Útoky DOS

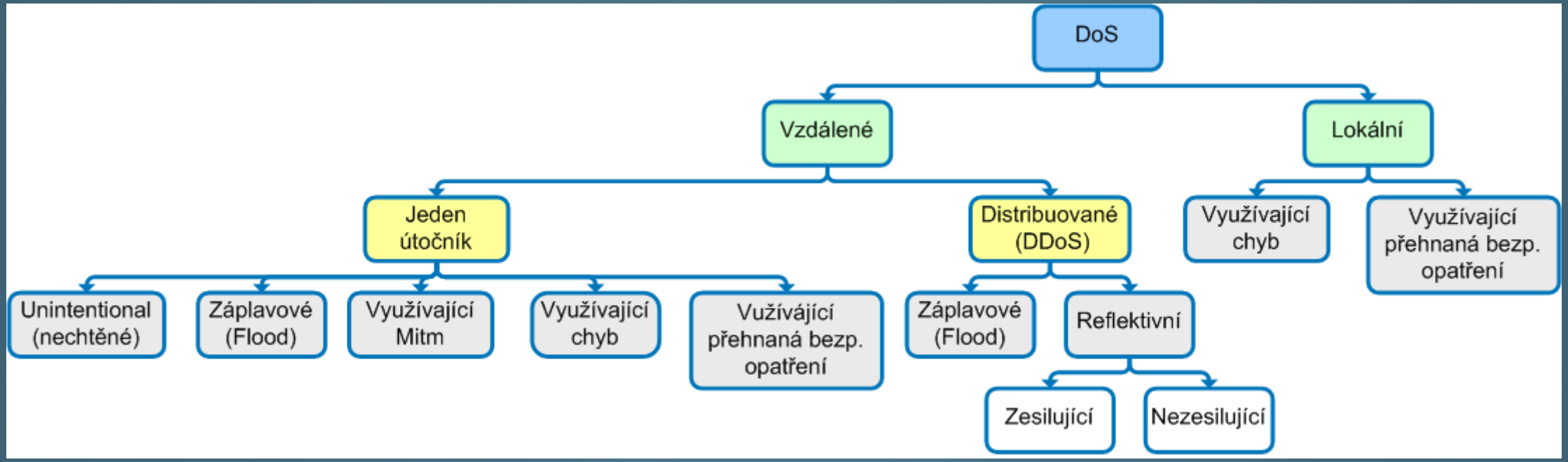
DOS – DENIAL OF SERVICE

JIŘÍ MARTINŮ, 2017

Nejznámější druhy DOS

- **Reflektivní útoky**
- **Zesilující útoky**
- **Smurf**
- **Fraggle**
- **TTL Záplava (TTL Expiration flood)**
- **SYN Záplava (SYN Flood)**
- **DNS zesilující útok (DNS Amplification Attack)**

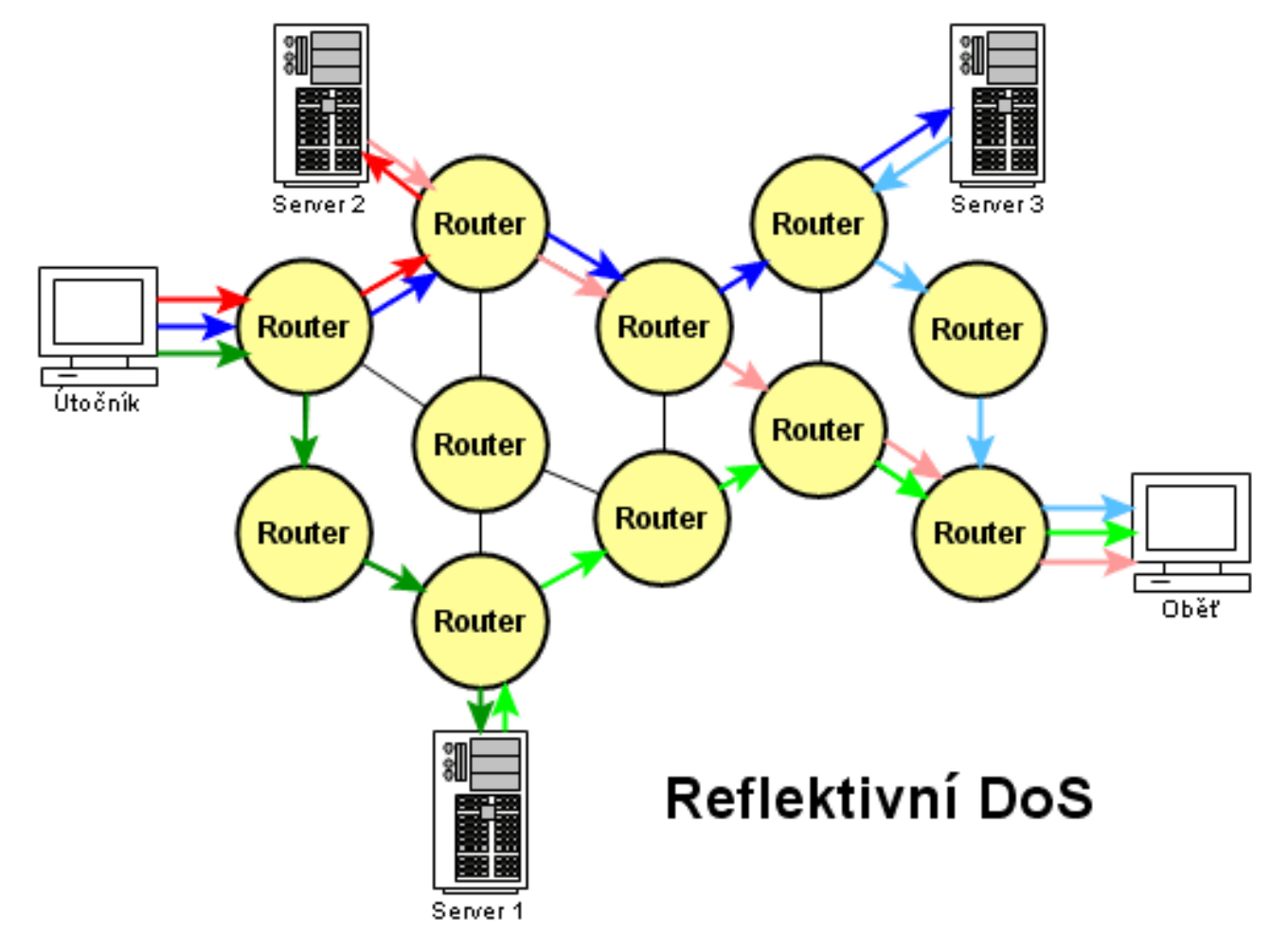
Rozdělení nejznámějších DOS útoků



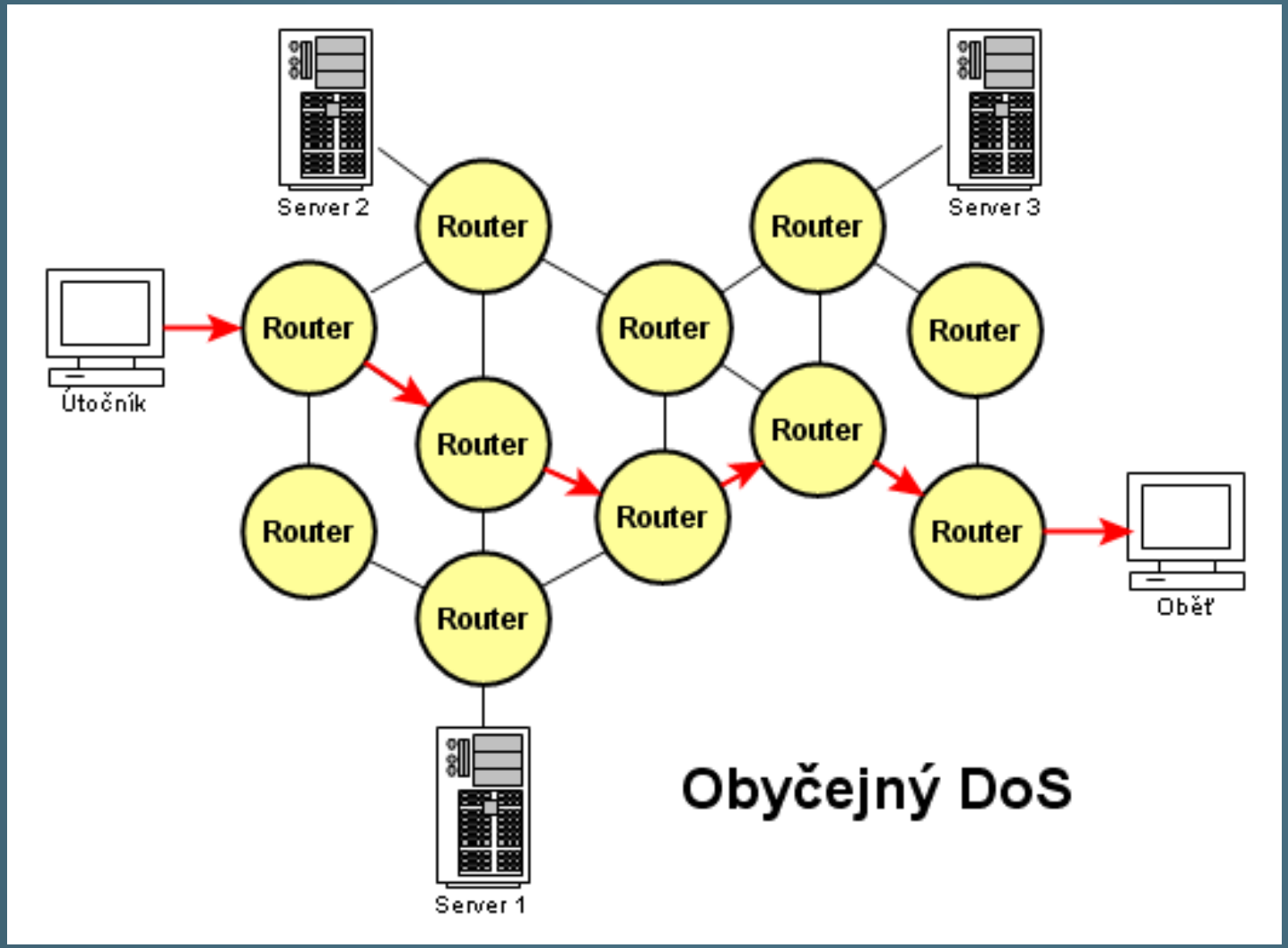
Reflektivní útoky

- **Zahlcení linky** prostřednictvím jiných zařízení (routery, počítače)
- Minimální možnost vystopování útočníka
- Při útoku se **neustále mění zdroj útoku** (odkud se útok „odráží“ – proto název reflektivní)
- Primární útočník téměř vždy **falšuje svou IP adresu**

Reflektivní útoky



Běžný („obyčejný“) DOS útok



Reflektivní útoky – jak probíhají?

- Útočník si nejprve vytvoří seznam síťových zařízení, která k útoku použije
  - Nejčastěji pomocí skriptu nebo programu
- Pomocí programu zahájí útok
  - Vezme se první IP adresa a pošle se na ni několik paketů
  - Stejně se pokračuje s druhou a následujícími IP adresami seznamu
  - U všech odeslaných paketů je změněna adresa odesílatele, tedy útočníka, na adresu příjemce, tedy oběti útoku
- Odesílané pakety musí takové, aby na ně napadané koncové zařízení odpovědělo (tzn. na daném portu musí běžet nějaká služba, odtud Denial Of Service)
- Vše se maskuje malým počtem odesílaných paketů – ty jsou pak hůře zjistitelné (např. z logu, pokud jsou tyto pakety data vůbec logovány) apod. – ztratí se v něm…) Oběť často ani hned nezjistí, že je napadena…v tom jsou DOS útoky nebezpečné…

Zesilující útoky

- Vychází z reflektivních útoků
- Útočník pošle data o určité velikosti
- K oběti dorazí data větší velikosti
- Z toho plyne, že se musí na cestě vyskytnout prostředník, který data k původnímu paketu přidá (proto jsou zesilující útoky možné pouze u reflektivních DOS útoků)
- V současné době se jedná o nejsilnější „záplavové útoky“ (viz dále)

Smurf útoky

- Nejstarší reflektivní zesilující útok
- Podobný ICMP flood. Podobný princip, jen přidává zesílení.
- **Otázka**: Který příkaz používá protokol ICMP?

Smurf útoky

- Namísto pingu přímo na útočníka je **poslán ping na IP adresu sítě** s nastavením zdrojové IP adresy na IP adresu oběti.
- Následně všechny počítače z cílové sítě odpoví paketem „ICMP Echo reply“ oběti.
- **Zesílení** tedy závisí na **počtu** počítačů v dané síti

Smurf útoky - CVIČENÍ

- Spusťte program Ethereal (případně WireShark nebo jiný program k zachytávání paketů)
- Z databáze sítí, které mohou být použity k tomuto útoku nějakou vybrat. DB sítí, např.: http://www.powertech.no/smurf
- Spusťte program ***ping*** na vybranou adresu sítě

  (ping –n 1 adresa_site)
- Tím se odešle jede požadavek na odpověď (Echo).
- V programu pro zachytávání paketů zjistěte, kolik přišlo odpovědí.
- **Otázka**: Co jste zjistili? **Co ze zjištění plyne?**

Smurf útoky - CVIČENÍ

- Spusťte program Ethereal (případně WireShark nebo jiný program k zachytávání paketů)
- Z databáze sítí, které mohou být použity k tomuto útoku nějakou vybrat. DB sítí, např.: **http://www.powertech.no/smurf**
- Spusťte program ***ping*** na vybranou adresu sítě

  (ping –n 1 adresa_site)
- Tím se odešle jede požadavek na odpověď (Echo).
- V programu pro zachytávání paketů zjistěte, kolik přišlo odpovědí.
- **Otázka**: Co jste zjistili? **Co ze zjištění plyne?**
- **Odpověď: odpověď (Echo) přišla z několika IP adres, tzn., že odpověděly všechny (ideálně) počítače v dané síti**

Smurf útoky - vlastnosti

- Zesílení tohoto záplavového útoku se pohybuje až v desetinásobcích
- V současnosti existují i silnější útoky, ale SMURF je stále využíván a je vysoce efektivní
- ***Pozn.: používání IP adres sítí je v současnosti v síti Internet filtrováno, nicméně pořád existují sítě, kde je toto umožněno…***

Fraggle útoky

- Útok od stejného autora jako Smurf
- Velice podobný útoku Smurf
- Nepoužívá se ICMP (tedy příkaz *ping*)
- Využívá se protokol UDP, služby Echo a Chargen
  - Pošle se UDP datagram s cílovou adresou nastavenou na síť určenou k odražení dat.
  - Jako port je nejvíce využíván port 7 (echo) nebo 19 (chargen)
  - Echo vrátí data zpět, Chargen vrací jiná data
  - Tento útok se dnes již **téměř** nepoužívá, uvádíme jej z důvodu doplnění informací

Fraggle útoky - vlastnosti

- Záplavový reflektivní zesilující útok
- Menší zesílení než Smurf. **Otázka**: **PROČ?**

Fraggle útoky - vlastnosti

- Záplavový reflektivní zesilující útok
- Menší zesílení než Smurf. **Otázka**: **PROČ?**
- **Odpověď**: **Ne všechny počítače v dané síti využívají tyto porty (7, 19), tzn. služby**

TTL Záplava (TTL Expiration flood)

- Reflektivní útok
- Nevyžaduje vytváření seznamu síťových zařízení (využívaných pro účely útoku) předem
- Využívá hodnotu TTL – Time To Live
- **Otázka**: **Co je TTL?**

TTL Záplava (TTL Expiration flood)

- Reflektivní útok
- Nevyžaduje vytváření seznamu síťových zařízení (využívaných pro účely útoku) předem
- Využívá hodnotu TTL – Time To Live
- **Otázka**: **Co je TTL?**
- **Odpověď**:
  - **Hodnota, nejčastěji v rozmezí 64 – 255.**
  - **Hodnotu určuje operační systém, je možné ji změnit.**
  - **Všechna odchozí data mají nastavenu hodnotu TTL.**
  - **Každé zařízení na cestě k cíli (které pracuje s protokolem IP, tedy např. routery) dekrementují hodnotu TTL o 1.**

TTL Záplava (TTL Expiration flood)

- Při dosažení cíle mají data hodnotu TTL průměrně o 10 nižší, než výchozí hodnotu. Otázka: co nám tato skutečnost říká?

TTL Záplava (TTL Expiration flood)

- Při dosažení cíle mají (za normálních okolností) data hodnotu TTL **průměrně o 10 nižší**, než výchozí hodnotu. **Otázka: co nám tato skutečnost říká?**
  - **Odpověď: počet síťových uzlů (prvků pracujících s protokolem IP), kterými paket prošel na cestě k cíli.**

TTL Záplava (TTL Expiration flood)

- Při dosažení cíle mají (za normálních okolností) data hodnotu TTL **průměrně o 10 nižší**, než výchozí hodnotu. **Otázka: co nám tato skutečnost říká?**
  - **Odpověď: počet síťových uzlů (prvků pracujících s protokolem IP), kterými paket prošel na cestě k cíli.**
- V případě ztráty paketu (paket někde bloudí) se hodnota snižuje tak dlouho, dokud nedosáhne hodnoty 0. V tomto případě zařízení, které snížilo hodnotu TTL z 1 na 0 již paket neposílá dále, ale zdroji paketu (odesílateli) odešle zprávu, že vypršela doba životnosti paketu (tj. TTL). **Otázka: k čemu je to dobré?**

TTL Záplava (TTL Expiration flood)

- Při dosažení cíle mají (za normálních okolností) data hodnotu TTL **průměrně o 10 nižší**, než výchozí hodnotu. **Otázka: co nám tato skutečnost říká?**
  - **Odpověď: počet síťových uzlů (prvků pracujících s protokolem IP), kterými paket prošel na cestě k cíli.**
- V případě ztráty paketu (paket někde bloudí) se hodnota snižuje tak dlouho, dokud nedosáhne hodnoty 0. V tomto případě zařízení, které snížilo hodnotu TTL z 1 na 0 již paket neposílá dále, ale zdroji paketu (odesílateli) odešle zprávu, že vypršela doba životnosti paketu (tj. TTL). **Otázka: k čemu je to dobré?**
  - **Odpověď: tímto se zamezuje nekonečnému bloudění ztracených dat sítí a jejímu zahlcení těmito ztracenými pakety.**

TTL Záplava (TTL Expiration flood)

- Dalším využitím je trasování (zjišťování trasy k cíli), např. programem *traceroute* (Unix, Linux…) nebo *tracert* (Windows). Tyto programy vysílají paket s počáteční hodnotou TTL = 1 a vždy po návratu zprávy o nedoručení zvýší TTL o 1. Konečný počet síťových uzlů na trase k cíli (tzn., že se již nevrátí zpráva o nedoručení paketu) je aktuální hodnota TTL. Programy mají nastavenu max. defaultní hodnotu TTL (*tracert* např. 30)
- **V případě útoku** je jako IP adresa odesílatele nastavena adresa cíle (oběti útoku). TTL je v tomto případě nastaveno na nízkou hodnotu. Fiktivnímu odesílateli, tedy reálně cíli útoku, se pak od síťových uzlů vrací odpovědi o nedoručení paketu (po vypršení TTL).
  - Zesílení je v tomto případě nízké, průměrně 1.7

TTL Záplava (TTL Expiration flood) - CVIČENÍ

- Spusťte příkaz *ping –l 0 –i 255 LIBOBOLNÁ_IP_ADRESA*
- Parametr *-i* slouží k nastavení TTL a parametr *–l* k nastavení délky datového paketu (*ICMP Request*).
- V případě, že se vrátí odpověď, že je cíl nedostupný, snižte parametr *-i* a sledujte odpovědi (*ICMP Request*) programem pro zachytávání paketů (Ethereal, apod.). Zkuste hodnoty parametrů také zvýšit a sledujte rozdíly…
- Všimněte si, že ačkoli odesíláte např. 32 bytů, vrací se 70 bytů. Proto je zesílení průměrně 1.7

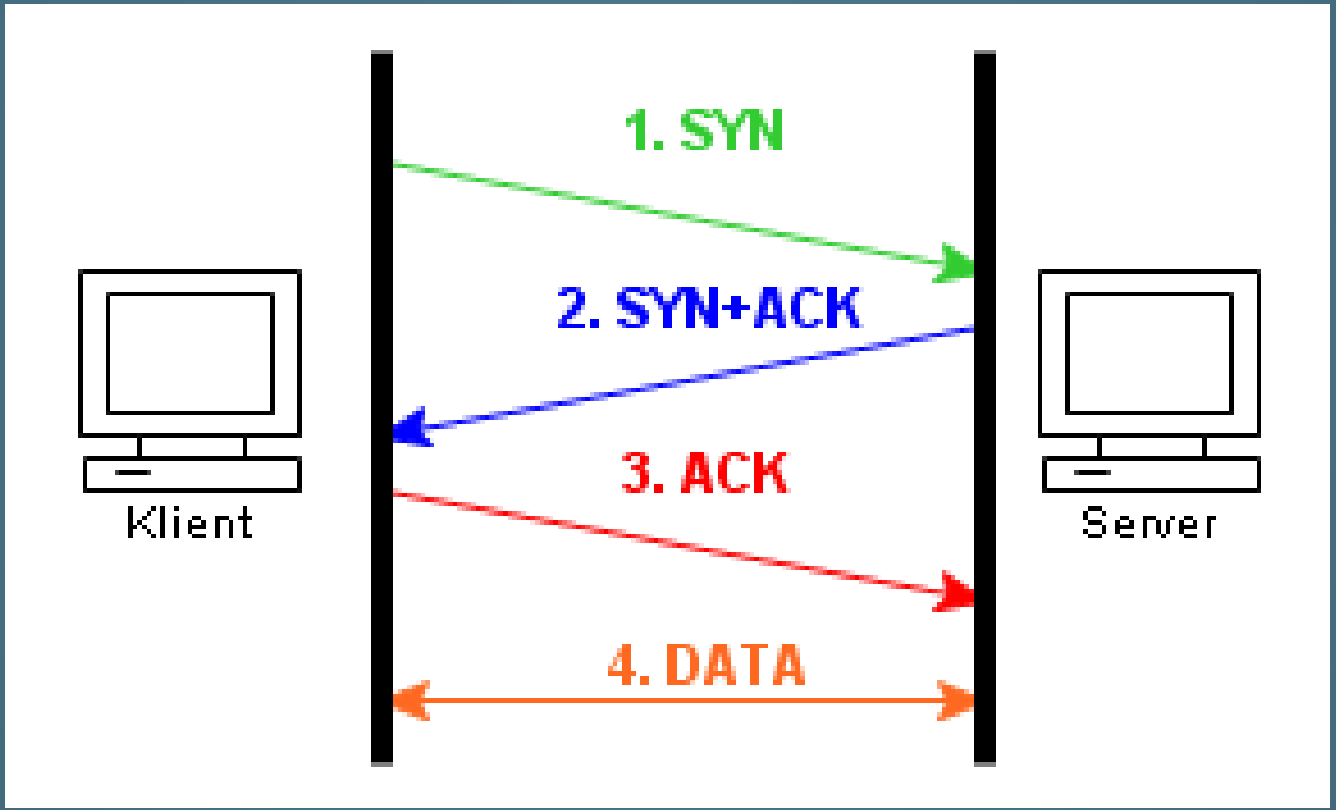
TTL Záplava (TTL Expiration flood) - vlastnosti

- Záplavový reflektivní útok
- Snadná implementace
- Bude použitelný ještě dlouhou dobu
- Zesílení průměrně 1.7

SYN Záplava (SYN Flood)

- Záplavový reflektivní útok
- Zdrojová adresa se nastaví na adresu oběti útoku
- Útočník (skript, program) vytvoří seznam zařízení využívaných k útoku
- Co je SYN?
  - Příznak v TCP paketu umožňující synchronizaci sekvenčních čísel
  - Nastavuje se při žádosti klienta o spojení
  - Server reaguje (v případě vyžádaného spojení) odesláním příznaků SYN+ACK, v případě nevyžádaného buď nereaguje anebo odešle nastavený příznak RST
  - Útok spočívá v tom, že si server alokoval prostředky pro komunikaci s klientem… Je-li takovýchto požadavků mnoho, vyčerpají se volné prostředky serveru (oběti) a server je pro další klienty nedostupný

SYN Záplava (SYN Flood)



SYN Záplava (SYN Flood)

- Záplavový reflektivní útok
- Zdrojová adresa se nastaví na adresu oběti útoku
- Útočník (skript, program) vytvoří seznam zařízení využívaných k útoku
- Útočící skript pak posílá TCP pakety s nastaveným příznakem SYN a adresou oběti jako zdrojovou adresou
- Zařízení se domnívají, že s nimi oběť míní komunikovat/navázat spojení a pošlou jí zpět pakety s nastavenými příznaky SYN a ACK
- Vzhledem k tomu, že oběť nic takového nečeká a z důvodu nefiltrování těchto zpráv neodešle paket s příznakem RST (neodešle vlastně žádný paket), útočící zařízení se domnívají, že se paket ztratil a odešlou jej znovu.
- To se děje většinou 4x, proto má tento útok 4násobné zesílení a tudíž je velmi nebezpečný
- Výhodou pro útočníka je rovněž snadná dostupnost zařízení (PC, serverů…), které mohou být k útoku využity

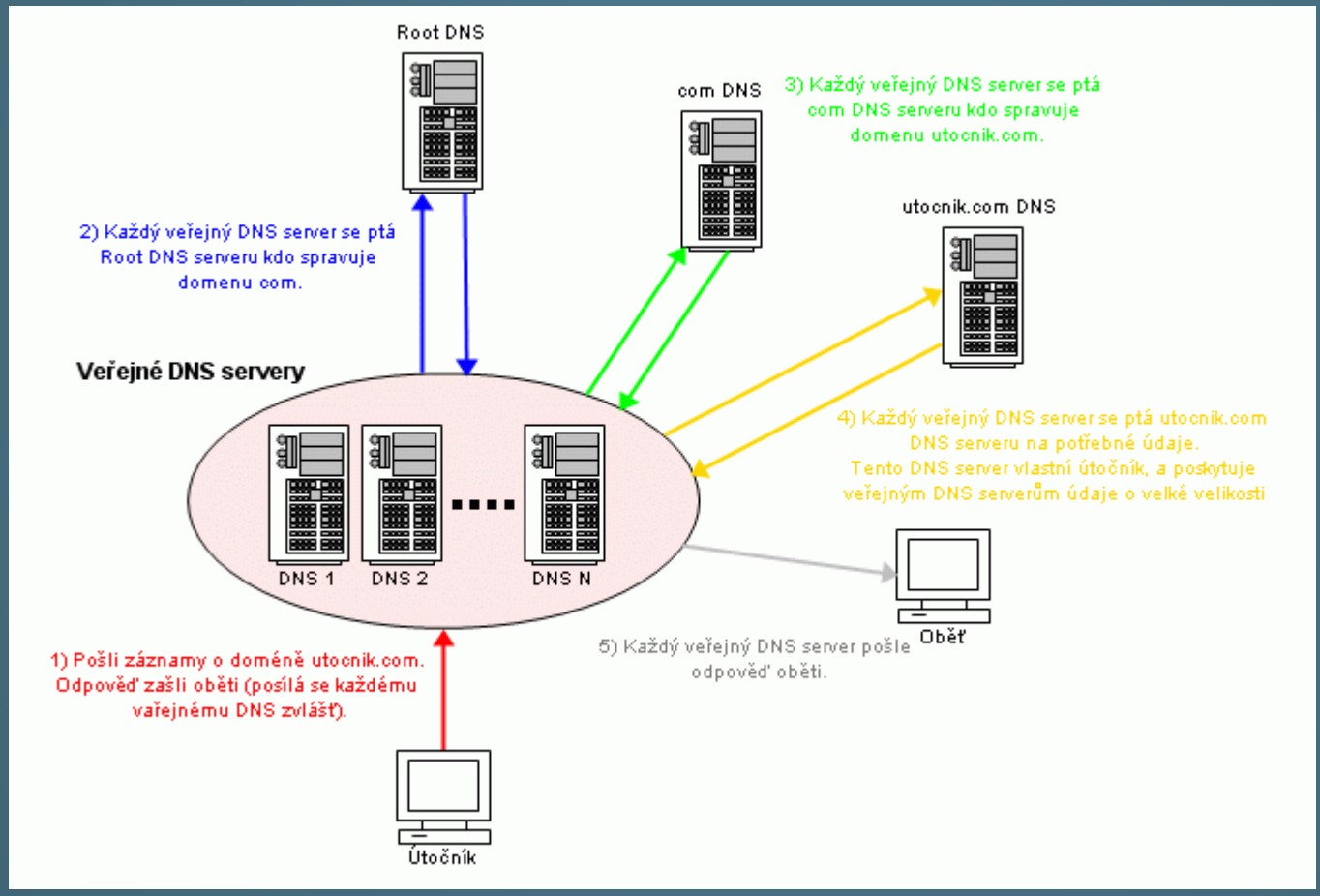
SYN Záplava (SYN Flood) - vlastnosti

- Záplavový reflektivní útok
- Možnost využití téměř všechny počítače jako zdroje útoku
- Čtyřnásobné zesílení
- Velmi nebezpečný
- Bude fungovat ještě dlouhou dobu…

DNS zesilující útok (DNS Amplification Attack)

- Jeden z novějších typů DOS útoků
- Na veřejný Relay DNS server (DNS server umožňující dohledání požadovaného záznamu) se odešle dotaz se zdrojovou adresou nastavenou na adresu oběti
- UDP odpověď umožňuje většinou až 512-bytovou odpověď. Pokud je položen dotaz na doménu, obsahující dlouhé textové popisy, pak lze dosáhnout maximální velikosti odpovědi, kterou DNS server odešle. Průměrně se velikosti odpovědí pohybují okolo 80 bytů. Při „šikovném“ dotazu tak lze dosáhnout sedminásobného zesílení u běžného DNS serveru.
- Běžně útočník využívá předpřipravenou doménu, která posílá DNS serveru velké objemy dat. Tyto domény jsou většinou domény, které hackeři modifikovali k zasílání takovýchto velkých objemů dat…
- U rozšířeného DNS (EDNS) je možná odpověď až 4kB! To pak znamená dosažení až 73násobného zesílení!!!
- DNS servery pak po obdržení požadavku a dotazu na doménu, která vrátí velký objem dat, odesílají oběti odpovědi ve velikosti, která 73krát přesahuje velikost požadavku. Je-li takovýchto DNS serverů více, dojde k zahlcení linky oběti.

DNS zesilující útok (DNS Amplification Attack)



DNS zesilující útok (DNS Amplification Attack) - CVIČENÍ

- Na Linuxu spustit příkaz *dig DOMENA any*
- V OS Windows spustit příkaz *nslookup* a pak zadat *set type=any* a poté název libovolné domény
- V Etherealu, případně příkazové řádce sledovat velikost vracených dat

DNS zesilující útok (DNS Amplification Attack) - vlastnosti

- Záplavový reflektivní zesilující útok s opravdu velkým zesílením
- Vysoce nebezpečný
- Velmi složitá obrana proti tomuto druhu útoku

Děkuji za pozornost