1. Přednáška: Úvod do síťové bezpečnosti

Bezpečnost ICT 2

Zdeněk Martinásek

Vysoké učení technické v Brně
martinasek@feec.vutbr.cz

2022

Informační bezpečnost

1. Úvodní informace
   - Hodnocení, požadavky
   - Přednášky
   - Laboratorní cvičení (teorie)
   - Studijní podklady
2. Síťová bezpečnost
   - Základní pojmy
   - Síťové útoky

Úvodní informace

- Garant: doc. Ing. Zdeněk Martinásek, Ph.D.
- **Problémy k TIC2 řeší: Zdeněk Martinásek**.
- martinasek@.vut.cz.
- Přednáška: úterý 11:00 - 12:50 T12 SF 2.162 (nepovinné).
  - **doc. Ing. Zdeněk Martinásek, Ph.D.**
  - **doc. Ing. Lukáš Malina, Ph.D.**
- Cvičení: úterý/středa 13:00, 16:00 SC 5.37 (povinné).
- **Ing. Karel Kuchař, Ing. Eva Holasová**.
- Aktuální informace https://moodle.vut.cz/course/view.php?id=242388

Hodnocení, požadavky

- Definuje každý rok vyhláška garanta v e-learningu.
- Celkem lze získat maximálně 100 bodů. Pro úspěšné absolvování předmětu je nutné získat zápočet z laboratorního cvičení a minimálně 50 bodů celkem.
  - Maximálně **15 bodů** za správné plnění úkolů v laboratorním cvičení.
  - Maximálně **15 bodů** za projekt.
  - Maximálně **70 bodů** ze závěrečné zkoušky.
- Zápočet je nutný k absolvování zkoušky a je udělen na základě výsledků laboratorních cvičení.
- **min. 15 bodů** a **max. 2 absence** (prezenční forma výuky).

Přednášky I (teorie)

1. Úvod do síťové bezpečnosti (Z)
2. Bezpečná konfigurace bezdrátových sítí (Z)
3. Penetrační testování webových aplikací (**Roman, hlasování!**)
4. Penetrační testování síťové infrastruktury(Z)
5. Systémy IDS a IPS (Z)
6. Bezpečná konfigurace přepínačů a směrovačů (L)
7. Firewally a aplikační filtry (L)

Přednášky II (teorie)

8. DoS útoky a testování výkonosti síťové infrastruktury (L)
9. OWASP Top 10, Penterep (Z)
10. Příprava penetračního testera SE (**Zvaná p. Hejda**)
11. Bezpečnostní audity, řízení rizik (**1x NUKIB**)
12. Protokoly pro zvýšení bezpečnosti sítí (VPN, IPsec, TOR, atd.) (L)

Laboratorní cvičení (předběžná osnova)

1. Seznámení s laboratoří, CTF.
2. Zabezpečení bezdrátových sítí (WLAN).
3. Penetrační testování - webové aplikace.
4. Penetrační testování - síťová infrastruktura.
5. Systémy IDS/IPS (problematika logování).
6. Bezpečnost a konfigurace přepínačů a směrovačů (CISCO) - zadání projektů.

Laboratorní cvičení (předběžná osnova)

7. Firewally a aplikační filtry
8. Zátěžové testovaní a DDoS útoky.
9. Pentest OWASP, Penterep.
10. CTF Dovolená snů.
11. Kontrola projektů.

Zdroje - literatura

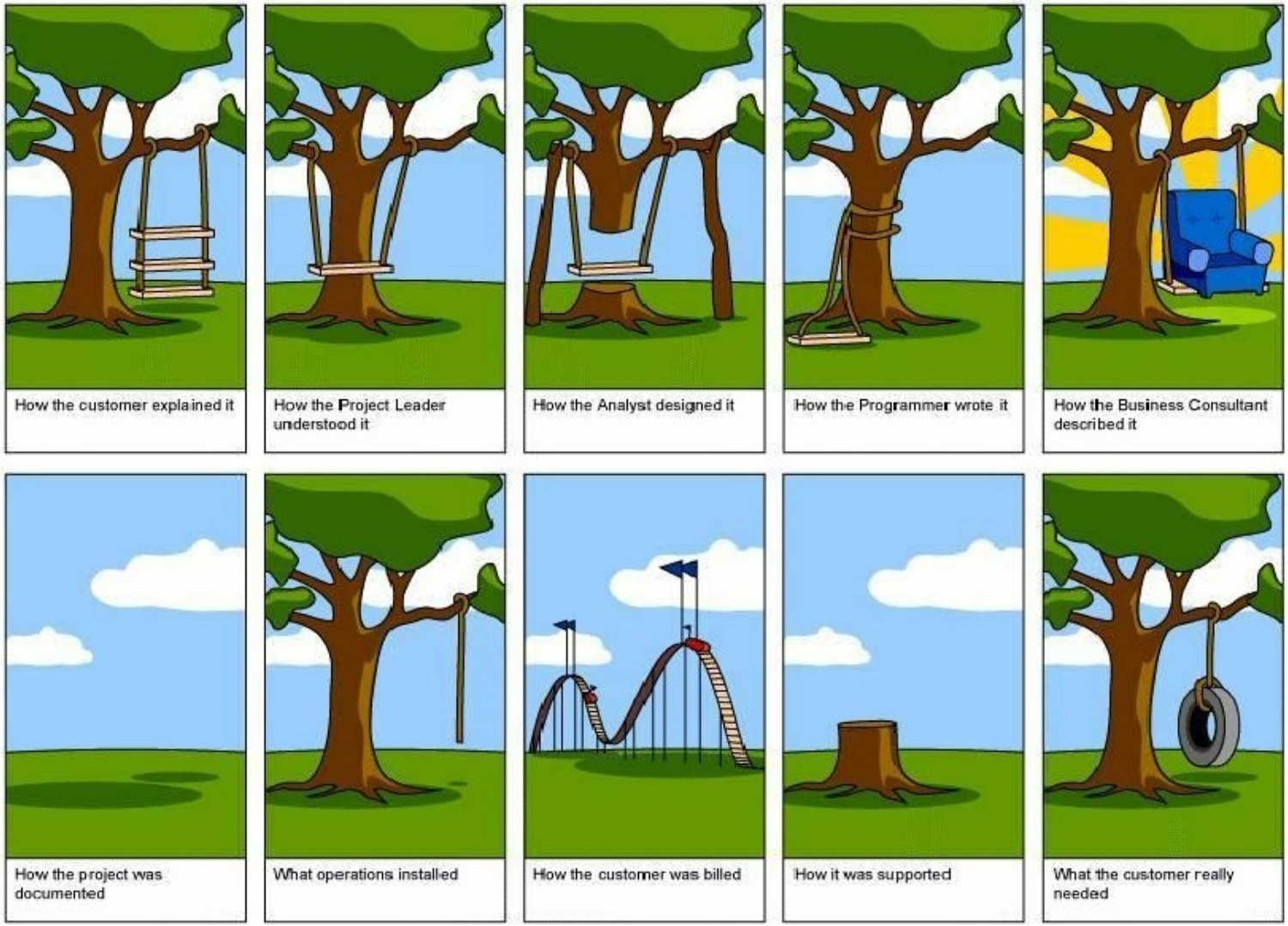
Studijní podklady:

- Veškeré materiály v e-learningu.
- Přednášky a materiály ke cvičení.
- *Vlastní zápisky.*

Rozšiřující zdroje:

- DAVIS, Michael. Hacking exposed malware: malware. New York: McGraw-Hill, c2010, xxi, 377 s. ISBN 978-0-07-159118-8.
- DEFINO, Steven a Larry GREENBLATT. Official certified ethical hacker review guide: for version 7.1. Boston: Course Technology, 2012, xxi, 329 s. ISBN 978-1-133-28291-4.
- BOYLES, Tim a Larry GREENBLATT. CCNA security: study guide. Hoboken: Wiley Publishing, 2010, xv, 516 s. ISBN 978-0-470-52767-2.
- STALLINGS, William. Cryptography and network security: principles and practice. Seventh edition. xix, 731 pages. ISBN 01-333-5469-5.
- PROSISE, Chris. Počítačový útok: Detekce, obrana a okamžitá náprava. Vyd. 1. Praha: Computer Press, 2002, xxii, 410 s. ISBN 80-722-6682-9.

Proč zabezpečení selhává v praxi ...



Základní pojmy

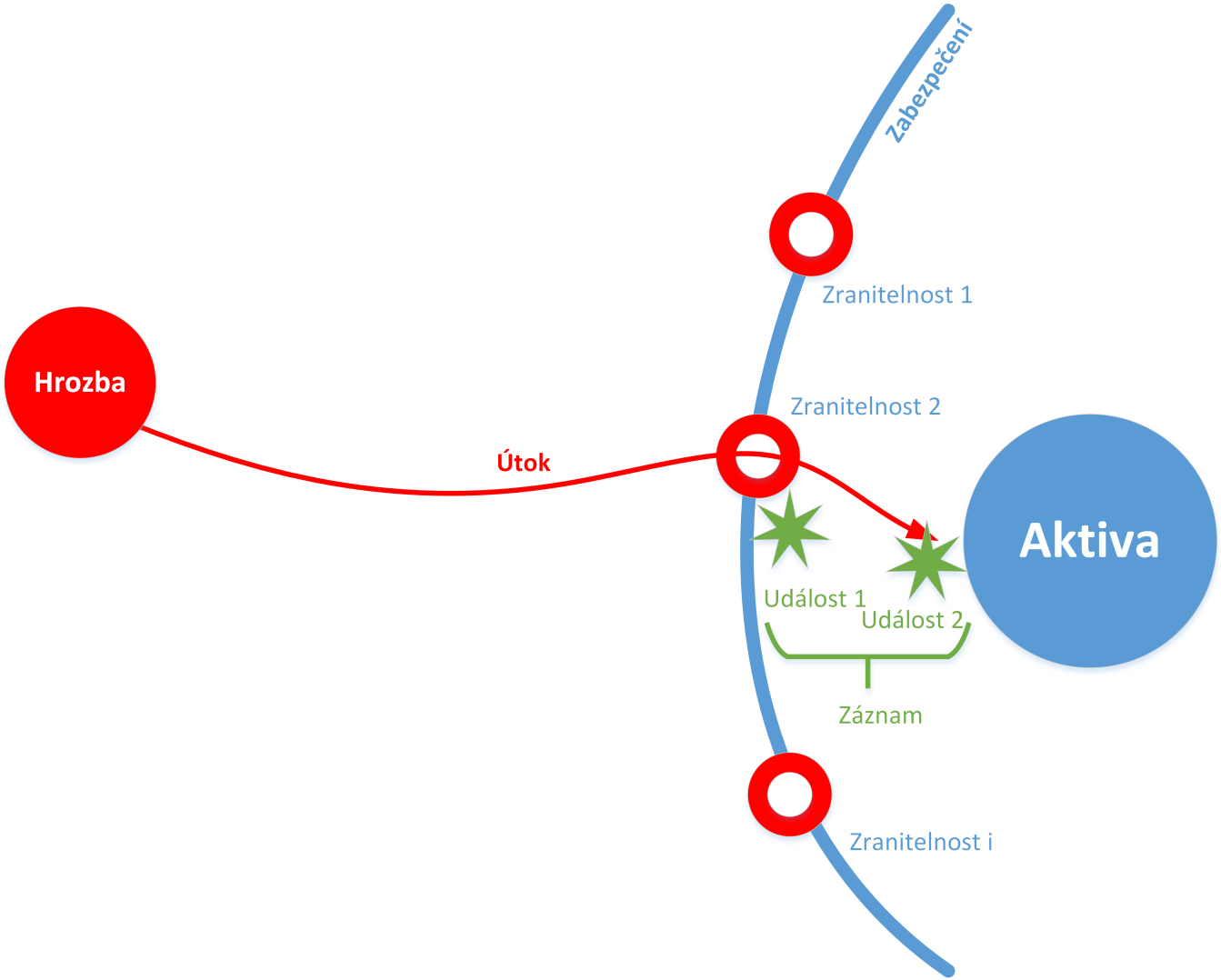
- **Aktiva** - je cokoliv, co je nějakým majitelem považováno za cenné (data, služby, software, hardware atd.).
- **Hrozba** (threat) - jakákoliv možnost ztráty aktiv, popsána:
  - nositelem hrozby (konkurenční firma),
  - objektem hrozby (databáze zákazníků),
  - mechanismem hrozby (krádež databáze, zkopírování dat).
- **Ochrana** - jakékoliv opatření, které snižuje četnost nebo velikost ztrát aktiv (různý charakter např. administrativní, organizační, personální nebo technické opatření).
- **Bezpečnost**[1] - stav, kdy ztráty aktiv nepřekračují stanovenou míru.

[1] Široký pojem, jemuž bývá v různých oblastech lidské činnosti připisován různý význam.

Základní pojmy

- Bezpečnost **NEmůže** být absolutní (ochrana proti všem hrozbám),
  - neexistuje ochrana,
  - nákladné, cena vyšší než cena aktiv.
- Ucelený systém ochran určený ke *komplexní*, *systematické* a *efektivní* ochraně aktiv budeme nazývat **zabezpečení**.
- **Slabina** (vulnerability) - zranitelné místo (vulnerability), zabezpečení nezajišťuje ochranu některých aktiv nebo ochrana těchto aktiv je nedostačující.
- **Riziko** (risk) – pravděpodobnost využití zranitelného místa.
- **Incident** (attack) - jakákoliv realizace (tj. uskutečnění) hrozby.
- **Průnik/dopad** (impact) - pokud při incidentu došlo ke ztrátě aktiv, důsledek útoku, rozsah škod.

Základní pojmy



Základní pojmy

Základní pojmy

- **Počítačová síť** - je souhrnné označení pro technické prostředky, které realizují spojení a výměnu informací mezi počítači, umožňují uživatelům komunikaci.
- Pojmem **bezpečnost sítě** rozumíme **neustálý proces (nikoliv stav)**, kterým se snažíme dosáhnout a udržet uspokojivé zabezpečení počítačové sítě.

Základní pojmy

- **Kybernetická bezpečnost** (Cyber Security) - je odvětví výpočetní techniky známé jako informační bezpečnost, uplatňované jak u počítačů tak i sítí.
- Cílem **informační bezpečnosti** je ochrana aktiv před krádeží, korupcí, nebo přírodní katastrofou při zachování dostupnosti legitimním uživatelům.
- Jak to chápe právo ?[2]
- Kybernetickou bezpečnost právo vnímá jako ochranu národního kyberprostoru před bezpečnostními hrozbami.

[2] To jistě víte z jiného předmětu.

Základní pojmy

- Síťové technologie se rychle vyvíjí a s nimi také znalosti a nástroje potenciálních útočníků.
- Zamyšlení, problém nemožnosti se přizpůsobení (př. doprava) . . . co je tedy důležité ? Jak na to ?
- Neustále se vzdělávat v oboru, neustále testovat - neustálé kolo, analýza, zabezpečení a testování!

Bezpečnost - sítě a služeb

- K zajištění bezpečnosti sítě opět využíváme **bezpečnostní služby**:
  - autentizace – ověření identity,
  - řízení přístupu – na základě přidělených práv (autorizace),
  - zajištění důvěrnosti přenášených dat,
  - zajištění integrity dat,
  - nepopíratelnost - ochrana proti odmítnutí původu zprávy.
- pro tyto služby používáme **různé kryptografické primitiva, mechanizmy a zařízení**,
- jednotlivé mechanismy včetně testování jsou **probrány na přednáškách** TIC2.

Účastníci - role

- **Alice** a **Bob** – legitimní uživatel (subjekt, osoby, procesy, počítače, good guys atd.), označení poprvé použil Ron Rivest 1978,
- **Eve** - nelegitimní uživatel (subjekt, útočník, bad guy, Mallory, Oscar, Trudy),
  - Odesílatel (sender) je entita (někdo/něco), která legitimně zasílá zprávu (budeme je označovat Alice, A).
  - Příjemce (reciever) je entita, která zprávu legitimně přijímá (budeme je označovat Bob, B).
  - Útočník (eavesdropper, adversary, opponent atd.) je entita, která není ani odesílatelem ani příjemcem zprávy, a která se pokouší prolomit bezpečnostní mechanismus komunikace mezi A a B (ozn. E, M apod.).

Síťové útoky - historie

- Po dlouhou dobu byla bezpečnost sítí (obecně ICT) **ignorována**,
- **nepředpokládalo se masivní propojení počítačů** (Internet),
- žádné zabezpečení, hesla atd.,
- následně počítačový průmysl „přežíval“, snažil se překonat technologické a ekonomické překážky,
- učiněno spoustu kompromisů.

Síťové útoky - současnost

- Počítače jsou všudypřítomné, jsou velmi výkonné a levné,
- počítače jsou propojeny (Internet, cloud řešení) a vzájemně závislé (dopad chyby),
- prudký nárůstu zájmu o bezpečnost IT,
- **motivace** - např. Mallware (viry, červi, atd.) způsobil v r.2007 ekonomické ztráty více než 75 miliard dolarů,
- četnost internetových útoků se zvyšuje, roste jejich závažnost a propracovanost.

Síťové útoky - dělení

- Rozděleních je **nejednotné**, aktivní útoky X pasivní, aktivní útočník X pasivní, softwarové útoky, hardwarové atd.,
- **vnitřní útoky**, škody způsobené nedbalostí (představuje útok), útok ze strany vlastních zaměstnanců,
- **vnější útoky** (náhodný či promyšlený útok zvenčí),

Síťové útoky - dělení

- V tomto kurzu použijeme dělení:
- **Pasivní útočník** - využívá základní prostředky, odposlech komunikace, hádání přístupových údajů atd.,
- **Aktivní útočník** - disponuje pokročilými prostředky výpočetní a komunikační technologie k sofistikovaným útokům (nutná investice, speciální sondy, zrcadla/opakovače provozu, generátor síťového provozu, speciální software, malware atd.). Předpokladem je, že útočník je rovněž i teoreticky vybaven a má základní znalosti o bezpečnosti cílového systému.

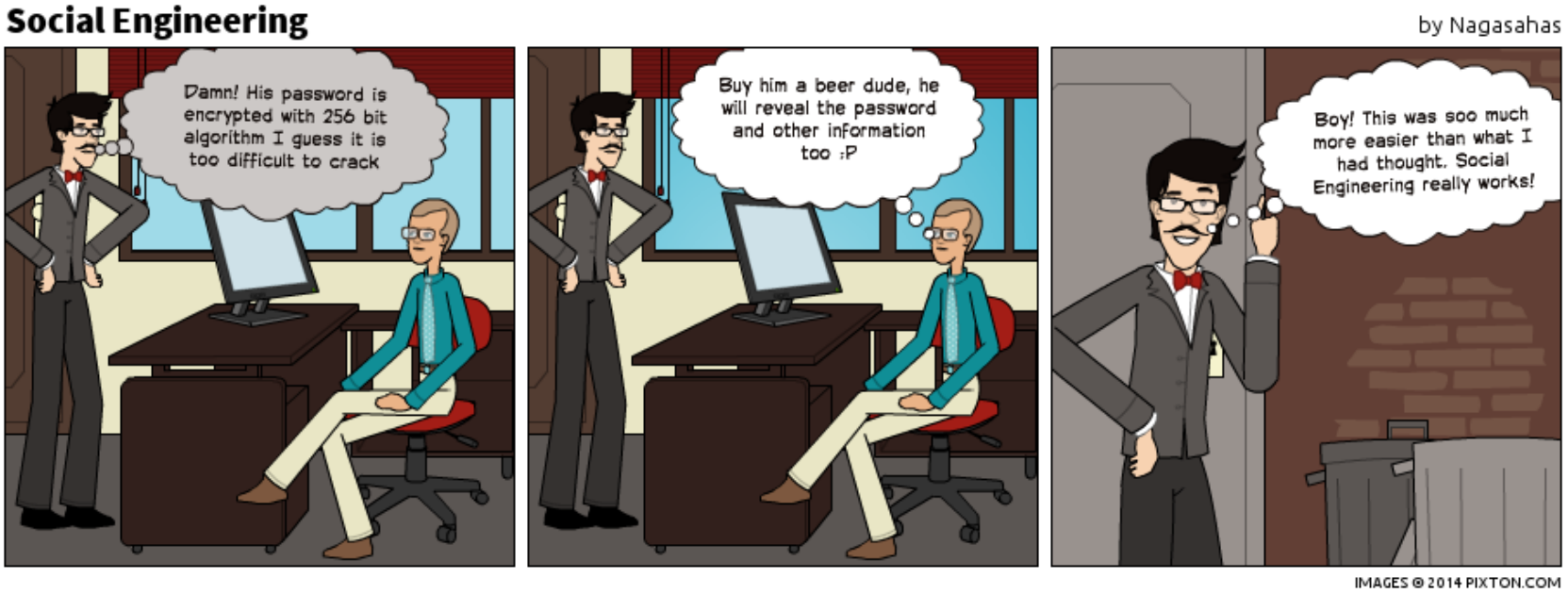
Síťové útoky - pasivní útočník

- **Odposlech dat** - možnost zachytit a přečíst přenášená data na komunikační lince, hrozba je aktuální při přenosu nezašifrovaných dat, realizovatelnost bezdrátová X drátová komunikace (fyzický přístup k přenosovému médiu).
- **Analýza provozu komunikace** - komunikace může být zašifrovaná, útočník sleduje například četnost přenášených dat, interval vysílání a přijímání dat, potvrzovací zprávy, tvar komunikačních hlaviček, strukturu záhlaví, atd. (zneužití informací proti poskytovateli nebo uživateli - dovolená).

Síťové útoky - pasivní útočník

- **Útok na slabou autentizaci** - pomocí hrubé síly útočník zkouší opakovaně slabé autentizační údaje (jméno/heslo (tzv. slovníkový útok)), či generuje autentizační zprávy za účelem průniku do systému za jiného uživatele, tento útok je v praxi velmi reálný.
- **Sociální inženýrství** - v dnešní době často používané, závisí na informovanosti (neznalosti) uživatelů, příkladem útoku je zisk přístupových údajů od uživatele, který tyto data vyzradí na základě mylné předpokladu, že svá data vkládá či posílá autorizovaným entitám (falešný správce sítě, falešné webové stránky atd.).

Síťové útoky - pasivní útočník



Síťové útoky - pasivní útočník

- **Skenování** - nalezení dostupných systémů a síťových služeb, základní skenovací technikou je ICMP (Internet Control Message Protocol) echo neboli ping. Následné skenovaní portů se testuje různé TCP (Transmission Control Protocol) a UDP (User Datagram Protocol) porty k odhalení portů, na kterých naslouchají síťové služby.
- Útočník touto technikou získá seznam **aktivní serverů a služeb** poskytovatele, na které následně může provést cílený útok.
- Většině realizovaných kybernetických útoků předchází skenování.

Síťové útoky - aktivní útočník

- **Modifikace přenášených dat** - útočník přenášená data zachytí a cíleně modifikuje, chyba systému nebo v horším případě nesprávnou odezvu.
- **Útok opakováním** (replay attack) - útočník si zaznamená komunikaci a následně po určité době pošle záznam stejnému příjemci (např. elektronický převod peněz, obrazový záznam z kamery apod.). Ochrana před tímto typem útoku spočívá ve specifikaci zprávy, tak aby dvě stejné zprávy od jednoho uživatele nebyly totožné (časové razítka).

Síťové útoky - aktivní útočník

- **Útok mužem uprostřed** (Man in the Midlle attack) - vnoří mezi komunikující strany, tedy musí oklamat obě komunikující strany (klient a server), musí ustanovit dva šifrovací klíče pokud je plánováno šifrování komunikace. Tyto metody bývají nazývané *spoofing* a mezi nejznámější patří například ARP spoofing, DHCP spoofing, SSL spoofing atd. (viz laboratorní úloha).
- Tento útok se často aplikuje na protokol ustanovení klíče Diffie-Hellman, proto se otisk ustanoveného klíče touto metodou ověřuje nezávislým komunikačním kanálem (nebo jinými metodami). Další způsob ochrany spočívá v nasazení metody autentizace, která ztěžuje oklamání komunikujících stran, např. použitím certifikátů.

Síťové útoky - aktivní útočník

- **Útoky na dostupnost služeb** (Denial of Service, DoS) - směřovány na webové servery, kdy se snaží o jejich vyřazení činnosti pomocí vyčerpání komunikační, výpočetní či paměťové kapacity serveru. Většina těchto útoků zneužívá chyby v implementaci TCP/IP protokolu (SynFlood, Ping of Deth atd.).
- Distribuované útoky (Distributed Denial of Service DDoS). Distribuovaných útoků se účastní zpravidla velké množství počítačů, které dokáží soustředěným útokem zahltit kapacitu i těch největších linek či výpočetních kapacit (v dnešní době není problém útok o intenzitě 20Gb/s).
- Ochranou proti těmto útokům je použití IPS (Intrusion Prevention Systems) a vhodně nakonfigurovaných firewallů.

Síťové útoky - aktivní útočník

- **Útoky postranním kanálem** (Side-channels attacks) - představují v současné době účinný a efektivní způsob kryptoanalýzy na doposud bezpečné kryptografické algoritmy jako je např. AES (Advanced Encryption Standart) nebo RSA (Rivest, Shamir, Adleman), které jsou implementovány na bezpečných zařízeních (typicky čipové karty, mikro kontroléry, chytré telefony, PC (TLS) atd.). Tyto neinvazivní útoky jsou cíleny na implementaci konkrétního kryptografického algoritmu (protokolu) na rozdíl od klasického způsobu kryptoanalýzy, která se snaží odhalit chybu v matematické podstatě algoritmu.

Děkuji za pozornost!
Dotazy ?

martinasek@feec.vutbr.cz

Reference I

[1] Matt Bishop.
Introduction to computer security.
2005.

[2] Karel BURDA.
Bezpečnost informačních systému.
Brno:[sn], 2005.

[3] Matt Curtin.
Introduction to network security.
Kent Information Services Inc, 1997.

[4] William Stallings.
Cryptography and network security: principles and practices.
Pearson Education India, 2006.