ЗАШТИТА ПОДАТАКА

ЗАШТИТА СИСТЕМА

Distributed Denial of Service Attacks

Преглед

- Биће објашњено:
  - DDoS
  - типови напада
  - противмере

DDoS

- Distributed denial of service (DDoS) напади представљају значајну сигурносну претњу за корпорације
- DDoS напади чине рачунарске системе неприступачним, тако што затрпавају сервере, мрежу, па чак и крајње корисничке системе бескорисним саобраћајем како легитимни корисници више не могу да приступе тим ресурсима
- Denial of service (DoS) напад је покушај да се спрече легитимни корисници неког сервиса да користе тај сервис
- Када напад долази од стране једног корисника назива се DoS напад
- Озбиљнија претња је DDoS напад
- Код DDoS напада, нападач регрутује одређени број рачунара путем интернета како би истовремено и координисано упутио напад на мету

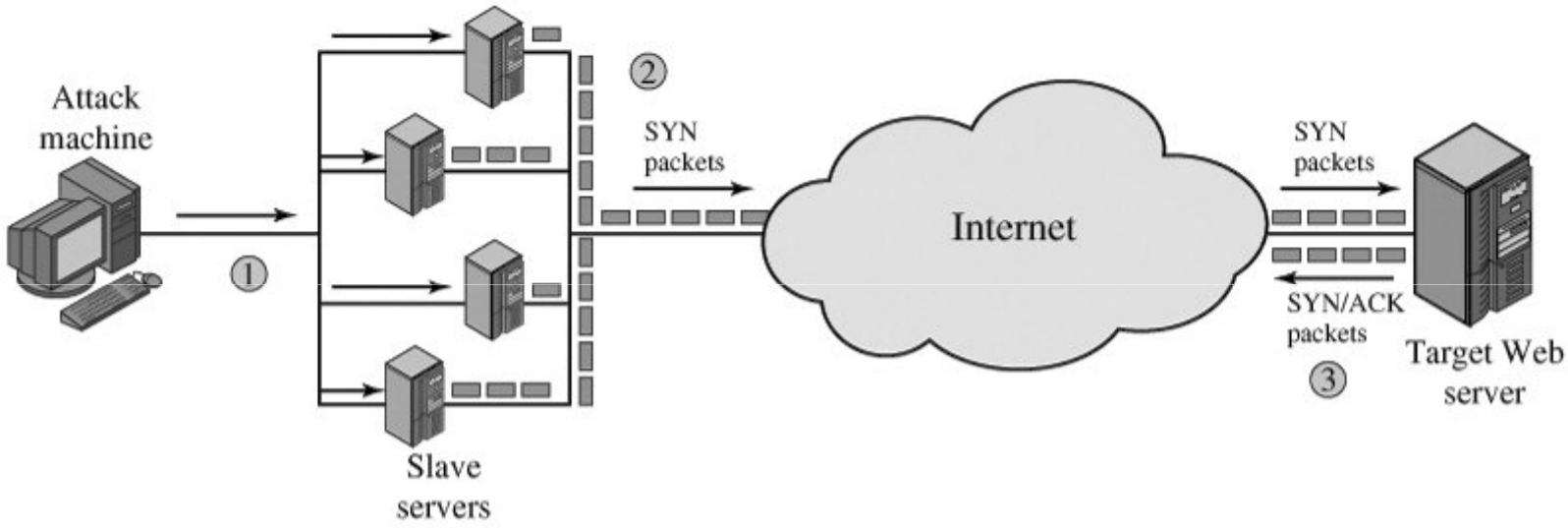
DDoS подела

- DDoS напад покушава да заузме ресурсе мете како она не би могла да пружи услугу за коју је намењена
- Један начин да се поделе DDoS напади је по типу ресурса који заузимају
- Ресурс који се заузима је или интерни ресурс неког рачунара или капацитет за пренос података

DDoS пример

- Једноставан пример заузимања интерних ресурса је напад затрпавањем SYN пакетима
- Кораци:
  - Нападач преузима контролу над одређеним бројем рачунара на интернету
  - Рачунарима које је заузео наређује да контактирају сервер и они почињу да шаљу TCP/IP SYN (synchronize/initialization) пакете са погрешним повратним IP адресама
  - Сваки SYN пакет је захтев да се отвори TCP конекција. За сваки такав пакет сервер одговара са SYN/ACK (synchronize/acknowledge) пакетом, покушавајући да успостави TCP конекцију, али безуспешно, због погрешне IP адресе. Сервер одржава структуру података за сваки SYN захтев, чекајући одговор и како се обим саобраћаја повећава понестаје му ресурса, чиме више легитимни корисници не могу да приступе серверу

DDoS пример (2)

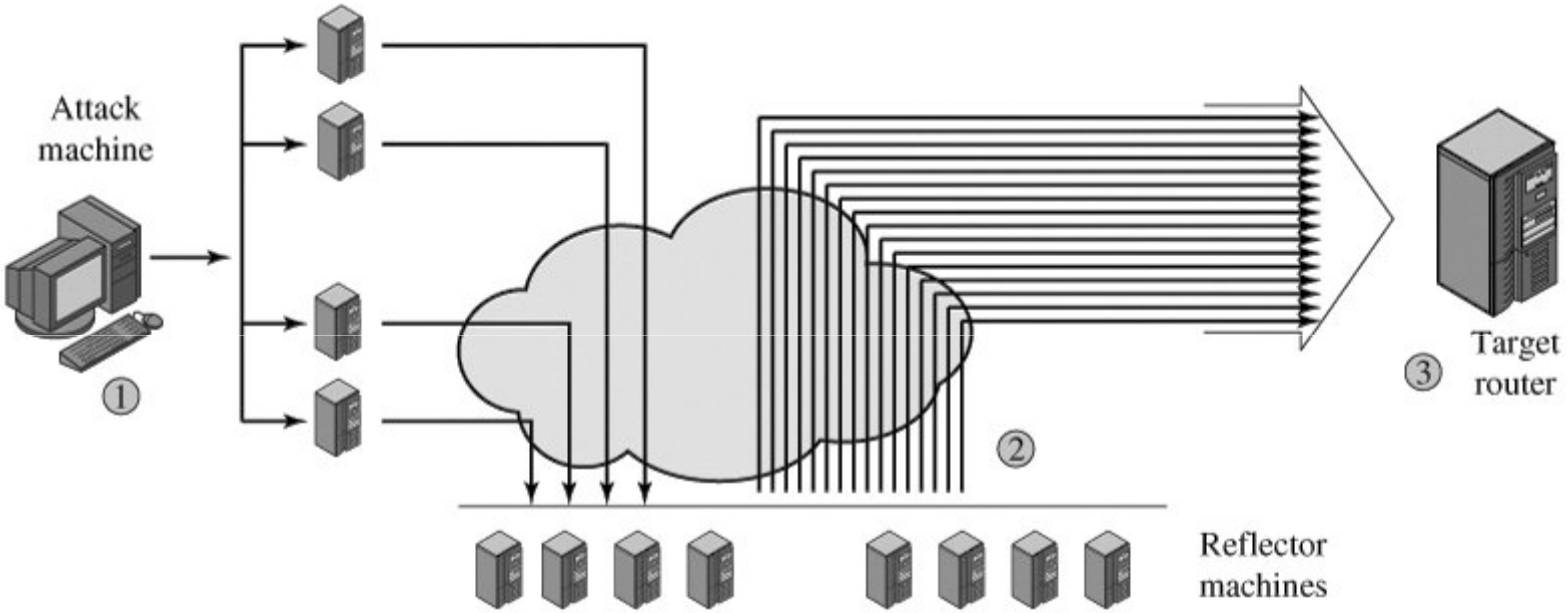


(a) Distributed SYN flood attack

DDoS пример (3)

- Пример напада који заузима ресурсе за пренос података је напад ICMP пакетима.
- Кораци:
  - Нападач преузима контролу над одређеним бројем рачунара на интернету и наређује им да шаљу ICMP ECHO пакете са повратном IP адресом мете групи корисника који служе као рефлектори
    - Internet Control Message Protocol (ICMP) је протокол на IP нивоу који служи да се размењују контролни пакети између рутера и рачунара. ECHO пакет захтева да примаоц одговори са echo reply пакетом пошиљаоцу како би се проверило да ли је могућа комуникација између њих.
  - Рефлектори примају поруку и одговарају на њу, шаљући одговоре мети напада
  - Рутер мете напада је преплављен пакетима и не остаје места за регуларан саобраћај

DDoS пример (4)

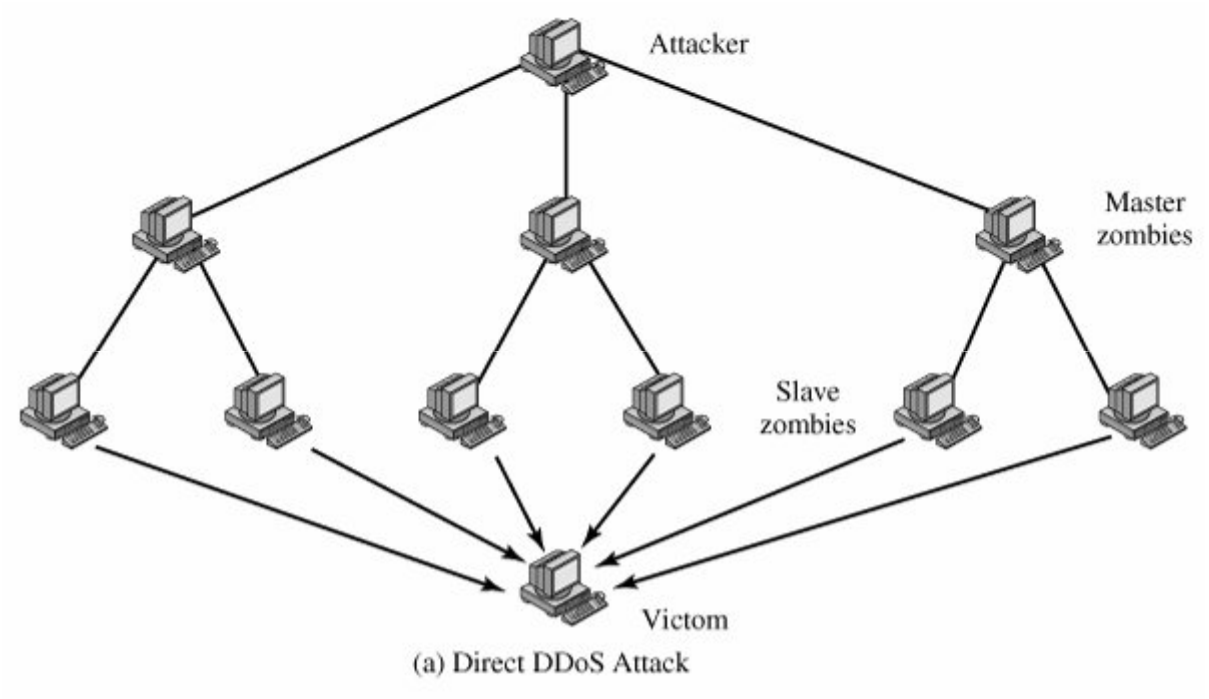


(a) Distributed ICMP attack

DDoS подела (2)

- Други начин да се поделе DDoS напади је по томе да ли су директни или рефлектовани
- Код директних DDoS напада, нападач подметне зомби програм на одређени број рачунара.
- Често постоје два нивоа зомби машина: газде и слуге
- Нападач координише и активира газде зомбије, а они затим то исто раде са слугама
- Коришћење два нивоа чини да је теже открити правог нападача

DDoS подела (3)

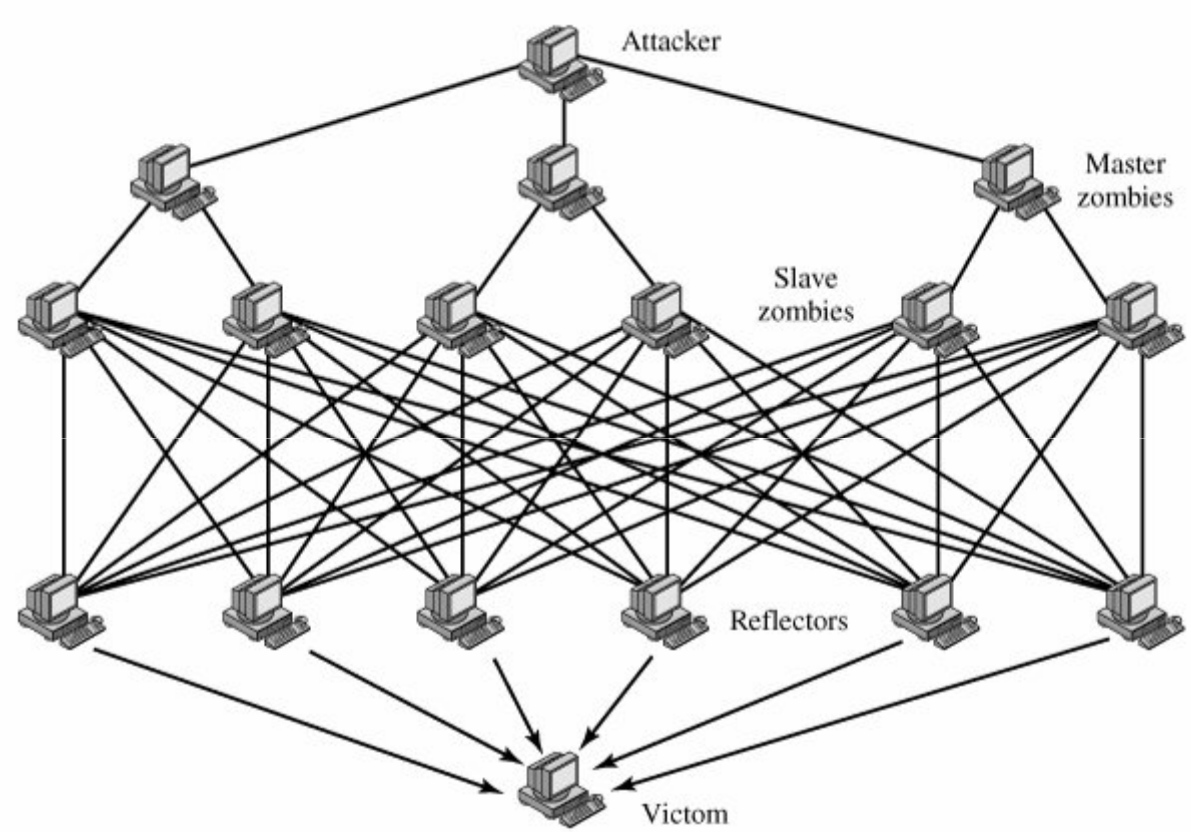


(a) Direct DDoS Attack

DDoS подела (4)

- Рефлектовани DDoS напад додаје још један ниво у претходну шему
- Слуге зомбији конструишу пакете који као повратну адресу имају адресу мете и шаљу их насумичним рачунарима на интернету
- Ови рачунари одговарају пакетима које шаљу мети
- Рефлектовани DDoS напад може укључити већи број машина и већу количину саобраћаја него директан DDoS напад
- Теже је детектовати извор напада

DDoS подела (5)



(b) Reflector DDoS Attack

DDoS противмере

- Постоје три линије одбране од DDoS напада:
- Превенција напада: Омогућити жртвама напада да издрже напад без одбијања сервиса регуларним корисницима. Укључују примену полиса за искоришћење ресурса, помоћне ресурсе на захтев, итд.
- Детекција и филтрирање напада: Покушај да се детектује напад чим почне и да се реагује тренутно. Минимизује се ефекат напада. Укључује филтрирање пакета за које се сумња да су део напада.
- Детектовање и идентификовање извора напада: Покушај да се детектује извор напада као први корак у спречавању будућих напада.
- Изазов у баратању са DDoS нападима представља број различитих начина на које их је могуће извести.
- Потребно је стално усавршавање противмера.