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

**1. Útoky na datové sítě**

* **Denial of Service (DoS) a Distributed Denial of Service (DDoS)**: Útočník přetíží síťové prostředky nebo služby tak, aby je uživatelé nemohli využívat. DDoS je verze útoku, kdy útok provádí více zařízení najednou.
* **Man-in-the-middle (MITM)**: Útočník zachytává a případně i modifikuje komunikaci mezi dvěma stranami, aniž by to tyto strany věděly.
* **Phishing**: Útočníci posílají falešné e-maily nebo zprávy, které mají za cíl získat citlivé informace, jako jsou hesla nebo platební údaje.
* **Malware**: Jedná se o škodlivý software, který infikuje systémy, často za účelem získání přístupu k síti nebo zisku citlivých dat (ransomware, spyware).
* **Packet sniffing**: Útočník zachytává data, která se přenášejí přes síť, například za účelem získání hesel nebo citlivých informací.
* **SQL injection**: Útočník vkládá škodlivé SQL dotazy do formulářů na webu s cílem získat nebo upravit data uložená v databázi.
* **Pharming**: Pharming je útok, který přesměruje uživatele na podvodný web i při správném zadání adresy. Útočníci manipulují DNS nebo lokální soubory k získání citlivých dat.

**2. Strategie obrany**

* **Šifrování**: Zajišťuje, že data přenášená po síti jsou nečitelná pro ty, kdo k nim nemají oprávnění.
* **Autentizace a autorizace**: Zajištění, že přístup k síti mají pouze oprávněné osoby (použití hesel, několika násobná autentizace, digitálních certifikátů).
* **Segmentace sítě**: Rozdělení sítě na menší části ( použití VLAN) omezuje pohyb útočníků v případě narušení.
* **Zálohování**: Pravidelné zálohování důležitých dat umožňuje rychlou obnovu v případě útoku.

**3. ACL**

Access Control Lists jsou seznamy pravidel, které určují, kdo nebo co má přístup k určité části sítě nebo ke konkrétním zdrojům. ACL se používají zejména na směrovačích a přepínačích k omezení síťového provozu a řízení přístupu na základě:

* IP adres
* Protokolů (např. TCP, UDP)
* Čísel portů (např. HTTP, FTP)

ACL pomáhají filtrovat provoz na základě těchto kritérií a jsou klíčovým prvkem pro zajištění bezpečnosti sítě, protože umožňují řídit, které zařízení mohou komunikovat s konkrétními síťovými zdroji.

**Typy ACL**

* Standardní ACL (1-99): Filtrování podle zdrojové IP adresy, nejčastěji aplikováno co nejblíže cílovému zařízení.
* Rozšířené ACL (100-199): Umožňuje filtrování na základě různých kritérií, jako je IP adresa, protokoly (TCP, UDP, ICMP), porty a další. Obvykle umístěno blíže zdroji provozu.
* Povolení všeho: Jednoduché pravidlo pro povolení veškeré komunikace mezi všemi zařízeními.
* Pojmenované ACL: Flexibilnější verze ACL, kde můžeme určit pravidla pomocí názvů, blokování určitého portu nebo služby.
* Reflexivní ACL: Umožňuje přístup zvenčí jen tehdy, pokud byl původně iniciován zevnitř sítě.
* Dynamické ACL: Přístup je povolen až po autentizaci (Telnet) a poté se pravidla dynamicky přizpůsobují.
* Časové ACL: Omezuje přístup na základě časových podmínek, například povolení internetu jen v určitých hodinách.

**4. Firewally**

Firewall je zařízení nebo software, který monitoruje a filtruje síťový provoz na základě předdefinovaných bezpečnostních pravidel. Zabezpečení pomocí Firewallu může být Softwarové nebo Hardwarové.

* **Packet-filtering firewall**: Filtruje jednotlivé pakety na základě jejich hlaviček (IP adres, portů a protokolů).
* **Stateful firewall**: Sleduje stav připojení a na základě toho rozhoduje, zda má paket povolit nebo zablokovat.
* **Application-layer firewall**: Pracuje na aplikační vrstvě a kontroluje specifické aplikace (HTTP, FTP) a jejich chování.

Firewally chrání síť před neoprávněným přístupem, blokují škodlivý provoz a mohou také fungovat jako síťové brány.

**5. Demilitarizované zóny (DMZ)**

Demilitarizovaná zóna je speciální síťová oblast, která slouží jako přechodová zóna mezi interní sítí a internetem. Slouží k umístění veřejně dostupných služeb (webové servery, e-mailové servery), které potřebují komunikovat jak s interní sítí, tak s internetem. DMZ poskytuje dodatečnou vrstvu ochrany, protože přístup k citlivým vnitřním systémům je oddělený a kontrolovaný.