Analýza komunikace na TCP/IP sítích

Vít Knobloch, Filip Krul

Květen 2021

1 Analýza protokolů

1.1 Dynamic Host Configuration Protocol

1.1.1 Postup přidělení IP adresy

1. PC si po připojení do sítě zažádá o novou adresu vysláním packet s žádostí na port 67 na routeru
2. Router pošle acknowledge packet se všemi potřebnými informacemi
3. Počítač si na každém adaptéru nastaví IP, která mu byla přiřazena

1.1.2 Zdrojové a cílové L2 a L3 adresy rámců / paketů s DHCP datagramy

1. Request
   (a) Src mac: 08:d2:3e:6f:a7:bb, Dst mac: ff:ff:ff:ff:ff:ff
   (b) Src IP: 0.0.0.0, Dst IP: 255.255.255.255
2. Acknowledge
   (a) sourse mac: 88:c3:97:33:d1:7a, destination mac: 08:d2:3e:6f:a7:bb
   (b) Src IP: 192.168.31.1, Dst IP: 192.168.31.74

1.1.3 Doba zapůjčení IP adresy

21600s neboli 6h

1.1.4 Název sledovaného PC

Client name: LAPTOP-HOSE8VR1

1.1.5 Zapůjčená IP adresa

Your (client) IP address: 192.168.31.74

1.1.6 Maska podsítě

Subnet Mask: 255.255.255.0

1.1.7 IP adresa výchozí brány

192.168.31.1

1.1.8 IP adresa DHCP serveru

192.168.31.1

1.2 Adress Resolution Protocol

- "ARP"
  - PC se zeptá všech na sítí, kdo má ip adresu default gateway (v mém případě 192.168.31.1) a požádá, aby někdo, kdo to ví, zaslal na IP počítače, načež router odpoví, že adresa default gatewaye je na macadresse 88:c3:97:33:d1:7a (pro mě)
  - dotaz je na ff:ff:ff:ff:ff:ff, což znamená, že na všechny, a odpověď jde přímo na toho kdo se ptal
  - Obsah
    - typ (request nebo odpověď)
    - sender Mac address
    - sender IP address
    - Target Mac address
    - Target IP address
- "arp -a" - ano

1.3 Internet Control Message Protocol

- Request
  - Typ 8 - ping request
  - checksum
  - identifier
  - sequence number
  - data (32 bytes)
- Reply
  - Typ 0 - ping Reply
  - checksum
  - identifier same as in request
  - sequence number same as in request
  - data (32 bytes) same as in request
- Mezi mnou a školním serverem je 8 zařízení

1.4 Domain Name System

- Získávání IP adresy
  1. PC dns serveru pošle dns query packet, ve které se ptá na IP stránky `seznam.cz`
  2. dns server se podíva, jestli ji zná, a pokud ne, tak se ptá dál
  3. když dns server dostane odpověď, tak ji přepošle PC
  4. PC v odpovědi najde (několik) IP adres hledané stránky
- Zdrojové a cílové rámce
  1. query
     - Src: 08:d2:3e:6f:a7:bb, Dst: 88:c3:97:33:d1:7a
     - Src: 192.168.31.74, Dst: 192.168.31.1
  2. response
     - Src: 88:c3:97:33:d1:7a, Dst: 08:d2:3e:6f:a7:bb
     - Src: 192.168.31.1, Dst: 192.168.31.74
- Dotazované doménové jméno: `Name: www.seznam.cz`
- Mozne adresy:
  - 77.75.75.172
  - 77.75.74.176
  - 77.75.74.172
  - 77.75.75.176

1.5 Hypertext Transfer Protocol

- Obsah požadavku zaslaného webovým prohlížečem.
  - Host
  - typ připojení
  - Použitý prohlížeč
  - co prohlížeč přijímá
  - jaký encoding prohlížeč přijímá
  - jaké jazyky prohlížeč přijímá
- Obsah odpovědi zaslané serverem
  - Datum
  - Typ serveru
  - kdy byla data naposledy upravena
  - Etag
  - Délka obsahu
  - jak dlouho ma připojení vydržet
  - typ připojení
  - typ obsahu
- Z kolika webových serverů se celkem načítala data pro zvolenou webovou stránku? Ze dvou.

1.6 File Transfer Protocol

- login
  - Pokuste se najít zachycené přihlašovací údaje. - Jednoduché, jsou posílány v plaintextu
  - transfer
- transfer
  - Pomalý start
    1. PC pomalu začne posílat data
    2. receiver čeká na nějakou určitou definovanou dobu na posláni acknowledge
    3. pokud je rozdíl mezi dobou přijetí posledniho packetu a posláním acknowledge, tak se timeout na posílani ack zkrátí
    4. toto se opakuje dokud nejsou ty hodnoty podobné, což znamená, že je timeout optimální
  - Window Size - kolik je receiver ochotný přijmout dat najednou

1.7 Zabezpečení

1. Komunikace je encrypted
2. Bez filtru jde moc packetů na to, aby se v tom mohl člověk zorijentovat

2 Analýza útoků

Oba dva útoky využívají princip man in the middle, kdy přesměrují internetový provoz cílového počítače tak, aby procházel skrze útočící počítač. Toho poté využíjí, aby zachytili DNS dotaz cílového počítače, a místo skutečné IP adresy dotazovaného serveru vrátí cílovému počítači IP adresu podvodného serveru. Útoky se liší v tom, jakým způsobem přimějí cílový počítač komunikovat skrze útočníka.

2.1 DHCP útok

V případě DHCP útoku si útočník zřídí podvodný DHCP server a čeká na DHCP request cíle, poté mu odpoví se svou vlastní IP adresou jako default gateway adresou. Od té doby přistupuje cílový počítač k vnějšímu internetu skrze útočníka. Ve chvíli, kdy přijde DNS query cíle na adresu serveru www.seznam.cz, tak jí útočící počítač nepřepošle na skutečnou default gateway, ale odpoví s nesprávnou adresou.

2.2 ARP útok

V případě ARP útoku útočník zasílá podvodné odpovědi na dotazy ohledně MAC adresy routeru. Cílem je, aby si cílový počítač uložil do své ARP cache MAC adresu útočníka místo skutečné MAC adresy default gateway uzlu. Pokud si cílový počítač uloží podvrženou MAC do ARP cache, tak začne veškerou svou komunikaci do vnějšího internetu posílat skrze útočníka. Ten potom opět čeká na DNS query na adresu www.seznam.cz a vrátí adresu podvodného serveru.