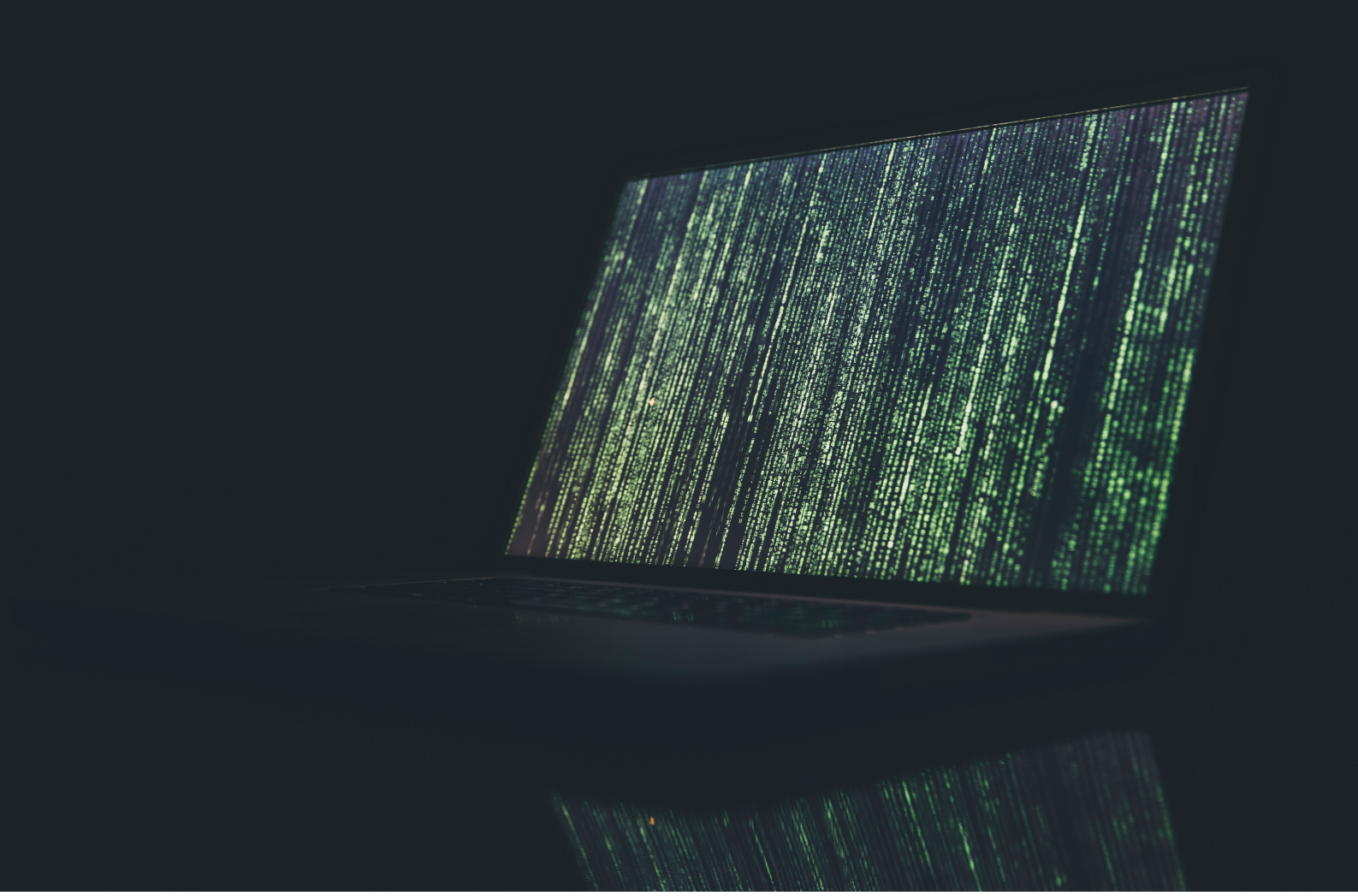


DDoS И ТИПОВИ DDoS НАПАДА

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ

СРБ-ЦЕРТ

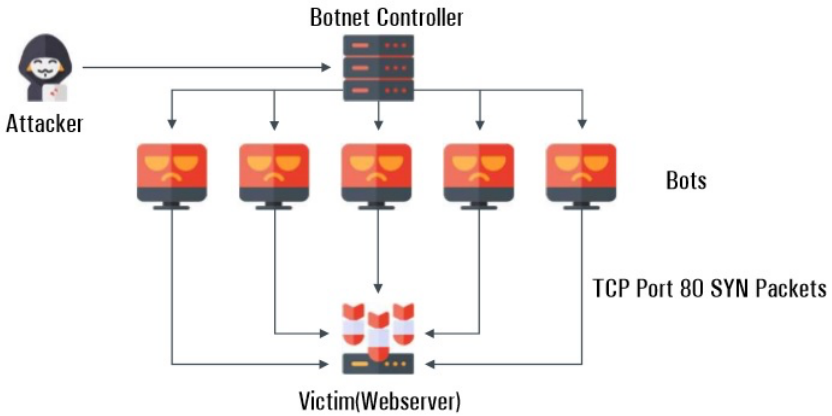
О DDoS НАПАДУ

Напад са циљем онемогућавања или ометања функционисања ИКТ система (енгл. „*Denial-of-service attack*" – DoS) је покушај нападача да онемогући приступ серверу или сервисима који су намењени крајњим корисницима.

На пример, може се покренути напад за пресретање корисника и онемогућавање коришћења веб страница за online куповину. ДДоС може успорити доступност мреже и системских ресурса или оштетити сервер.

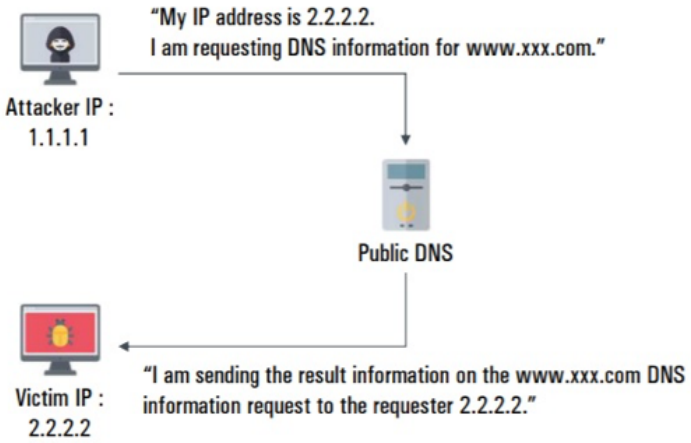
Вишеструки напад са циљем онемогућавања или ометања финкционисања ИКТ система (енгл. „*Distributed denial-ofservice attack*" – DDoS) има за циљ да се поремети нормалан саобраћај сервера, услуге или мреже, преплављујући инфраструктуру већом количином интернет саобраћаја. DDoS напади постижу ефикасност користећи више компромитованих рачунарских система као извора саобраћаја.

Стандардни DDoS напад одвија се тако што нападач пошаље велику количину злонамерног саобраћаја директно на одређени сервер и мрежу. Једна од метода напада отворена за нападача је слање саобраћаја помоћу мреже ботова (*Botnet*), која представља аутоматизовани напад који скенирамрежне адресе и шири заразе на рањивим рачунарима, што омогућава хакерима да преузму контролу над зараженим рачунарима и претворе их у ботове. Ботнет је заправо већи број зомби (хост) система заражених злонамерним софтвером и који могу међусобно комуницирати и контролисати једни друге путем интернет везе. Као што је приказано на Слици 1, ако нападач изврши DDoS напад користећи ботнет мрежу, неки или сви зомбији повезани са ботнетом такође покрећу нападе. Као резултат тога, DDoS напад се повећава да би се изазвало преоптерећење ресурса код жртве и напади се вршеистовремно на више мрежа и ка већем броју земаља, ако је то могуће.



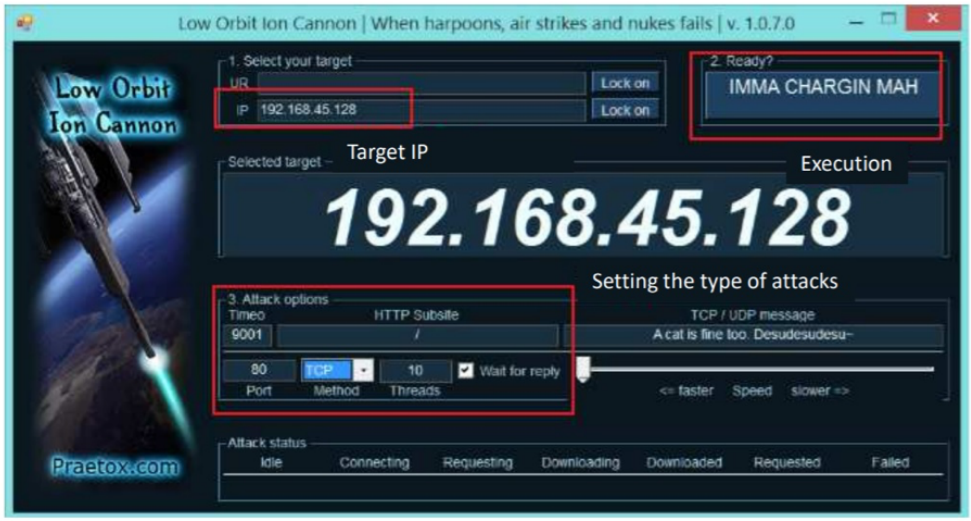
Слика 1 – Стандардни DDoS *SYN Flood* напад

Рефлектовани DDoS напад настаје када нападач користи украдену IP адресу. Ако нападач користи IP адресу циљаног система напада уместо сопствене IP адресе приликом слања захтева за регуларан приступ веб серверу, након тога стиже регуларни одговор веб сервера који шаље одговор за тражену услугу на злоупотребљену IP адресу (жртва). Поред тога, заједно са нападом се углавном користи итехнологија појачања (*amplification technology*), која појачава одговор жртве више од упућених захтева, повећавајући на тај начин ефикасност напада. Као што је приказано на Слици 2, нападач подмеће лажну IP адресу и лажно се представља као жртва, а затим шаље злонамерне *DNS* захтеве ка јавном *DNS* серверу. Чак и ако нападач пошаље мањи захтев, жртва добија велику количину одговора од јавног *DNS* сервера због коришћења технологије појачања.



Слика 2 – Пример *DNS* рефлектованог и појачаног напада

На Интернету, нападач лако може доћи до разних бесплатних и плаћених DDoS алата за нападе, укључујући *Low Orbit Ion Cannon* (LOIC) и *High Orbit Ion Cannon* (HOIC), као што је приказано на Слици 3, који су креирани као *open source* алати.

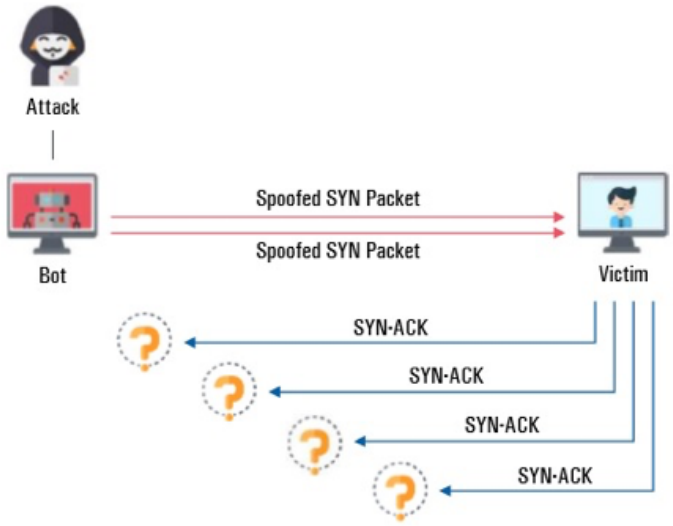


Слика 3 – Екран LOIC GUI-а

ТИПОВИ СТАНДАРДНИХ DDoS НАПАДА

SYN Flood напад

SYN Flood је један од најстаријих типова DDoS напада и најчешће коришћена метода. Нападач шаље *TCP* (*SYN*) захтеве за повезивање континуирано како би систем жртве трошио ресурсе сервера, тако да корисници који иначе користе ове ресурсе, не могу приступити серверу. Када сервер прими *SYN* захтев за повезивање, сервер држи комуникацију отвореном и чека потврду (*SYN-ACK*) поруке од клијента, која се користи за потврду везе. Међутим, *SYN Flood* троши ресурсе сервера све док не истекне подешено време везе, зато што није послао *SYN-ACK* поруку. Као резултат тога, сервер жртве не успоставља везу са корисницима и на тај начин узрокује прекид услуге.



Слика 4 – Стандардни *SYN Flood* напад

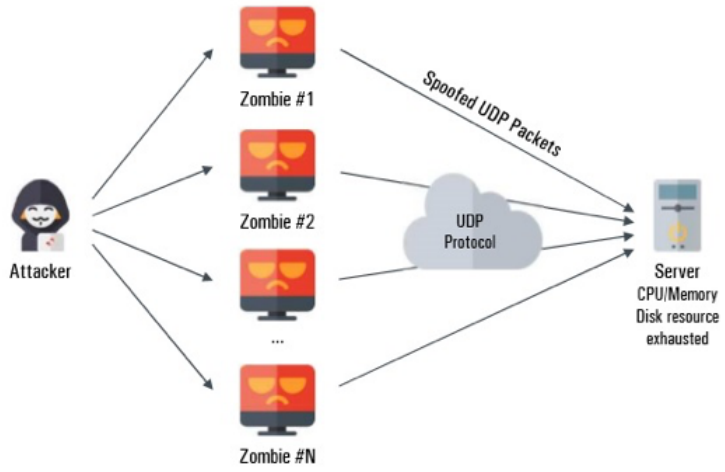
Мере заштите од *SYN Flood* напада

- Прегледом мрежних логова проверите да ли *TCP SYN flag* проверава *SYN Flood*. Могу се користити алати за анализу мреже као што су *TCPdump* или *Wireshark*.
- Проверити *TCP SYN* пакет да ли је нормалан и да не указује да постоји злонамерна активност. Међутим, може се сматрати DDoS нападом ако се у кратком временском периоду направи више *SYN* пакета.
- Подесите *TCP Keepalive* и правило *maximum connection* на свим периферним уређајима као што су *firewall* и *proxy* сервер, како би се смањила штета проузрокована *SYN Flood* нападима.
- Утицај *SYN Flood-a* се може ублажити употребом SYN *cookie-a* на *firewall* уређају. Ако се користи *SYN* cookie, *firewall* проверава *TCP* везу између клијента и сервера пре него што је саобраћај преусмерен ка серверу. Ако нападач не пошаље коначну поруку потврде за успоставу везе, *firewall* прекида везу.
- Ако је напад откривен, затражите помоћ и пружање мера заштите од ИСП-а да бисте ублажили напад.

ТИПОВИ СТАНДАРДНИХ DDoS НАПАДА

UDP Flood напад

UDP Flood је врло сличан SYN Flood DDoS нападу. Нападач шаље велику количину саобраћаја ка циљаном серверу користећи ботнет мреже. *UDP Flood* се разликује од *TCP Flood-a* по томе што је релативно бржи и употребљава цео пропусни опсег који је доступан у серверском мрежном окружењу, уместо да користи ресурсе сервера, и на тај начин прекида приступ корисницима. Овај напад се може десити покретањем апликативног програма који чека на пријем пакета када је на серверу отворен *UDP* порт (нпр. порт 50555) за примање *UDP* пакета. Ако нема пакета који је на чекању на одговарајућем порту, сервер одговара на *UDP* пакет користећи *ICMP Destination Unreachable* пакет. Велики број већих *UDP* пакета се шаље током напада и користи се цео расположив пропусни опсег тако да већина сервера брзо одговори.



Слика 5 – Стандардни *UDP Flood* напад

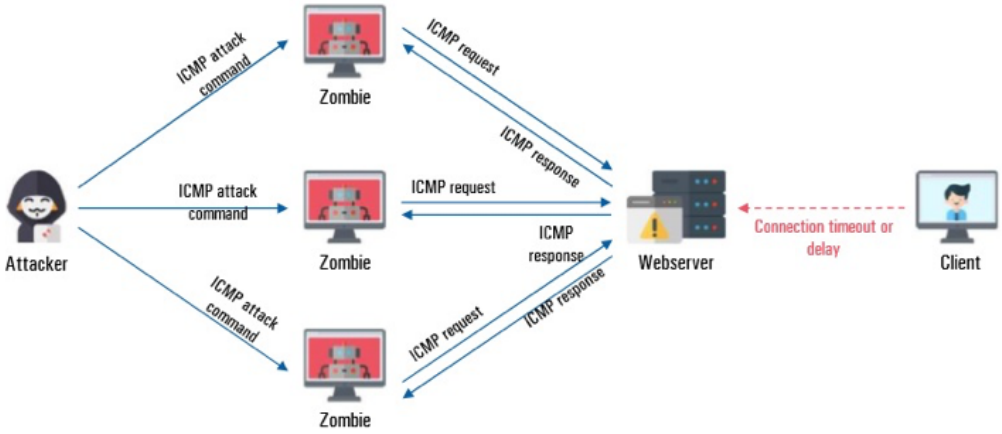
Мере заштите од *UDP Flood* напада

- Прегледом мрежних логова покушајте да нађете *UDP* пакете који су под нападом тако што ћете проверти да ли постоји *UDP Flood* и проверите захтеве за комуникацију са нерегуларних мрежних портова примљених са више IP адреса. Многи интернет сервиси користе *UDP*. Уобичајени *UDP* портови су 53 (*DNS*), 88 (*Kerberos*), 137/138/445 (*Windows*) и 161 (*SNMP*).
- Да бисте умањили штету насталу услед *UDP flood* напада, подесите правилно периферне мрежне уређаје као што је *firewall*, који омогућава долазни саобраћај само за потребне и одобрене портове.
- Ако је напад откривен, затражите помоћ и пружање мера заштите од ИСП-а да бисте ублажили напад.

ТИПОВИ СТАНДАРДНИХ DDoS НАПАДА

ICMP Flood напад

ICMP Flood напад се одвија тако што нападач, користећи ботнет мрежу, пошаље велики број *ICMP* пакета ка циљном серверу да би искористио цео пропусни опсег и прекинуо приступ корисницима. Овај напад захтева довољно *ICMP* захтева и одзивног саобраћаја да би се искористио цео пропусни опсег ка циљаној мрежи. Пример овог напада је команда ping која се обично користи за тестирање везе између две тачке у мрежи. Међутим, величина *ping-а* и циклични захтеви се подешавају помоћу команди и параметара и искоришћавају цео доступни пропусни опсег у мрежи.



Слика 6 – Стандардни *ICMP Flood* напад

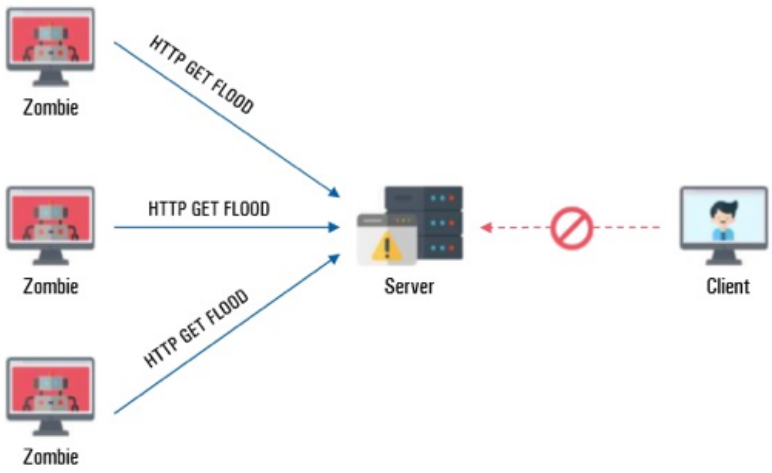
Мере заштите од *ICMP Flood* напада

- Прегледом мрежних логова покушајте да нађете захтеве од стране много корисника за улазне *ICMP* пакете и на тај начин проверите да ли постоји *ICMP Flood*.
  → *ICMP* се проверава употребом алата који се користи за прегледање логова (нпр. *Wireshark*).
  → *ICMP* не користити мрежне портове као што су *TCP* и *UDP*. *ICMP* протокол се може идентификовати по броју транспортног протокола, „1“, заглавља IP пакета.
- Подесите праг (*threshold*) за *ICMP* пакет на мрежном уређају попут рутера и на тај начин минимизирајте штету проузроковану *ICMP Flood-ом*. Поставите дозвољени праг за пакет у секунди за ICMP захтев на суседним рутерима. Када је постављен праг, улазни *ICMP* пакет ће се неко време игнорисати, ако је праг прекорачен. Праг пакета у секунди ефикасно спречава оптерећење мреже *ICMP* пакетима.
- Ако је напад откривен, затражите помоћ и пружање мера заштите од ИСП-а да бисте ублажили напад.

ТИПОВИ СТАНДАРДНИХ DDoS НАПАДА

HTTP Flood напад

HTTP Flood спечава кориснике да користе ресурсе веб сервера слањем велике количине захтева *HTTP GET* порука ка циљаном веб сајту. У овом случају, веб сервер покушава да одговори на нападачеве захтеве, али нападач не обрађује потврду и допушта да веб сервер чека. Као резултат тога, веб сервер одржава везу на чекању додељивањем фиксних ресурса свакој вези за одређени временски период за проверу потврде. Нападач прави много *HTTP GET* захтева ка веб серверу и не враћа потврду. Тако нападнути веб сервер користи све комуникационе ресурсе и корисници не могу да приступе услугама веб сајта.



Слика 7 – Класичан *HTTP Flood* напад

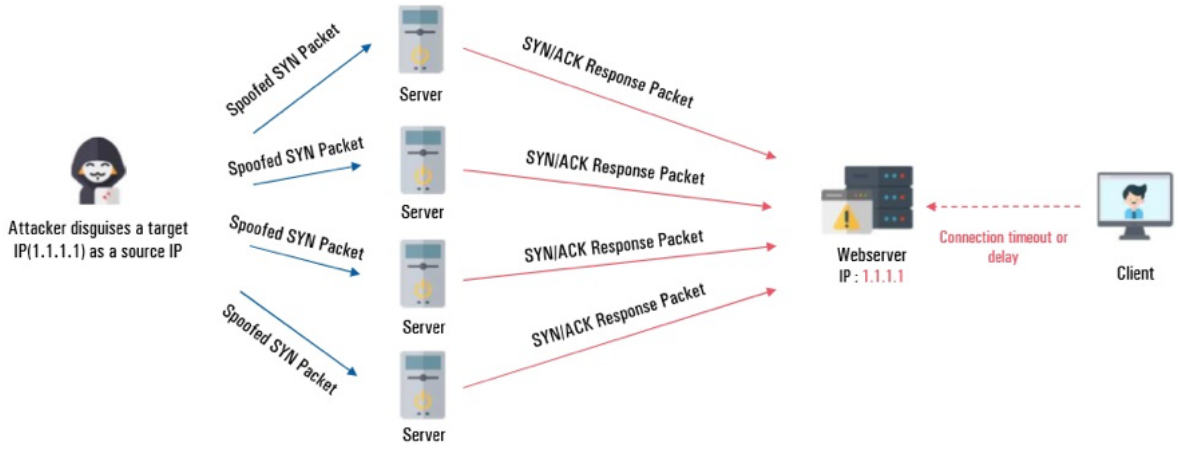
Мере заштите од *HTTP Flood* напада

- 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*.
- Тешко је предузети мере предострожности за блокирање ове врсте напада зато што се користи уобичајени начин пружања веб сервиса. Није ефикасан начин ни блокирања свих изворишних IP адреса, као и IP адреса обичних корисника, јер је већина напада са изворишних IP адреса део ботнета. Штете настале овим нападом могу се умањити коришћењем Web application firewall-a (*WAF*).
- Ако је напад откривен, затражите помоћ и пружање мера заштите од ИСП-а да бисте ублажили напад.

ТИПОВИ РЕФЛЕКТОВАНИХ DDoS НАПАДА

SYN + ACK рефлектовани напад

SYN+ACK Flood је ДРДоС (*Distributed Reflection Denial of Service)* метода напада. Нападач краде IP адресу жртве и шаље *SYN* пакете ка серверу да би га искористио као рефлектор, тако што сервер шаље жртви *SYN/ACK* пакете као потврду. Када жртва добија велику количину *SYN/ACK* пакета, троши своје ресурсе за обраду пакета, што узрокује оптерећење на серверу у току процеса и онемогућава приступ ресурсима обичним корисницима. Како има форму ДРДоС-а, рефлектовани сервери шаљу поново пакете, ако им друга страна (жртва) не пошаље потврде јер их сматра неуспелим преносом пакета, повећава се ефикасност напада.



Слика 8 - *SYN+ACK* рефелтовани напад

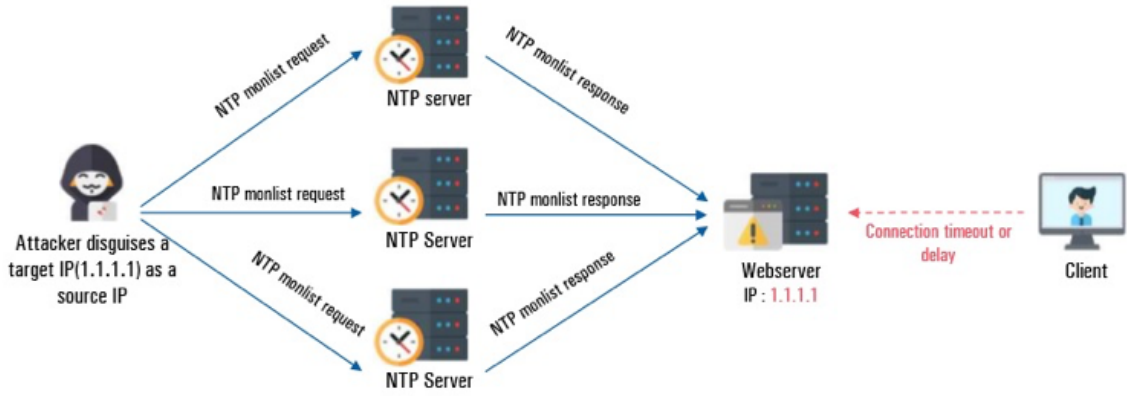
Мере заштите од *SYN + ACK* рефлектованог напада

- 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*.
- Тешко је предузети мере предострожности за блокирање ове врсте напада зато што се користи уобичајени начин пружања веб сервиса. Није ефикасан начин ни блокирања свих изворишних IP адреса, као и IP адреса обичних корисника, јер је већина напада са изворишних IP адреса део ботнета. Штете настале овим нападом могу се умањити коришћењем *Web application firewall-a* (*WAF*).
- Ако је напад откривен, затражите помоћ и пружање мера заштите од ИСП-а да бисте ублажили напад.

ТИПОВИ РЕФЛЕКТОВАНИХ DDoS НАПАДА

NTP рефлектован и појачан (*reflection and amplification*) напад

NTP (*Network Time Protocol*) рефлектовани напад је врста напада где нападач генерише саобраћај на серверу. *NTP* се користи за синхронизацију времена између сервера и клијента, као и између самих сервера, а користи се *UDP* 123 порт. Нападач краде IP адресу веб сервера којег циљано жели да нападне и тражи од *NTP* сервера да пошаље велику количину одговора пакета (фиксне величине пакета) ка циљном серверу. Ефикасност напада може се значајно повећати коришћењем технологије појачања (*amplification* technology), која омогућава да одговор *NTP* сервера буде већи од захтева који је послао нападач. Када нападач затражи *monlist* са многих *NTP* сервера који су отворени на Интернету, ти сервери одједном шаљу своје одговоре на захтевани *monlist* ка циљном серверу. Затим циљни сервер користи све доступне мрежне пропусне опсеге и не може да пружи услуге корисницима.



Слика 9 – *NTP* рефлектовани напад

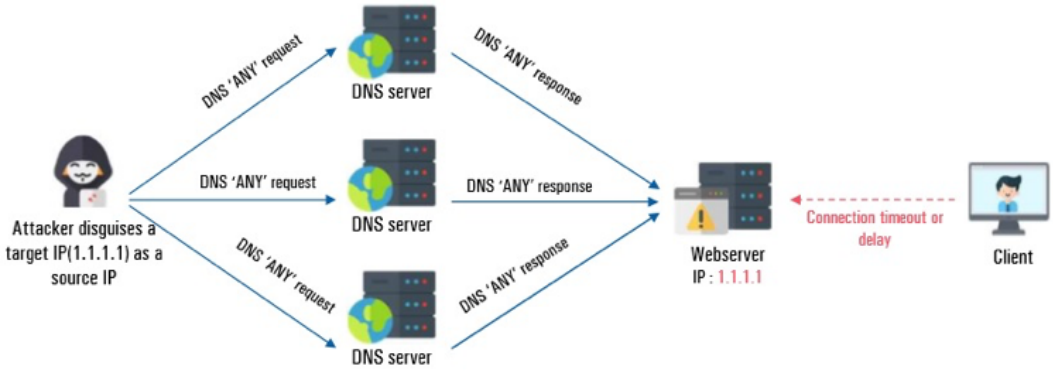
Мере заштите од *NTP* рефлектованог и појачаног (*reflection and amplification*) напада

- Да бисте открили да ли је упитању *NTP* рефлектовани и појачан напад, потребно је да прегледом мрежних логова проверите пакете са *UDP* портом 123 и одређене величине пакета између извора.
- Предузмите следеће превентивне мере да бисте се одбранили од улазних напада и спречили NTP сервер да се користи за напад на друге кориснике:
  - → Користите *NTP* верзију сервера 2.4.7 или новије верзије да бисте у потпуности избегли команду *monlist* или користите *NTP* верзију која не користи команду *monlist*, као што је *OpenNTPD*.
  - → Ако се сервер не може надоградити (upgraded) на новије верзије, додајте у конфигурациони фајл *ntp.conf* „*disable monitor*" и поново покрените *NTP* процес да бисте онемогућили функцију *monlist* упита.
  - → Примените правила рестрикције на firewall-у, која спречавају неовлашћене пакете да комуницирају са *NTP* сервером.
- Ако је напад откривен, проследите све битне информације које се користе за напад (IP адреса, величина пакета итд.) ИСП-у и затражите филтрирање саобраћаја.

ТИПОВИ РЕФЛЕКТОВАНИХ DDoS НАПАДА

DNS рефлектован и појачан (*reflection and amplification)* напад

За *DNS* (*Domain Name System*) рефлектовани напад, нападач користи *DNS* систем за слање велике количине порука. *DNS* систем конвертује character-based адресе домена које су уносили корисници Интернета за IP адресе. *DNS* рефлектовани напад користи поступак којим нападач краде IP адресу жртве и шаље *DNS lookup* захтеве ка јавном *DNS* серверу. Јавни *DNS* сервер шаље одговор на захтев жртви. Величина одговора зависи од опција које је нападач одредио у *DNS lookup* захтеву. Нападач у захтеву може да користи опцију *ANY* да би добио максималан ефекат појачања, који враћа све информације о *DNS* зони. Када нападач украде IP адресу жртве и почне да шаље *DNS lookup* захтев на више јавних *DNS* сервера, жртва добија појачан одговор, који на крају за циљ има да искористи све расположиве пропусне опсеге жртве.



Слика 10 – *DNS* рефлектовани напад

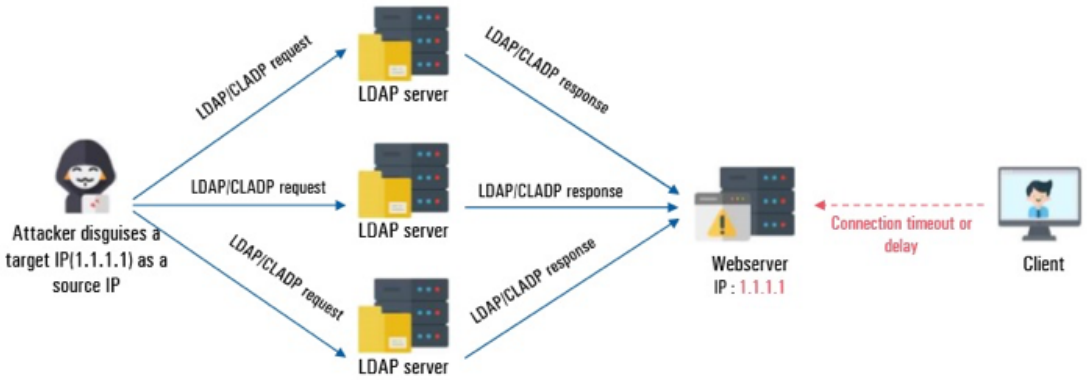
Мере заштите од *DNS* рефлектованог и појачаног (*reflection and amplification*) напада

- Да бисте открили да ли је упитању *DNS* рефлектовани и појачан напад, потребно је да прегледом мрежних логова проверите долазне *DNS query* одговоре без *DNS query* захтева.
- *DNS* сервиси не би требало да користе функцију *DNS* рекурзије у складу са упутствима које дају *DNS* програмери (*BIND*, *Microsoft*, итд.)
  → Следећи сајтови врше проверу и тестирају да ли се јавни *DNS* сервер може искористити за нападе:
  https://dnschecker.org/
  https://www.whatismyip.com/dns-lookup/
  https://mxtoolbox.com/DNSLookup.aspx
  http://openresolverproject.org/
- Ако је напад откривен, обратите се ИСП-у и захтевајте да се пакети филтрирају пре него што се пошаљу ка серверу.

ТИПОВИ РЕФЛЕКТОВАНИХ DDoS НАПАДА

CLDAP рефлектован и појачан (*reflection and amplification*) напад

Када се ради о *CLDAP* (*Connection-less Lightweight Directory Access Protocol*) рефлектованом нападу, нападач краде циљану IP адресу и шаље *CLDAP* захтеве *LDAP* серверу. *CLDAP* се користи за креирање, претраживање и измену дељениих Интернет директоријума и користи *UDP* порт 389. *CLDAP* рефлектовани напад се одвија тако што нападач пошаље *CLDAP* упите на више *LDAP* сервера који користе украдену IP адресу. *LDAP* сервер шаље одговоре на захтев на украдену IP адресу жртве. Жртва не може да пружи услуге јер не може да се избори са великом количином *LDAP/CLDAP* саобраћаја која пристиже у исто време. *UDP LDAP* протокол повећава ефикасност напада употребом технологије појачања, који се може појачати од 52 до 70 пута.



Слика 10 – *CLDAP* рефлектовани напад

Мере заштите од *CLDAP* рефлектованог и појачаног (*reflection and amplification*) напада

- Потребно је да прегледате логове захтева који користе *UDP* порт 389 на извору.
- Приликом покретања *LDAP* сервера, подесите правила на *firewall*-у како би се спречило искоришћавање *LDAP* сервера за напад.
- Ако је напад откривен, обратите се ИСП-у и захтевајте да се пакети филтрирају пре него што се пошаљу ка серверу.

Извор:

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