Základní pojmy týkající se bezpečnostních hrozeb:

- Hrozba: Událost nebo situace, která může způsobit poškození systému, dat nebo služeb.
- Zranitelnost: Slabá místa v systému, která mohou být zneužita pro útok.
- Riziko: Pravděpodobnost, že hrozba způsobí škodu, a velikost této škody.

Typy motivace kybernetických útoků:

- Finanční zisk: Například krádež finančních údajů nebo vydírání obětí.
- Ideologie: Například politické nebo náboženské motivace.
- Praktický zisk: Například získání přístupu k cenným informacím.
- Zábava: Například poškozování systémů nebo krádež dat pro potěšení.

Příklady základních nástrojů:

- Průzkum sítě - Nástroje pro průzkum sítě jsou používány ke zjištění topologie sítě a identifikaci aktivních zařízení v síti, jako jsou routery, přepínače a servery. Mezi nástroje pro průzkum sítě patří například nmap, ping a traceroute.
- Lámání hesel - Nástroje pro lámání hesel jsou používány k odhalení hesel a přístupových údajů. Tyto nástroje mohou být buď pasivní, jako jsou keyloggers, nebo aktivní, jako jsou programy pro hrubou silu. Mezi nástroje pro lámání hesel patří například John the Ripper, Hashcat a Cain and Abel.
- Úprava paketů - Nástroje pro úpravu paketů umožňují útočníkům modifikovat obsah paketů, které cestují přes síť. Tyto nástroje mohou být použity ke změně obsahu paketů a k manipulaci s komunikací mezi dvěma zařízeními. Mezi nástroje pro úpravu paketů patří například Wireshark a tcpdump.
- Odposlech - Nástroje pro odposlech jsou používány k zachytávání komunikace mezi dvěma zařízeními v síti. Tyto nástroje mohou být pasivní, což znamená, že jen zachytávají komunikaci, nebo aktivní, což znamená, že mohou manipulovat s komunikací. Mezi nástroje pro odposlech patří například tcpdump, Wireshark a Ettercap.
- Objev/zneužití zranitelnosti - Nástroje pro objev a zneužití zranitelnosti jsou používány k nalezení a využití chyb v softwaru nebo hardwaru. Tyto nástroje mohou být použity k získání neoprávněného přístupu k systému. Mezi nástroje pro objev a zneužití zranitelnosti patří například Metasploit, Nessus a Nmap.
- Šifrování - Nástroje pro šifrování jsou používány ke šifrování dat tak, aby byla komunikace mezi dvěma zařízeními bezpečná. Tyto nástroje mohou být použity k šifrování komunikace nebo k šifrování souborů. Mezi nástroje pro šifrování patří napří

Typy malwaru a běžné příznaky jeho přítomnosti:

- Viry: škodlivý software, který se šíří tím, že infikuje soubory a programy na počítači. Virus se aktivuje a šíří se při spuštění infikovaného souboru nebo programu. Běžné příznaky přítomnosti viru jsou zpomalení systému, nečekané změny v souborech a chování počítače, chyby při spouštění programů nebo odhalení neznámých procesů v Task Manageru.
- Trojské koně: škodlivý software, který se maskuje jako neškodný program a snaží se získat přístup k počítači. Trojský kůň se může šířit skrze infikované e-maily, webové stránky nebo přes malvéry. Běžné příznaky přítomnosti trojského koně jsou zpomalení systému, změna hesel, nečekané soubory a ikony na ploše, ovládání počítače zvenčí, získávání citlivých informací, jako jsou hesla nebo bankovní údaje.
- Červi: škodlivý software, který se šíří samostatně po síti nebo internetu a infikuje další počítače. Červ se může šířit pomocí zranitelností operačního systému nebo softwaru. Běžné příznaky přítomnosti červa jsou zvýšená aktivita sítě, přetížení síťového provozu, zpomalení systému, neznámé procesy v Task Manageru nebo vysoká zátěž procesoru.

- Ransomware: škodlivý software, který šifruje data na počítači a vyžaduje výkupné za jejich dešifrování. Ransomware se může šířit skrze infikované e-maily, webové stránky nebo přes malvéry. Běžné příznaky přítomnosti ransomware jsou nečitelné soubory, výzvy k zaplacení výkupného, omezený přístup k počítači nebo zablokování obrazovky.
- Spyware: škodlivý software, který sleduje a shromažďuje citlivé informace o uživateli a jeho počítači bez jeho vědomí. Spyware se může šířit skrze infikované e-maily, webové stránky nebo přes malvéry. Běžné příznaky přítomnosti spyware jsou změna nastavení webového prohlížeče, zpomalení systému.

Základní kategorie síťových útoků zahrnují:

- Průzkum (reconnaissance) - tento typ útoku spočívá v sběru informací o cílové síti, službách a systémech. Cílem útočníka je získat co nejvíce informací o cíli, aby mohl snadněji naplánovat další útoky.
- Získání přístupu (gaining access) - tento typ útoku spočívá v získání přístupu k cílovému systému nebo sítovým zařízením. Útočník může získat přístup prostřednictvím různých způsobů, například prostřednictvím exploitů, slabých hesel nebo sociálního inženýrství.
- Odepření služby (denial of service, DoS) - tento typ útoku spočívá v zablokování služeb nebo systémů v cílové síti tak, aby uživatelé nebyli schopni využívat služby. Útočník může použít různé metody, jako je zaplavení síťového toku nebo vyčerpání zdrojů cílového systému.

Několik příkladů útoků v rámci každé kategorie:

- Průzkum - port scanning, ping sweep, DNS enumeration, OS fingerprinting
- Získání přístupu - brute-force útoky na hesla, využití exploitů, sociální inženýrství, phishing
- Odepření služby - flood útoky, ping of death, syn flood, smurf attack
- TCP/IP protokoly jsou základem síťové komunikace a často jsou zneužívány útočníky k různým útokům:
- IP (Internet Protocol) - útočník může podvrhnout IP adresu a provádět tzv. IP spoofing, aby skryl svou identitu a provedl DoS útok.
- UDP (User Datagram Protocol) - útočník může využít UDP flood, což je DoS útok, který vyplní cílovou síť UDP pakety.
- TCP (Transmission Control Protocol) - útočník může využít TCP SYN flood, což je DoS útok, který vyčerpává zdroje cílového systému.
- ARP (Address Resolution Protocol) - útočník může využít ARP poisoning, což je útok, při kterém útočník ovládne ARP tabulku cílového zařízení a pak směruje provoz na svůj systém.
- Zneužití protokolu DNS k útokům
- Protokol DNS (Domain Name System) slouží ke konverzi doménových jmen na IP adresy. Zneužití tohoto protokolu se často vyskytuje v podobě DNS spoofingu, při kterém útočník manipuluje s DNS odpověďmi tak, aby byly směrovány na falešné IP adresy. Tento útok se často používá k přesměrování uživatelů na škodlivé webové stránky nebo k ukradení citlivých informací.
- Zneužití protokolu DHCP k útokům
- Protokol DHCP (Dynamic Host Configuration Protocol) slouží ke konfiguraci IP adres a dalších síťových nastavení na zařízeních v síti. Útočníci mohou zneužít tento protokol k přiřazení falešných IP adres, což může vést k odepření služby nebo k útoku typu man-in-the-middle.
- Zneužití protokolu HTTP k útokům

- Protokol HTTP (Hypertext Transfer Protocol) se používá ke komunikaci mezi webovými servery a klienty. Útočníci mohou zneužít tento protokol k útokům typu Cross-Site Scripting (XSS) nebo SQL injection, kdy se škodlivý kód vkládá do webových stránek a využívá se k útokům na uživatele.
- Zneužití protokolu SMTP k útokům
- Protokol SMTP (Simple Mail Transfer Protocol) slouží k přenosu emailů mezi servery. Útočníci mohou využít tento protokol k útokům typu phishing, kdy se vydávají za legitimní uživatele a snaží se uživatele nalákat k odkazům na falešné webové stránky, kde mohou být poškozeny.
- Zneužití protokolu SSH k útokům
- Protokol SSH (Secure Shell) se používá k zabezpečenému přístupu na vzdálený počítač. Útočníci mohou zneužít tento protokol k útokům typu brute force, kdy se pokouší uhádnout hesla k účtům, nebo k útokům typu man-in-the-middle, kdy útočník zachytává provoz mezi klientem a serverem.
- Zneužití protokolu SNMP k útokům
- Protokol SNMP (Simple Network Management Protocol) slouží k monitorování a správě síťových zařízení. Útočníci mohou využít tento protokol k útokům typu SNMP reflection, ento útok využívá chybně nakonfigurované síťové prvky, které umožňují SNMP dotazy z libovolné IP adresy. Útočník tedy může poslat dotaz s podvrženou IP adresou, který bude směřován na cílový server s vysokou propustností, což může vést k jeho přetížení a odmítnutí služeb pro legitimní uživatele.
-