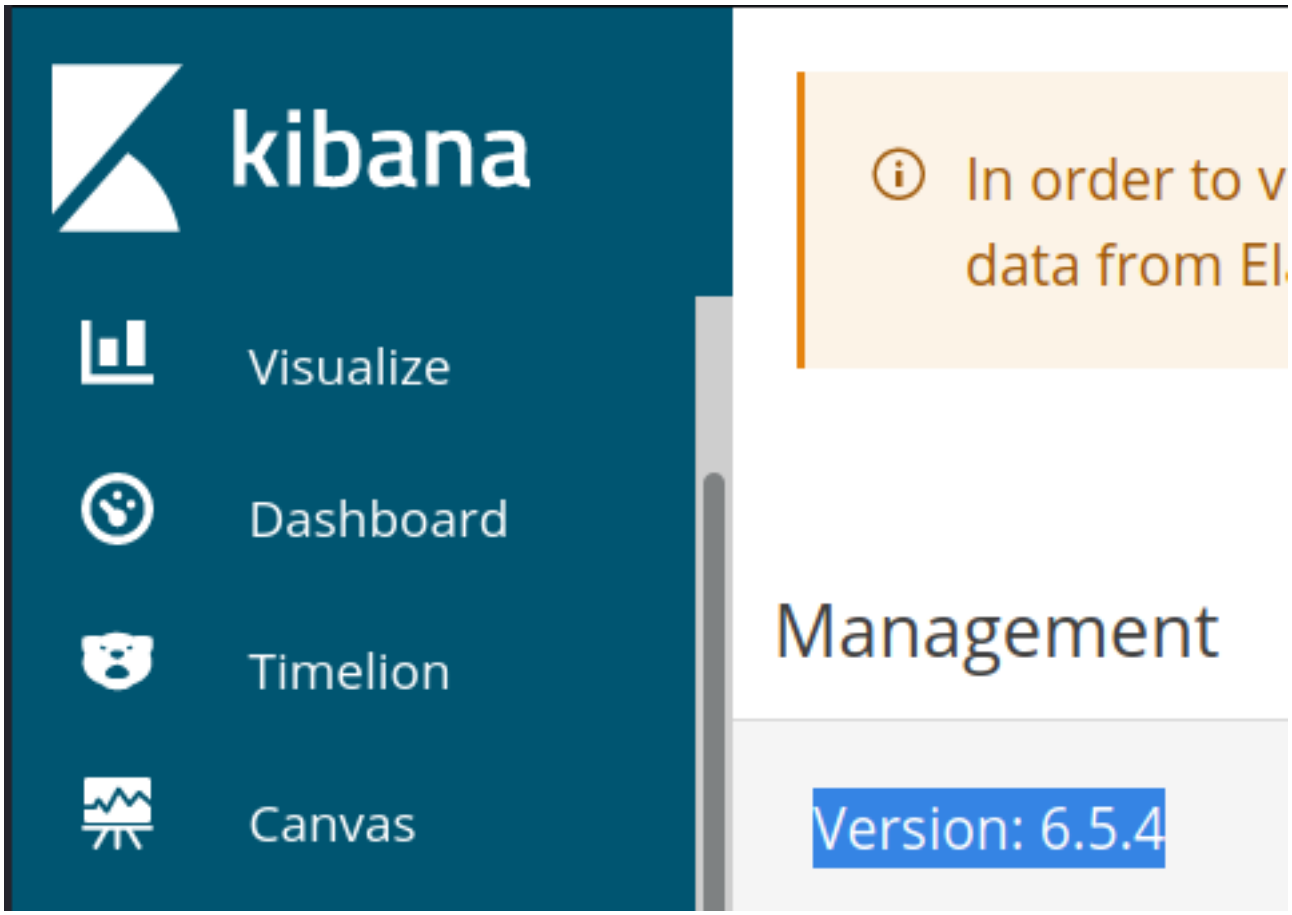
Deep Scan



This scan let me know that there is something different on port 5601 as I visited port 80, listed directories and found nothing interesting, so I went to port 5601 and there I found something very interesting, **a version**.

FootHold

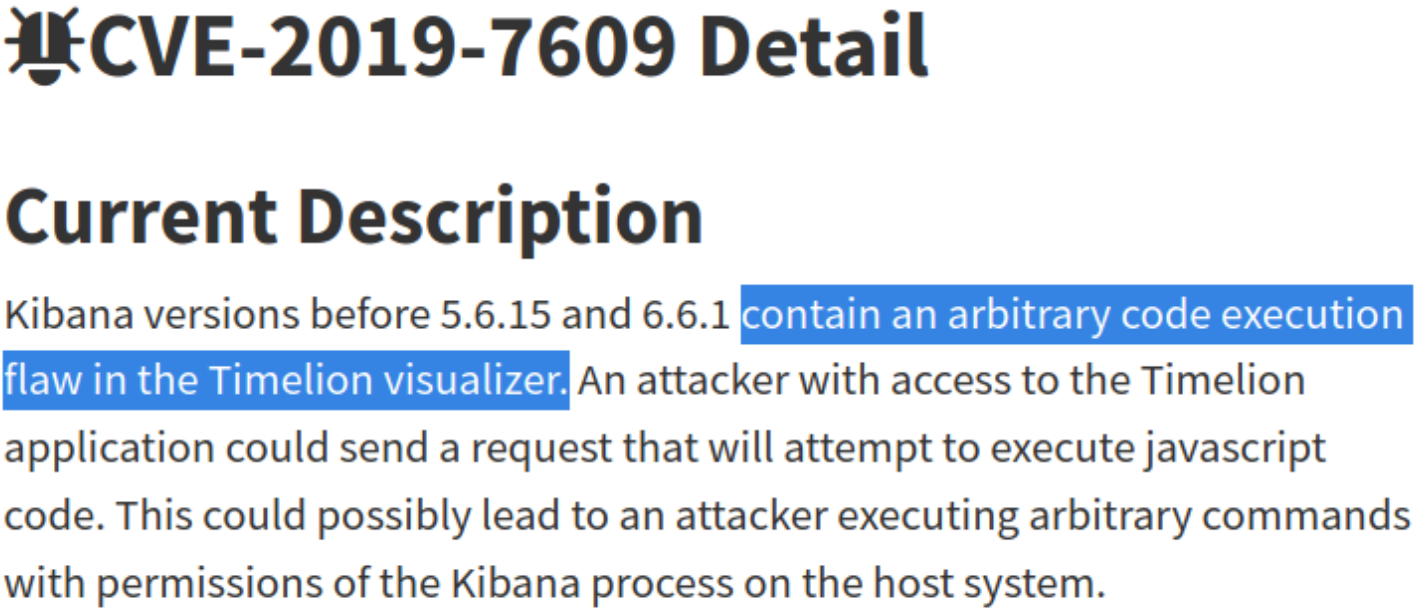
When I visited this port, I entered a data visualization panel, and there was a version that allowed me to enter the system.



While searching for vulnerabilities I found the following CVE:

→ CVE-2019-7609

CVE-2019-7609



Searching for exploits I came across the following one on GitHub, it's very good and simple to use, which for a malicious attacker makes everything much easier.

https://github.com/LandGrey/CVE-2019-7609/

When using it remember, use python2 and have netcat listening!

Once inside the system you can find the first flag very easily.

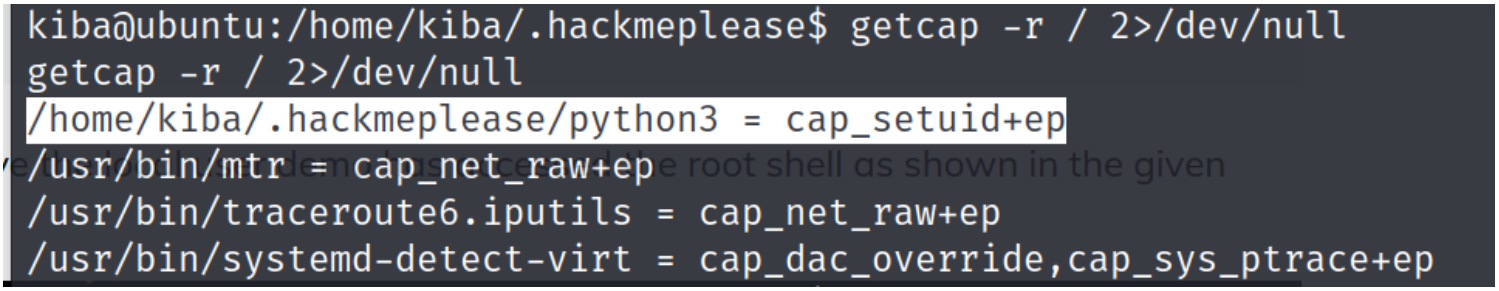
Privilege Escalation

On this machine to be able to escalate privileges you need to understand the "linux capabilities", so to do that I leave you the following link:

https://www.hackingarticles.in/linux-privilege-escalation-using-capabilities/

You need to get the following command to get the capabilities:

→ **getcap -r / 2>/dev/null**



In the home directory there is another hidden directory with a copy of python3, and it has the capabilitie "cap_setuid+ep" which allows to change the UID.

To escalate our privileges we need to enter the hidden directory and execute the following command:

→ ./python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'

And now we own the system!