Denial of Service

Michal Meriač

Všetci vieme čo to je, takže...

- Zamedzenie prístupu k službe
- Vyčerpaním systémových zdrojov
- Zahltením pásma...

Motivácie pre DoS

- Hacktivism
- Vydieranie
- Konkurenčný boj
- Poškodenie prevádzkovateľa
- ...

DoSaaS

- **DoS as a Service**
- Booters/Stressers
- Botnet na prenájom
- **Nitol / IMDDOS / Avzhan / ChinaZ**

Úrovne sieťových DoS

1. Volume based
2. Protocol attack
3. Application layer

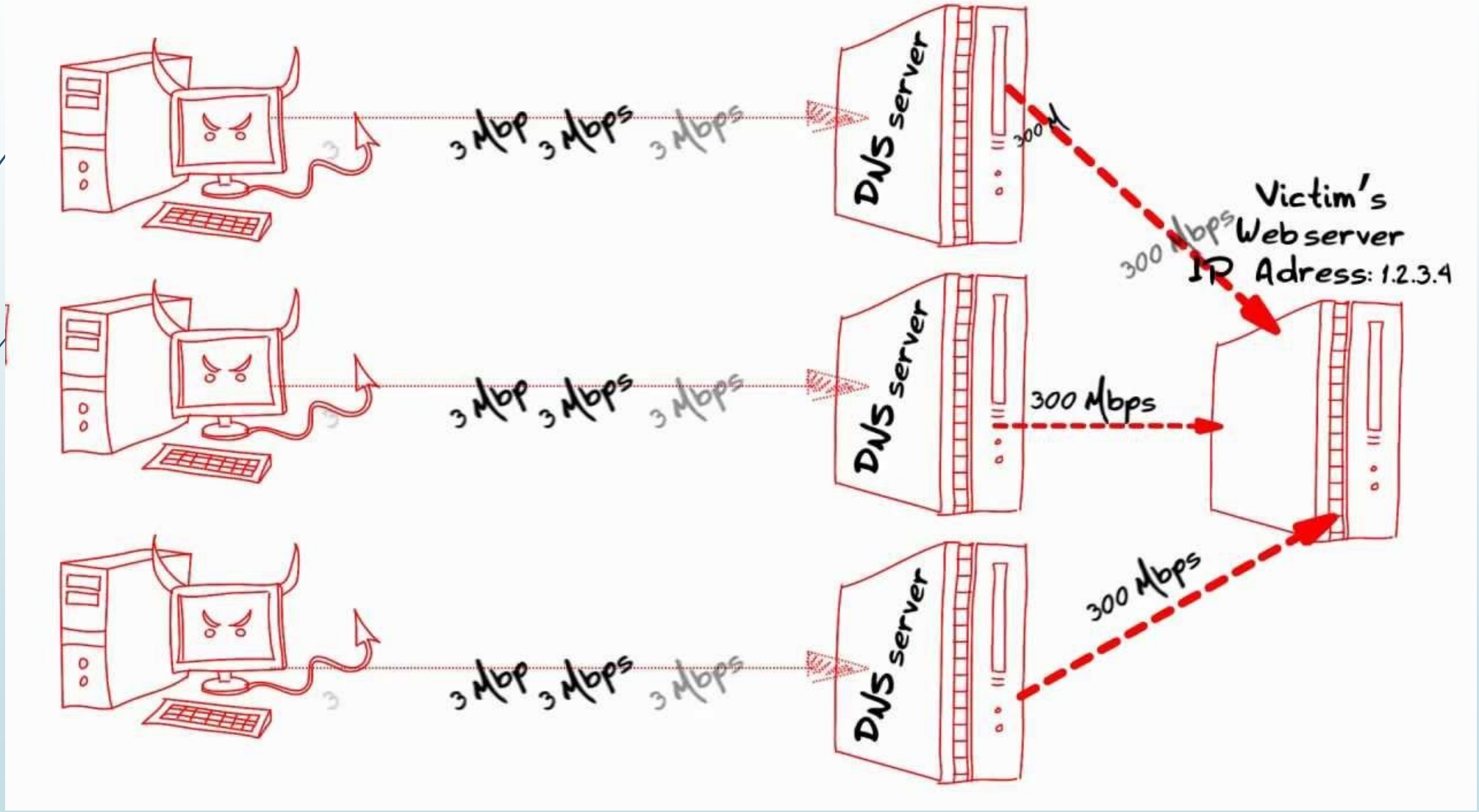
1. Volume based

- Vygenerovanie čo največšieho trafficu
- DNS
- NTP
- Amplification
- Botnety

Amplifikačné útoky

- Pomerne malý traffic od útočníka/ov vygeneruje veľký traffic od Amplifiera
- Kombinácia so **Spoofingom** zdrojovej IP adresy
- DNS
  - **~80-byte** Dotaz
  - **X-násobne** večšia Odpoveď (<50x)
  - DNSSEC
  - Open Resolvers
- **dig ANY isc.org @x.x.x.x +edns=0 +notcp +bufsize=4096**

DNS Amplification



2. Protocol based

- SYN Flood
- UDP Flood
- Smurf
- Ping of Death, Fragmentačné útoky (Historické)

3. Application layer

- Útok na konkrétnu službu (http server, SIP, ...)
- HTTP:
  - HTTP Flood
  - Slowloris
  - Slow read
  - Distribuovane napr. cez XSS
- SIP
  - Inviteflood

Nástroje pre DoS - Windows

- **LOIC** (TCP, UDP) / **HOIC**(HTTP)
- **HULK**
- **UDP Flooder**
- **Rudy**
- **OWASP Switchblade**

Nástroje pre DoS - Linux

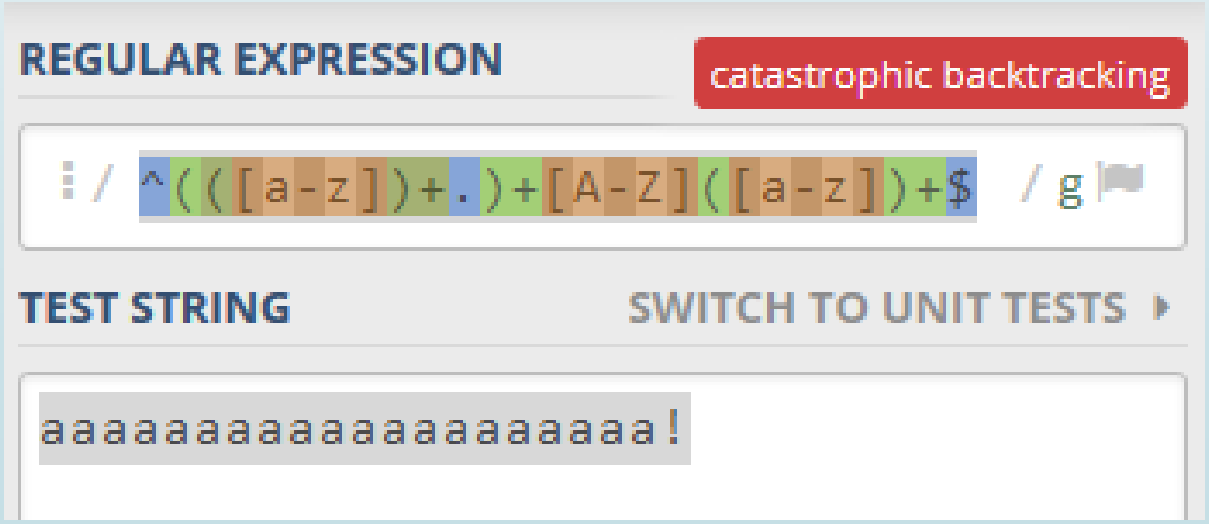
- **Hping3**
- **ToR's Hammer**
- **Slowhttptest**
- **GoldenEye**

Randomizácia

- Sťaženie filtrácie DoS
- Dotazy na rôzne pathy v URL
  - http://example.com
  - http://example.com/profile
  - http://example.com/index
- Hlavička requestu
- Obfuskácia zdrojových adries

Exploit DoS

- Crash/Halt
- Neočakávaný input, Buffer overflow, …
- Exploit-db.com
- Regex
  - ^(([a-z])+.)+[A-Z]([a-z])+$



Vďaka za pozornosť

Referencie

- blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack
- incapsula.com/ddos/ddos-attacks
- 
  Black Hat USA 2013 - Lessons from Surviving a 300Gbps Denial of Service Attack
  - youtube.com/watch?v=w04ZAXftQ_Y