Sveučilište u Mostaru

**Fakultet strojarstva, računarstva i elektrotehnike**

**SEMINARSKI RAD**

**Analizatori protokola**

Profesor: dr.sc. Drago Žagar Student: Jozo Skoko

Mostar, 2018. godina.

Sadržaj

**1 UVOD**

U složenom svijetu mreža problemi se često događaju. Određivanje točnog uzroka problema u radu složenih sustava je zahtejvno i često može biti jako opasno. U tim slučajevima stručni inženjeri koriste tajno oružje koje se zove analizator protokola. Analizator protokola omogućuje da inžinjer odredi izvor gotovo bilo koje pogreške pod uvjetom da se obrazuje na temeljnom protokolu.

Ovaj seminarski rad predstavit će što je analizator protokola, koji programi se koriste za njegovo korištenje, njegovu konkretnu ulogu, te neke vrste analizatora protokola koje danas imamo.

**2 ANALIZATOR PROTOKOLA**

**2.1 Što je analizator protokola**

Analizator protokola ili "nosač paketa", alat je koji se koristi za presretanje prometa, pohranjivanje i prikazivanje u dekodiranom, čitljivom stanju čovjeku. Suvremeni analizatori protokola kao što je Wireshark mogu čak i otkriti rudimentarne probleme samostalno, a zatim provesti statističke analize sa zarobljenim podacima.

Bez obzira na značajke, analizatori protokola rade na istom osnovnom putu. Oni se umetnu u mrežni stog i kopiraju sav promet u međuspremnik ili datoteku. Većina će također postaviti mrežni upravljački program u "promiskujući način", što u osnovi dopušta tim alatima da preuzimaju sav promet koji ulazi u mrežni stog umjesto da samo prikuplja promet namijenjen samom sustavu. Analizatori protokola dolaze u obliku namjenskih hardvera koji se mogu povezati s ugrađenim uređajem. Međutim, da bi se tumačili podatci koji se dobiju od hardvera, potrebno je korisničko sučelje koje prikazuje podatke sabirnice u obliku koji je čitljiv za ljude. Dakle, ukratko, analizator protokol je kombinacija namjenskih hardvera i softvera koji rade zajedno. Radeći zajedno, hardver bilježi podatke, a softver prikazuje snimljene podatke.

Ali nisu sva sučelja ista. Neki samo prikazuju snimanje podataka, dok drugi omogućuju pretraživanje, definiranje filtara, prepoznavanje uzoraka i dekodiranje, u stvarnom vremenu.



Slika 2.1: Izgled analizatora protokola(TPI4000)

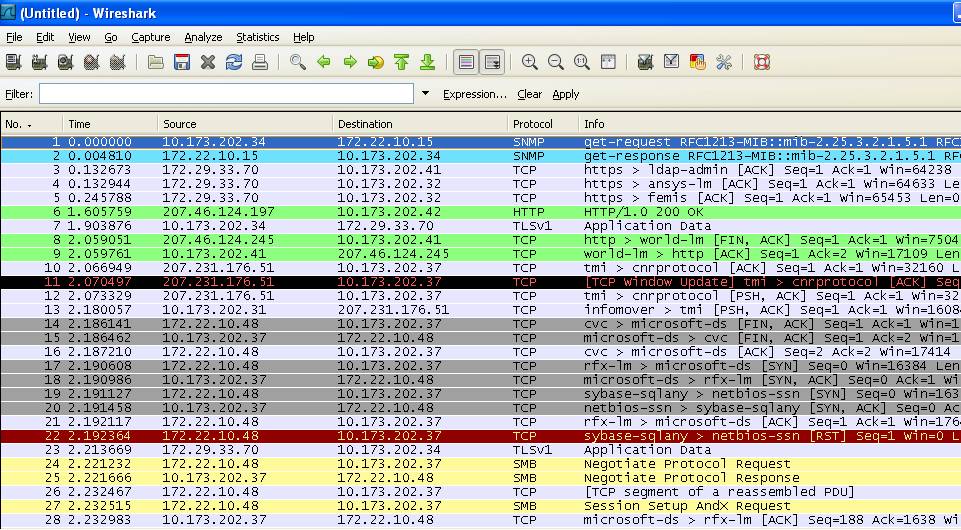
**2.2 Upotreba analizatora protokola**

Upravitelj mreže mora biti pažljiv za analizu i zaštitu mrežnog prometa od prijetnji i slabih performansi. Upravitelji često trebaju otkloniti poteškoće s mrežom kako bi osigurali učinkovito i brzo okruženje mrežnog prometa.

Analizator protokola prikazuje cjelokupan status svih mrežnih aktivnosti pružajući potpunu sliku širine pojasa i korištenja resursa. Ako resurs koristi preveliku širinu pojasa, upravitelj mreže može osloboditi resurs prekidanjem postupka. Međutim, novo primijenjene aplikacije i čvorovi mreže mogu imati neke konfiguracije i probleme s radom, no one se mogu riješiti za nekoliko sekundi pomoću analizatora protokola. Svako djelovanje analizatora protokola izvodi se u stvarnom vremenu.

Ključne funkcije i upotrebe analizatora protokola uključuju:

* Analizirajući mrežna pitanja i probleme
* Praćenje sigurnosti mreže otkrivanjem neovlaštenih pokušaja hakiranja mreže
* Izoliranje elemenata koji uzrokuju štetu
* Praćenje ukupne propusnosti WAN-a (i pojedinačne potrošnje korisnika)
* Generiranje cjelovitog izvješća o mrežnim statistikama organiziranim u tabličnom obliku, grafičkim grafikonima ili kao izravni podaci
* Praćenje podataka koji se prenose ili su u pokretu
* Praćenje ukupnih WAN/LAN i korisničkih/krajnjih točaka sigurnosnih problema i statusa
* Filtriranje neželjenih sadržaja i sprječavanje neovlaštenog pristupa
* Izvođenje operacija otklanjanja pogrešaka na strani klijenta/poslužitelja zbog pogrešaka/problema s komunikacijom
* Praćenje konfiguracije proxy poslužitelja, status vatrozida i konfiguracija, zaštita od neželjenih poruka i ostali sigurnosni aspekti
* Posluživanje kao primarni izvor podataka za praćenje i upravljanje svakodnevnim mrežama
* Reverse inženjerski vlasnički protokoli preko mreže



Slika 2.2: Upravljanje analizatorom protokola - softverski prikaz(Whireshark)

**3 VRSTE ANALIZATORA PROTOKOLA**