Útoky Denial of Service

- Jeden z mnoha základních forem útoků na vnitřní sítě
  - Založen na přetížení systému
  - Výsledkem je omezení výkonnosti serveru nebo úplný výpadek cílového systému
  - Útok může být zaměřen na síťové komponenty nebo na hostitelské systémy
- Další z mnoha základních forem útoku jsou
  - Skenování portů
  - Přetečení bufferů
  - Prolomení hesla

Přetížení systému

- Cílem DoS je ztlumit skutečný provoz „odpadním“ provozem
  - Dochází k vytěsňování reálných přenosů
    - Klienti na základě detekce zahlcení zpomalují vysílání
    - Směrovače musí přebytečné pakety odstraňovat
      - Zahozené pakety vedou k exponenciálnímu nárůstu času opakování
      - Směrovače jsou přetíženy

- Servery se mohou přetížit zvyšováním počtu požadavků na vytvoření spojení
  - Vytváření TCP spojení vyžaduje zapamatování stavu a odezvu serveru
  - Server požaduje odpověď na SYN od klientů
  - Klienti ale neodpovídají na výzvu serveru

IP spoofing (navádění k nepravostem)

- Navádění systému, aby vložil odlišné zdrojové IP adresy do IP záhlaví
  - DoS útočníci navádějí ze dvou důvodů
    - Nechtějí být odhaleni
    - Spoofing může přidat další zatížení
- Jestliže navádíte s cizími ale legitimními IP adresami
  - Může být spuštěn Reset buď z napadeného počítače, nebo z počítače s použitou IP adresou
    - Okamžité uvolnění zdrojů serveru
  - Pečlivý výběr sekvenčních čísel na straně serveru může ukončit pokus o navázání spojení
- Jestliže navádíte s náhodně vybraným IP

- Odpověď serveru na klientské SYN se ztratí
- Server uvolní zdroje ale typicky až za 75 sekund

Klíčové prvky DoS útoku

- Převedení těžiště činnosti na jiné uzly
  - Princip – co je jednoduché pro mě musí být složité pro tebe
  - Př.: IP spoofing
    - Já: generuji SYN pakety jak rychle to jen jde (mikrosekundy)
    - Ty: timeout odstraňuje SYN každých 75 sekund

Charakteristiky DoS útoku

- Musí být rozšířen na mnoho systémů
  - Typickým cílem je útočit z mnoha míst najednou
    - Umožňuje lepší využití síťových zdrojů
    - Pomáhá čelit preventivnímu měření
    - Pomáhá zatajit útočníka
- DoS software je lehce dostupný a lze jej jednoduše napsat
  - Mnohý lze najít v IRC
- DoS útoky jsou často předcházeny prolomením systému a instalací DoS programů
  - Dává o mnoho více anonymity útočníkovi

Usnadnění DoS útoků

- V počítačové síti běží mnoho systémů
- Počítačová síť je velmi rozlehlá
- Mnozí uživatelé jsou naivní – dávají šanci uchvátit vzdálený systém
- Protokoly internetu jsou známé, to vytváří podmínky pro využití jejich slabin
- Mnoho volného software, ve kterém mohou být zahrnuty utajené funkce
- Nedostatečná ochranná politika používání a managementu
- Velmi rozsáhlý software s mnoha známými děrami
- Nedostatek prostředků pro zastavení útoků

Chování se při DoS útoku

- Neuchovávej stav dokud nedostaneš od klienta ACK
  - DoS útočníci, používající spoofing neposílají ACK
    - Jinak by si museli zapamatovat stav
  - Užívej kryptografii abys předcházel ukládání stavu
    - Pošli klíč pro jedno použití jako odpověď serveru na SYN
    - Odpověď s ACK musí vrátit klíč

- Prostředky detekce proniknutí
    - Zachyť útok na firewallu, pokud jej rozpoznáš
    - Snort
- IP metody zpětného trasování

Snort (Open Source Intrusion Detection System)

- Systém pro detekci útoků (Intrusion Detection Systém)
- Je schopen provádět analýzu toku dat v reálném čase a logování paketů v IP sítích
- Může provádět analýzu protokolů, vyhledávání údajů
- Je schopen detekovat různé útoky a sondování
- Používá jazyk pro popis toku dat
- Obsahuje automat pro detekci podle tohoto popisu
- Umožňuje informovat o útoku v reálném čase (syslog, soubor, sockety, …)