Day 7 - Skilling Up

Scenario

Task 12 [Day 7] Skilling Up

Previously, we saw mcsysadmin learning the basics of Linux. With the on-going crisis, McElferson has been very impressed and is looking to push mcsysadmin to the security team. One of the first things they have to do is look at some strange machines that they found on their network.

Check out the supporting material here.

hmm strange machine that they found in the network uh, let's use nmap to scan it

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/Desktop/research]
└─$ nmap -A -oN day7 10.10.0.236
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-28 11:26 EST
Nmap scan report for 10.10.0.236
Host is up (0.20s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 1b:50:31:d9:93:f8:0f:f7:a0:8f:79:ba:6b:5d:92:df (RSA)
|   256 ad:27:08:b0:b0:29:d6:f4:b7:67:dd:45:3c:65:d9:53 (ECDSA)
|_  256 da:3b:79:5f:48:aa:1a:64:fa:5f:58:02:3a:84:74:ca (ED25519)
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          39922/udp6  status
|   100024  1          46445/udp   status
|   100024  1          55157/tcp6  status
|_  100024  1          58833/tcp   status
999/tcp open  http    SimpleHTTPServer 0.6 (Python 3.6.8)
|_http-server-header: SimpleHTTP/0.6 Python/3.6.8
|_http-title: Directory listing for /
```

Question: how many TCP ports under 1000 are open?
- 3

Question: What is the name of the OS of the host?

the nmap unable to exactly find out what's the exact OS the host use but if we check out the TCP/IP fingerprint here we found that it was a linux host!

```
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=11/28%OT=22%CT=1%CU=41705%PV=Y%DS=2%DC=I%G=Y%TM=5FC27B
OS:00%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OP
OS:S(O1=M505ST11NW6%O2=M505ST11NW6%O3=M505NNT11NW6%O4=M505ST11NW6%O5=M505ST
```

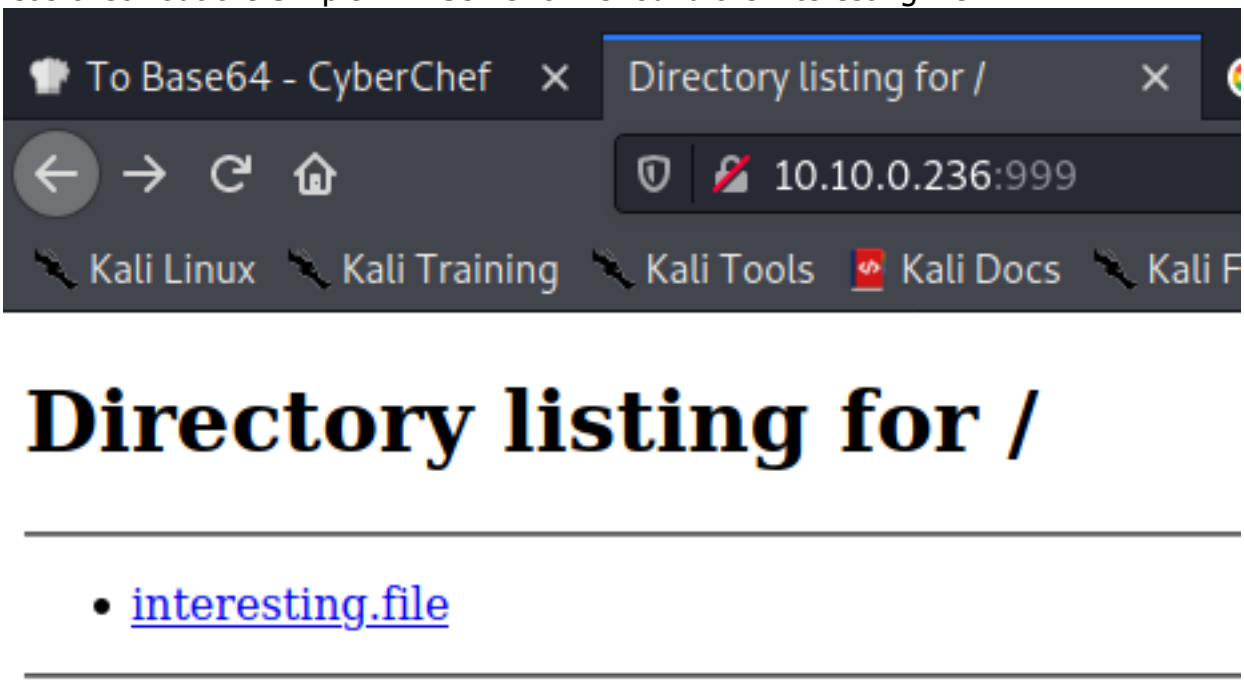
-linux

Question: What version of SSH is running?

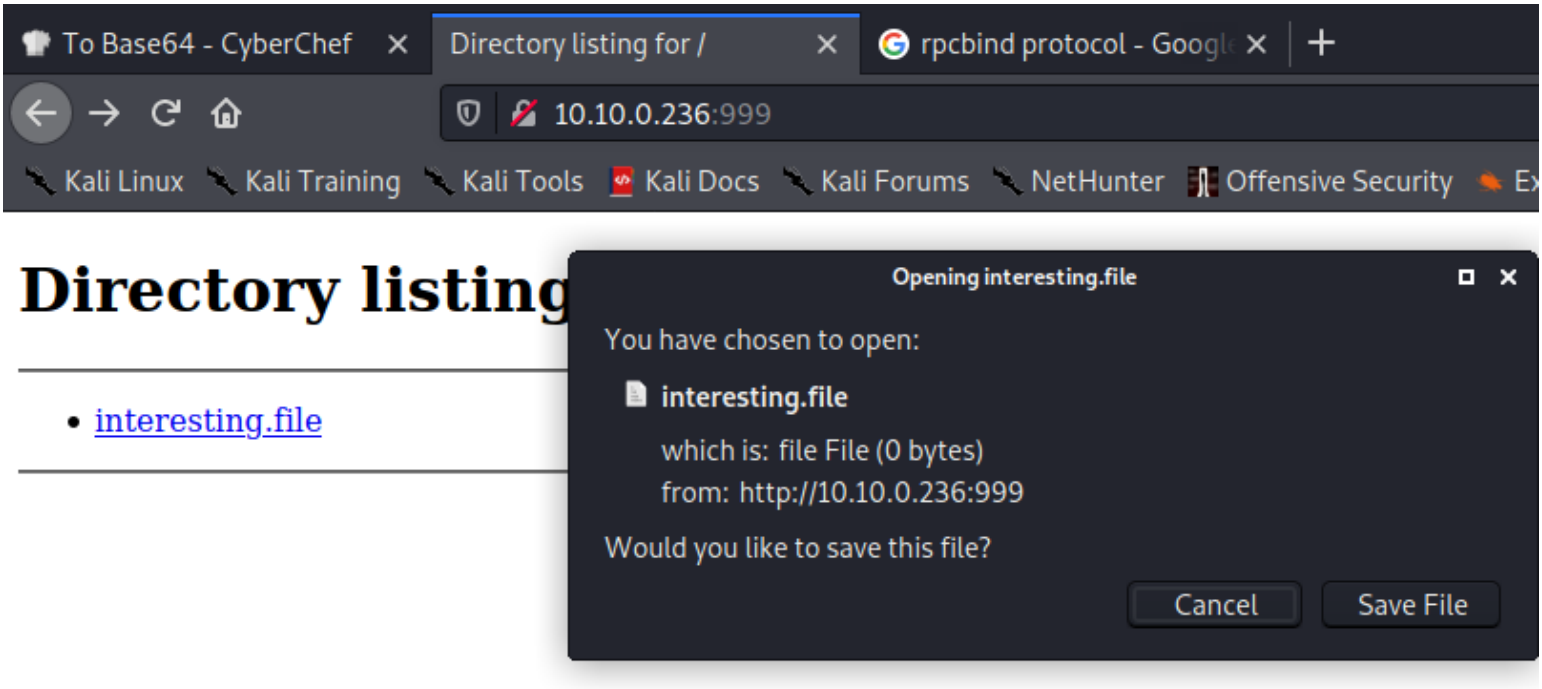
```
22/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)
```

- 7.4

let's check out the SimpleHTTPServer & we found the interesting.file



& we can access it!



Question: What is the name of the file that is accessible on the server you found running?
- interesting.file