ZAŠTITITE SVOJU FIRMU I ZAPOSLENE

DDoS I TIPOVI DDoS NAPADA

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

SRB-CERT

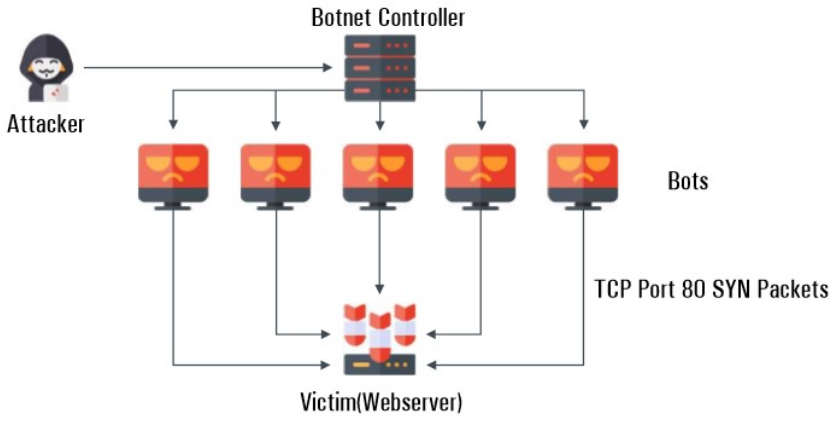
O DDoS NAPADU

Napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. „*Denial-of-service attack*" – *DoS*) je pokušaj napadača da onemogući pristup serveru ili servisima koji su namenjeni krajnjim korisnicima.

Na primer, može se pokrenuti napad za presretanje korisnika i onemogućavanje korišćenja veb stranica za online kupovinu. DDoS može usporiti dostupnost mreže i sistemskih resursa ili oštetiti server.

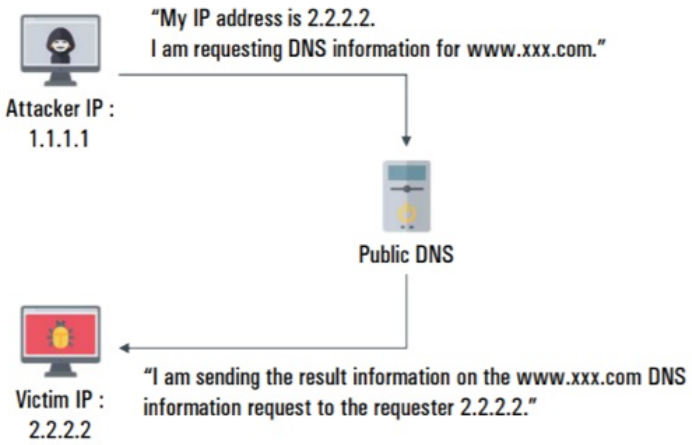
Višestruki napad sa ciljem onemogućavanja ili ometanja finkcionisanja IKT sistema (engl. „*Distributed denial-ofservice attack*" – DDoS) ima za cilj da se poremeti normalan saobraćaj servera, usluge ili mreže, preplavljujući infrastrukturu većom količinom internet saobraćaja. DDoS napadi postižu efikasnost koristeći više kompromitovanih računarskih sistema kao izvora saobraćaja.

Standardni DDoS napad odvija se tako što napadač pošalje veliku količinu zlonamernog saobraćaja direktno na određeni server i mrežu. Jedna od metoda napada otvorena za napadača je slanje saobraćaja pomoću mreže botova (*Botnet*), koja predstavlja automatizovan i napad koji skenira mrežne adrese i širi zaraze na ranjivim računarima, što omogućava hakerima da preuzmu kontrolu nad zaraženim računarima i pretvore ih u botove. *Botnet* je zapravo veći broj zombi (host) sistema zaraženih zlonamernim softverom i koji mogu međusobno komunicirati i kontrolisati jedni druge putem internet veze. Kao što je prikazano na Slici 1, ako napadač izvrši DDoS napad koristeći botnet mrežu, neki ili svi zombiji povezani sa botnetom takođe pokreću napade. Kao rezultat toga, DDoS napad se povećava da bi se izazvalo preopterećenje resursa kod žrtve i napadi se vrše istovremno na više mreža i ka većem broju zemalja, ako je to moguće.



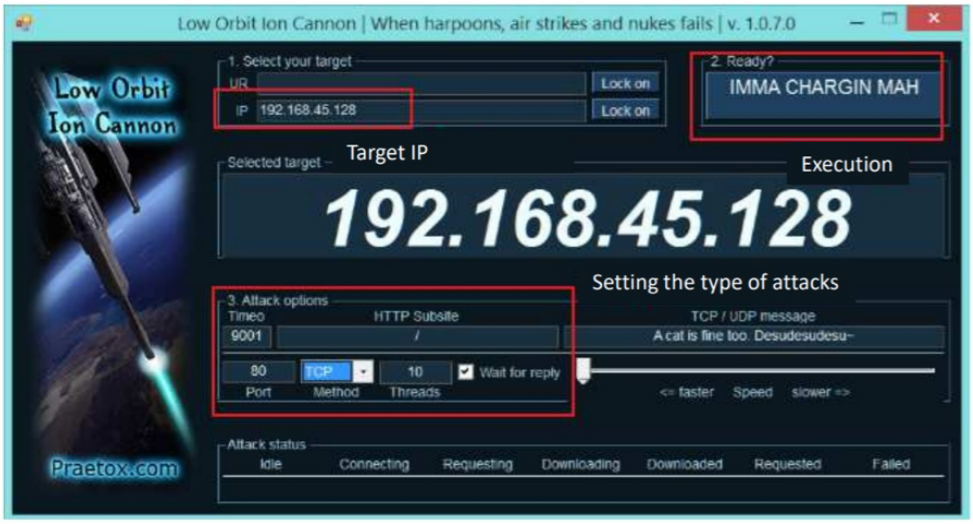
Slika 1 – Standardni DDoS *SYN Flood* napad

Reflektovani DDoS napad na sta je kada napadač koristi ukradenu IP adresu. Ako napadač koristi IP adresu ciljanog sistem a napada umesto sopstvene IP adrese prilikom slanja zahteva za regularan pristup veb serveru, nakon toga stiže regularni odgovor veb servera koji šalje odgovor za traženu uslugu na zloupotrebljenu IP adresu (žrtva). Pored toga, zajedno sa napadom se uglavnom koristi i tehnologija pojačanja (*amplification technology*), koja pojačava odgovor žrtve više od upućenih zahteva, povećavajući na taj način efikasnost napada. Kao što je prikazano na slici 2, napadač podmeće lažnu IP adresu i lažno se predstavlja kao žrtva, a zatim šalje zlonamerne DNS zahteve ka javnom DNS serveru. Čak iako napadač pošalje manji zahtev, žrtva dobija veliku količinu odgovora odjavnog DNS servera zbog korišćenja tehnologije pojačanja.



Slika 2 – Primer *DNS* reflektovanog i pojačanog napada

Na Internetu, napadač lako može doći doraznih besplatnih i plaćenih DDoS alata za napade, uključujući *Low Orbit Ion Cannon* (*LOIC*) i *High Orbit Ion Cannon* (*HOIC*), kao što je prikazano na Slici 3, koji su kreirani kao *open source* alati.

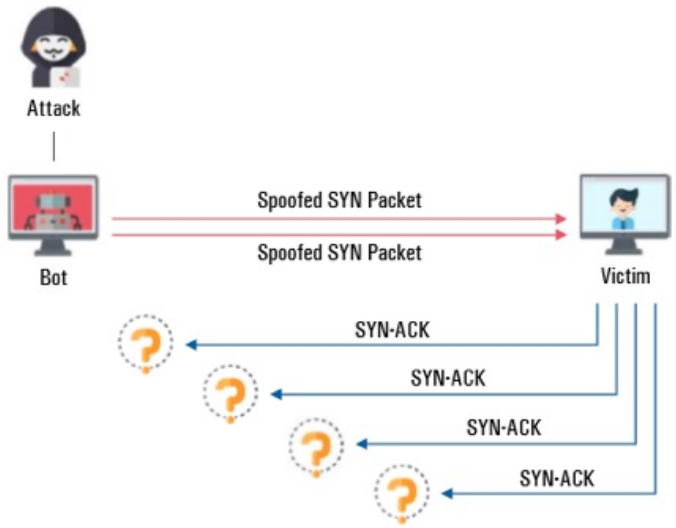


Slika 3 – Ekran LOIC GUI-a

TIPOVI STANDARDNIH DDoS NAPADA

SYN Flood napad

SYN Flood je jedan od najstarijih tipova DDoS napada i najčešće korišćena metoda. Napadač šalje *TCP* (*SYN*) zahteve za povezivanje kontinuirano kako bi sistem žrtve trošio resurse servera, tako da korisnici koji inače koriste ove resurse, ne mogu pristupiti serveru. Kada server primi *SYN* zahtev za povezivanje, server drži komunikaciju otvorenom i čeka potvrdu (*SYN-ACK*) poruke od klijenta, koja se koristi za potvrdu veze. Međutim, *SYN Flood* troši resurse servera sve dok ne istekne podešeno vreme veze, zato što nije poslao *SYN-ACK* poruku. Kao rezultat toga, server žrtve ne uspostavlja vezu sa korisnicima i na taj način uzrokuje prekid usluge.



Slika 4 – Standardni *SYN Flood* napad

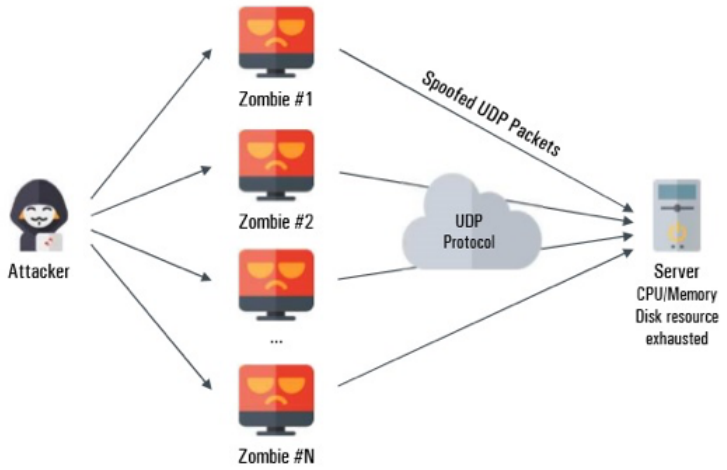
Mere zaštite od *SYN Flood* napada

- Pregledom mrežnih logovaproverite da li TCP SYN flag proverava SYN Flood. Mogu se koristiti alati za analizu mreže kao što su TCPdump ili Wireshark.
- Proveriti TCP SYN paket da li je normalan i da ne ukazuje da postoji zlonamerna aktivnost. Međutim, može se smatrati DDoS napadom ako se u kratkom vremenskom periodu napravi više SYN paketa.
- Podesite TCP Keepalive i pravilo maximum connection na svim perifernim uređajima kao što su firewall i proxy server, kako bi se smanjila šteta prouzrokovana *SYN Flood* napadima.
- Uticaj *SYN Flood*-a se može ublažiti upotrebom *SYN cookie*-a na *firewall* uređaju.Ako se koristi *SYN cookie*, *firewall* proverava *TCP* vezu između klijenta i servera pre nego što je saobraćaj preusmeren ka serveru. Ako napadač ne pošalje konačnu poruku potvrde za uspostavu veze, *firewall* prekida vezu.
- Ako je napad otkriven, zatražite pomoć i pružanje mera zaštite od *ISP*-a da biste ublažili napad.

TIPOVI STANDARDNIH DDoS NAPADA

UDP Flood napad

UDP Flood je vrlo sličan *SYN Flood* DDoS napadu. Napadač šalje veliku količinu saobraćaja ka ciljanom serveru koristeći botnetmreže. *UDP Flood* se razlikuje od *TCP Flood*-a po tome što je relativno brži i upotrebljava ceo propusni opseg koji je dostupan u serverskom mrežnom okruženju, umesto da koristi resurse servera, i na taj način prekida pristup korisnicima. Ovaj napad se može desiti pokretanjem aplikativnog programa koji čeka na prijem paketa kada je na serveru otvoren *UDP port* (npr. port 50555) za primanje *UDP* paketa.Ako nema paketa koji je na čekanju na odgovarajućem portu, server odgovara na *UDP* paket koristeći *ICMP Destination Unreachable* paket. Veliki broj većih *UDP* paketa se šalje tokom napada i koristi se ceo raspoloživ propusni opseg tako da većina servera brzo odgovori.



Slika 5 – Standardni *UDP Flood* napad

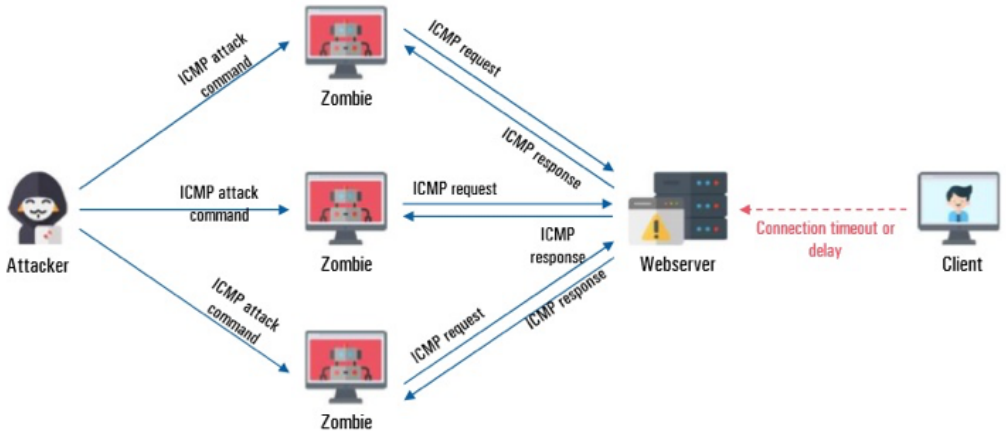
Mere zaštite od *UDP Flood* napada

- Pregledom mrežnih logova pokušajte da nađete *UDP* pakete koji su pod napadom tako što ćete proverti da li postoji *UDP Flood* i proverite zahteve za komunikaciju sa neregularnih mrežnih portova primljenih sa više IP adresa. Mnogi internet servisi koriste *UDP*. Uobičajeni *UDP* portovi su 53 (*DNS*), 88 (*Kerberos*), 137/138/445 (*Windows*) i 161 (*SNMP*).
- Da biste umanjili štetu nastalu usled *UDP flood* napada, podesite pravilno periferne mrežne uređaje kao što je *firewall*, koji omogućava dolazni saobraćaj samo za potrebne i odobrene portove.
- Ako je napad otkriven, zatražite pomoć i pružanje mera zaštite od *ISP*-a da biste ublažili napad.

TIPOVI STANDARDNIH DDoS NAPADA

ICMP Flood napad

ICMP Flood napad se odvija tako što napadač, koristeći *botnet* mrežu, pošalje veliki broj *ICMP* paketa ka ciljnom serveru da bi iskoristio ceo propusni opseg i prekinuo pristup korisnicima. Ovaj napad zahteva dovoljno *ICMP* zahteva i odzivnog saobraćaja da bi se iskoristio ceo propusni opseg ka ciljanoj mreži. Primer ovog napada je komanda ping koja se obično koristi za testiranje veze između dve tačke u mreži. Međutim, veličina *ping*-a i ciklični zahtevi se podešavaju pomoću komandi i parametara i iskorišćavaju ceo dostupni propusni opseg u mreži.



Slika 6 – Standardni *ICMP Flood* napad

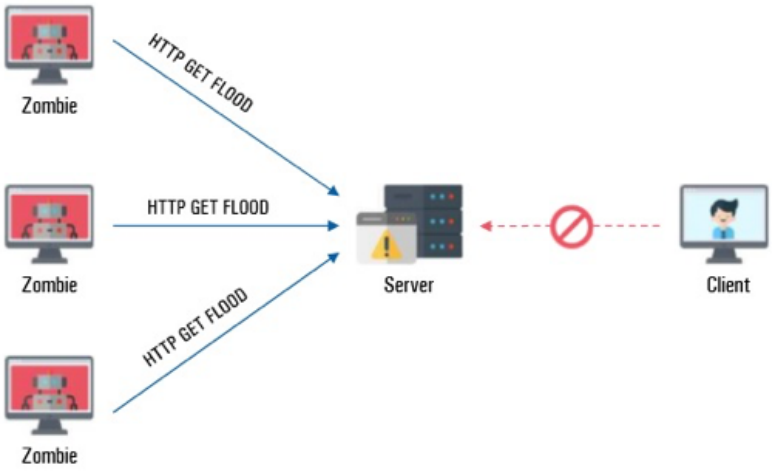
Mere zaštite od *ICMP Flood* napada

- Pregledom mrežnih logova pokušajte da nađete zahteve od strane mnogo korisnika za ulazne *ICMP* pakete i na taj način proverite da li postoji *ICMP Flood*.
  → *ICMP* se proverava upotrebom alata koji se koristi za pregledanje logova (npr. *Wireshark*). *ICMP* ne koristiti mrežne portove kao što su *TCP* i *UDP*.
  → *ICMP* protokol se može identifikovati po broju transportnog protokola, „1“, zaglavlja IP paketa.
- Podesite prag (*threshold*) za *ICMP* paket na mrežnom uređaju poput rutera i na taj način minimizirajte štetu prouzrokovanu *ICMP Flood*-om. Postavite dozvoljeni prag za paket u sekundi za *ICMP* zahtev na susednim ruterima. Kada je postavljen prag, ulazni *ICMP* paket će se neko vreme ignorisati, ako je prag prekoračen. Prag paketa u sekundi efikasno sprečava opterećenje mreže *ICMP* paketima.
- Ako je napad otkriven, zatražite pomoć i pružanje mera zaštite od *ISP*-a da biste ublažili napad.

TIPOVI STANDARDNIH DDoS NAPADA

HTTP Flood napad

HTTP Flood spečava korisnike da koriste resurse veb serveraslanjem velike količine zahteva *HTTP GET* poruka ka ciljanom veb sajtu. U ovom slučaju, veb server pokušava da odgovori na napadačeve zahteve, ali napadač ne obrađuje potvrdu i dopušta da veb server čeka.Kao rezultat toga, veb server održava vezu na čekanju dodeljivanjem fiksnih resursa svakoj vezi za određeni vremenski period za proveru potvrde.Napadač pravi mnogo *HTTP GET* zahteva ka veb serveru i ne vraća potvrdu. Tako napadnuti veb server koristi sve komunikacione resurse i korisnici ne mogu da pristupe uslugama veb sajta.



Slika 7 – Klasičan *HTTP Flood* napad

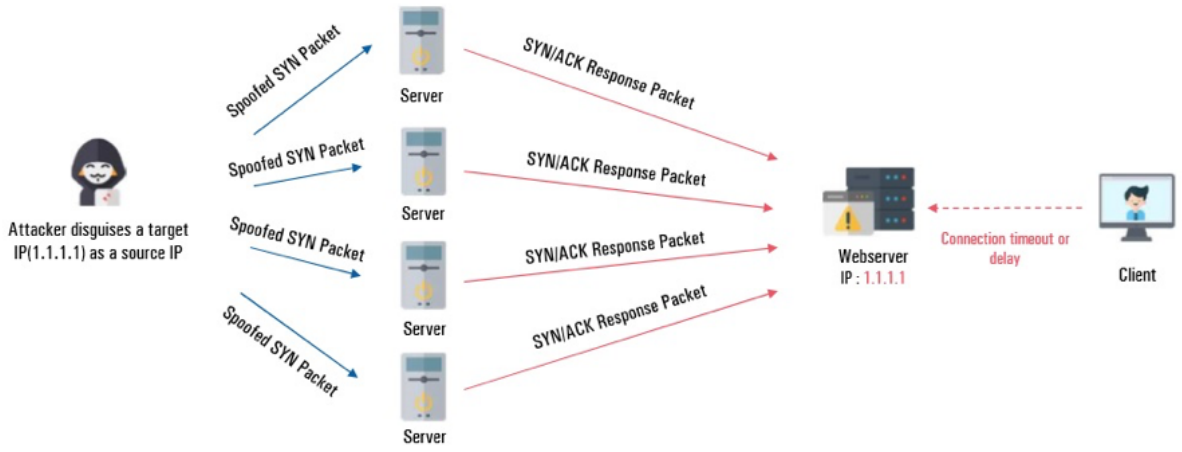
Mere zaštite od *HTTP Flood* napada

- Pregledom mrežnih logova pokušajte da nađete zahteve pomoću porta 80 i *TCP* protokola i na taj način proverite da li postoji *HTTP GET Flood*. Mogu se koristiti alati za analizu mreže kao što su *TCPdump* ili *Wireshark*.
- Teško je preduzeti mere predostrožnosti za blokiranje ove vrste napada zato što se koristi uobičajeni način pružanja veb servisa. Nije efikasan način ni blokiranja svih izvorišnih IP adresa, kao i IP adresa običnih korisnika, jer je većina napada sa izvorišnih IP adresa deo botneta. Štete nastale ovim napadom mogu se umanjiti korišćenjem *Web application firewall*-a (*WAF*).
- Ako je napad otkriven, zatražite pomoć i pružanje mera zaštite od *ISP*-a da biste ublažili napad.

TIPOVI REFLEKTOVANIH DDoS NAPADA

SYN + ACK reflektovani napad

SYN+ACK Flood je DRDoS (*Distributed Reflection Denial of Service*) metoda napada. Napadač krade IP adresu žrtve i šalje *SYN* pakete ka serveru da bi ga iskoristio kao reflektor, tako što server šalje žrtvi *SYN/ACK* pakete kao potvrdu. Kada žrtva dobija veliku količinu *SYN/ACK* paketa, troši svoje resurse za obradu paketa, što uzrokuje opterećenje na serveru u toku procesa i onemogućava pristup resursima običnim korisnicima. Kako ima formu DRDoS-a, reflektovaniserveri šalju ponovo pakete, ako im druga strana (žrtva) ne pošalje potvrde jer ih smatra neuspelim prenosom paketa,povećava se efikasnost napada.



Slika 8 - *SYN+ACK* refeltovani napad

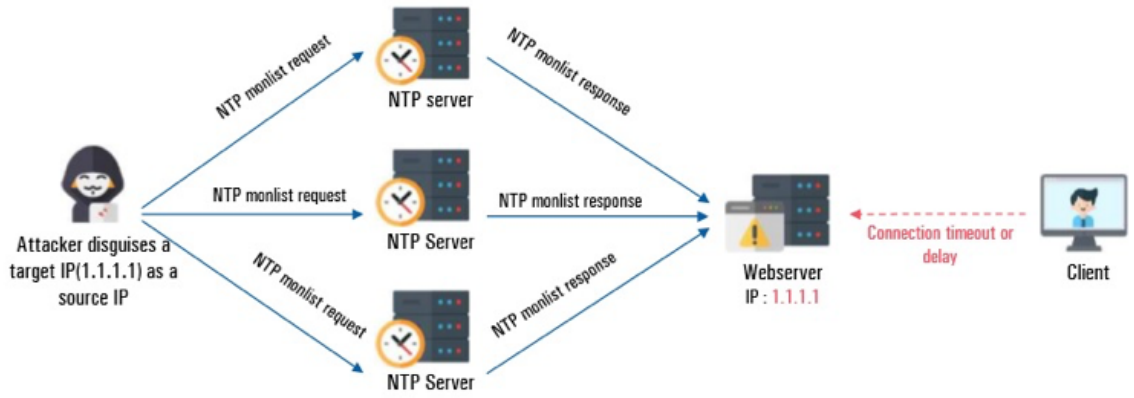
Mere zaštite od *SYN + ACK* reflektovanog napada

- Прегледом мрежних логова покушајте да нађете захтеве помоћу порта 80 и *TCP* протокола и на тај начин проверите да ли постоји *HTTP GET Flood*. Могу се користити алати за анализу мреже као што су *TCPdump* или *Wireshark*.
- Primanje *TCP SYN/ACK* paketa se odvija u procesu trostrukog rukovanja *(three-way handshaking*). Sam paket je normalanog izgleda i veličine, ali se može posumnjati na DDoS napad ako se broj paketa povećava brzo u kratakom vremenskom periodu.
- Da biste umanjili štetu nastalu usled *SYN/ACK Flood* napada, podesite pragove (*threshold*) za odredišne IP *SYN/ACK* pakete na perifernim mrežnim uređajima kao što su *firewall* i *proxy* server.
- Ako je napad otkriven, zatražite pomoć i pružanje mera zaštite od *ISP*-a da biste ublažili napad.

TIPOVI REFLEKTOVANIH DDoS NAPADA

NTP reflektovani pojačan (*reflection and amplification*) napad

NTP (*Network Time Protocol*) reflektovani napad je vrsta napada gde napadač generiše saobraćaj na serveru. *NTP* se koristiza sinhronizaciju vremena između servera i klijenta, kao i između samih servera, a koristi se *UDP 123 port*. Napadač krade IP adresu veb servera kojeg ciljano želi da napadne i traži od *NTP servera* da pošalje veliku količinu odgovorapaketa (fiksne veličine paketa) ka ciljnom serveru. Efikasnost napadamože se značajno povećati korišćenjem tehnologije pojačanja (*amplification technology*), koja omogućava da odgovor *NTP* servera bude veći od zahteva koji je poslao napadač. Kada napadač zatraži monlist sa mnogih *NTP* servera koji su otvoreni na Internetu, ti serveri odjednom šalju svoje odgovore na zahtevani monlist ka ciljnom serveru. Zatim ciljni server koristi sve dostupne mrežne propusne opsege i ne može da pruži usluge korisnicima.



Slika 9 – *NTP* reflektovani napad

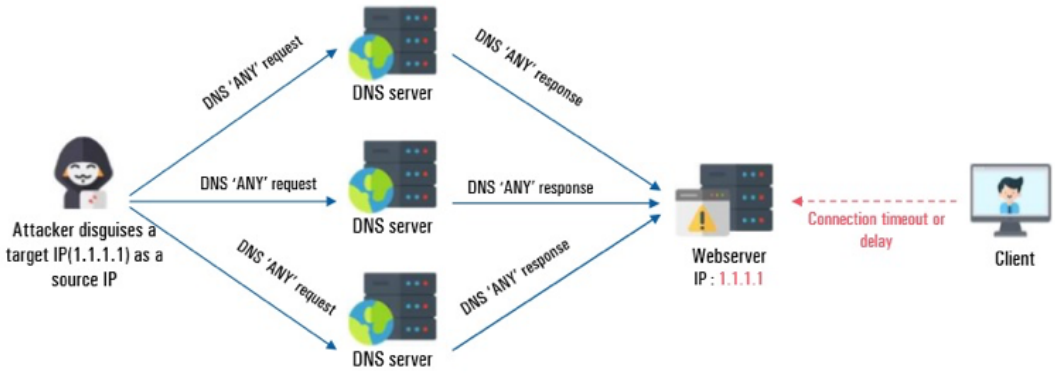
Mere zaštite od *NTP* reflektovanog i pojačanog (*reflection and amplification*) napada

- Da biste otkrili da li je upitanju *NTP* reflektovani i pojačan napad, potrebno je da pregledom mrežnih logova proverite pakete sa *UDP* portom 123 i određene veličine paketa između izvora.
- Preduzmite sledeće preventivne mere da biste se odbranili od ulaznih napada i sprečili *NTP* server da se koristi za napad na druge korisnike:
  - → Koristite *NTP* verziju servera 2.4.7 ili novije verzije da biste u potpunosti izbegli komandu *monlist* ili koristite *NTP* verziju koja ne koristi komandu *monlist*, kao što je *OpenNTPD*.
  - → Ako se server ne može nadograditi (*upgraded*) na novije verzije, dodajte u konfiguracioni fajl *ntp.conf* „*disable monitor*“ i ponovo pokrenite *NTP* proces da biste onemogućili funkciju *monlist* upita.
  - → Primenite pravila restrikcijena *firewall*-u, koja sprečavaju neovlašćene pakete da komuniciraju sa *NTP* serverom.
- Ako je napad otkriven, prosledite sve bitne informacije koje se koriste za napad (IP adresa, veličina paketa itd.) *ISP*-u i zatražite filtriranje saobraćaja.

TIPOVI REFLEKTOVANIH DDoS NAPADA

DNS reflektovani pojačan (*reflection and amplification*) napad

Za *DNS* (*Domain Name System*) reflektovani napad, napadačkoristi *DNS* sistem za slanje velike količine poruka. *DNS* sistem konvertuje *character-based adrese* domena koje su unosili korisnici Interneta za IP adrese. *DNS* reflektovani napad koristi postupak kojim napadač krade IP adresu žrtve i šalje *DNS lookup* zahteveka javnom *DNS* serveru. Javni *DNS* server šalje odgovor na zahtev žrtvi. Veličina odgovora zavisi od opcija koje je napadač odredio u *DNS lookup* zahtevu. Napadač u zahtevu može da koristi opciju *ANY* da bi dobio maksimalan efekat pojačanja, koji vraća sve informacijeo *DNS* zoni. Kada napadač ukrade IP adresu žrtve i počne da šalje *DNS lookup* zahtev na više javnih *DNS* servera, žrtva dobija pojačan odgovor, koji na kraju za cilj ima da iskoristi sve raspoložive propusne opsege žrtve.



Slika 10 – *DNS* reflektovani napad

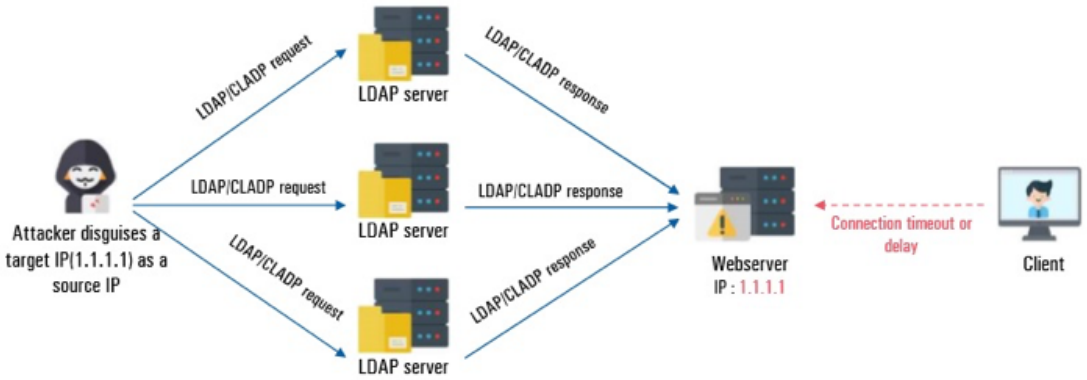
Mere zaštite od *DNS* reflektovanog i pojačanog (*reflection and amplification*) napada

- Da biste otkrili da li je upitanju *DNS* reflektovani i pojačan napad, potrebno je da pregledom mrežnih logova proverite dolazne *DNS query* odgovore bez *DNS query* zahteva.
- *DNS* servisi ne bi trebalo da koriste funkciju *DNS* rekurzije u skladu sa uputstvima koje daju *DNS* programeri (*BIND*, *Microsoft*, itd.)
  → Sledeći sajtovi vrše proveru i testiraju da li se javni *DNS* server može iskoristiti za napade:
  https://dnschecker.org/
  https://www.whatismyip.com/dns-lookup/
  https://mxtoolbox.com/DNSLookup.aspx
  http://openresolverproject.org/
- Ako je napad otkriven, obratite se *ISP*-u i zahtevajte da se paketi filtriraju pre nego što se pošalju ka serveru.

TIPOVI REFLEKTOVANIH DDoS NAPADA

CLDAP reflektovani pojačan (*reflection and amplification*) napad

Kada se radi o *CLDAP* (*Connection-less Lightweight Directory Access Protocol*) reflektovanom napadu, napadač krade ciljanu IP adresu i šalje *CLDAP* zahteve *LDAP* serveru. *CLDAP* se koristi za kreiranje, pretraživanje i izmenu deljeniih Internet direktorijuma i koristi *UDP port 389*. *CLDAP* reflektovani napad se odvija tako što napadač pošalje *CLDAP* upite naviše *LDAP* servera koji koriste ukradenu IP adresu. *LDAP* server šalje odgovore na zahtev na ukradenu IP adresu žrtve. Žrtva ne može da pruži usluge jer ne može da se izbori sa velikom količinom *LDAP*/*CLDAP* saobraćaja koja pristiže u isto vreme. *UDP LDAP* protokol povećava efikasnost napada upotrebom tehnologije pojačanja, koji se može pojačati od 52 do 70 puta.



Slika 10 – *CLDAP* reflektovani napad

Mere zaštite od *CLDAP* reflektovanog i pojačanog (*reflection and amplification*) napada

- Potrebno je da pregledate logove zahteva koji koriste *UDP port 389* na izvoru.
- Prilikom pokretanja *LDAP* servera, podesite pravila na *firewall*-u kako bi se sprečilo iskorišćavanje *LDAP* servera za napad.
- Ako je napad otkriven, obratite se *ISP*-u i zahtevajte da se paketi filtriraju pre nego što se pošalju ka serveru.

Izvor:

Guidance on Responding to Denial of Service Attack for SME - KISA