Denial of Service

Počítačová obrana a útok

Radek Hučín, HUC0019

April 4, 2017

Vysoká škola báňská - Technická univerzita Ostrava

Motivace

Jak v poslední době vzrůstá počet a síla útoků typu DoS/DDoS, je načase se na ně čím dál více a lépe připravovat a nasazovat moderňejší ochrany.

Rozdělení - 4 typy obrany

Rozdělení - obrana

- Do It Yourself
- Specialized On-Premises Equipment
- ISP – DoS mitigation
- Cloud Mitigation Provider

Obrana obecně

- Blackholing and sinkholing
- IPS based prevention
- DDS based defense
- Firewalls
- Routers, L3 Switches
- Upstream filtering

U cloudové ochrany je možné na úrovni DNS či BGP posílat provoz službě, která provoz pročistí.

Služby

- Cloudflare
- Prolexic (Akamai)
- Impreva Incapsula
- Radware DefensePipe

Rozdělení DoS útoků

Rozdělení - DoS

- Volume Based Attacks (UDP, ICMP flood . . .)
- Protocol Attacks (SYN flood, Ping of Death, Smurf . . .)
- Application Layer Attacks (HTTP flood, Slowloris, . . .)

Volume Based Attacks

- obrana může být obtížná až nemožná
- ideální ochrana - robustná síťová infrastruktura (cloud mitigation)
- až v případě zvládnutí celkového provozu je možné zvažovat další filtrování

Protocol Attacks

- limitovat počet spojení na ip adresu
- blacklist / whitelist
- filtrování pomocí firewallu

Application Layer Attacks

- ochrana musí být v samotné aplikaci nebo v aplikačním firewallu
- ochrana pomocí timoutu (Sloworis, Slow read,..)
- filtrování podle paternů v requestech
- filtrace na základě reputace IP adresy

Zahrňte ochranu před DoS do security procesů

Procesy

- penetrační testování
- aplikační testing - source code analysis, fuzz testing, load & stress testing
- fyzická bezpečnost
- testování politik a procesů zahrnující i sociální inženýrství
- load a stress testing pro identifikaci maximální propustnosti různých zařízení na cestě (server, firewall, IPS, . . .)

Co a proč vlastně bráním?

Rozsah obranných opatření je především otázkou "byznysového" rozhodnutí, které musí zohlednit důležitost konkrétní služby.

Ideální ochrana neexistuje

Každý typ útoku vyžaduje jiný přístup, jiná opatření a není možné očekávat zázraky.

References I

[1] https://en.wikipedia.org/wiki/Denial-of-service_attack

[2] https://www.incapsula.com/ddos/

[3] https://www.root.cz/clanky/ddos-utoky-jak-se-ucinne-branit/

[4] https://www.security-portal.cz/clanky/seznamte-se-—dos-ddos-útoky

[5] http://www.networkworld.com/article/2170051/tech-primers/tech-primers-four-ways-to-defend-against-ddos-attacks.html