Bezpečnost síťových aplikací

2019/2020

Př 11

Důvody, typy a metodika kyber útoků

- Důvody
  - Zneužití / Obohacení / Sláva / Zlost / Neznalost
- Typy útoků
  - Technické x Sociální, Vlastnost x Chyba
- Metody
  - Brutal-force
  - Man in the middle
  - Stack buffer overflow
  - DoS, DDoS

Důvody kyber útoků I.

- Zneužití – chci zdroj jen použít
  - Šíření spamu / virů
  - Botnet
  - Přestupní bod k dalším cílům
- Obohacení – chci něco cizího
  - Utajovaná data – obchodní tajemství
  - Zdroj informací k další činnosti – zdrojáky
  - Data jako zdroj vydírání
    - Firemní x osobní

Důvody kyber útoků II.

- Sláva – chci všem ukázat že můžu...
  - Často děti / nedoceněný pracovník ...
  - Snaha blýsknout se, ale I získat reference pro práci
  - Kombinace s šířením “propagandy”
- Zlost – snaha ublížit / poškodit
  - Konkurenci – práce x vztahy (Facebook)
  - Propuštěný / nespokojený zaměstnanec

Důvody kyber útoků III.

- Neznalost – vlastně nevím co dělám
  - “S knihou v ruce” - zkouším – neznám následky
  - Fakt nevím co dělám - uživatel

!!! Důvod je důležitý !!!

- Různé následky – co věc se stalo
- Různé důsledky – co vše může následovat
- Opakování se problémů

Typy útoků I.

- Technické
  - Zneužívám chyb / nedostatků technologie
    - Syn snoop
  - Využívám sílu technologie
    - DoS, DDoS
- Sociální
  - Využívám neznalosti / důvěřivost lidi
  - Manipulace s jedinci či organizacemi
  - Využití částěčně neveřejných informací

Typy útoků II.

- Zneužití vlastností – znám technologii
  - TCP / UDP / ICMP / DNS
    - Ping of Death a Teardrop,SYN Attack, Smurf attack a UDP flood
  - Legitimní chování služby s nelegitimním cílem
    - Spam,nedoručitelné maily, změna odesilatele
    - Podvržení identity – DNS / email / WWW stránka
  - Odposlechnutí
    - Man-in-the-middle, ARP poisoning

Typy útoků III.

- Využití chyb programů / služeb
  - Chyby v programech - vstupy
    - Stack buffer overflow
    - Podstrčení části kódu – include($_GET[“x”]);
    - SQL Injection
    - XSS
    - Známe chyby v Frameworku / neaktuálnost

Nejběžnější útoky I.

- Brutal force
  - Hádaní hesel hrubou silou
    - Proti službě
      - Jde logovat řešit fail2ban
      - Omezit počet přihlášení v čase
    - Proti otisku DB hesel
      - Zamezit scizení – práva, ACL, chroot
      - Solení a šifrování hesel
      - Jednorázová hesla
      - Biometrické klíče

Nejběžnější útoky II.

- DoS, DDoS
  - Odmítnutí / nedostupnost
    - Přímý útok - “regulérní dotaz”
      - Botnet generující nadměrný trafic
      - Vyhledávání náročných URL
      - Chyby v přesměrování: obraný tok reklamy např
      - “Náhodné” DNS dotazy: přetížení auth. serverů
      - Částěčné dotazy
        - » Pošlu jen část spojení: SYN Attack
        - » Pomalé pokládání dotazů: Slowloris

Nejběžnější útoky III.

- DoS, DDoS
  - Odmítnutí / nedostupnost
    - Nepřímý útok – generuju jen trafic
      - Botnet generující nadměrný trafic
      - Často postižena více linka než cílový stroj
      - Nepotvrzovaný UDP stream: Smurf attack a UDP flood
      - Servisní protokol ICMP: Ping of Death a Teardrop,
      - Často vedené ze zahraničí – dočasného odstavení transitu
      - Rozmělnění, analýza a online filtrace - Radware

Nejběžnější útoky IV.

- Man in the middle
  - Odposlouchávání provozu
    - Nutnost být / zařídit na správném místě
    - Útočník je mezi zdrojem a cílem a může
      - Odposlouchávat, filtrovat, modifikovat provoz
    - Často kombinované s ARP poisoning
      - Pokud nemám ja se dostat mezi přesměruju provoz
    - Možnost využít routovací protokoly
    - Podrvžená DNS – proxy - upravené dat
    - Problém slabých šifer SHA1

Nejběžnější útoky V.

- Buffer/Stack Overflow Attack
  - Chyba v programu, která způsobí zásad do cizí paměti
  - Často léta neodhalená
  - Dovolí spustit cizí kód:
    - Pád systému
    - Eskalace oprávnění – často na roota

Nejběžnější útoky VI.

- SQL Injection
  - Chybně ošetřené parametry – často na WWW
  - Detekce možná vzdáleně a automatizovaně
    - Wapiti, sqlmap
  - Možnost přistupu do SQL I OS !!
    - Nutné logy k zjištění rozsahu
  - “přídavky” k proměnným
    - 1=1, ; drop table XX, UNION select...,

Nejběžnější útoky VII.

- Spuštění cizího kódu
  - Chybně ošetřené parametry
    - Např $_GET, $_POST
  - Detekce možná vzdáleně a automatizovaně
    - Wapiti, w3af
  - Možnost spustit jiný lokální I vzdálený kod
    - Include /etc/passwd, http://.....
  - Možnost zakazovat funkce OS
    - disable function

Atypické útoky

- Telefonní sítě
  - Spíše historie, dnes vše po IP
- Sociální sítě
  - Kyber šikana, narůstající problém
- Atypická zařízení
  - Tiskárny, telefony, auta, ledničky, ….
  - V budoucnosti bude stále častější