**UNIVERZITET U KRAGUJEVCU**

**FAKULTET TEHNIČKIH NAUKA U ČAČKU**



**SEMINARSKI RAD**

Tema: Zaštita od DDOS-a

**Studijski program**:Osnovne akademske studije - informacione tehnologije

**Predmet**: Bezbednost i zaštita računarskih mreža

**Profesor**:  **Studenti**:

Dr Marjan Milošević Nenad Janković 60/2018

Nikola Petrašinović 63/2018

2021. godina

# SADRŽAJ

1. UVOD -
2. Šta je DDoS? -
3. Podela DDoS-a

3.1 Protokol napadi

* 1. Volumetrijski napadi

3.3 Napadi aplikacijskog sloja

1. Najćešći DDoS napadi? -
   1. UDP Flood -
   2. ICMP Flood-
   3. SYN Flood -
   4. Ping of death
   5. Slowloris
2. Ko je ugrožen od DDoS napada?
3. DDoS alati
4. Prevencija i zaštita od DDoS napada
   1. Softveri i usluge za zaštitu
      1. IndusFace AppTrana
      2. SolarWinds Security event manager
      3. Sucuri website firewall
      4. Cloudflare
      5. Link11
      6. AWS Shield
5. Zaključak
6. Literatura

# UVOD

Kako bi se definisao odgovor na temu kako se zaštiti od DDoS napada bilo bi poželjno prvo razmotiriti šta on predstavlja. DDoS napadi se prvi put pojavljuju početkom ovog veka, iz godine u godinu sve ih je više, sve su obimniji i intenzivniji. Teško ih je sprečiti, preživeli su test vremena, jeftino se mogu iznajmiti i mogu imati dugoročne i razorne posledice. DDoS (Distributed Denial-of-Service) su napadi sa više hiljada računara kojima je cilj da dovedu do preopterećenja veb servera, mreže ili nekog drugog dela infrastruktuare i tako onemoguće pristup njihovim korisnicima.

Moderni DDoS napadi generišu ogromne količine saobraćaja pomoću botova (botnet). Botovi predstavljaju mrežu računara koji su zaraženi malicioznim softverom zbog čega napadač ima kontrolu nad njima sa udaljene lokacije.

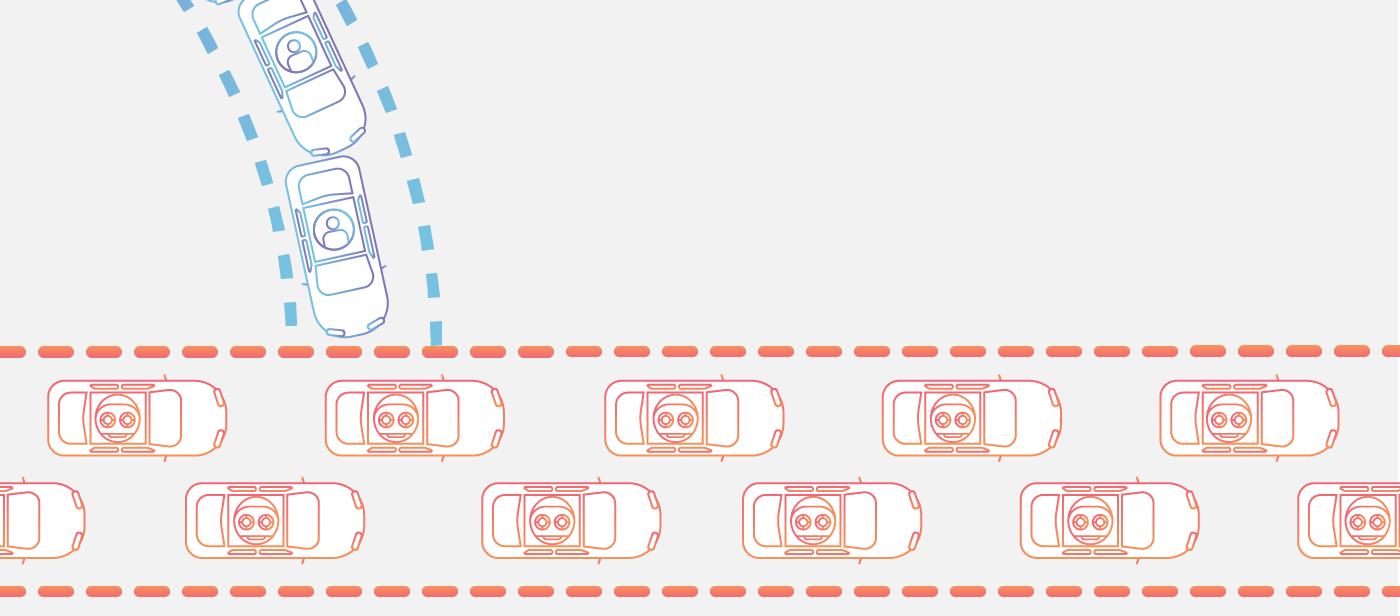
Ugroženi su svi koji imaju veb sajt - državne institucije, kompanije, pa čak i pojedinci. Motivi su različiti: hakerski, ucena, uznemiravanje, privlačenje pažnje i ostvarivanje konkurentske prednosti (naročito u onlajn igricama). Jedna od najpoznatijih meta DDoS napada je Sony Playstation. Iz kompanije kažu da se napadi dešavaju bukvalno svakoga dana, pored Sony-a česta žrtva napada je i Xbox.

DDoS napade je relativno lako izvesti, teško ih je sprečiti i generalno su veoma efikasni. Druge kompanije koje nisu direktna meta napada su ponekad kolateralna šteta. Kada je saobraćaj preopterećen, i drugi sajtovi koje je hostovao isti provajder mogu postati nedostupni.Svako može biti žrtva.

U nastavku biće detaljno opisani DDoS napadi, vrste napada, motivi, ko su mete napada. Najvažnije od svega, uslediće opis prevencije i zaštite. Za svaku vrstu napada postoji neki vid zaštite. Zaštita se svodi na korišćenje sigurnosnih programa i usluga. Na samom kraju sledi zakljčak infomacija navedinih u ovom radu.

# ŠTA JE DDOS?

DDoS (Distributed Denial-of-Service) su napadi sa više hiljada računara kojima je cilj da dovedu do preopterećenja veb servera, mreže ili nekog drugog dela infrastrukture i tako onemoguće pristup njihovim korisnicima. Na primer, DDoS napad na link onemogućava pristup internetu, dok DDoS napad na veb server dovodi do „obaranja“ veb sajta. DDoS napadi postižu efikasnost korišćenjem višestrukih komprovitovanih računarskih sistema kao izvor za napad. Eksploatisane mašine mogu uključivati računare i druge mrežne uređaje kao što su IoT uređaji. Slikovit prikaz DDoS napada mogao bi se predstaviti neočekivanom gužvom na autoputu, koja sprečava redovni saobraćaj da teče.



Slika 1. Slikovit prikaz DDoS napada saobraćajnom gužvom

## KAKO DDOS RADI?

Napadi se izvode pomoću mreže uređaja koji su povezani na internet. Ove mreže se sastoje od računara i drugih uređaja (kao što su IoT uređaji) koji su zaraženi malverom, što omogućava da ih napadač kontroliše daljinski. Ovi pojedinačni uređaji se nazivaju botovi (ili zombiji), a grupa botova se naziva botnet. Kada se botnet uspostavi, napadač je u mogućnosti da usmeri napad slanjem daljinskih instrukcija svakom botu. Kada botnet cilja na žrtvin server ili mrežu, svaki bot šalje zahteve na IP adresu cilja, što potencijalno dovodi do preopterećenja servera ili mreže, što rezultuje uskraćivanjem usluge normalnom saobraćaju. Zbog toga što je svaki bot legitiman internet uređaj veoma je teško odvojiti normalan saobraćaj od lažnog.

## KAKO INDETIFIKOVATI DDOS NAPAD?

Najteži deo DDoS napada je to što nema nikakvih upozorenja za predstojeći napad. Izuzetak je kada neke velike hakerske grupe šalju pretnje pre napada ali uglavnom napadači pokreću napad bez ikakvih upozorenja. Vreme koje prođe od početka napada do njegovog indetifikovanja predstavlja glavni gubitak žrtve. Neki od tragova koji otkrivaju da je DDoS napad u toku:

* Sa jedne IP adrese se šalje veliki broj zahteva za kratak vremenski interval
* Server šalje 503 odgovor zbog prekida usluge
* TTL (time to live) na ping zahtevu istekne
* Iznenadno spor pristup internetu

# PODELA DDOS NAPADA?

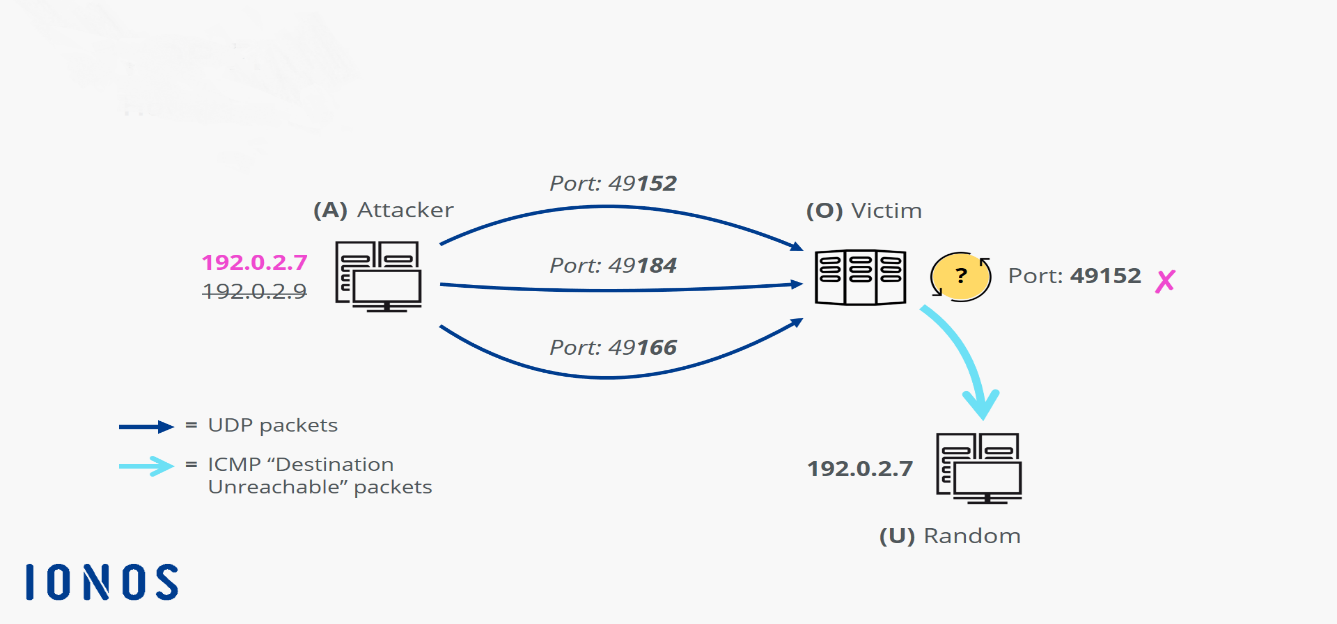
## NAPADI PROTOKOLA

Petrasko radii….

# NAJČEŠĆI DDOS NAPADI?

## UDP FLOOD

Napad u kojem napadač preplavljuje nasumične portove na ciljanom hostu sa IP paketima koji sadrže UDP datagrame. Prijemni host proverava da li postoje aplikacije povezane sa ovim datagramima i ne pronalazeći nijednu šalje nazad paket „Destination Unreachable“. Kako se sve više i više prima UDP paketa šalje odgovor za iste, sistem postaje preopterećen sa gubitkom mogućnosti da izvrši interakciju sa ostalim klijentima. U okviru UDP flood napada, napadač može da lažira IP adresu paketa, kako bi se uverio da povratni ICMP paketi ne stignu do svog izvora, postižući anonimnost napada.



Slika 2. Prikaz UDP FLOOD napada

UDP (user datagram protocol) predtsavlja mrežni protocol bez veze i sesije. Pošto UDP saobraćaj ne zahteva trosmerno rukovanje kao TCP, on radi sa nižim troškovima resursa i idealan je za saobraćaj koji ne treba da se proverava. Međutim, ova ista svojstva doprinose lakoj zloupotrebi UDP protokola. U nedostatku početnog rukovanja, da bi se uspostavila važeća veza, veliki obim saobraćaja može da se pošalje preko UDP kanala na bilo koji host, bez ugrađene zaštite koja bi ograničila brzinu pristizanja saobraćaja. To znači da ne samo da su UDP flood napadi visoko efikasni, već i da se mogu izvršiti uz pomoć relativno malo resursa. Jedna vrsta UDP FLOOD napada naziva se “napad alfabetskom supom”. UDP ne definiše specifične formate paketa, pa stoga napadači mogu da kreiraju velike pakete (ponekad i preko 8 KB), popune ih proizvoljnim tekstom ili brojevima (otuda „alfabetska supa“) i pošalju ih napadnutom hostu. Kada žrtva primi pakete ispunjene smećem na datom portu, proverava da li neka aplikacja iščekuje te pakete. Kada utvrdi da nijednoj apikaciji nisu potrebni pristigli paketi žrtva odgovara sa ICMP paketom nedostupno odredište.

## ICMP FLOOD

ICMP (Internet Control Message Protocol) flood napad poznat i kao ping flood napad, predstavlja uobičajen DDoS napad u kojem napadač pokušava da preplavi ciljani uređaj ICMP echo zahtevima (pingovima). Obično se ICMP poruke eho-zahteva i eho-odgovora koriste za pingovanje mrežnog uređaja u cilju dijagnostikovanja povezanosti između pošiljaoca i primaoca. Slanjem ping zahteva žrtvi, mreža je primorana da u jednakom broju paketa šalje odgovore što rezultuje preopterećenjem ciljane mreže. Neke vrste napada mogu uključivati prilagođene alate ili programske kodove kao na primer [hping](https://en.wikipedia.org/wiki/Hping) i [scapi](https://www.tutorialspoint.com/python_penetration_testing/python_penetration_testing_dos_and_ddos_attack.htm). ICMP flood DDoS napad zahteva da napadač zna IP adresu cilja. Na osnovu toga koju IP adresu napadač zna razlikuju se napadi:

Napad u lokalnoj mreži – u ovoj vrsti DDoS napada, ping zahtevi ciljaju određeni računar na lokalnoj mreži. U ovom slučaju, napadač mora prethodno da dobije IP adresu odredišta.

Napad na ruter - ping poplava cilja rutere sa ciljem da prekine komunikaciju između računara na mreži. U ovoj vrsti DDoS napada, napadač mora imati internu IP adresu lokalnog rutera.

Slepi ping – uključuje korišćenje eksternog programa za otkrivanje IP adrese žrtvinog računara ili rutera pre pokretanja DDoS napada.

ICMP flood napadi preplavljuju mrežu ciljanog uređaja lažnim saobraćajem, zbog toga legitimni zahtevi su sprečeni da prođu.

## SYN FLOOD

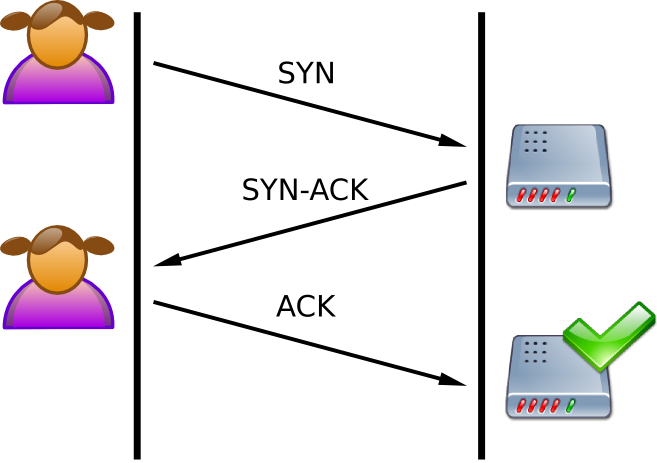
Predstavlja DDoS napad koji može da cilja bilo koji sistem povezan na internet i pruža usluge TCP mrežnog protokola. Tip DoS napada u kojem napadač šalje seriju SYN zahteva žrtvi. DDoS napad se postiže korišćenjem TCP protokola i načinom na koji se uspostavlja veza između dva sistema.

Klijent i server razmenjuju niz poruka koje izgledaju ovako:

Klijent zahteva vezu slanjem SYN poruke serveru.

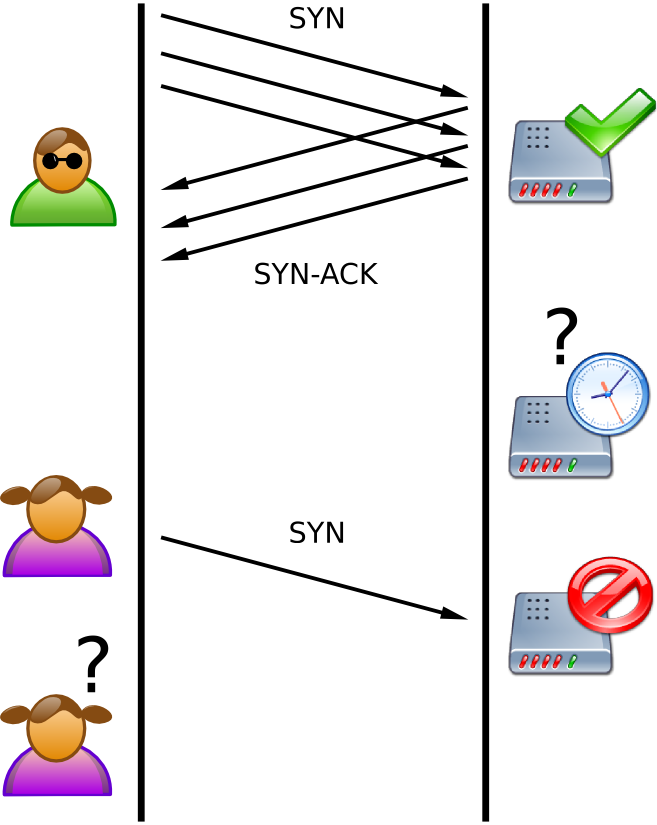
Server odgovara i potvrđuje vezu slanjem poruke SIN-ACK klijentu.

Klijent potvrđuje slanjem ACK poruke i tako se konekcija uspostavlja.



Slika 3. Potpuno trosmerno TCP rukovanje

Ova vrsta komunikacije se naziva i TCP trosmerno rukovanje, gde je sa leve strane prikazan legitimni korisnik, a sa desne strane server kome se šalje zahtev za povezivanje. Ranjivost je zasnovana na obavezi servera da čuva i registruje sve SYN zahteve i čuva ih u memoriji dok se veza ne završi. Napadač šalje veliki broj SYN zahteva sa lažne IP adrese ili drugih računara. Na sve posalate SYN zahteve dobija SYN-ACK poruku ali nikad ne odgovara sa ACK zahtevom prisiljavajući server da čuva poluotovrene TCP konekcije. Kada iskoristi sve resurse za takve poluotvorene veze, server više ne može da obrađuje novopristigle legitimne SYN zahteve, čime uskraćuje usluge redovnim korisnicima. Konkretna implementacija napada može se izvršiti promenom IP adrese zahteva nepostojećom (spoofing), ili podešavanjem napadačevog klijenta da ne šalje ACK pakete, odbijajući odgovor serveru.



Slika 4. Prikaz SYN FLOOD napada

fff

# Literatura

1. “What is DDoS attack?”, AWS, <https://aws.amazon.com/shield/ddos-attack-protection/>, 03.11.2021.
2. “What is DDoS attack – DDoS meaning”, Kaspersky, <https://www.kaspersky.com/resource-center/threats/ddos-attacks>, 03.11.2021.
3. “DDoS Attacks”, Imperva, <https://www.imperva.com/learn/ddos/ddos-attacks/>, 04.11.2021
4. “7 Tips for Defending Your Network against DDoS Attacks”, Corero, <https://www.corero.com/blog/7-tips-for-defending-your-network-against-ddos-attacks/>, 05.11.2021
5. “8 best DDoS protection services”, Pc & Network Downloads, [https://www.pcwdld.com/best-ddos-protection-services 06.11.2021](https://www.pcwdld.com/best-ddos-protection-services%2006.11.2021)
6. “Šta je DDoS napad?”, Mint, <https://mint.rs/baza-znanja/sta-je-ddos-napad/> 02.12.2021
7. “Primer DDoS napada?”, SafetyDetetives, <https://sr.safetydetectives.com/blog/sta-je-ddos-napad/> 04.12.2021
8. “Šta je DDoS?”, Myserveraname, [https://hr.myservername.com/what-is-ddos-attack 04.12.221](https://hr.myservername.com/what-is-ddos-attack%2004.12.221)