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

Vnitřní

Ochrana:

- Fyzické zabezpečení (přístup do místnosti, izolace od rušení, záložní napájení, požární ochrana, náhradní díly)
- Operační systém (velká paměť, stabilní verze OS, záloha systému, zákaz nepoužívaných služeb, portů a rozhraní, způsob přihlášení a jeho logování, opatření proti zcizení hesla

Útoky:

1. **ARP soofing** – útočník pošle ARP REPLY (IP adresa brány + MAC adresu útočníka) + ARP REPLY (IP oběť + MAC adresa útočníka)
   Při komunikaci obě strany budou používat MAC adresu útočníka
2. **DHCP spoofing** – útočník má vlastní DHCP server a zasílá odpověď s IP adresou z odpovídajícího rozsahu, ale DNS server a výchozí brána mají IP adresu útočníka
3. **Přetečení zásobníku** – přetečení alokované paměti (např. ARP, směrovací tabulka)

Vnější

ochrana pomocí firewallu před útoky hrubou silou

Útoky:

1. **TCP SYN Flood** – množství polootevřených spojení TCP
2. **Smurf Attack** – ICMP zpráva na broadcastovou adresu s pozměněnou podvrhnutou zdrojovou IP adresou oběti
3. **Útok ze sítě Botnet** – ovládnutí velkého počtu strojů jako bílých koňů a útok na oběť
4. **Nákaza** z interních přenosných médií a externích zdrojů (**viry**, **červy**, **Trójské koně**)
5. **Phishing** – podvodná technika k vylákání citlivých údajů založená na sociálním inženýrství. společné znaky:
6. **Pharming** – podobná technice Phishing, podvodné stránky
7. **Útoky na webové aplikace –** Cross Site Scripting – narušení správné interpretace webových stránek využitím bezpečnostních chyb ve skriptech
8. **SQL Injection** – napadá databázové vrstvy přes vrstvu aplikační (např. špatně filtrované uživatelské vstupy, které jsou přímo vloženy do SQL dotazů)

Hraniční směrovač

1. **Single Router přístup** – bezpečnostní politiky jsou konfigurovány na tomto zařízení
2. **Defense-in-Depth přístup** – hraniční směrovač funguje v první linii obrany jako „screeening router“, druhou linií obrany je firewall
3. **Demilitarizovaná zóna (DMZ)** - střední prostor pro služby (servery), které musí zůstat přístupné z internetu pro vnější sítě a zároveň umožňuje vnitřní síti chráněný přístup přes firewall

Access control list

- Seznam podmínek pro propouštění nebo zahazování paketů.
- Podmínky jsou prováděny postupně, při shodě se paket propustí nebo zahodí, a další podmínky se už neprovádějí.
- Pokud se žádná podmínka neshoduje, paket se zahodí.

Pravidla použití:

- Na rozhraní se použije maximálně jeden ACL pro protokol (např. IP) a pro směr (příchozí, odchozí).
- ACL mohou filtrovat jednotlivé IP adresy (host) nebo celé sítě (s wildcard).
- Jednotlivé IP adresy se mají filtrovat před sítěmi.
- Příkaz "ALL" se používá pro všechny IP adresy.

Typy ACL

1. **Standardní (1-99):** Filtrování podle zdrojové IP adresy, umístěny co nejblíže cíli.
2. **Rozšířené (100-199):** Filtrování podle transportního (TCP, UDP, ICMP) nebo IP protokolu, zdrojové a cílové IP adresy, čísla portu nebo typu protokolu. Umístěny co nejblíže zdroji.
3. **Povolení všeho:** access-list "číslo" permit ip any any
4. **Pojmenované ACL:** Specifikace typu (standardní/rozšířené), např. zákaz HTTP na portu 80:
5. **Reflexivní ACL:** Blokují komunikaci z vnějšku, pokud nebyla zahájena z vnitřní sítě (kontrola TCP ACK/RST).
6. **Dynamické ACL:** Přístup umožněn po autentizaci přes Telnet, dynamická podmínka přidána do rozšířeného ACL.
7. **Časové ACL:** Kontrola přístupu podle času, např. přístup k internetu pouze o přestávkách.

Zabezpečení pomocí Firewallu

a) **Softwarové** – tvořeny SW službou na směrovači, zatěžují systémové prostředky.
b) **Hardwarové** – samostatné HW zařízení

Statefull firewall (stavový firewall)

Schopen určit, zda paket patří k existujícímu toku dat.

Výhody stavového firewallu:

- Filtruje nežádoucí provoz.
- Přísnější kontrolu bezpečnosti
- Zlepšuje výkon přes paketové filtry nebo proxy servery.
- Zabraňují falšování a DoS útoku
- Logování poskytuje více informací než filtrování paketů.

Nevýhody stavového firewallu:

- Nezabrání útokům na aplikační vrstvě
- Ne všechny protokoly jsou stavové (např. UDP, ICMP).
- Některé aplikace otevírají více připojení, které vyžadují zcela novou řadu otevřených portů.
- Nepodporují ověřování uživatelů