IPK 2018 DHCP Starvation útok

Obsah

Autor

- jmeno: Adam Petráš
- login: xpetra19

Zadání

Vašim úkolem je:

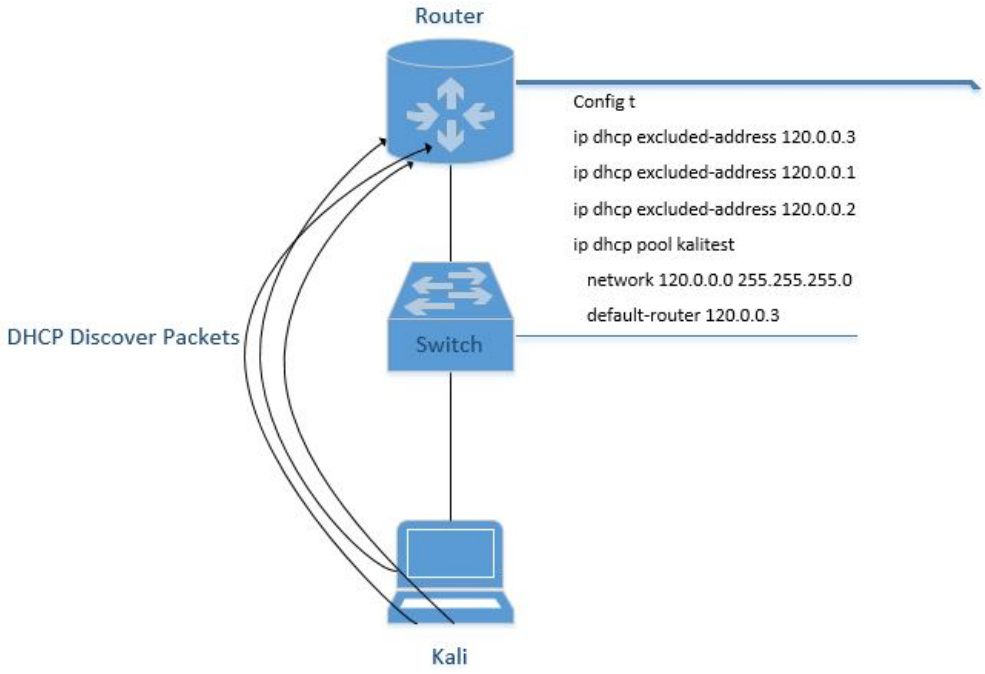
- Nastudovat problematiku DHCP útoků a relevantní informace uvést v projektové dokumentaci. (až 6 bodů)
- Naprogramovat aplikace realizující DHCP Starvation útok, který by vyčerpal adresní pool legitimního DHCP serveru (až 12 bodů)
- Demonstrovat činnost aplikací v podmínkách Vaší vlastní testovací sítě. (až 2 body)

Teorie

DHCP je protokol, který slouží na automatickou konfiguraci zařízení. Typicky jde o koncové zařízení například počítač, telefon atd. Díky DHCP tyto zařízení dostanou přidělenou IP adresu, masku, default gateway, DNS atd. Co se stane pokud nebude tento mechanismus fungovat? Nebude fungovat připojení v rámci sítě, ani internetu. Tomuto typu se říká DoS (Denial of Service attack).

DHCP starvation attack spočívá prově v tom, že každý DHCP server má přesně definovaný konečný počet IP adres, které dokáže jednotlivým zařízením přidělit. Například pokud budu mít IP adresu 192.168.0.0 a masku 255.255.255.0 (také jako 192.168.0.0/24), tak může přidělit maximálně 253 použitelných adres. První adresa(192.168.0.1) adresa sítě a poslední adresa(192.168.0.255) adresa broadcastu jsou využity. Pokud si útočník vyžádá jední počítačem volné IP adresy, které má server k dispozici, tak potřebuje ke každé IP adrese falešnou MAC adresu. Poté vyčerpá serveru všechny IP adresy. Po vyřazení DHCP serveru je možné převzít úlohy DHCP a tím pádem můžeme operovat s falešným DNS serverem a podobně.

Obrázek ukazuje jak funguje DHCP útok který vysílá obrovské množství DHCP požadavků s falešnými MAC adresami.



Řešení

Řešení projektu probíhalo ve více fázích. Prvně jsem studoval co to vlastně je DHCP starvation attack zjistil jsem, že může být veden více způsoby a vybral jsem pro mě asi nejzajímavější a to je posílání `DHCP Discovery` packetů. Dale je zde možnost posílání RAW socketů, nebo vytvoření DHCP rogue serveru a jako poslední je posílání Release packetů. Inspiroval jsem se softwarem *yersinia* na Kali linuxu. V další fázi probíhala implementace v jazyce C++. Další fází bylo testování na domácí síti. Testování probíhalo tak, že jsem spustil wireshark po spustění wiresharku na dané zařízení jsem spustil program a sledoval co se děje. Dále jsem při testování zjistil, že pokud spustím aplikaci, tak nemůžu nic dělat. Najednou zamrzne celé spojení s routerem. Ve Wiresharku bylo jasně vidět, jakou mají packety cílouvou, zdrojovou adresu, velikost packetu, protokol, atd. Jako poslední fáze byla dokumentace zdrojového kódu a dokumentace projektu.

Implementace

Vytvořím socket poté socketu přídám adresu. Vytvořím socket jako broadcastový. Spojím socket a zařízení. Pote spojím socket k sockaddr.

Nekonečný cyklus kde nastavuju hodnoty dhcp packetu například opcode, typ hardware, flagy, ID, klientovskou, serverovou a dhcp IP, poté vygeneruju MAC adresu a přiřadím ji. Nakonec nastavím optiony DHCP packetu. Poté zadefinuju typ komunikace port a adresu a packet pošlu. Nakonec vypíšu MAC adresu a "Discovery packet sent!" A to v nekonečné smyčce dokola.

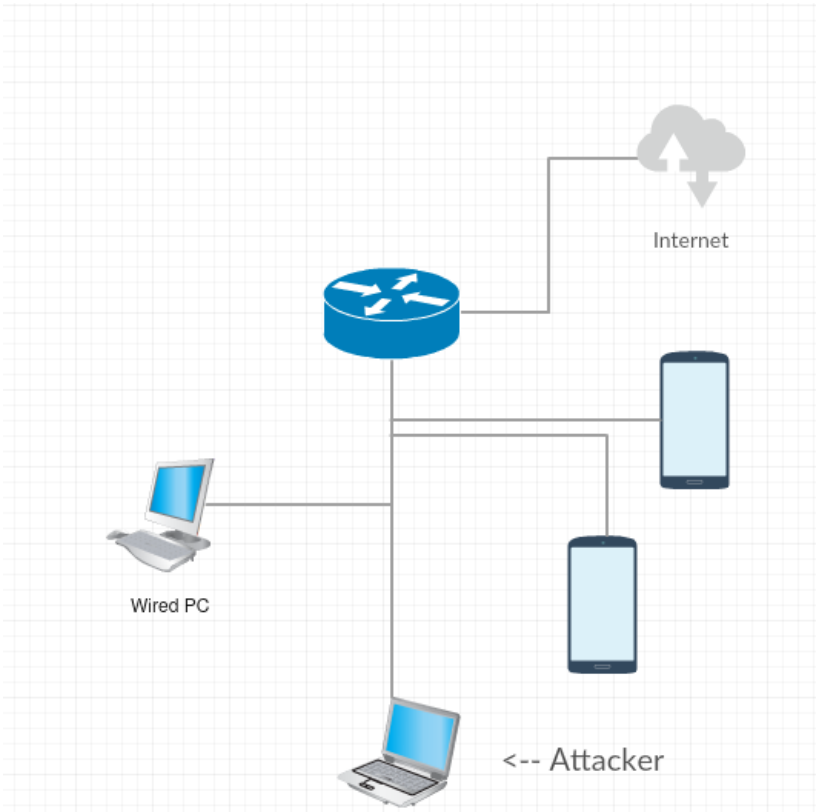
Příklad

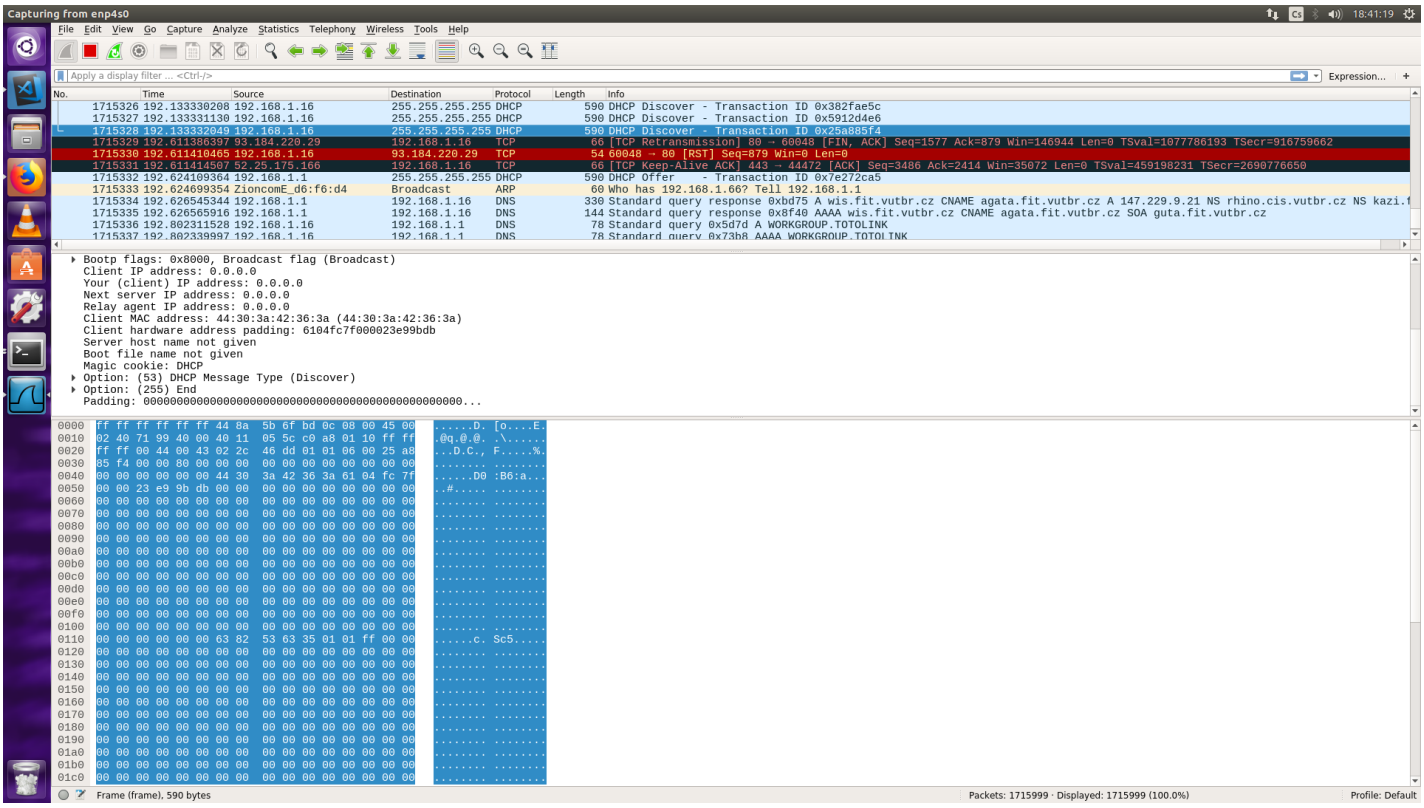
```
sudo ./dhcp -i *interface*
sudo ./dhcp -h
sudo ./dhcp --help
```

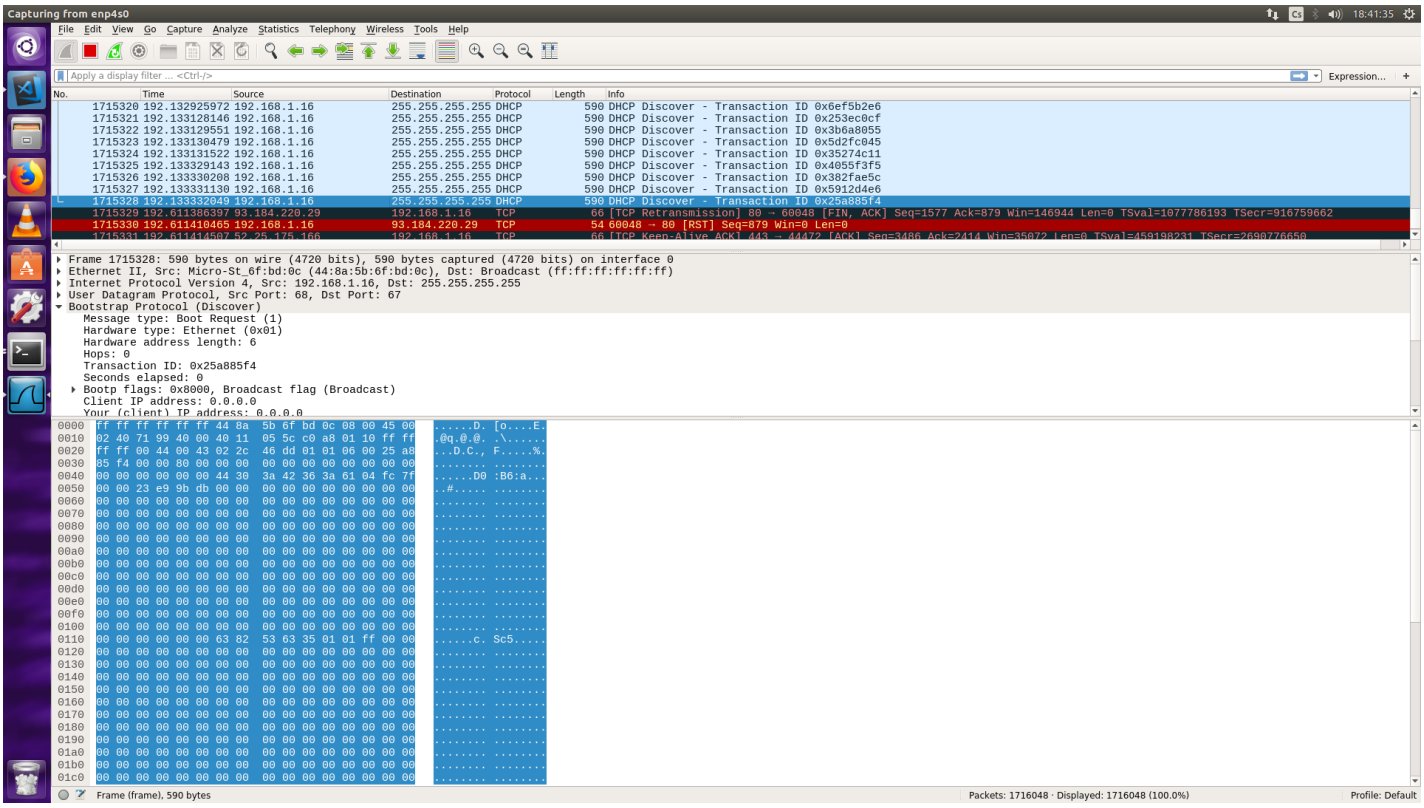
interface je jméno rozhraní dle OS, na které útočník vygeneruje patřičný provoz s kompromitačními účinky na DHCP server

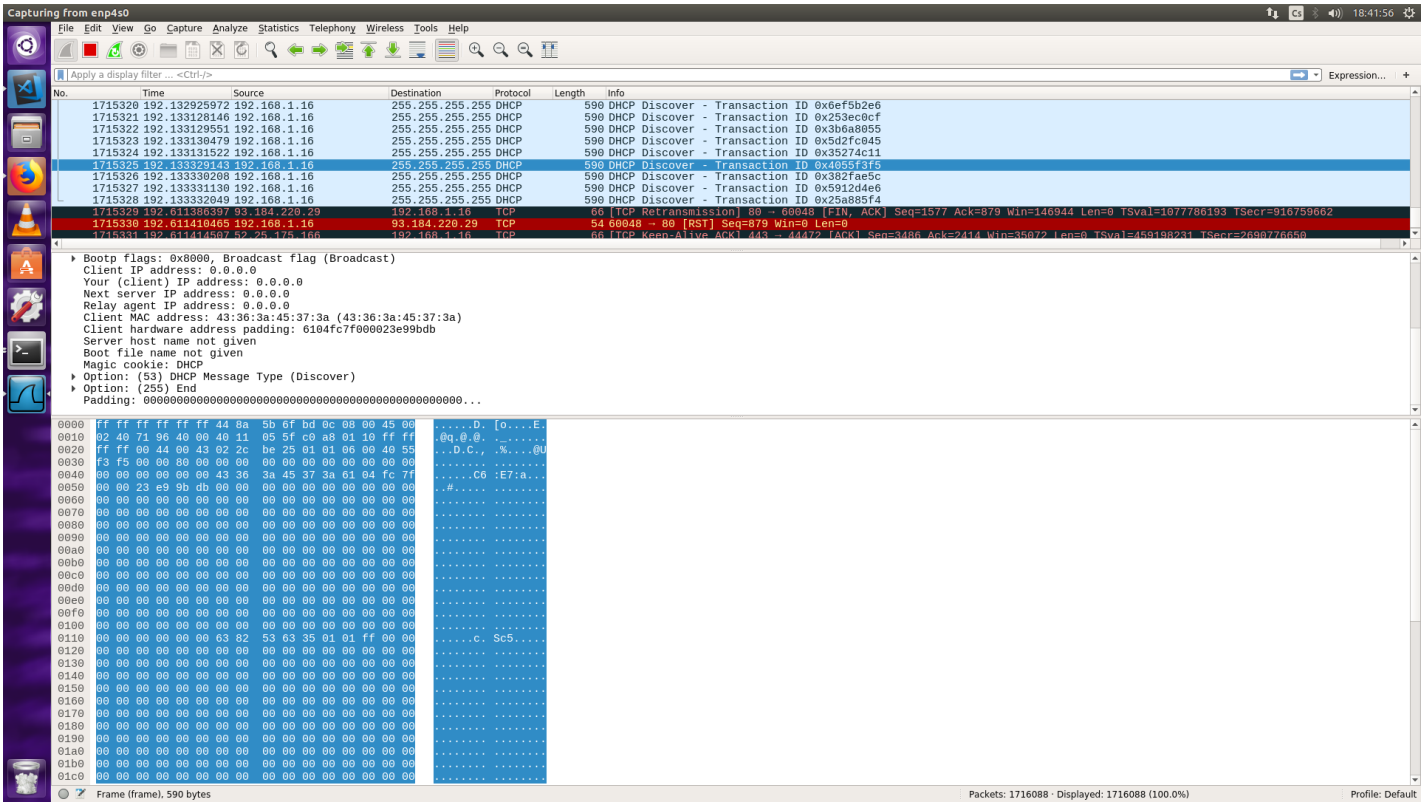
Demonstrace z testování

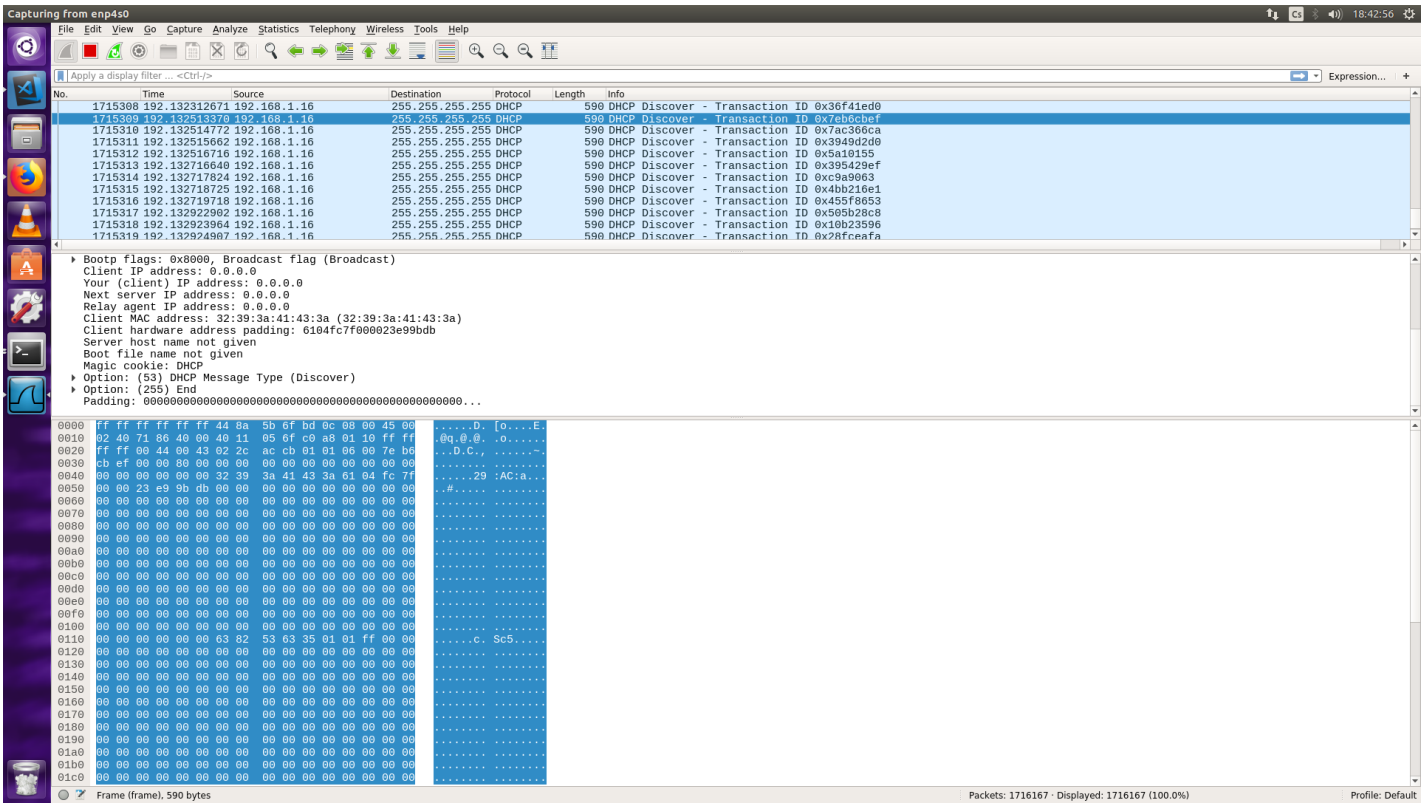
Topologie mé domácí sítě:


Internet
Wired PC
<-- Attacker


Capturing from enp4s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1715326 192.133330208 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x382fae5c
1715327 192.133331130 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x5912d4e6
1715328 192.133332049 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x25a885f4
1715329 192.611386397 93.184.220.29 192.168.1.16 TCP 66 [TCP Retransmission] 80 → 60048 [FIN, ACK] Seq=1577 Ack=879 Win=146944 Len=0 TSval=1077786193 TSecr=916759662
1715330 192.611410465 192.168.1.16 93.184.220.29 TCP 54 60048 → 80 [RST] Seq=879 Win=0 Len=0
1715331 192.611414507 52.25.175.166 192.168.1.16 TCP 66 [TCP Keep-Alive ACK] 443 → 44472 [ACK] Seq=3486 Ack=2414 Win=35072 Len=0 TSval=459198231 TSecr=2690776650
1715332 192.624109364 192.168.1.1 255.255.255.255 DHCP 590 DHCP Offer - Transaction ID 0x7e272ca5
1715333 192.624699354 ZioncomE_d6:f6:d4 Broadcast ARP 60 Who has 192.168.1.66? Tell 192.168.1.1
1715334 192.626545344 192.168.1.1 192.168.1.16 DNS 330 Standard query response 0xbd75 A wis.fit.vutbr.cz CNAME agata.fit.vutbr.cz A 147.229.9.21 NS rhino.cis.vutbr.cz NS kazi.f
1715335 192.626565916 192.168.1.1 192.168.1.16 DNS 144 Standard query response 0x8f40 AAAA wis.fit.vutbr.cz CNAME agata.fit.vutbr.cz SOA guta.fit.vutbr.cz
1715336 192.802311528 192.168.1.16 192.168.1.1 DNS 78 Standard query 0x5d7d A WORKGROUP.TOTOLINK
1715337 192.802339997 192.168.1.16 192.168.1.1 DNS 78 Standard query 0x73b8 AAAA WORKGROUP.TOTOLINK
Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: 44:30:3a:42:36:3a (44:30:3a:42:36:3a)
Client hardware address padding: 6104fc7f000023e99bdb
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Option: (255) End
Padding: 0000000000000000000000000000000000000000000000000000...
0000 ff ff ff ff ff ff 44 8a 5b 6f bd 0c 08 00 45 00 ......D. [o....E.
0010 02 40 71 99 40 00 40 11 05 5c c0 a8 01 10 ff ff .@q.@.@. .\......
0020 ff ff 00 44 00 43 02 2c 46 dd 01 01 06 00 25 a8 ...D.C., F.....%.
0030 85 f4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0040 00 00 00 00 00 00 44 30 3a 42 36 3a 61 04 fc 7f ......D0 :B6:a...
0050 00 00 23 e9 9b db 00 00 00 00 00 00 00 00 00 00 ..#..... ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0110 00 00 00 00 00 00 63 82 53 63 35 01 01 ff 00 00 ......c. Sc5.....
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Frame (frame), 590 bytes
Packets: 1715999 · Displayed: 1715999 (100.0%)
Profile: Default


Capturing from enp4s0
18:41:35
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1715320 192.132925972 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x6ef5b2e6
1715321 192.133128146 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x253ec0cf
1715322 192.133129551 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x3b6a8055
1715323 192.133130479 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x5d2fc045
1715324 192.133131522 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x35274c11
1715325 192.133329143 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x4055f3f5
1715326 192.133330208 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x382fae5c
1715327 192.133331130 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x5912d4e6
1715328 192.133332049 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x25a885f4
1715329 192.611386397 93.184.220.29 192.168.1.16 TCP 66 [TCP Retransmission] 80 → 60048 [FIN, ACK] Seq=1577 Ack=879 Win=146944 Len=0 TSval=1077786193 TSecr=916759662
1715330 192.611410465 192.168.1.16 93.184.220.29 TCP 54 60048 → 80 [RST] Seq=879 Win=0 Len=0
1715331 192.611414507 52.25.175.166 192.168.1.16 TCP 66 [TCP Keep-Alive ACK] 443 → 44472 [ACK] Seq=3486 Ack=2414 Win=35072 Len=0 TSval=459198231 TSecr=2690776650
Frame 1715328: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
Ethernet II, Src: Micro-St_6f:bd:0c (44:8a:5b:6f:bd:0c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x25a885f4
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
0000 ff ff ff ff ff ff 44 8a 5b 6f bd 0c 08 00 45 00 ......D. [o....E.
0010 02 40 71 99 40 00 40 11 05 5c c0 a8 01 10 ff ff .@q.@.@. .\.....
0020 ff ff 00 44 00 43 02 2c 46 dd 01 01 06 00 25 a8 ...D.C., F.....%.
0030 85 f4 00 00 80 00 00 00 00 00 00 00 00 00 00 00 ....
0040 00 00 00 00 00 00 44 30 3a 42 36 3a 61 04 fc 7f ......D0 :B6:a...
0050 00 00 23 e9 9b db 00 00 00 00 00 00 00 00 00 00 ..#..... ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0110 00 00 00 00 00 00 63 82 53 63 35 01 01 ff 00 00 ......c. Sc5.....
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Frame (frame), 590 bytes
Packets: 1716048 · Displayed: 1716048 (100.0%)
Profile: Default


Capturing from enp4s0
18:41:56
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1715320 192.132925972 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x6ef5b2e6
1715321 192.133128146 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x253ec0cf
1715322 192.133129551 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x3b6a8055
1715323 192.133130479 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x5d2fc045
1715324 192.133131522 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x35274c11
1715325 192.133329143 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x4055f3f5
1715326 192.133330208 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x382fae5c
1715327 192.133331130 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x5912d4e6
1715328 192.133332049 192.168.1.16 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x25a885f4
1715329 192.611386397 93.184.220.29 192.168.1.16 TCP 66 [TCP Retransmission] 80 → 60048 [FIN, ACK] Seq=1577 Ack=879 Win=146944 Len=0 TSval=1077786193 TSecr=916759662
1715330 192.611410465 192.168.1.16 93.184.220.29 TCP 54 60048 → 80 [RST] Seq=879 Win=0 Len=0
1715331 192.611414507 52.25.175.166 192.168.1.16 TCP 66 [TCP Keep-Alive ACK] 443 → 44472 [ACK] Seq=3486 Ack=2414 Win=35072 Len=0 TSval=459198231 TSecr=2690776650
Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: 43:36:3a:45:37:3a (43:36:3a:45:37:3a)
Client hardware address padding: 6104fc7f000023e99bdb
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Option: (255) End
Padding: 0000000000000000000000000000000000000000000000000000...
0000 ff ff ff ff ff ff 44 8a 5b 6f bd 0c 08 00 45 00 ......D. [o....E.
0010 02 40 71 96 40 00 40 11 05 5f c0 a8 01 10 ff ff .@q.@.@. _......
0020 ff ff 00 44 00 43 02 2c be 25 01 01 06 00 40 55 ...D.C., .%....@U
0030 f3 f5 00 00 80 00 00 00 00 00 00 00 00 00 00 00 ....
0040 00 00 00 00 00 00 43 36 3a 45 37 3a 61 04 fc 7f ......C6 :E7:a...
0050 00 00 23 e9 9b db 00 00 00 00 00 00 00 00 00 00 ..#..... ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0110 00 00 00 00 00 00 63 82 53 63 35 01 01 ff 00 00 ......c. Sc5.....
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Frame (frame), 590 bytes
Packets: 1716088 · Displayed: 1716088 (100.0%)
Profile: Default



Zdroje

- Obrana proti DHCP
- Útok na Kali linuxu
- Informace o portech a možnostech konfigurace
- Hlavní zdroj informací!