Zabezpečení sítí

Útoky na datové sítě rozdělení: PASIVNÍ a AKTIVNÍ

Pasivní
- cílem pasivních útoků je získat/využít informace ze systému
- nemají vliv na systémové prostředky
- útočník pouze monitoruje kom. kanál a ohrožuje důvěrnost dat
- cíl pasivních útoků je získat přenášené informace odposloucháváním/monitorováním přenosu

Aktivní
- aktivní útoky se pokoušejí měnit systémové prostředky nebo ovlivnit jejich funkčnost
- útočník při tomto útoku se snaží odstranit, přidat nebo nějak změnit přenášená data
- existuje velká spousta druhů útoků, proto se zaměřím pouze na některé z nich:

1. **DoS**(odepření služby) a **DdoS**(distribuované odepření služby) útoky

- typ útoku na internetové služby/stránky, jehož cílem je znefunkčnit a znepřístupnit cílovou službu ostatním uživatelům
- extremní zatížení CPU cílového serveru

Typy Dos a DDoS útoků:
- Ping of death: útočník vytvoří abnormálně velký ping IP packet
- Teardrop attack: tento útok způsobí, že offsety se navzájem překrývají, napadený systém se pokusí pakety rekonstruovat ale selže, cílový systém je poté zmatený a zhroutí se

Možné obrany:
- Firewall

2. **MitM**(Man in the middle) útok

- k útoku MitM dojde, když se hacker vloží mezi komunikaci klienta a serveru

Typy MitM útoků:
- Session hijacking: v tomto typu útoku MitM útočník "unese" relaci mezi klientem a serverem, útočící pc nahradí svou IP adresu za klientovu, zatímco server pokračuje v relaci, věřící že komunikuje s klientem
- IP spoofing: používá útočník k přesvědčení systému, že komunikuje s důvěryhodnou entitou, a poskytuje útočníkovi přístup do sytému. Funguje to tak, že útočník odešle paket se zdrojovou IP adresou důvěryhodného hostitele namísto vlastní Ipadresy

Možné obrany:
- vzájemná výměna veřejných klíčů jiným, bezpečným kanálem
- ověřením získaných veřejných klíčů jiným způsobem
- voěřením klíčů pomocí el. podpisu obou účastníků

3. **Phishing** útok

- podvodná technika používaná útočníkem k získávání citlivých údajů
- principem phishingu je rozesílání e-mailů nebo odkazů, tento útok vyzývá adresáta k zadání osobních údajů na falešnou stránkz, která je velmi podobná té oficiální

Možné obrany:
- dodržování bezpečnostních pravidel, co nejméně poskytovat citlivé údaje
- pečlivé zkontrolování e-mailové adresy/domény

4. **SQL injection** útok

- napadení databázové vrsttvy programu vsunutím kódu přes neošetřený vstup a vykonání vlastního pozměňujícího poškozujícího SQL příkazu

Možné obrany:
-

5. **Malware** útok

- neboli škodlivý software je nežádoucí sw nainstalovaný ve vašm pc bez vašeho souhlasu

Možné obrany:
- antiwiry, nerozklikávat nedůvěryhodné odkazy

Firewally
- síťové zařízení, které slouží k řízení a zabezpečení síťového provozu
-

Demilitarizované zóny
-

ACL(acces control list)
- je sada dat informující os počítače, který následně uděluje uživatelům přístupová práva k určitým objektům v systému(např. k souboru nebo k adresáři)
- každý uživatel ma jedinečný atribut zabezpečení, které určuje, kteří uživatelé k němu mají přístup