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

* Zabezpečení sítě je minimalizace zranitelných míst v síti

**Útoky a strategie obrany**

Ochrana

* Fyzické zabezpečení – zařízení je umístěno do uzavřené místnosti, přístupné pouze oprávněným osobám. Místnost je izolována od elektrostatického a magnetického rušení, má požární zabezpečení a klimatizaci a je napájeno přes UPS
* Zabezpečení operačního systému – směrovač s maximální možnou pamětí (ochrana před útoky DoS, podpora škály bezpečnostních služeb)
* Omezení nežádoucích přístupů – eliminuje potenciální zneužití nevyužitých portů a služeb

Útoky

Využití důvěryhodnosti

* Man In the Middle (MITM) – útočník se bude snažit stát nepozorovaně prostředníkem komunikace dvou stran, aby mohl odposlouchávat přenášenou komunikaci nebo ji měnit
* DHCP spoofing – útočník připojí do sítě vlastní DHCP server, který odpovídá na DHCP žádosti uživatelů, ale pošle jim jiné DHCP odpovědi, než by to udělal správný DHCP server
* ARP spoofing – útočník pošle oběti ARP REPLY paket, který říká, že brána má MAC adresu útočníka (při komunikaci obě strany budou používat MAC adresu útočníka)
* Exploit – program, který využívá nevědomě vytvořené softwarové chyby v programu a způsobuje přetečení zásobníku
* Přetečení zásobníku – zásobník = pevně alokovaná oblast paměti, kam si systém ukládá data (arp a směrovací tabulka atd.)

pokud útočník zahltí tuto paměť, může dojít k přetečení dat mimo rozsah a k poškození dat

* Phishing – útočníky používají tuto techniku k vylákání citlivých údajů rozesíláním podvodných emailů, které jsou téměř nerozeznatelné od oficiálních
* Pharming – (podobné Phishingu, ale manipuluje s DNS záznamy) pokud oběť přistupuje na stránky (např. elektronické bankovnictví), načtou se mu díky upravených DNS záznamům podvodné stránky, které vypadají úplně stejně
* SQL Injection – napadá databáze, útočník může zaútočit na špatně filtrované uživatelské vstupy, které jsou přímo vloženy do SQL dotazů – tím získá propojení s databází a může s ní
* Denial of service (DoS) - cílem je znepřístupnit služby, počítače nebo celé sítě – útočník zahlcuje oběť požadavky, které způsobují vyčerpávání jeho zdrojů, zpomalení funkce a následný pád
* IP spoofing – zfalšování zdrojové IP adresy útočníka a následné odeslání cílovému počítači (oběti), před kterým chce útočník svou IP adresu utajit – využívá se na DoS útok

Útoky pomocí ICMP zpráv

* Ping of Death – útočník manipuluje velikostí ICMP echo request zprávy tak, že přesahuje maximální povolenou velikost (65 535 bytů), což může způsobit pád cílového zařízení.
* Smurf Attack – útočník pošle falešné ICMP echo request zprávy s falešnou zdrojovou IP adresou na broadcastovou adresu sítě, což způsobí, že všechna zařízení v síti odpoví oběti, což může vést k významnému přetížení
* Ping flooding – útočník zaplavuje cílový server nebo zařízení obrovským množstvím ICMP zpráv, což způsobuje přetížení sítě a výpadek služeb
* DDoS – útočník napadne pomocí trojských koňů stovky zařízení a pak je využije na určitý cíl, aby prováděly DoS útok

**Typy ACL**

* Standardní (1-99) – umí filtrovat jen zdrojovou IP adresu
* Rozšířené (100-199) – filtrují provoz v závislosti na zdrojové a cílové adrese, protokolu a případně číslu portu nebo typu zprávy ICMP a jsou umístěny co nejblíže ke zdroji
* Pojmenované – typ ACL, kde jsou pravidla pojmenována pro lepší správu, může být buď standardní, nebo rozšířená, ale obsahuje vlastní jméno, což usnadňuje jejich identifikaci a úpravy
* Reflexivní – blokují komunikaci z vnějšku, pokud nebyla zahájena z vnitřní sítě
* Dynamické – přístup umožněn po autentizaci přes Telnet, dynamická podmínka přidána do rozšířeného ACL
* Časové – kontrola přístupu podle času, např. přístup k internetu pouze o přestávkách

**Firewall**

* oddělují chráněné oblasti od okolí a chrání neoprávněným uživatelům přistupovat k chráněným síťovým zdrojům´

Typy Firewall

* filtrace podle přihlášení – průchod paketů je určen shodou přihlašovacích údajů jak na straně klienta, tak serveru
* transparentní firewall – filtruje provoz mezi dvojicí přemostěných rozhraní
* hybridní firewall – kombinuje různé varianty bran

Výhody

* Ochrana před neoprávněným přístupem
* Filtrace provozu
* Monitoring a logování
* Prevence útoků
* Kontrola přístupu

Nevýhody

* Omezení legitimního provozu
* Zpoždění v síti
* Nejistota v případě útoku
* Komplexnost správy
* Závislost na technologiích

**Demilitarizovaná zóna**

* část sítě ohraničené firewallem nebo sadou firewallů
* DMZ definují části sítě, které jsou důvěryhodné a části, které jsou nedůvěryhodné
* design Firewall je především o rozhraní zařízení umožňujících nebo popírání provoz založený na zdroj, cíl a druh provozu