15. Zabezpečení sítí - útoky na datové sítě a strategie obrany, ACLs, firewally, demilitarizované zóny

POČÍTAČOVÉ SÍTĚ A PROGRAMOVÁNÍ

Bezpečnostní služby v síti

- Utajení a důvěryhodnost dat – šifrování
- Autentizace – ověření totožnosti
- Autorizace – řízení přístupu, práva
- Integrita (konzistence) – zajištění, že zpráva nebyla pozměněna
- Nepopiratelnost – odesílatel a adresát nemohou popřít akci

Útoky

Průzkum sítě

- Neautorizovaný sběr informací
    - Např.: hromadná ping
    - **Ochrana:** zakázat odpovědi na firewallu

Odchytávání paketů

- Využívá se program Wireshark

Získání přístupu

- Prolomení hesla (Brute Force, odchycení hesla v plain textu (POP3, Telnet))

Man in the middle

- Útočník se stane prostředníkem komunikace
- **DHCP Spoofing**
    - Útočník do sítě připojí svůj DHCP server a klientům přiřazuje správné IP adresy, ale sám se nastaví jako brána či DNS server.
    - **Ochrana:** DHCP snooping **(**Na switchi se nastaví důvěryhodný port směrem k DHCP serveru, pokud přijde DHCP offer z jiného portu, zahodí se.)
- **ARP spoofing**
    - Útočník odpovídá na ARP request a doplní vlastní MAC → komunikace „teče“ přes útočníka.
    - **Ochrana:** Filtrace paketů (zahození paketů s konfliktními informacemi), šifrování dat a autentizace.

Phishing

- Sociální inženýrství, vylákání citlivých údajů, často podvodné emaily.
- Znaky podvodných zpráv: http odkazy na jiné stránky než uvedené v textu.
- Spustitelné přílohy, časový nátlak, gramatické nedostatky či v cizím jazyce.

Pharming

- Úprava lokálních cechovaných DNS záznamů, popřípadě útok na DNS server.
- Při překladu domény dostaneme podvodnou IP adresu a připojíme se na špatnou stránku.
- **Typické znaky:** nezabezpečené připojení (http://), stránka nevypadá „správně“
- **Obrana:** antivirové programy, dvoufázové přihlášení, VPN

Cross Site Sctipting (XSS)

- Podstrčení podvodného scriptu v jinak důvěryhodné stránce,
- **Persistentní** – podvodný kód je uložen přímo na serveru stránky
- **Nepersistentní** – skript je vložen jiným způsobem (při vyhledávání, komentářem)
- **Ochrana:** Správný návrh stránky na straně serveru.

SQL injection

- Napadení databáze přes aplikaci (speciální vstup nebo úprava URL)
- **Ochrana:** Ošetření vstupů (escapování „\n“), omezení práv (zakázat uživateli příkaz DROP TABLE).

DoS (Denial of Service)

- Oběť (server, síť, …) je přehlcena požadavky a musí se vypnout.
- Mnoho broadcast vysílání, pingů.
- **Ochrana:** Omezit broadcast, zabránit spoofingu, firewall.

DDoS (Distributed Denial of Service)

- Jako DoS, ale z mnoha zařízení najednou tzv. zombies které dohromady tvoří botnet.
- Nefunguje filtrace pomocí IP, protože každý zombie má vlastní.
- Zombies ani neví, že jsou součástí útoku, protože program běží na pozadí.

TCP SYN flood

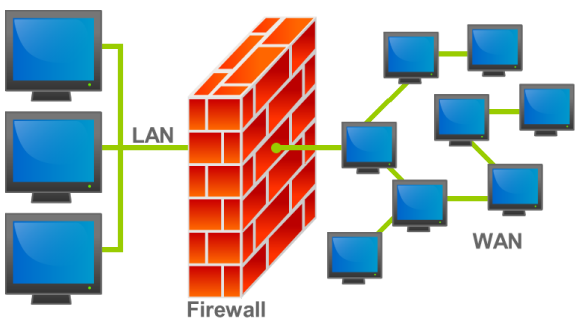
- Útočník odesílá požadavky pro otevření TCP spojení.
- Oběť odpoví, ale nedostane potvrzení a tato polootevřená spojení se hromadí ve vyrovnávací paměti.

ACL – Access Control List

- U počítačových sítí se jako ACL označuje seznam pravidel popisující porty nebo (síťové) démony, které jsou dostupné na počítači (či jiném zařízení na síťové vrstvě), a u každé seznam zařízení a sítí, které mohou tuto službu používat.
- ACL mohou být jak na konkrétních serverech, tak i na routerech.
- Zpravidla existují oddělená ACL pro příchozí a odchozí data. Viz též firewall.
- Aplikace na L2 vrstvě rozhraní přepínače.
- Standard IP ACL – filtrace pomocí IP adresy.
- Extended IP ACL – filtrace na základě protokolu a zdrojové i cílové IP adresy
- MAC Extended ACL – filtrace na základě protokolu a zdrojové i cílové MAC adresy.

Firewall

- Firewall je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení.
- Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje.
- Chrání síť před útoky z vnější.



- Nesmí nepříznivě ovlivňovat provoz v dané síti (zpoždění).
- Nesmí obsahovat data ani prostředky, které by mohl útočník zneužít.

Druhy

Paketový filtr

- Zpracovává pakety a rozhoduje o jejich zahození.
- **Statické filtrování** – nakonfigurovaná pravidla (ACL)
- **Dynamické filtrování** – při odchozím provozu lze dynamicky měnit pravidla
- **Stavový firewall** – paketový filtr rozšířený o tabulku probíhajících TCP spojení

Circuit Gateways

- Brány na transportní vrstvě, řízení na základě cílové nebo zdrojové IP adresy, nekontroluje obsah paketů.

Aplikační brána

- O zahození rozhoduje na základě aplikačních dat.

NAT (Network Address Translation)

- Překlad privátních adres na veřejné
- Ochrana vnitřních uživatelů sítě, jejich adresy zůstávají vnějšku skryté.

Demilitarizovaná zóna

- Podsíť, která je z bezpečnostních důvodů oddělena od zbytku sítě.
- Jsou v ní služby dostupné z celého internetu.