TCP, UDP a NAT

Miloš Liška

liska@fi.muni.cz

12. 4. 2019

Cíle cvičení

- Získat přehled o fungování protokolu TCP
- Získat základní zkušenost s fungováním NAT na L4
- Prozkoumat některé vlastnosti protokolu UDP

Protokoly

TCP

Základy TCP

- V tomto cvičení budeme analyzovat základy chování protokolu TCP na vzroku dat nasbíraného při odesílání cca 3MB dat (kniha Vojna a mír).
  - wget http://147.251.54.177/book-war-and-peace.txt
- Na 147.251.54.177 běží webserver s jednoduchým CGI skriptem, který přijme soubor pomocí HTTP POST. Na rozhraní s adresou 147.251.54.177 je nakonfigurovaný token bucket, který zahazuje některé pakety.
- Stažený soubor s textem knihy Vojna a mír budeme uploadovat na server **147.251.54.177** a analyzovat vzniklý provoz nástrojem Wireshark.

Základy TCP

- Notebooky budou připojeny do standardní KYPO sítě skrz společný switch
- DHCP
- TCP (Generic) Segmentation Offload
  - sudo ethtool -K <dev> tso off
  - sudo ethtool -K <dev> gso off
  - sudo ethtool -k <dev>
- Ve Wiresharku Edit → Protocols → TCP → Allow subdissector to reassemble TCP streams = **FALSE**

Zadání

V zachyceném provozu:

1. Analyzujte zdrojové a cílové IP adresy a čísla TCP portů klientského PC a serveru.
2. Najděte a popište TCP handshake mezi klientským PC a serverem.
3. Nalezněte v proudu TCP dat mezi klientským PC a serverem rámec obsahující příkaz HTTP POST a na následující sekvenci rámcu, pomocí kterých klientské PC odesílá text knihy Vojna a mír, popište jak a kdy odesílá server potvrzení jednotlivých TCP paketů.

Zadání

4. Zjistěte jaká je velikost payloadu TCP paketů pomocí kterých je odeslaný celý text knihy Vojna a mír a čím je daná?
5. Zjistěte zda došlo k retransmisi některého z TCP paketů? Kterého/kterých? Na základě čeho?
6. Vypočítejte rychlost přenosu textu knihy Vojna a mír z klientského PC na server. Jak rychlost přenosu ovlivňuje RTT.

NAT

Základy NAT

- V tomto cvičení se podíváme na základy fungování Native Address Translation na L4 ISO/OSI modelu.
- Notebooky budou připojeny do standardní KYPO sítě skrz společný switch
- DHCP
- Lokální provoz analyzujte pomocí nástroje Wireshark
- Provoz na serveru budeme pořizovat pomocí nástroje tcpdump centrálně
  - sudo tcpdump -i ens3 -s 65535 -w <some-file>
  - wget http://147.251.54.177/dump.pcap

Zadání

Přistupte webovým prohlížečem na `http://147.251.54.177`

1. Identifikujte vaše privátní a veřejné IPv4 adresy. Který uzel v síti řeší NAT?
2. Popište mapování zdrojových a cílových portů při komunikaci mezi klientem a serverem v obou směrech. Dochází k jejich přemapování? Pokud ano, popište jak a proč.

Základy UDP

Základy UDP

- V tomto cvičení prozkoumáme chování protokolu UDP při odesílání multimediálních dat s vysokým datovým tokem.
- Všechny notebooky budou zapojeny do switche v jedné společné síti
- Do sítě je zapojen generátor provozu
- Základní konfigurace sítě na noteboocích
  - sudo ip a add 10.0.0.x/24 dev <dev>
  - x je přidělené číslo počítače, nezapomeňte vypnout network-manager
  - sudo ip link set dev <dev> mtu 9000

Zadání

Nástrojem Wireshark zachyťte alespoň 5s vzorek provozu na lokálním síťovém rozhraní. Podle zachyceného provozu:

1. Analyzujte provoz se zdrojovou IP adresou ff02::1. Je tato zdrojová adresa něčím zajímavá? Je něco zajímavého na velikosti UDP paketů? Co popisuje pole Length v hlavičce paketu?
2. Pomocí nástroje Statistics->IO/Graph ve Wiresharku proveďte analýzu průběhu využití šířky pásma UDP streamem. Jaký je přibližně průměrný bitrate přijímaného UDP streamu? Jak a proč se změní graf využití šířky pásma s 1s intervalem a intervalem menším než 1s.