Analýza komunikace na Tcp/Ip sítích

by Timushev Fedor, Meister Stepan

1. Analýza protokolů

1.1. Dynamic host configuration protocol (DHCP)

- Postup přidělení IP adresy:
  Discover → Offer → Request → ACK (Acknowledgement);

- Zdrojové a cílové L2 a L3 adresy rámců / paketů s DHCP datagramy:
  d8:3b:bf:b7:49:68, 192.168.0.1;

- Doba zapůjčení IP adresy:
  2 hodiny;

- Název sledovaného PC:
  Scarlet;

- Zapůjčená IP adresa:
  192.168.0.106;

- Maska podsítě:
  255.255.255.0;

- IP adresa výchozí brány:
  192.168.0.1;

- IP adresa DHCP serveru:
  192.168.0.1;

1.2. Address resolution protocol

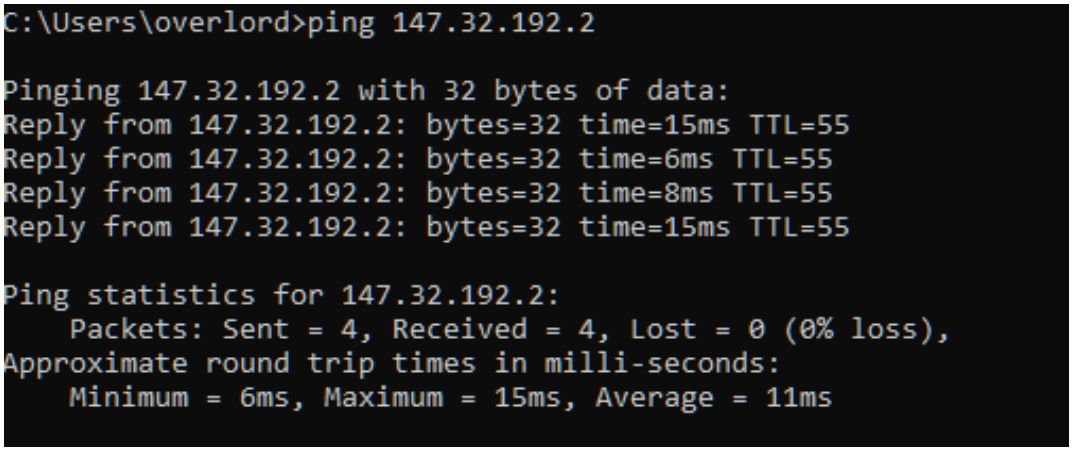
- Postup získání MAC adresy výchozí brány:
  Zeptej se kdo má adresu, odešli této adrese → Adresu je na této mac adrese;

- Zdrojové a cílové L2 adresy ARP rámců:
  d8:3b:bf:b7:49:68;

- Poznamenejte si obsah ARP rámců:
  Sender: ip, mac; target: ip, mac; hardware: type, size; protocol: size type;

1.3. Internet Control Message Protoco

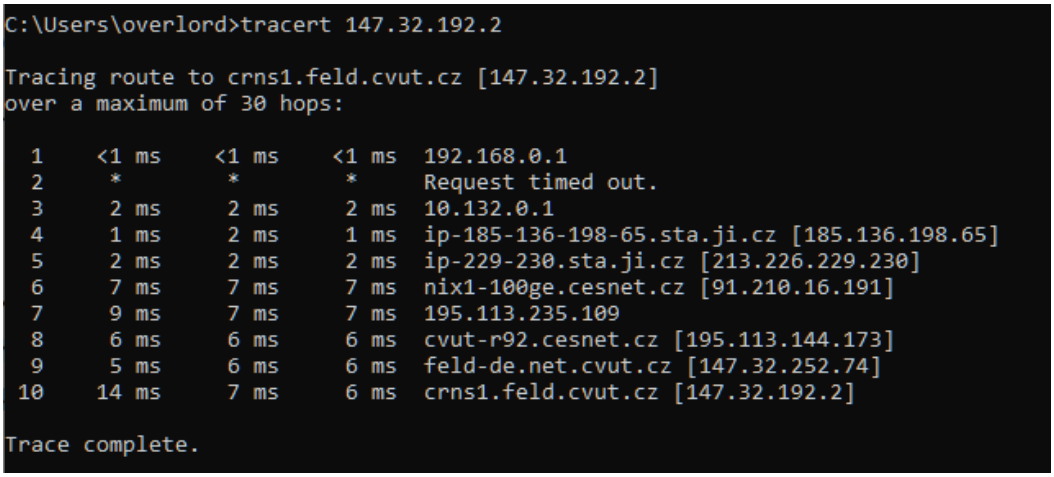
- Na PC zadejte do příkazové řádky příkaz „ping 147.32.192.2“. – jedná se o DNS server na ČVUT FEL, můžete použít i jiný vhodný server:



Img 1. Ping serveru

- Poznamenejte si obsahy zpráv požadavku (Echo Request) a příslušné odpovědi (Echo Reply):
  Request - 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9
  Reply - 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9

- Zjistěte prostřednictvím příkazové řádky a příkazu „tracert“ počet síťových mezilehlých zařízení mezi sledovaným PC a libovolným serverem:



Img 2. Počet síťových mezilehlých zařízení

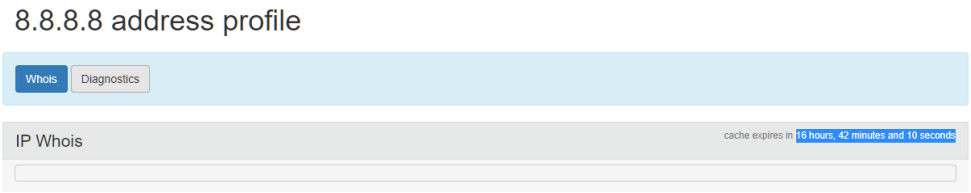
1.4. Domain Name System

- Zdrojové a cílové L2 a L3 adresy rámců / paketů s DNS datagramy:
  d8:3b:bf:b7:49:68, 192.168.0.1;

- Dotazované doménové jméno:
  www.seznam.cz;

- IP adresa dotazované stanice (tedy serveru www.seznam.cz):
  77.75.74.172, 77.75.74.176;

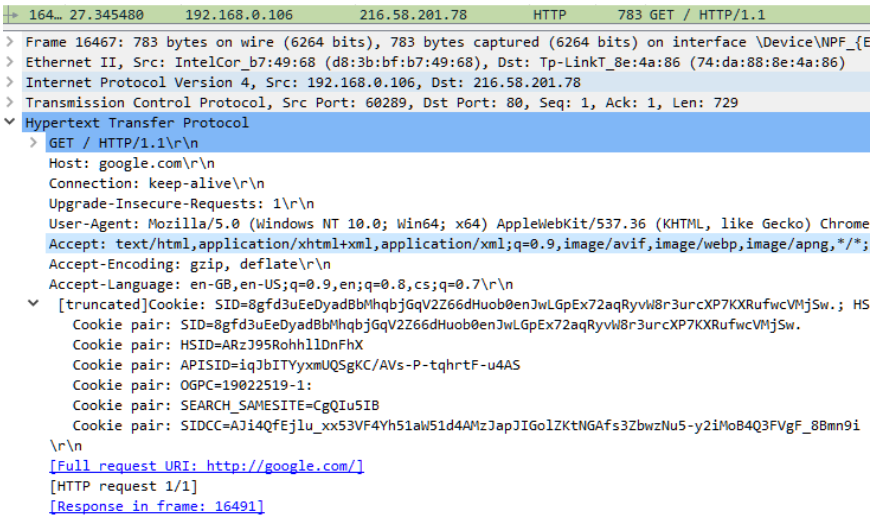
- Z volně dostupných databází doménových jmen (tzv. „whois“ služeb) zjistěte datum vypršení pronájmu doménového jména libovolného serveru:



Img 3. Datum vypršení pronájmu doménového jména

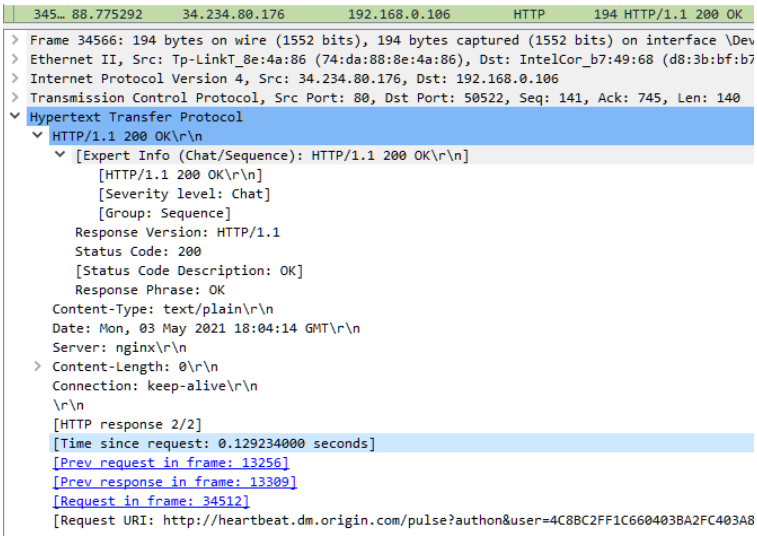
1.5. Hypertext Transfer Protocol:

- Obsah požadavku zaslaného webovým prohlížečem:
  Jmeno serveru, typ připojení, encoding, jazyk, cookies



Img 4. Obsah požadavku

- Obsah odpovědi zaslané serverem:
  Kod statusu, znění odpovedí, typ obsahu, datum, tzp připojení, doba od požadovku

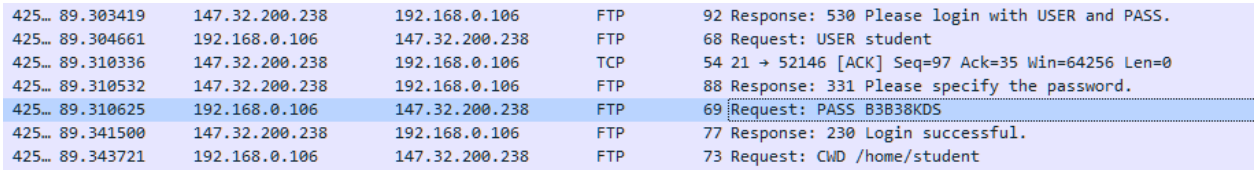


Img 5. Obsah odpovědi

- Z kolika webových serverů se celkem načítala data pro zvolenou webovou stránku: ze dvou;

1.6. File Transfer Protocol:

- Pokuste se najít zachycené přihlašovací údaje:



425…	89.303419	147.32.200.238	192.168.0.106	FTP	92 Response: 530 Please login with USER and PASS.
425…	89.304661	192.168.0.106	147.32.200.238	FTP	68 Request: USER student
425…	89.310336	147.32.200.238	192.168.0.106	TCP	54 21 → 52146 [ACK] Seq=97 Ack=35 Win=64256 Len=0
425…	89.310532	147.32.200.238	192.168.0.106	FTP	88 Response: 331 Please specify the password.
425…	89.310625	192.168.0.106	147.32.200.238	FTP	69 Request: PASS B3B38KDS
425…	89.341500	147.32.200.238	192.168.0.106	FTP	77 Response: 230 Login successful.
425…	89.343721	192.168.0.106	147.32.200.238	FTP	73 Request: CWD /home/student

Img 6. Zachycené přihlašovací údaje

- Analyzujte mechanismus navázání TCP spojení:

  Pro navázání spojení se používá třícestný handshake (potřesení ruky). V průběhu navazování spojení se obě strany dohodnou na čísle sekvence (sequence number).

  Číslo sekvence a odpovědi (sequence, acknowledgement number) jsou 32bitové hodnoty uváděné v TCP hlavičce.

  Pro navázání spojení se posílá TCP segment, který má nastaveny příznaky (flags) v TCP hlavičce. Navázání spojení probíhá ve třech krocích.

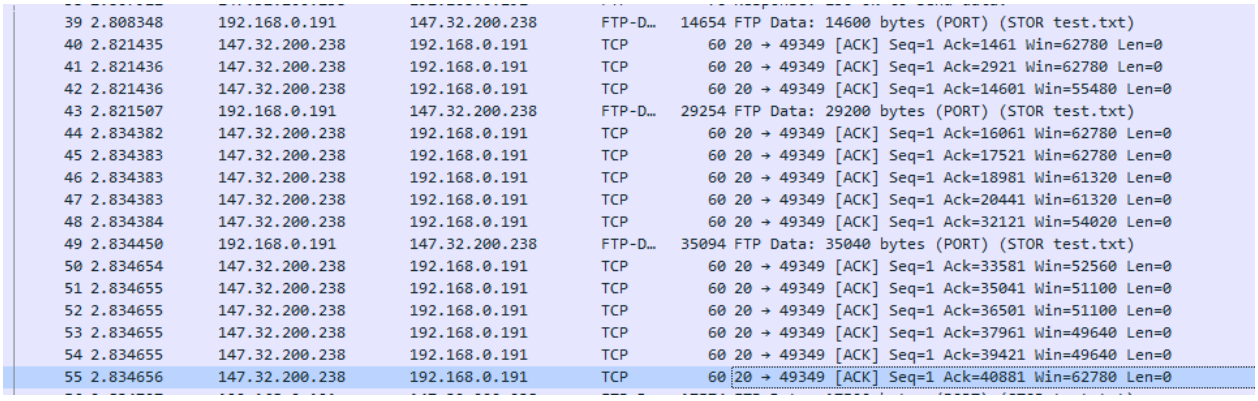
- Mechanismus pomalého startu:

  Tento mechanizmus se používá při zahájení přenosu mezi stanicemi nebo když dojde k zahlcení sítě.

  Po sestavení spojení může vysílací stanice zvolit poměrně velkou počáteční velikost Klouzavého okna. Správnou velikost pak odvodí samočasovací algoritmus na základě doby návratu potvrzení.

  Je zde však velké riziko zahlcení sítě příliš velkým počtem segmentů. Nebudou se vracet potvrzení a vysílač včas nezaregistruje, že překročil kapacitu sítě.

  Princip spočívá v přidání dalšího okna, tzv. okna zahlcení, které se nastaví na velikost jednoho segmentu. Vysílací stanice odešle jeden segment a pak čeká na potvrzení zprávou ACK. Jakmile přijde potvrzovací zpráva ACK jednoho segmentu, vysílací stanice zvětší hodnotu okna o jedna, tedy na 2 segmenty, a tyto segmenty odešle atd.

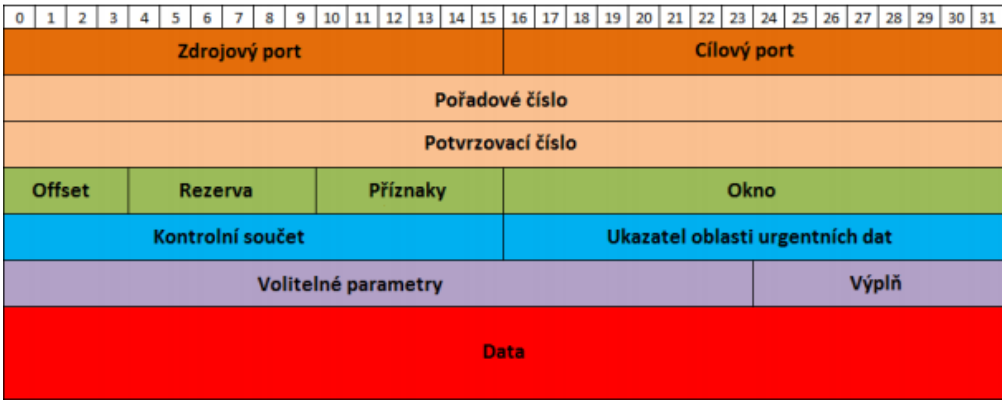


39	2.808348	192.168.0.191	147.32.200.238	FTP-D…	14654 FTP Data: 14600 bytes (PORT) (STOR test.txt)
40	2.821435	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=1461 Win=62780 Len=0
41	2.821436	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=2921 Win=62780 Len=0
42	2.821436	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=14601 Win=55480 Len=0
43	2.821507	192.168.0.191	147.32.200.238	FTP-D…	29254 FTP Data: 29200 bytes (PORT) (STOR test.txt)
44	2.834382	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=16061 Win=62780 Len=0
45	2.834383	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=17521 Win=62780 Len=0
46	2.834383	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=18981 Win=61320 Len=0
47	2.834383	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=20441 Win=61320 Len=0
48	2.834384	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=32121 Win=54020 Len=0
49	2.834450	192.168.0.191	147.32.200.238	FTP-D…	35094 FTP Data: 35040 bytes (PORT) (STOR test.txt)
50	2.834654	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=33581 Win=52560 Len=0
51	2.834655	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=35041 Win=51100 Len=0
52	2.834655	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=36501 Win=51100 Len=0
53	2.834655	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=37961 Win=49640 Len=0
54	2.834655	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=39421 Win=49640 Len=0
55	2.834656	147.32.200.238	192.168.0.191	TCP	60 20 → 49349 [ACK] Seq=1 Ack=40881 Win=62780 Len=0

Img 7. Vysílací stanice zvětší hodnotu okna o n-segmentu

- Mechanismus řízení datového toku pomocí pole Window Size v hlavičkách TCP segmentů:

  TCP využívá k řízení toku dat Klouzavé okno. Od ostatních protokolů pro řízení se však liší oddělením funkce potvrzování přijatých dat od přidělování kreditů pro vysílání. V hlavičce TCP segmentu jsou důležitá pole, která slouží pro řízení toku dat. Jsou to pole Sekvenčního čísla SN, pole Potvrzovacího čísla AN, a pole Klouzavého okna W.

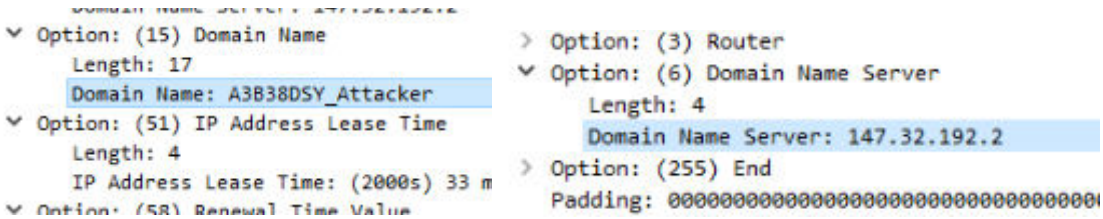


Img 8. Hlavička TCP segmentu

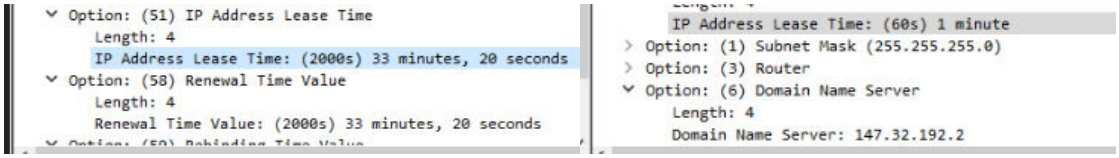
Přijímací stanice přijaté TCP segmenty potvrdí jednotlivě či kumulativně vysláním potvrzovacího segmentu, případně využitím datového segmentu zasílaného v opačném směru. Vysílací stanice obdrží tento potvrzovací segment a z pole AN přečte SN očekávaného TCP segmentu. V potvrzovacím segmentu se také nastavuje velikost Klouzavého okna W, ve kterém přijímací stanice přiděluje vysílací stanici další kredity. Přijímací stanice má možnost potvrdit přijaté segmenty, ale vysílací stanici nové kredity nepřidělit

1.7. DHCP Útok:

- Pro online výuku pouze analyzujte trace dostupný z Moodle. Místo přednastavených filtrů aplikujte klíčové slovo dhcp ekvivalentní přednastavenému fitru „DHCP“ a *filtr dns && dns.qry.name==www.seznam.cz && !(eth.src == 00:0c:42:ef:e0:f2)*, který odpovídá filtru „DNS (Attack)“:



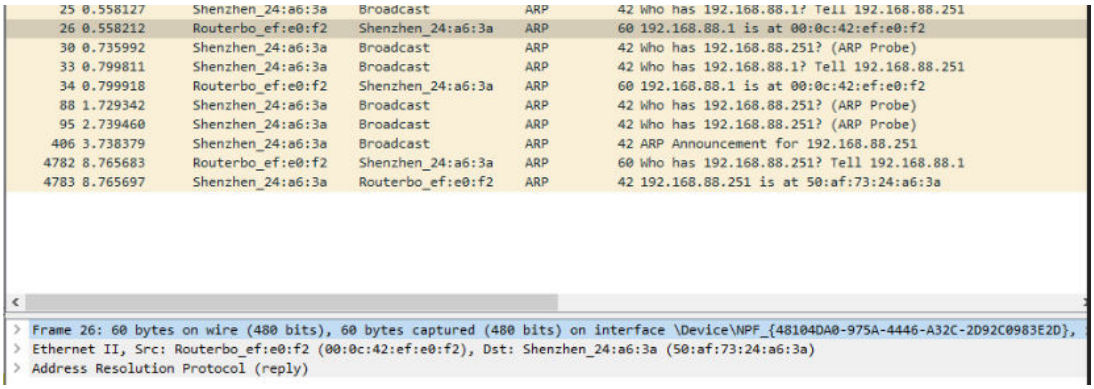
Img 9. Attacker domain jmeno misto standartní adresy



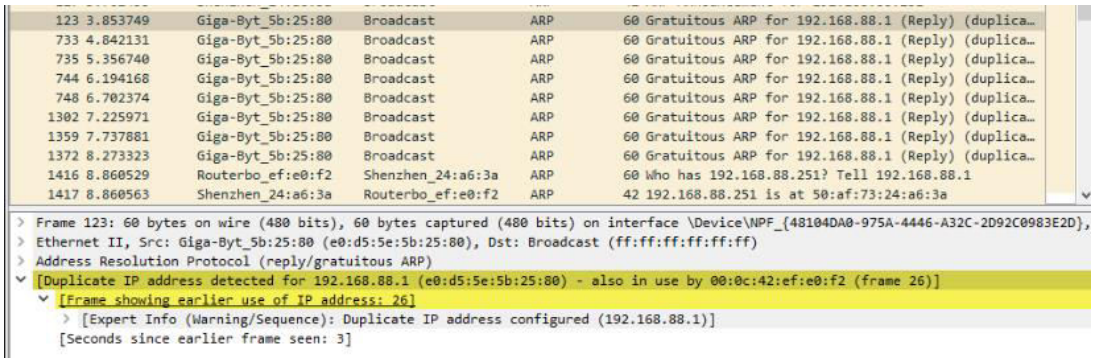
Img 10. Čas připojení při útoku

1.8. DHCP Útok:

- Pro online výuku pouze analyzujte trace dostupný z moodle. Místo přednastavených filtrů aplikujte klíčové slovo arp ekvivalentní přednastavenému fitru „ARP“ a filtr *dns && dns.qry.name==www.seznam.cz && !(eth.src == 00:0c:42:ef:e0:f2)*, který odpovídá filtru „DNS (Attack)“:



Img 11. Běžné připojení



Img 12. Falešná IP adresa útočníka