62. BEZPEČNOST SYSTÉMŮ A SITÍ

- základní cíle bezpečnosti:
  - důvěrnost
  - integrita
  - dostupnost
- pro přenos dat:
  - důvěrnost přenosu
  - autentizace
  - integrita přenosu
  - nepopiratelnost

- další pojmy:
  - zranitelná (slabá) místa
  - hrozby
  - aktiva

  ⇒ rizika

  ↳ bezpečnostní opatření
  - reaktivní
  - preventivní

  ← fyzická, personální, administrativní, technická (logická)

- cíle bezpečnostních funkcí BEZPEČNOSTNÍ FUNKCE
  - důvěrnost – analýza skrytých kanálů, opětovné použití prostředků, řízení přístupu (povinné, nepovinné)
  - integrita – řízení přístupu, DVB, autonomní testování, zálohování, oddělení rolí
  - dostupnost – přidělování prostředků, robustnost, zotavení z chyb, oprava za běhu
  - účtovatelnost – identifikace + autentizace, audit
- nemůžeme mít na úkor bezpečnosti omezenou funkcionalitu nebo použitelnost IS – musí zde být rovnováha

- typy hackerů
  - black hats – uškodit, ukrást, zničit, zisk, vydírání
  - white hats – etický hacker, hledá chyby a zranitelnosti, najmutý organizací
  - gray hats – pro své potěšení, vidí v tom poslání, nahlašují chyby, cílem není zisk
  - script kiddies
  - kyber-teroristi – v zájmu, víry, státu, ...

- fáze hackování
  - průzkum – sbírání informací o tom systému na který se bude útočit
    - pasivní
    - aktivní – hrozí odhalení
  - skenování – získávání informací do hloubky
  - získání přístupu – průnik do systému – hlavní část útoku
  - eskalace privilegií – získání vyšších oprávnění – root
  - udržení přístupu – třeba otevření zadních vrátek pro příští
  - zakrytí stop
- testování – simulování činnosti hackera a odhalování toho kudy by se do systému mohl dostat a odhalování zranitelností
  - black box – z pohledu reálného hackera, který nic nezná
  - white box – z pohledu nastrčeného zaměstnance který zná principy a stane se z něj hacker
  - grey box – něco mezi

  ⇒ zkoumají se zranitelnosti a slabá místa

- fáze průzkumu – sběr informací
  - průzkum sítě
  - identifikace aktivních uzlů
  - hledání otevřených portů
  - mapování sítě
  - SW nástroje: nmap, ...
  - sociální sítě jako zdroj
  - social engineering

- footprinting – hledání stop, získávání informací jakkoliv veřejných a přímých o cíli útoku
  - aktivní – vyžadují skenování a akce útočníka – nebezpečí odhalení
  - pasivní – veřejné info na webu, na sociálních sítích, v DNS, social engineer.
    - ↳ hledání v DNS záznamech whois, nslookup, ...
  - bez anonymizace a pseudonymizace ⇒ TOR systém
- sběr informací pomocí google vyhledávače
  - kamery
  - nezabezpečené soubory
  - zranitelná místa
  - anonymní googlení

- skenování – portů, uzlů v sítě, protokolů atd.., aplikací, ..., služeb, ..
  - identifikace OS pomocí skenování a jeho verze atd..
  - nmap
- jak se skrývat při skenování a zabránit tak odhalení?
  - anonymizéry využít
  - PROXY využít
  - IP spoofing – vydávat svou IP za jinou

Email spoofing
- email vypadá že jde od někoho jiného – od šéfa

- zachytávání paketů v síti a jejich analýza a zisk informací
  - zjistí se více o zařízeních a aplikacích co komunikují
  - protokoly bez zabezpečení – HTTP bez SSL atd..
  - wireshark
- ARP/MAC flooding – switch si drží v CAM tabulce záznamy o přeposílaných paketech a kdy komu co přeposlal
  - útočník daný přepínač zahltí různými zprávami tak, že se mu zaplní CAM tabulka
  - potom se přepínač chová jako ethernetový HUB a rozesílá na všechny porty zprávy (jakoby broadcast) ⇒ zde už útočník odposlouchává

  ARP cache poisoning také se může dělat
- MAC spoofing – uživatel s danou MAC poslouchá na portu
  - útočník se s tou samou MAC připojí na jiný port a přepínač si myslí že akorát uživatel přešel na jiný port a posílá útočníkovi zprávy
- nástroje pro detekci, identifikaci, pozorování a reportování podezřelých a neoprávněných aktivit v síti a metody
  - zachycují komunikaci
  - detekují škodlivý, podezřelý kód
  - monitorují a reportují divné chování

    ⋮
- → firewally – SW
  - filtrování ~~[illegible]~~ logická pravidla pro filtrování paketů
  - např. i stavový firewall
  - WAF – web application firewall
- → Honeypot – dobré pro odhalení zero-day zranitelností před nasazením do ostrého provozu

- lámání hesel – slovníkový útok – nejpoužívanější hesla
  - útok silou (brute force attack) – všechny možné kombinace
  - hybridní útok – slovníkový ale zkouší velká & malá písmena, čísla..
  - replay útok – zachytí komunikaci a zkusí ji pak někdy poslat znovu

– keyloggery – logují stisknutí kláves (i spyware)
  - HW
  - SW

– velké problémy s bezpečností jsou u starších verzí Windows bez aktualizací

– využívání 0-day zranitelností u Win
  ↳ využití ještě před vydáním opravy/aktualizace
  – i nově vydaný SW může mít nějakou takovou chybu, než se vydá oprava je nutné třeba dané služby vypnout

– spoofing – vydávání se za někoho jiného

– buffer overflow útok – přístup za hranice bufferu – ~~vydávání~~ zisk dat z jiné adresy
  – řešení je audit kódu a různé kontroly

– zlepšení/udržení bezpečnosti
  - Menší oprávnění – udělovat minimální potřebná oprávnění – nic navíc
    – nepovolovat přístup ke správcovským účtům vzdáleně přes síť
  - Minimalizace ~~[illegible]~~ útoku (cílů) – odebírat nepoužívané programy, soubory, knihovny a uživatelské účty
    – vypnout nepoužívané služby
  - Silná hesla
  - Dobrý firewall – dobře nastavený – co nejmenší oprávnění
    – vše zakázat a jen něco povolovat co je třeba

– Rootkity
  - aplikační
  - jaderné (OS)
  - cíle jsou knihovny

  – sada programů které umí maskovat a skrývat přítomnost škodlivého SW (trojanů, virů, červů, spywarů, atd.) v systému
  – skrývají adresáře, volání, složky, komunikaci atd..
  – pro ně pomáhají zneužít síťových služeb

– Social engineering – prohrabávání odpadků a hledání informací
  – předstírání, že jsem zaměstnanec
  – předstírání, že jsem technická podpora
  – nahlížení přes rameno
  – rozhazování flashek se škodlivým SW
  – Phishing – snaha získat citlivé informace (hesla, PIN, informace o uživatelích, bankovních kartách) tak že se vydávám za banku třeba – falešné maily a
  – Vishing – voice phishing – jako phishing ale přes telefon (maily, využívá spoofing
    a další – se útočník vydává třeba za IT podporu firmy s tím že použije phone spoofing
  – sběr dat na sociálních sítích, vyhledávače, útok s využitím známostí
  – nespokojený zaměstnanec může být velký problém

⌊ nikoho ...