PV210 Bezpečnostní analýza síťového provozu

Útoky podle vrstev sítě II

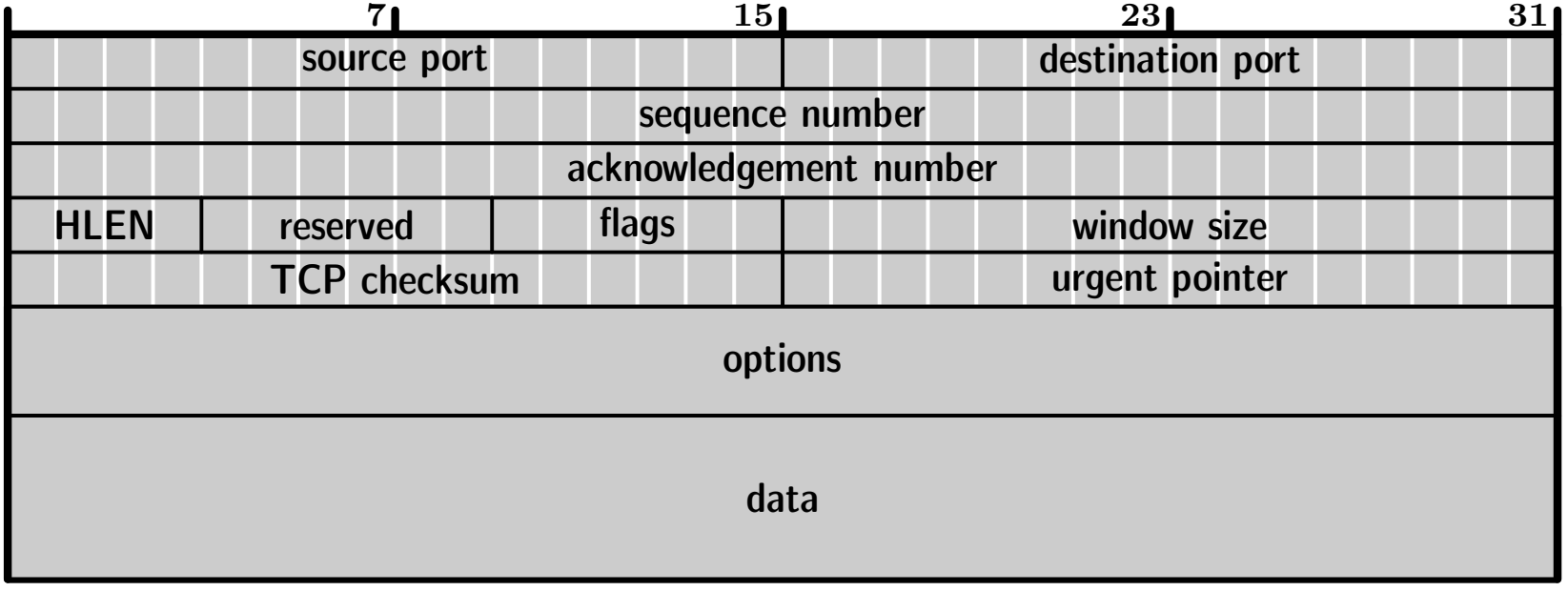
RNDr. Jan Vykopal, Ph.D.

1. 10. 2014

Rozvrh I

- 1. 10. Útoky podle vrstev sítě II. Vykopal
- 3. 10. Cvičení sk. PV210/02 – Wireshark a hloubková analýza paketů. Vykopal
- 8. 10. Základní prvky zabezpečení sítě. Zadání 1. domácího úkolu. Vykopal
- 10. 10. Cvičení sk. PV210/01 – První úkol – hledání útoku v PCAPu (Wireshark). Vykopal
- 15. 10. Úvod do bezpečnostního monitorování sítě. Jirsík
- 17. 10. Cvičení sk. PV210/02 – První úkol – hledání útoku v PCAPu (Wireshark). Vykopal
- 22. 10. Jednoduché metody zpracovávající síťové toky Odevzdání 1. úkolu. Vykopal

Protokol TCP: opakování I



Příznaky (flags): SYN ACK RST FIN PSH URG

Protokol TCP: opakování II

Navázání spojení

- Server „poslouchá” na určitém portu – čeká na zahájení spojení.
- Klient posílá TCP segment s příznakem SYN, nastavuje sekvenční číslo, velikost okna a obvykle také max. velikost segmentu.
- Server odpovídá segmentem SYN+ACK, potvrzuje (SN klienta + 1) a nastavuje vlastní parametry (SN, WS a volitelně MSS).
- Klient odpovídá segmentem ACK, potvrzuje (SN serveru + 1).

- Ukázka provozu ve Wiresharku.

Protokol TCP: opakování III

Ukončení spojení

- Ukončuje se zvlášť každý směr spojení, vyvolává buď klient nebo server.
- V praxi se ale většinou ukončí obě poloviny spojení bezprostředně za sebou.
- Ukončující strana: segment s příznakem FIN
- Druhá strana: segment s příznakem ACK

Záplava TCP SYN

- Útok typu DoS, poprvé zveřejněn v roce 1996.
- Útočník vyšle velké množství paketů TCP SYN.
- Server si alokuje zdroje pro každé z nově otevíraných spojení.
- Útočník ale nedokončí navázání spojení.
- Server čeká na dokončení a je postupně zahlcován novými požadavky na spojení.
- Pokud útočník podvrhne svou adresu, je nevystopovatelný; server odpovídá „nicnetušícímu” stroji $\Rightarrow$ odražený útok.

Záplava TCP SYN – obrana

- Lze realizovat např. nástrojem *LetDown* ze sady *Complemento*, viz `http://complemento.sourceforge.net/howto/#LetDown`.
- Obrana: **omezení počtu nových spojení** z určitého zdroje v daném časovém okně nebo použití **TCP SYN cookies**, dále viz RFC 4987.
  - server po obdržení žádosti o navázání spojení (SYN) pošle klientovi odpověď a tuto žádost ihned vyhodí z fronty (= nedrží stav),
  - do odpovědi nevložil náhodné číslo sekvence, ale vygenerované podle daných pravidel,
  - obdrží-li server od klienta potvrzení odpovědi (SYN+ACK), je podle čísla sekvence schopen zpětně odvodit, zda se jedná o korektní paket či ne.

Skenování portů

- Cílem je zjistit, jaké TCP či UDP porty jsou na daném souboru počítačů otevřené.[1]
- Samo o sobě není škodlivé, má i legitimní použití – jedna z funkcí nástroje *nmap*.
- Zneužíváno k průzkumu běžících služeb a následnému útoku.
- Společný princip: útočník/auditor postupně posílá speciálně vytvořené pakety na posloupnost portů.
- Existuje několik typů skenování: SYN, connect, NULL, FIN, Xmas, ACK, UDP, ...
- V principu neexistuje obrana, ale lze poměrně jednoduše detekovat.

[1] A co IPv6?

TCP SYN sken

- Útočník předstírá navázání spojení – vyšle TCP SYN. Je-li odpověď:
- SYN+ACK: port je otevřený, naslouchá,
- RST+ACK: port není otevřený,
- žádná: může to ukazovat na firewall.
- Následně obvykle přeruší ustanovení TCP spojení (three-way handshake).
- Další zdroj: **man nmap**.

Ukázka TCP SYN skenování portů IS MU – nmap

```
root@medea:~# nmap -sS 147.251.49.10

Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-10-22 18:30 CEST
Interesting ports on is.muni.cz (147.251.49.10):
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 9.31 seconds
```

UDP sken

- UDP je nespojový (connectionless) protokol.
- Není možné využít techniky skenování TCP portů.
- Skenování je pomalejší a obtížnější než v případě TCP.

- Nmap skenuje UDP porty zasláním prázdné UDP hlavičky.
- V případě zavřeného portu zašle stroj *ICMP port unreachable*.
- Pokud zašle jiné chyby pomocí ICMP, je nejspíš filtrován.
- Pokud stroj nijak neodpoví, je port otevřen nebo filtrován.

- Ukázka skenování UDP portů stroje ntp.muni.cz ve Wiresharku.

Únos TCP spojení

- TCP connection hijacking využívalo nedostatečné náhodnosti počátečních sekvenčních čísel.
- Opraveno v implementacích stacku v dnešních operačních systémech.
- V kombinaci s odposlechem (např. pomocí ARP spoofingu) lze realizovat i dnes v pozici *man-in-the-middle*.
- Útočník může ukončit spojení s klientem/serverem (ten má pocit, že jde o výpadek spojení) a dál komunikovat se serverem/klientem.
- V Linuxu lze použít nástroj *Hunt*.
- Pozor na SYN cookies, paradoxně mohou usnadnit útok.
- Únos TCP spojení pomocí SYN cookies

  `http://www.jakoblell.com/blog/2013/08/13/quick-blind-tcp-connection-spoofing-with-syn-cookies/`

Povrhnutí odpovědi DHCP serveru – nový klient

- Poprvé klient žádá o informace pro připojení do sítě pomocí zprávy *DHCP Discover*, kterou pošle všem v dané síti.
- **Kdokoliv** může odpovědět zprávou *DHCP Offer*, kde nabízí požadované údaje.
- Platí „kdo dřív příjde, ten dřív mele”. Útočník se tedy snaží odpovědět rychleji než legitimní server.
- Přidělená (zapůjčená) adresa a další údaje mají omezenou platnost (tzv. lease time).

Povrhnutí odpovědi DHCP serveru – stávající klient

- Pokud klient žádá znovu o adresu legitimní server, posílá přímo jemu *DHCP Request* se svou poslední adresou.
- Útok lze realizovat vyčerpáním přidělovaných adres.
- Server pak přestane odpovídat na další žádosti a po vypršení platnosti přidělené adresy začnou klienti posílat opět *DHCP Discover*.
- Jde o vnitřní útoky. Lze je realizovat pomocí linuxového nástroje *ettercap* nebo *yersinia*.
- Obrana: DHCP snooping.

Útoky na DNS

- Protokol DNS patří k základním protokolům dnešního internetu.
- Je však zranitelný (ať už v principu nebo jeho implementace).
- Primárně funguje nad protokolem UDP, v případě většího objemu komunikace nad TCP.
- Bezstavový UDP dává větší šance útočníkům, např. není nutno unášet spojení jako v případě TCP.
- Obrana: nasazení DNSSEC(?) – `http://www.dnssec.net/`
- Další zdroj: RFC 3833 Threat Analysis of the Domain Name System.

- Ukázka DNS provozu ve Wiresharku.

Podvržení odpovědi DNS serveru

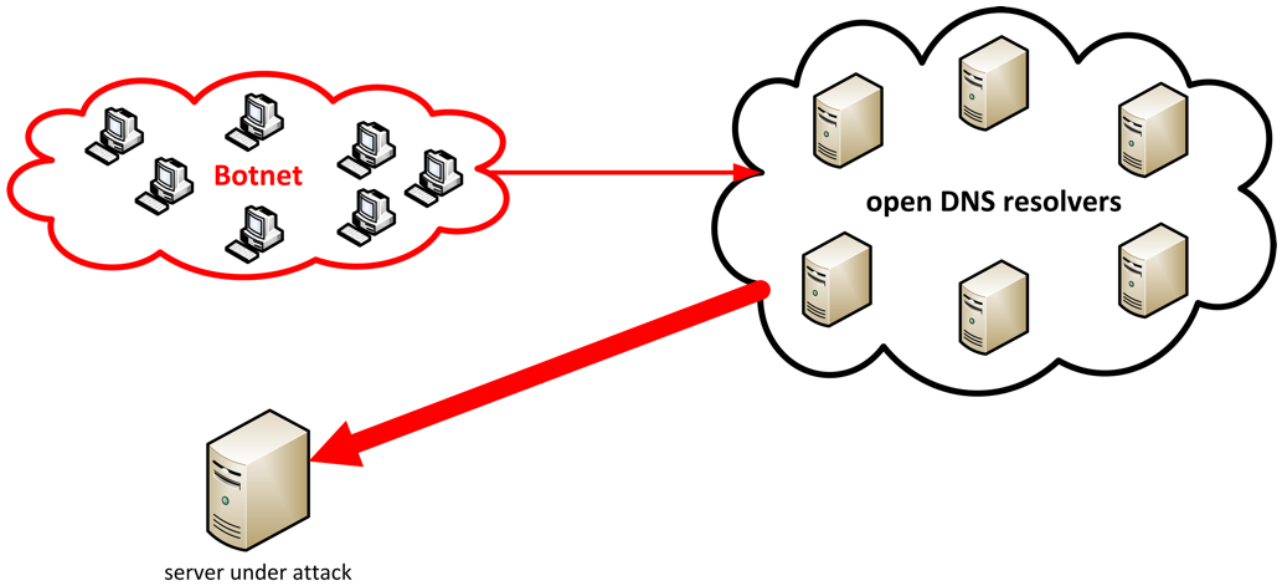
- DNS dotaz je identifikován ID dotazu, IP adresami a porty.
- Podobně jako u DHCP, klient akceptuje první korektní příchozí odpověď.
- Útočník se typicky snaží podvrhout odpověď a vydávat se za DNS server.
- Lze provést na lokální i globální úrovni.
- Často nutně spojeno s dalšími útoky (např. ARP spoofing pro odposlech požadavků na server či DoS na server).
- Odposlech dotazů není vždy nutný, někdy stačí hádat (a využít narozeninový paradox: 750 dotazů ~ 98,65 %).
- Podvržení útočníkova DNS serveru lze následně použít pro phishing.

Podvržení odpovědi DNS serveru – odkazy

- Podrobně na `http://web.archive.org/web/20101109131447/http://www.securesphere.net/download/papers/dnsspoof.htm`.
- Detekce využití (ne)náhodných portů: `https://www.dns-oarc.net/oarc/services/dnsentropy`

DoS útok pomocí DNS – zesílení požadavků

- Zneužití tzv. DNS open resolverů, serverů, které odpovídají na požadavky přicházející z vnějšku sítě.
- Útočník podvrhne zdrojovou IP adresu požadavku a open resolver pošle odpověď oběti útoku.
- Viz `https://www.cert.be/docs/dns-amplification-attacks-and-open-dns-resolvers`



Útoky na webové aplikace I

- **SQL injection** – vložení SQL dotazu nebo jeho části pomocí uživatelského vstupu.
- Např. `SELECT * FROM users WHERE id = '0' OR 'x'='x';`
- Viz `https://www.owasp.org/index.php/SQL_Injection` – Example 3.

- **Cross site scripting (XSS)** – vložení škodlivého kódu do důvěryhodného webového obsahu.
- Také zneužívá neošetřené vstupy, umožňuje spustit kód.
- Viz `https://www.owasp.org/index.php/XSS` – Example 1, Cookie Grabber.

- **Cross site request forgery (CSRF)** – provedení požadavku bez vědomí "přihlášeného"uživatele.
- Např. `<img src="http://bank.com/transfer.do?acct=MARIA&amount=100000" width="1" height="1" border="0">`

- Viz `https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29`

Útoky na webové aplikace II

- Obrana vývojářů: ošetření vstupů, implementace bezpečnostních mechanizmů – např. pseudonáhodné ID požadavku.
- Ochrana uživatelů: paranoia – speciální prohlížeč pro bankovní operace, blokování externího obsahu atp.
- Nástroje pro audit: např.
  - *w3af* – `http://w3af.sourceforge.net/`,
  - *Nikto* – `http://cirt.net/nikto2`,
  - *RATS* – `http://code.google.com/p/rough-auditing-tool-for-security/`.
- Příručka pro penetrační testery: `https://www.owasp.org/images/b/b9/Testing_guide_V4_portrait.pdf`

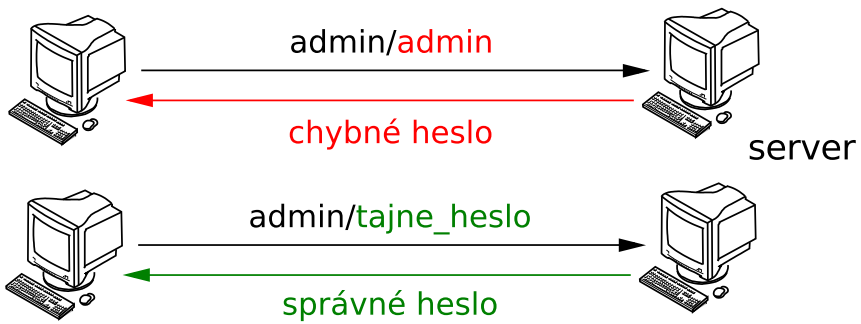
Aktuálně: Shell Shock – neošetřený vstup v BASH

- Umožňuje vzdálené spuštění kódu pomocí proměnných prostředí.
- Zasahuje linuxové systémy a MacOS (ne Windows).
- Více než 20 let stará chyba, objevena 24. 9. 2014.
- Vzápětí se objevily pokusy o její zneužití i aktualizace opravující tuto chybu.
- Další informace: CVE[2]-2014–6271.
- `$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"`

[2] Common Vulnerabilities and Exposures

Útoky hroubou silou a slovníkové útoky

- Útočník zkouší velké[3] množství dvojic (*jmeno*, *heslo*) s cílem prolomit autentizaci vybrané služby.
- Hrubá síla: všechny možné řetězce, slovník: slova, nejčastěji používané (= zapamatovatelné) řetězce.

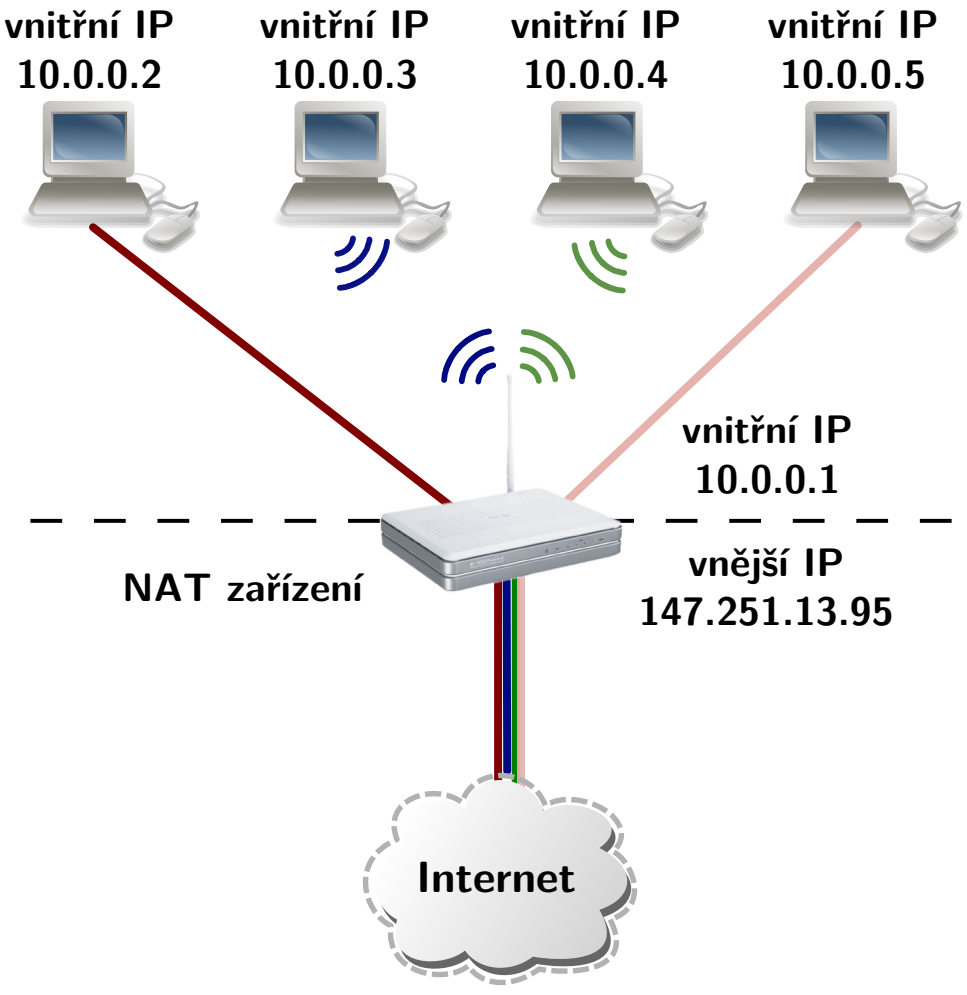


[3] Někdy uspěje i s poměrně malou sadou kombinací (např. botnet Chuck Norris, červ Morto)

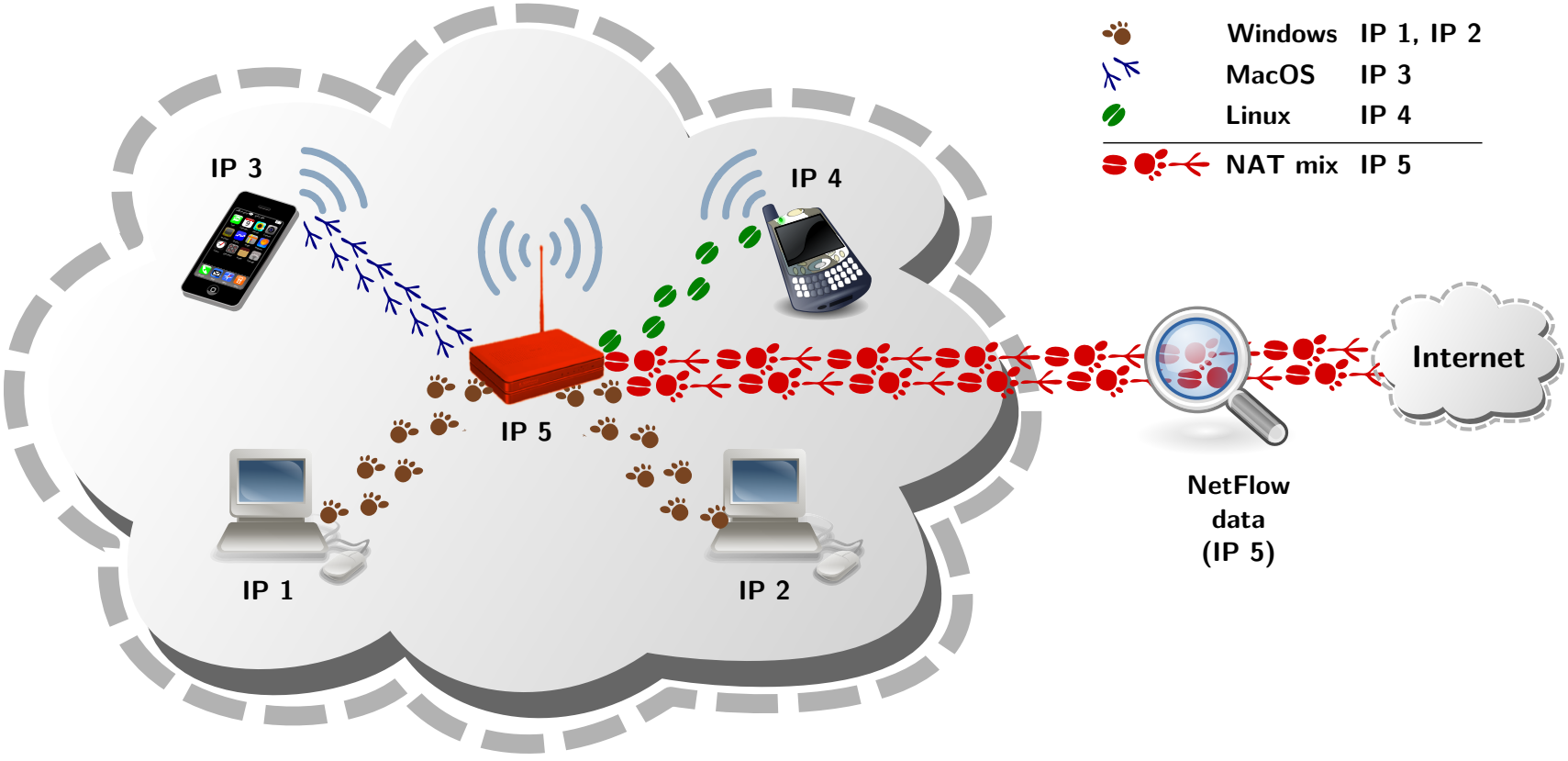
Útoky hroubou silou a slovníkové útoky II

- Napadané služby: SSH, RDP, Telnet, webové aplikace, LDAP
- Obrana: nepoužívat hesla (ale třeba certifikáty), sledovat neúspěšné pokusy na úrovni služby v logu (po několika pokusech zablokovat účet $\Rightarrow$ DoS, nasadit CAPTCHA) nebo sítě (detekční vzor tohoto typu útoků)

Zneužití Network Address Translation (NAT) I



Zneužití Network Address Translation (NAT) II



Další útoky

- Útok na SSL a TLS: *man-in-the-middle* „proxy” a falešný certifikát, Heartbleed (CVE-2014-0160).
- Útoky na slabiny protokolů elektronické pošty.
- Google hacking, SHODAN (`http://www.shodanhq.com/`)
- Zneužití flashových aplikací (keylogger), PDF souborů (zajímavý analyzátor PDF: `http://esec-lab.sogeti.com/dotclear/index.php?pages/Origami`)
- . . . a **mnohé** další.

Shrnutí

- Uvedené útoky jsou jen subjektivním výběrem z nejznámějších, nejčastějších a/nebo nejnebezpečnějších.
- Většinou jde o aktivní útoky = obecně je lze detekovat.
- Existuje mnoho volně dostupných nástrojů realizující tyto útoky.
- Dnešní trend: odražené a zesilující útoky stavějící na podvržení zdrojové adresy.

Další literatura I

- SANS: Critical Security Controls

  `http://www.sans.org/critical-security-controls/`
- 10 největších bezpečnostních chyb podle OWASP

  `https://www.owasp.org/index.php/Top_10_2013`
- SANS: každoroční seriál Cyber Security Awareness Month

  `http://isc.sans.edu/diary.html?storyid=7504`
- Praktické zkušenosti s (D)DoS útoky

  `http://www.nic.cz/files/nic/doc/Tomas_Hala.pdf`

Další literatura II

- Videa k aplikačním útokům (HTTP)

  `http://security.radware.com/experts-insider/Learn-from-Experts/`
- 11 Offensive Security Tools for SysAdmins

  `http://hackertarget.com/11-offensive-security-tools/`
- S. M. Bellovin: *A Look Back at Security Problems in the TCP/IP Protocol Suite*.

  `https://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf`
- Zneužití tiskáren: `http://www.youtube.com/watch?feature=player_embedded&v=w-otgRCx6rA#!`