**Kyberbezpečnost – kybernetické útoky**

**Útoky na síťovou infrastrukturu a serverové služby**

Typy:

**DoS** – zahlcení příjemce požadavky, které není schopen obsloužit (zpracovat), důsledkem jsou výpadky poskytovaných služeb, pády procesů, restarty

**DDoS** – funguje podobně jako DoS, k útoku je použito velké množství počítačů, důsledky stejné jako u DoS, mezi nejčastější typy útoků patří tzv. amplification attack

**Útoky:**

**Historické** – Ping of Death, Smurf attack

**PoD (Pinf of Death)** – využívá skutečnosti, že cílový systém může být zahlcen požadavky, kde velikost packetů přesahuje max. limit IP vrstvy (65536 B), takové packety se fragmentují a na straně příjemce se opět musí sestavit => přetečení bufferu, pády, zamrznutí, restarty. Moderní OS jsou proti tomuto historickému útoku dobře chráněné.

**Smurf attack** – využívá špatné konfigurace routerů, pokud špatně nastavený router přijme broadcast packet, rozešle ho na všechny hosty v subnetu. Paket obsahuje falešnou IP odesílatele (IP oběti), každý z hostů v subnetu pak pošle na adresu oběti odpověď (provoz se násobí).

**DNS amplification** – zneužití tzv. open DNS resolveru (špatně nakonfigurovaný DNS zneužitelný útočníkem, na takový DNS server posílá dotazy botnet, adresa odesílatele je zaměněná za adresu oběti, každý dotaz je sestaven tak, aby vracel co největší odpověď => zahlcení systému oběti

**NTP amplification** – funguje podobně jako DNS amplification, útočník opět zneužívá špatně nakonfigurovaný NTP server pro generování obrovského množství odpovědí, které jsou směrovány na IP adresu oběti

**SSDP attack** – zneužití protokolu UPnP, útočník posílá Discovery packet na všechna UPnP zařízení, jako adesa odesílatele je podstrčená adresa oběti, všechny UPnP zařízení pak směrují své odpovědi na oběť, odpovědi obsahují velké množství dat

**Application Layer attack** – zneužití aplikačního protokolu (např. http) k zasílaní falešných požadavků oběti ve velkém množství, velmi obtížná obrana proti tomuto typu útoku

**DNS flood** – zahlcení DNS resolveru velkým množstvím nekorektních požadavků, DNS server pak nemá kapacitu řešit regulérní dotazy klientů, není možné kontaktovat cílové servery

**SYN flood, ACK flood** – zneužití protokolu TCP, útočník posílá packety SYN pro navázání spojení, ale nečeká na odpověď, oběť naopak očekává další komunikaci dle třícestného handhaku, čímž vyčerpává své systémové prostředky

**Http flood, ICMP flood, UDP flood, QUIC flood** – všechny tyto útoky mají společné to, že se snaží zahltit oběť obrovským množstvím požadavků, které není schopná zpracovat, dochází k vyčerpání systémových prostředků

**Útoky na VLAN (VLAN hopping)**

**Switch spoofing** - útočník předstírá, že je switch s trunkovými porty, snaží se tak získat přístup ke všem VLAN. Tento typ útoku lze zneužít pouze, pokud jsou VLAN porty na switchi nastavené v módu dynamic.

**Double tagging** - útočník záměrně do rámce přidává dva TAGy místo jednoho, první je TAG VLAN, ke které se chce útočník dostat, druhý je jeho vlastní. Druhý TAG se na cílovém switchi stripuje, ale původní zůstává a má umožnit přístup do napadené VLAN. Tento typ útoku lze zneužít pouze na Trunk portu s nastavenou Native VLAN

**Útoky na wifi**

**Útoky na dostupnost wifi – mají charakter DoS útoků**

* **rušení (jamming)** – útočník generuje šum, který koliduje s wifi signálem, proti tomuto útoku je obtížná obrana, ale je velmi náročný na vybavení a potřebnou energii k provedení
* **probe request flooding** – útočník se snaží AP zahltit velkým množstvím dotazů na dostupné wifi sítě (probe request frame), AP vyčerpává své HW prostředky a není schopné standardní komunikace s klienty. Podobně se dají zneužít falešné požadavky na autentizaci klienta.
* **RTS/CTS flooding** – úmyslné blokování vysílací kapacity zasíláním velkého množství falešných požadavků na vysílání bez skutečného záměru začít vysílat

**Útoky typu Deauthentication/Disassociation**

Pomocí zfalšované MAC adresy posílá útočník požadavky na de-autentizaci nebo de-asociaci (odpojení) klienta. Útoky mají velkou efektivitu, můžou být zneužity k opakovanému odpojení jednoho i všech klientů daného APOD. V nových wifi standardech jsou rámce sloužící k těmto účelům lépe chráněné proti zneužití.

**Útoky MITM**

* **RougeAP** – záměrné připojení nezabezpečeného AP k síti, k takovému AP se pak může připojit útočník, který má přístup do sítě. Do této kategorie se řadí i špatně nakonfigurované AP a AP, nad kterými získal kontrolu útočník.
* **Honeypots** – falešné nezabezpečené AP provozované útočníkem, které vytváří dostupnou otevřenou wifi síť. Pokud se klient připojí k takovému AP, všechna jeho data tečou přes útočníka. Ochrana je použití TLS nebo VPN při připojování k veřejným otevřeným wifi sítím.
* **EvilTwin** – falešné AP se snaží předstírat, že je regulérní AP, které klient dobře zná. Důsledky jsou stejné jako u Honeypots.

**Útok na proces autentizace klienta**

* **KRACK – Key Reinstallation Attack –** útok na 4cestný handshake, který slouží k připojení klienta k síti a vygenerování šifrovacího klíče. Tento klíč slouží šifrování komunikace mezi klientem a AP, měl by být jedinečný pro daného klienta a neměl by se používat opakovaně. Útočník donutí klienta opakovat 3. a 4. krok handshaku, donutit klienta resetovat tento klíč, může mu vnutit jiný klíč, může sbírat data pro odhalení klíče celé relace a dešifrovat přenášená data. Je to chyba v návrhu WPA a WPA2 protokolu, změna hesla k síti nepomůže, účinný je pouze update zařízení od výrobce nebo používání TLS a VPN.

**Útoky na e-mailovou komunikaci**

**Phishing**

Útočník se snaží vylákat z oběti přihlašovací údaje k důležitým službám, čísla platebních karet apod. Zneužívá k tomu různé formy podvržené mailové komunikace:

**TGTBT** – neuvěřitelná nabídka

**Sense of Urgency** – útočník se snaží oběti vnutit pocit, že je potřeba něco urgentně udělat – výhodná nabídka, napadení účtu apod.

**podvodné odkazy** – za takovými odkazy se může ukrývat malware nebo např. falešné přihlašovací stránky k nějaké službě, kterou oběť používá.

**Ransom** – vylákání výkupného na základě fiktivní události

**Podvodné e-maily (falšování identity odesílatele)** – fiktivní informace o změně bankovního účtu obchodního partnera oběti apod.

**Útoky na autentizační údaje**

* **lámání hesel** – zneužívá zranitelnost slabých hesel. Je možné provádět slovníkové útoky, při kterých útočník postupně zkouší databázi známých hesel, nebo používá tzv. bruteforce attack, při kterém se snaží vypočítat všechna možná hesla pro zadanou znakovou sadu a délku hesla. BF attack je velmi náročný na výkon a trvá velmi dlouho. Pokud se útočník dostane k hash hodnotě hesla, které není ošetřeno metodou salt, lze použít i tzv. rainbow tables, což je databáze vygenerovaných hesel s použitím daného hashovacího algoritmu.
* **malware (keyloggery)** – útočník se snaží kompromitovat systém oběti a zachytávat stisknuté klávesy na klávesnici, případně odchytit např. PINy a hesla zadávaná na telefonu.
* **útoky MITM** – útočník se snaží zachytit nezabezpečená hesla nebo jejich hashované podoby na nezabezpečeném komunikačním kanálu.

**Útoky na SQL databáze**

* **SQL injection** – zneužití databázových aplikací se špatně ošetřenými uživatelskými vstupy. Útočník může pomocí speciálních řídících znaků jazyka SQL změnit podobu SQL dotazu, který se spouští na databázovém serveru tím, že do něj vloží vlastní části SQL kódu. Takto pozměněný dotaz může sloužit ke krádeži citlivých dat (uživatelské účty, platební karty), jejich pozměnění nebo destrukci. Pokud daná aplikace používá ještě neošetřená systémová volání, je možné i vzdáleně ovládnout napadený systém. Obranou proti tomuto typu útoku je filtrování a validace dat poslaných klientem, správné escapování speciálních znaků nebo parametrizace SQL dotazů. Vhodným řešením je i procedurální zpracování dat na straně DB serveru.