DDoS (Distributed Denial of Service)

DDoS je útok na dostupnost služby. Útočník se nesnaží data ukrást, ale zabránit legitimním uživatelům v přístupu k nim. Představte si to jako situaci, kdy tisíce lidí najednou zaplní vchod do malého obchodu – skuteční zákazníci se pak nedostanou dovnitř a obchod nemůže fungovat.

K provedení útoku útočníci využívají tzv. **Botnety** – sítě infikovaných zařízení (počítače, servery, ale i chytré ledničky nebo kamery), které ovládají na dálku bez vědomí majitelů.

Jak DDoS útok funguje

Útok probíhá ve třech základních krocích:

```
1. **Nábor (Infection):** Útočník pomocí malwaru infikuje velké množství zařízení připojených k internetu.
2. **Příkaz (Command):** Útočník pošle instrukci ze svého řídicího centra (C&C server) všem "botům" v botnetu.
3. **Útok (Flooding):** Všechna zařízení začnou současně posílat obrovské množství požadavků na jednu konkrétní IP adresu oběti.
```

Typy DDoS útoků

DDoS útoky se dělí podle toho, na kterou vrstvu síťového modelu útočí:

1. Volumetrické útoky (Zahlticí)

Cílem je zaplnit celou přenosovou kapacitu (šířku pásma) internetové přípojky oběti.

- **Příklad:** UDP Flood, ICMP Flood.
- **Technika Amplification:** Útočník pošle malý dotaz na nezabezpečený server (např. DNS), který odpoví obrovským množstvím dat přímo oběti.

2. Protokolové útoky

Útočí na slabiny v síťových protokolech a vyčerpávají zdroje síťových prvků (firewally, load balancery).

- **Příklad:** SYN Flood – útočník zahájí tisíce pokusů o navázání spojení, ale nikdy je nedokončí, čímž serveru dojde paměť pro správu těchto „otevřených“ spojení.

3. Aplikační útoky (Layer 7)

Nejsložitější útoky, které napodobují chování skutečných uživatelů. Cílem je zahltit procesor serveru nebo databázi.

- **Příklad:** HTTP Flood – miliony požadavků na načtení konkrétní náročné stránky (např. vyhledávání na e-shopu).

Proč se útoky provádějí?

- **Vydírání:** Útočník požaduje výkupné (v kryptoměnách) za zastavení útoku.
- **Konkurenční boj:** Snaha poškodit reputaci konkurence nebo jí způsobit finanční ztráty během sezóny (např. Black Friday).
- **Hacktivismus:** Útok jako forma politického protestu.
- **Krycí manévr:** DDoS slouží k odvedení pozornosti bezpečnostního týmu, zatímco útočník tiše provádí jiný útok (např. krádež dat).

Obrana proti DDoS

Obrana vyžaduje specializovaná řešení, protože běžný server útok neustojí:

- **CDN (Content Delivery Network):** Sítě jako Cloudflare nebo Akamai dokáží díky své globální kapacitě útočný provoz rozptýlit a odfiltrovat.
- **Scrubbing centra:** Provoz je přesměrován do „čisticích center“, kde analytické systémy oddělí škodlivý provoz od požadavků skutečných uživatelů.
- **Rate Limiting:** Omezení počtu požadavků, které může jedna IP adresa poslat za vteřinu.
- **Anycast Routing:** Rozdělení příchozího provozu na více serverů po celém světě.

Související pojmy: Botnet, Malware, CDN, HTTP, DNS, IP adresa, Firewall, Kybernetická bezpečnost.