Zabezpečení sítí

Bezpečnostní služby v sítích

- Utajení a důvěrnost
- Řízení přístupu AAA – Authentication, Autorization, Accounting
- Integrita dat – zajištění že zpráva nebyla pozměněna
- Nepopiratelnost – dokázání, že odesílatel zprávu odeslal a příjemce ji přijmul

Útoky

- Průzkum sítě – neautorizovaný sběr informací
    - Například: hromadný ping
    - Ochrana: zakázání 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 informaceni), šifrování dat a autentifikace
- 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 cachovaných DNS záznamů, popřípadě útok na DNS server
    - Při překladu domény dostaneme podvodnou IP a připojíme se na špatnou stránku
    - Typické znaky: nezabezpečené připojení (http://), stránka nevypadá „správně“
    - Obrana: antivirové programy, dvoufázové přihlášení, VPN
- Cross Site Scripting (XSS) – podstrčení podvodného scriptu v jinak důvěryhodné stránce
    - Persistentní – podvodný kód je uložen přímo na severu 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

- 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

- 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, jejichž adresy zůstávají vnějšku skryté

Demilitarizovaná zóna

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