MI-PB-16

Bezpečnostní slabiny počítačových sítí a komunikačních protokolů, zabezpečení protokolů a sítí.

Pojmy

Event: pozorovatelný jev v systému nebo síti

Adverse event: event s negativními důsledky, např. pád systému, packet flood, zvýšení oprávnění

Computer security incident: narušení nebo hrozba narušení politik počítačové bezpečnosti nebo standardních bezpečnostních praktik
Security incident $\neq$ operations incident

Cíle síťové bezpečnosti:

- Confidentiality, Integrity, Availability
- $\mathrm{Risk} = \mathrm{threat} \times \mathrm{vulnerability}$
- Odstranění zranitelností, blokování hrozeb

Risk management:

- Identifikace faktorů, které by mohly poškodit nebo kompromitovat data
- Ohodnocení těchto faktorů -- cena dat vs. cena opatření
- Implementace cenově efektivních opatření

Omezení rizika:

- Rozčlenění
- Bezpečná selhání
- Defense-In-Depth
- Nízká oprávnění
- Security-by-Obscurity

Nejslabší článek bezpečnosti: člověk

Firewall

Blokování nepovoleného přístupu

Povolení pouze autorizovaných komunikací

Firewallem by se měl chránit každý segment lokální sítě

Typy:

- Software firewall: ochrana jednoho stroje
- **Packet Filter:** kontrola každého paketu, aplikace pravidel
- **Application Layer:** "porozumění" určitým aplikacím a protokolům (FTP, DNS, web, ...)
- **Stateful Filter:** udržuje sessions síťových toků, detekuje pakety, které do nich nepatří
- **NAT:** poskytuje základní ochranu

Útoky

Botnet:

- Síť synchronizovaných (spolupracujících) napadených zařízení
- Komunikace: centrální Command&Control vs. P2P

Vektor útoku: popisuje, jak lze útok provést a co útok využívá

Indikátor kompromitace: objekt pozorovaný na síti nebo v OS, který s vysokou spolehlivostí indikuje narušení počítače

Klasifikace: (Hansman et al.)

- 1. rozměr: kategorizace útoku podle vektoru
- 2. rozměr: podle cíle útoku
- 3. rozměr: zranitelnosti a exploity použité při útoku
- 4. rozměr: útoky, které mají payloady nebo dopad i mimo svůj rozsah
- lze přidat i další rozměry

Typy útoků:

- **Sběr informací**
  - **Scanning (vertical/horizontal):**
    - Objevení služeb nebo zařízení

        - UDP: jedna SRC_IP, jedna DST_IP, hodně DST_PORT, dlouhé timeouty
        - TCP SYN: jedna SRC_IP, jedna DST_IP, více DST_PORT, otevřený port = odpověď SYN&ACK
        - ICMP: jedna SRC_IP více DST_IP
        - Obrana: pouze nezbytné porty otevřené, zahazování místo odmítání, honeypot
    - OSINT (Open Source Intelligence)
- **Krádež přihlašovacích údajů**
    - Phishing
    - **Brute-force útoky:**
        - Hádání jména/hesla
        - Obrana:
            - Fail-2-ban
            - Omezený počet pokusů
- **Narušení komunikace**
    - **Man-in-the-Middle:**
        - Cíl: odposlech komunikace
        - Rogue DHCP Server
        - ARP cache poisoning (podvržená odpověď na ARP dotaz -- provoz přesměrován na útočníkovo zařízení)
        - DNS cache poisoning
        - Šifrovaná data:
            - SSL stripping: HTTPS $\rightarrow$ HTTP
            - Certificate Pinning: útočník injektuje škodlivý certifikát do systému oběti
            - TLS Protocol Downgrade
    - Poisoning
    - Hijacking
- **Narušení služby/operace**
    - **Denial of service:**
        - Způsobení pomalosti/nepoužitelnosti systému přetížením jeho prostředků
        - Nesofistikovaný, útočník nezíská žádné informace
        - Lze způsobit libovolnou zranitelností končící pádem aplikace
        - **DDoS:**
            - Velký synchronizovaný provoz z hodně různých zdrojů
            - Využití botnetů
            - Dopad na více zařízení: hlavní oběť je služba, na kterou se útočí, vedlejší oběti jsou kompromitované útočící systémy
        - **SYN-Flood:**

        - Hodně TCP paketů s příznakem SYN -- server alokuje prostředky pro připojení
        - Jedna SRC_IP, DST_IP, více SRC_PORT, DST_PORT
        - Obrana:
            - SYN Cookies
            - alokace zdrojů až po dokončení handshake
    - **UDP Flood:**
        - Hodně UDP paketů na náhodné porty
        - Obět odpoví ICMP Host Unreachable při dotazu na zavřený port
        - Produkce velkého množství ICMP paketů -- zpomalení serveru
    - **Ping of Death:**
        - Maximální velikost ICMP paketu: 64 kB
        - Hodně systémů s touto velikostí nepočítá -- buffer overflow, nestabilita
    - **DRDoS:**
        - Reflection
        - Zdroje (botnet) vyšlou Reflectorům (např. DNS resolverům) málo malých paketů se SRC_IP oběti
        - Reflectory jako odpověď vyšlou mnohonásobně větší pakety
    - **Obrana:**
        - nejefektivnější: na úrovni ISP
        - Limity připojení
        - Timeouty
        - Detekce anoálií
        - Load-balancing
  - Starvation
  - Deauthentication/Connection resetting
- **Exfiltrace dat**
  - **Covert Channels:**
    - Kanál, kterým jsou přenášena data způsobem, který narušuje bezpečnostní politiku
    - Obcházení detekce (firewall)
    - Komunikace malware
    - Header Bit crafting
    - ICMP data exfiltration (data buď v payloadu nebo zakódovaná do intervalů)
    - DNS: request na `<base64encodedpayload>.attackersite.com` , kde `attackersite.com` je útočníkova stránka s DNS serverem
    - Detekce: specifické signatury, anomálie (abnormálně velké pakety, hodně ICMP, DNS)
  - Tunely, VPN

Monitoring útoků:

- Host-based (logy, auditové nástroje) vs. Network-based (aktivní -- ping, traceroute, ... vs. pasivní)
- Sledování datových jednotek (paketů/rámců/bytů/...):
  - Counter: vysokoúrovňová informace (celkový počet paketů/bytů/chyb, ztrátovost)
  - Packet: "raw data", Deep Packet Inspection, pattern matching
  - Flow: vysokoúrovňový přehled, agregace

IP flow:

- Množina IP paketů procházející pozorovací bod v síti během nějakého časového intervalu. Všechny pakety patřící do jednoho flow mají společné vlastnosti odvozené od dat obsažených v těchto paketech a od zacházení s paketem v porozovacím bodě
- Uni-flow: jednosměrná komunikace mezi SRC_IP a DST_IP
- Bi-flow: obousměrná, párování záznamů (request + response)

Hrozby

Zdroje:

- Filozofie návrhu
- Slabina v infrastruktuře/protokolu
- Růst kyberprostoru, hackerské komunity
- Zranitelnost v OS
- Insider Effect -- hrozba zevnitř
- Sociální inženýrství
- Fyzická krádež

Motivace hrozeb:

- Terorismus
- Ekonomická/vojenská špionáž
- Pomsta
- Nenávist
- Sláva
- Chamtivost
- Ignorantství

ISO/OSI a zranitelnosti v něm, útoky

Dostál se na to prý ptá: https://fit-wiki.cz/škola/státnice/zkusenosti2019_leto/zkušenosti_ze_státnic

(když nevíš, piš DoS -- na každé vrstvě se dá něco rozbít)

- **Layer 1 (fyzická)**
  - Fyzická krádež zařízení
  - Mechanické poškození zařízení
  - Neautorizované změny v prostředí -- odpojování kabelů, napájení
- **Layer 2 (linková)**
  - Úmyslné Spanning Tree errors: Tvorba loopů ve spanning tree -- rámce cyklí donekonečna
  - ARP Cache Poisonong / ARP Spoofing: Podvržení odpovědi na ARP dotaz (neustálé posílání odpovědi s útočníkovou MAC adresou), provoz je přesměrován na zařízení útočníka
- **Layer 3 (síťová)**
  - Route spoofing: Propagace falešné síťové topologie
  - IP address spoofing: Falešná zdrojová adresa na škodlivých paketech
  - Ping flood
  - ICMP útoky (Covert channels)
- **Layer 4 (transportní):**
  - Port scanning
  - SYN flood
  - Zranitelnosti SSL/TLS (viz okruh 17)
- **Layer 5 (session)**
  - slabá/žádná autentizace
  - přihlašovací údaje v plaintextu
  - session hijacking (odposlech session ID, jeho neoprávněné použití)
- **Layer 6 (prezentační)**
  - špatné zacházení se vstupem
- **Layer 7 (aplikační)**
  - SQL Injection
  - Rogue DHCP Server
  - HTTP flood
  - Cross Site Scripting
  - Slow Lorris: DoS, kde server není zahlcen obřím návalem dat, ale posílá se jenom nezbytné množství dat, aby si server držel otevřená spojení, čímž vyčerpal svoje prostředky
  - SSL Stripping: donucení HTTPS stránky použít HTTP

Dynamic Host Configuration Protocol

Automatická konfigurace IP adresy, DGW, DNS serverů atd. pro nové zařízení v síti.

Fáze:

- Discovery:
  - klient vyšle UDP broadcast na 255.255.255.255
  - objevení DHCP serverů
- Offer:
  - DHCP server obdrží request na lease IP adresy
  - Rezervace IP pro klienta
  - Odeslání DHCPOFFER zprávy klientovi. Obsah zprávy: klient MAC, nabídnutá IP adresa, maska sítě, trvání zapůjčení adresy, IP adresy DHCP serveru
- Request:
  - Klient si vybere jednu z nabízených adres a odešle zprávu DHCPREQUEST serveru, od kterého nabídka přišla
- Acknowlodgement:
  - Server pošle DHCPACK paket s dobou trvání zapůjčení a dalšími informacemi

Útoky:

- **Rogue Servers:**
  - Trojan na napadeném stroji
  - Odesílá nesmyslné DHCP pakety ostatním
- **DHCP Starvation:**
  - Falešní klienti posílají serveru žádosti o adresy
  - Server vypotřebuje všechny dostupné adresy