NASTAVNO-NAUČNOM VEĆU ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija II stepena Elektrotehničkog fakulteta u Beogradu imenovala nas je za članove Komisije za pregled i ocenu master rada kandidata Aleksandra Pavlovića pod naslovom „**Tehnike DDoS napada i mehanizmi odbrane**". Nakon pregleda rada podnosimo sledeći

IZVEŠTAJ

1. Biografski podaci

Aleksandar Pavlović rođen je 12. decembra 1987. godine u Šapcu, gde je i završio Srednju tehničku školu. Elektrotehnički fakultet u Beogradu je upisao 2006. godine. Diplomirao je 2010. godine na Odseku za telekomunikacije i informacione tehnologije odbranom diplomskog rada „*Smart* antene". Tokom osnovnih studija postigao je prosečnu ocenu 9.31. Diplomske akademske master studije na smeru Sistemsko inženjerstvo i radio-komunikacije upisao je tokom 2010. godine.

2. Predmet master rada

Predmet ovog master rada je analiza postojećih tehnika i metoda DDoS napada, klasifikacija napada po slojevima OSI modela i resursima koji se prilikom napada ciljaju. U radu je analiziran konkretan primer servisa *firewall* na zahtev, koji simulira primenu *firewall* rešenja u mreži ISP provajdera. Analizirane su i tehnike rutiranja saobraćaja u mreži ISP-a zasnovane na OSPF protokolu rutiranja. Na osnovu analiza DDoS napada predložen je sistem za odbranu od DDoS napada u mreži velikih ISP-eva.

3. Osnovni podaci o master radu

Master rad kandidata Aleksandra Pavlovića „Tehnike DDoS napada i mehanizmi odbrane" obuhvata 73 strane štampanog teksta sa 40 slika i 2 tabele. Rad je organizovan, tako da sadrži uvod, jedanaest poglavlja i spisak literature.

4. Sadržaj i analiza rada

U uvodnom poglavlju dat je kratak opis DDoS napada i pregled poglavlja iz master rada.

U drugom poglavlju definisane su vrste DoS napada i dat je kratak vremenski prikaz bezbednosnih incidenata.

U trećem poglavlju klasifikovani su DDoS napadi prema resursu koji napadaju. Izvršena je podela na *Bandwidth*, logičke i protokol napade.

U četvrtom poglavlju su opisani neki od DoS napada na sloju veze.

U petom poglavlju su opisani napadi na mrežnom sloju. Date su osnovne informacije o IP protokolu, kao i o ICMP protokolu. Napadi koji su opisani u ovom poglavlju su *IP Options, IP Fragmentation, Ping of Death, Smurf* napadi.

U šestom poglavlju opisani su napadi na transportnom sloju. Date su osnovne informacije o TCP i UDP protokoli, kao i o napadima koji su realizovani na ovom sloju.

U sedmom poglavlju su opisani napadi na aplikativnom sloju. Opisan je DNS servis, HTTP protokol i napadi koji se javljaju na ovim servisima.

Osmo poglavlje opisuje neke od najpoznatijih alata za DDoS napade, među kojima su LOIC, HOIC, *Slowloris*.

Deveto poglavlje se bavi merama koje je neophodno implementirati kako bi se uticaj DDoS napada sveo na minimum.

U desetom poglavlju opisano je GRNET-ovo *FireCircle* centralizovano *firewall* rešenje, bazirano na BGP *flow-spec* oglašavanjima.

U jedanaestom poglavlju opisano je *firewall* rešenje koji treba da omogući Internet servis provajderu filtriranje DDoS napada zaštitu korisnika. Rešenje u osnovi koristi OSPF protokol rutiranja i CSF *Firewall* rešenje.

U dvanaestom poglavlju opisano je CSF *firewall* rešenje za *Linux* platformu. Istaknute su opcije koje mogu da omoguće zaštitu od DDoS napada.

5. Zaključak i predlog

Tokom izrade ovog master rada analizirane su neke od najpoznatijih DDoS pretnji na Internetu, izvršena je njihova klasifikacija prema sloju OSI i dat je opis svakog od njih. Analizirano je GRNET-ovo *firewall* rešenje, istaknute su njegove glavne prednosti i mane. Dat je i predlog centralizovanog *firewall* rešenja koje je realozovano na *Linux platformi* korišćenjem CSF *firewall*-a. Izradom ovog rada utvrđeno je:

- Analizirane su postojeće DDoS pretnje sa fokusom na resurse koje data pretnja napada, kao i sloj OSI modela na kom je napad realizovan.
- Analizirane su prednosti i mane GRNET-ovog *FireCircle* rešenja koje se ogledaju kroz:
    - Distribuiranost rešenja, jer filtriranje obavljaju ruteri unutar mreže ISP-a.
    - Mogućnost propagiranja ruta na susedne autonomne sisteme, kako bi se neželjeni saobraćaj filtrirao na pristupnim tačkama.
    - Ograničenost GRNET *FireCircle* rešenja po pitanju hardverske kompatibilnosti, jer je za implementaciju neophodno da ruteri koji obavljaju filtriranje budu na *Juniper* platformi.
    - Mali broj tehnika filtriranja dolaznog saobraćaja.
- Predloženo je novo *Firewall on Demand* rešenje koje koristi CSF *Firewall* kao centralni *firewall* servis. Implementacijom ovakvog *firewall* rešenja postignuto je:
    - Značajno više opcija filtriranja u odnosu na GRNET *FireCircle* rešenje.
    - Obezbeđena je daleko veća hardverska kompatibilnost u odnosu na GRNET *FireCircle* rešenje, jer filtriranje ne izvršavaju direktno ruteri nego *firewall* uređaj. Uloga rutera je da na što je moguće jednostavniji način proslede saobraćaj u incidentnim situacijama do *firewall*-a koji filtriranjem izdvaja dozvoljeni saobraćaj i šalje ga ponovo u režu provajdera.

Na osnovu svega izloženog, članovi Komisije predlažu Komisiji II stepena Elektrotehničkog fakulteta u Beogradu da rad Aleksandra Pavlovića, pod naslovom **„Tehnike DDoS napada i mehanizmi odbrane"** prihvati kao master tezu i da kandidatu odobri javnu usmenu odbranu.

Beograd, 16.9.2013.

Članovi komisije:

dr Aleksandar Nešković, vanr. prof.

dr Nataša Nešković, vanr. prof.