TCP a UDP

Miloš Liška

liska@fi.muni.cz

2022

Cíle cvičení

- Získat přehled o fungování protokolu TCP
- Prozkoumat některé vlastnosti protokolu UDP

Protokoly

TCP

Základy TCP

- Adresaci dostanete z DHCP (pokud jste ještě nedělali, tak na Linuxu nastavíte pomocí Network Manageru ev. pomocí dhclient eth0).
- 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 2% paketů v obou směrech.
- Stažený soubor s textem knihy Vojna a mír budeme uploadovat na server `http://147.251.54.177/file-upload/` a analyzovat vzniklý provoz nástrojem Wireshark.

Základy TCP

- Dump síťového provozu připravíme pomocí nástroje Wireshark (fakultativně pomocí nástroje tcpdump)
- Na eth0 je potřeba vypnout TCP (Generic) Segmentation Offload:
  - sudo ethtool -K <dev> tso off
  - sudo ethtool -K <dev> gso off
  - sudo ethtool -k <dev>
- Large Scan Offload (Windows):
  - `http://www.peerwisdom.org/2013/04/25/disabling-large-send-offload-windows/`

Základy TCP

- Spustíme dump provozu na eth0 ve Wiresharku a zároveň upload souboru na server.
- curl -v -F 'file=@/cesta/k/souboru/book-war-and-peace.txt' \
  http://147.251.54.177/file-upload/
- tcpdump -i eth0 -s 65535 -w output.pcap

Základy TCP

- Všichni si ve Wiresharku vypnou TCP packet reassembling!
- Edit → Preferences → Protocols → TCP → Allow subdissector to reassemble TCP streams = **FALSE**
- Ve Wiresharku je potřeba vypnout analýzu protkolu HTTP (potřebujete analyzovat dump provozu na úrovni protokolu TCP).
- Analyze → Enabled Protocols → http → Disable

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 rámců, 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 jednotlivých 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?

Základy UDP

Základy UDP

- V tomto cvičení prozkoumáme chování protokolu UDP při přijímání multimediálních dat s vysokým datovým tokem.
- Budeme sledovat příjem Full HD videa se snímkovou frekvencí 25 fps.
- Zkontrolujte, že linka je negociovaná na 1 Gbps (sudo ethtool <dev> nebo pomocí Network Manageru
- sudo ip link set dev enp0s31f6 mtu 9000
- Dump provozu připravíme a budeme budeme analyzovat opět nástrojem Wireshark

Zadání

V zachyceném provozu:

1. Analyzujte provoz s cílovou IP adresou 224.0.0.1.
2. Otázky ke zpracování:
   - Čím je tato adresa zajímavá?
   - Co popisuje pole Length v hlavičce paketu?
   - Je něco zajímavého na velikosti UDP paketů?
3. Pomocí nástroje Statistics->IO/Graph ve Wiresharku proveďte analýzu průběhu využití šířky pásma UDP streamem.
4. Otázky ke zpracování:
   - Jaký je přibližně průměrný bitrate přijímaného UDP streamu? Využijte buď IO/Graph a nebo samotný dump provozu.
   - Jak a proč se změní graf využití šířky pásma s 1s intervalem a intervalem menším než 1s? Co je příčinou pilovitého charakteru využití šířky pásma v případě intervalu menšího než 1s (ideálně nastavte interval 10ms a 1ms). Jaké využití šířky pásma pozorujete v grafu se subsekundovými intervaly. Využití šířky pásma při různě nastavených časových intervalech vysvětlete.

Protokoly

- Protokol bude zpracovaný promocí šabblony v IS MU - scanform-cv4.tar.bz2
- Využijte připravený soubor cviceni04.tex a doplňte odpovědi
- Protokol odevzdejte do odevzdávárny ideálně do 22. 4. 2022, odevzdávárna ale zůstane pravděpodobně otevřena déle
- Pokud nemáte nainstalovaný LaTeX, použijte Overleaf (`https://www.fi.muni.cz/tech/overleaf.html.cs`).
- Pokud jste se nemohli cvičení zúčastnit pracujte s dumpy síťového provozu ve studijních materiálech (vojna-a-mir-upload.pcap a ug.pcap).
- A pracujte samostatně.