Slovník kybernetickej bezpečnosti pre kurz CyberOps Associate

Obsahom tohto dokumentu je slovník vysvetľujúci základné pojmy súvisiace s kyberbezpečnosťou, ktoré sú obsiahnuté v kurze CyberOps Associate. Slovník nie je zoradený abecedne, ale podľa postupnosti uvádzania pojmov v jednotlivých kapitolách kurzu.

Kapitola 1 – The Danger

- **Threat Actor**: Všeobecné pomenovanie pre osobu vykonávajúcu útok.
    - **Amateurs**: Tiež nazývané ako „Script Kiddies“ sú útočníci, ktorí majú malé technické znalosti a pre svoje útoky len využívajú existujúce nástroje vytvorené expertami.
    - **Hacktivists**: Útočníci, ktorí využívajú svoje schopnosti, aby poukázali na existujúce problémy v politickom/sociálnom prostredí... Ich činnosť zvyčajne pozostáva zo zverejnenia rôznych citlivých informácií v podobe článkov, videí, prípadne vykonanie DDoS útokov na zamedzenie činnosti, proti ktorej bojujú.
    - **Organized Crime Groups**: Organizované skupiny vykonávajúce pokročilé útoky s cieľom vlastného obohatenia.
    - **State-sponsored Groups**: Skupiny vykonávajúce útoky na pokyn vlády – najčastejšie špionáž iných krajín, ...
    - **Terorist Groups**: Vykonávajú činnosť porušujúcu zákon.
- **Threat Impact**: Dopad hrozieb, čo je možné chápať ako množinu a cenu škôd, ktoré by vznikli po vykonaní útoku na cieľový systém.
    - **PII (Personally Identifiable Information)**: Akákoľvek informácia, ktorá by dokázala jedinečne identifikovať danú osobu. Napríklad meno, číslo občianskeho, dátum narodenia, číslo kreditnej karty a pod.
    - **PHI (Protected Health Information)**: Jedná sa o údaje súvisiace so zdravotným stavom danej osoby. Je to podmnožina PII.
    - **PSI (Personal Security Information)**: Podmnožina PII. Predstavuje množinu dát súvisiacu s danou osobou, ktoré sa zvyknú používať pre získanie prístupu do informačných systémov. Napr. používateľské mena, heslá a pod.
- **Intellectual Property**: Duševné vlastníctvo (myšlienky, nápady, ...).

Kapitola 2 – Fighters in the War Against Cybercrime

- **SOC (Security Operations Center)**: Bezpečnostné operačné centrum. Jednotka pre ochranu cieľovej organizácie. SOC obsahuje podľa expertízy ľudí 3 hlavné vrstvy:
    - **Tier1 – Alert Analyst**: Úlohou je monitorovanie prichádzajúcich hlásení (alert) a ich overenie, či sa jedná o skutočné bezpečnostné incidenty. Ak áno, tak vzniknutý bezpečnostný tiket posúvajú ľuďom na Tier2.

    - **Tier2 – Incident Responser**: Úlohou je hĺbková analýza incidentov, vytvorenie rád pre nápravu a odstránenie škôd.
    - **Tier3 – Threat Hunter**: Osoby s najväčšou expertízou. Implementujú detekčné nástroje a ich úlohou je vyhľadať hrozby, ktoré do teraz neboli detegované.
    - **SOC Manager**: Riadi všetky zdroje SOC a predstavuje kontaktný bod.
- **SIEM (Security Information and Event Management)**: Systém, ktorého úlohou je zber, analýza, a klasifikácia dát z rôznych systémov (firewall, sieťové zariadenia, IDS, ...) za účelom detekcie a vyšetrovania hrozieb. Ďalšími vlastnosťami SIEM-u sú agregácia dát (zber dát z rôznych zdrojov), korelácia (spájanie súvisiacich dát) a analýza hlásení.
- **SOAR (Security Orchestration, Automation and Response)**: Systém s podobnými funkcionalitami ako SIEM, avšak navyše obsahuje: threat inteligence (spojenie s globálnou „inteligenciou" – napr. Cisco Talos, ...). Tiež obsahuje prvky automatizácie pre vyšetrovanie incidentov a vykonávanie akcií podľa vytvorených playbook-ov, ktoré sa vykonajú ako reakcia na detegované hrozby.
- **KPI (Key Performance Indicators)**: Metriky, ktorými je možné merať výkonnosť SOC.
    - **Dwel Time**: Čas, ktorý je útočník v systéme obete bez jeho odhalenia.
    - **MTTD (Mean Time to Detect)**: Doba trvania odhalenia prebiehajúceho incidentu.
    - **MTTR (Mean Time to Respond)**: Doba potrebná na zastavenie prebiehajúceho incidentu a vykonanie náprav.
    - **MTTC (Mean Time to Contain)**: Doba potrebná pre zastavenie incidentu tak, aby nemohol poškodzovať ďalšie zdroje.
    - **Time to Control**: Doba potrebná pre zastavenie šírenia škodlivého kódu v sieti.

Kapitola 3 – The Windows Operating System

Kapitola neobsahuje pojmy súvisiace s kyberbezpečnosťou. Je to prezentácia k vysvetleniu práce s OS Windows.

Kapitola 4 – Linux Overview

Kapitola neobsahuje pojmy súvisiace s kyberbezpečnosťou. Je to prezentácia k vysvetleniu práce s OS Linux.

Kapitola 5 – Network Protocols

- **Tracing the Path**: Proces stopovania komunikácie, počas ktorého dôjde k identifikácií zdroja, cieľa a sieťových zariadení, cez ktoré komunikácia prechádzala.

Kapitola 6 – Ethernet and Internet Protocol (IP)

Kapitola neobsahuje pojmy súvisiace s kyberbezpečnosťou. Je to prezentácia k Ethernetovej technológii a IP protokolu.

Kapitola 7 – Connectivity Verification

Kapitola neobsahuje pojmy súvisiace s kyberbezpečnosťou. Je to prezentácia k protokolu ICMP.

Kapitola 8 – Address Resolution Protocol

- **ARP Spoofing**: Útok založený na tom, že útočník sfalšuje údaje v ARP odpovedi, ktorú následne odosiela do siete.
- **ARP Poisoning**: Je dôsledok ARP Spoofing-u, kedy po prijatí falošného mapovania medzi IP a MAC dôjde k otráveniu ARP tabuľky falošným záznamom.
- **DAI (Dynamic ARP Inspection)**: Ochranný mechanizmus, ktorý nedovolí útočníkovi odoslať ARP odpoveď s falošným mapovaním. Je založený na DHCP Snooping Binding databáze, kde na základe údajov z tejto tabuľky sa porovnávajú údaje v tele ARP odpovede. Falošné ARP správy sú následne zahadzované rozhraním prepínača, na ktorom je spustený mechanizmus DAI.

Kapitola 9 – The Transport Layer

Kapitola neobsahuje pojmy súvisiace s kyberbezpečnosťou. Je to prezentácia k protokolom TCP a UDP.

Kapitola 10 – Network Services

Kapitola neobsahuje pojmy súvisiace s kyberbezpečnosťou. Je to prezentácia k protokolom DHCP, DNS, NAT, FTP, POP, IMAP, SMTP a HTTP.

Kapitola 11 – Network Communication Devices

Kapitola neobsahuje pojmy súvisiace s kyberbezpečnosťou. Je to prezentácia k vysvetleniu funkcie koncových zariadení, smerovačov, prepínačov, VLAN, protokolu STP a Wi-Fi technológie.

Kapitola 12 – Network Security Infrastructure

- **Public Zone**: Zóna obsahujúca verejne dostupné zariadenia – štandardne vonkajší svet / internet.
- **Private Zone**: Zóna obsahujúca súkromné zdroje organizácie. Nazývaná aj dôveryhodná zóna. Z vonka siete do nej nie je povolený prístup. Komunikácia je povolená len z vnútra zóny smerom von + povolené sú odpovede na nadviazanú komunikáciu.
- **DMZ (Demilitarized Zone)**: Zóna, do ktorej je možný prístup ako zo súkromnej tak aj verejnej zóny. Avšak z DMZ nie je priamo povolený prístup do súkromnej zóny. Štandardne sa v nej nachádzajú servery, ktoré chceme, aby boli prístupné z internetu.
- **Firewall**: Sieťové zariadenie slúžiace na filtrovanie sieťovej prevádzky. Štandardne sa nachádza na okraji siete.
    - **ZPF (Zone-based Policy Firewalls)**: Firewall, pracujúci so zónami, kde každý zdroj/sieť sa nachádza v nejakej zóne, pričom sa na Firewall-e následne explicitne definujú podmienky, medzi akými zónami je možná aká komunikácia.

- **Stateless Firewall (Packet Filtering)**: Firewall pracujúci na 3 a 4 vrstve OSI modelu. Jeho úlohou je filtrovanie prevádzky na náklade zdrojovej/cieľovej IP, zdrojového/cieľového portu a čísla protokolu.
- **Stateful Firewall:** Firewall pracujúci na 3, 4 a 5 vrstve OSI modelu. Najpoužívanejší typ firewall-u, umožňujúci pracovať s tabuľkou nadviazaných spojení vzhľadom k čomu dokáže povoľovať aj odpovede na nadviazané spojenia z vnútra siete.
- **Application Gateway Firewall (Proxy Firewall)**: Podobný ako Statefull Firewall, no navyše umožňuje pracovať aj so 7 vrstvou OSI modelu, čím umožňuje pracovať priamo so samotným obsahom prenášaných správ (payload) a tak vykonávať hĺbkovú kontrolu.
- **NGFW (Next-generation Firewalls)**: Oproti aplikačnému Firewall-u obsahuje navyše integrovanú IPS (Intrusion Prevention) funkcionalitu, blokovanie aplikácií, pripojenie sa ku globálnej inteligencií bezpečnostných riešení, ...
- **Host-based Firewall**: Softvér spustený na koncových zariadeniach (PC/Server).
- **Transparent Firewall**: Zvyčajne hardvérové zariadenie filtrujúce prevádzku medzi dvojicou rozhraní.
- **Hybrid Firewall**: Kombinácia predošlých dvoch typov firewall-ov.

- **IPS (Intrusion Prevention System)**: Systém, cez ktorý prechádza všetka komunikácia. Táto komunikácia je analyzovaná na rôzne bezpečnostné hrozby a v prípade odhalenia hrozby dochádza k okamžitému zastaveniu komunikácie, čo umožňuje predchádzať útokom.
  - **Host-based IPS**: Kontrola vykonávaná na koncovom zariadení.
  - **Network-based IPS**: Kontrola vykonávaná na sieťovom zariadení – štandardne pred vstupom do súkromnej zóny.
- **IDS (Intrusion Detection System)**: Systém, na ktorý sa odosielajú kópie prenášanej komunikácie. Úlohou tohto systému je následne zozbierané dáta analyzovať a v prípade odhalenia hrozby vygenerovať upozornenie a notifikovať o tejto udalosti zodpovedné entity.
- **AMP (Cisco Advanced Malware Protection)**: Riešenie pre pokročilú analýzu softvéru a tvorbu ochranných systémov. Obsahuje funkcionality potrebné pred, počas a po skončení útoku.
- **WSA (Cisco Web Security Appliance)**: Systém umožňujúci pokročilú kontrolu Web-ovej komunikácie, či už prichádzajúcej, alebo odchádzajúcej z chráneného prostredia.
- **ESA (Cisco Email Security Appliance)**: Systém umožňujúci pokročilú kontrolu Email-ovej komunikácie, či už prichádzajúcej, alebo odchádzajúcej z chráneného prostredia.
- **VPN (Virtual Private Network)**: Technológia umožňujúca vytvorenie virtuálneho tunelu medzi dvojicou bodov, pričom na transport je použitá nezabezpečená sieť, napr. Internet. Vytvorený tunel je následne možné zabezpečiť šifrovaním a tým vytvoriť bezpečný komunikačný kanál.

Kapitola 13 – Attackers and Their Tools

- **Asset**: Akýkoľvek zdroj, ktorý má pre nás hodnotu a je ho potrebné chrániť (dáta, servery, databáza, zamestnanci, ...).
- **Threat**: Možné nebezpečenstvo – napr. ak máme uložené dáta v nezašifrovanej podobe, tak hrozbou je, že ak sa útočník dostane k dátam, tak ich bude vedieť čítať a teda zneužiť.
- **Vulnerability**: Zraniteľnosť v systéme. Napr. uložené dáta v čitateľnej podobe je zraniteľnosť nášho systému, ktorá môže byť zneužitá.

- **Attack Surface**: Celková množina zraniteľností, cez ktoré sa môže dostať útočník k našim chráneným zdrojom.
- **Exploit**: Mechanizmus / nástroj / škodlivý kód, ktorý dokáže zneužiť zraniteľnosť nášho systému s cieľom dostať sa k chráneným zdrojom.
- **Risk**: Pravdepodobnosť, že daná zraniteľnosť bude zneužitá, vzhľadom k hodnote zdroja, ku ktorému dá útočníkovi prístup. Systém s číslami účtov je pre útočníka lákavejší, ako jedálny lístok v reštaurácii.
    - **Risk Acceptance**: Ak je cena rizika menšia, ako jeho riadenie, tak sa je s daným rizikom možné zmieriť a akceptovať ho. Ak by cena zabezpečenia bola vyššia ako cena chráneného zdroja, tak nemá zmysel investovať financie a čas do zabezpečenia.
    - **Risk Avoidance**: Proces, kedy robíme všetko pre to, aby sme predišli rizikám, aj za cenu, že prestaneme využívať isté služby a vykonávať isté aktivity (tým ale prichádzame o isté výhody).
    - **Risk Reduction**: Najpoužívanejšia stratégia riadenia rizika, kedy sa snažíme čo najviac redukovať riziká s tým, že sa hľadá optimálna cesta medzi obmedzovaním aktivít a zvýšením bezpečnosti.
    - **Risk Transfer**: Ak nemáme zdroje na riadenie rizika, tak je možné zodpovednosť za riziko presunúť na tretie strany, ktoré takéto služby poskytujú.
- **Countermeasure**: Protiopatrenie / procedúra, ktorú je možné vykonať, aby došlo k ochráneniu zdrojov a redukovaniu rizika.
- **Impact**: Dopad / potenciálne poškodenie chránených zdrojov v prípade vykonania útoku.
- **White Hat Hackers**: Etický hacker, ktorý využíva svoje programátorské schopnosti pre pomoc a vykonávanie etickej činnosti.
- **Gray Hat Hackers**: Vykonávajú kriminálnu činnosť / porušujú etiku – napr. zaútočia na chránený systém, s cieľom poukázať na niečo (znečisťovanie prírody, ...), no robia to bez vlastného obohatenia.
- **Black Hat Hackers**: Vykonávajú neetickú kriminálnu činnosť s cieľom obohatiť sa (krádež peňazí).
- **Script Kiddies**: Útočníci s malými schopnosťami, ktorí len využívajú existujúce nástroje.
- **Vulnerability Brokers**: Gray Hat, ktorí sa snažia objaviť zraniteľnosti v systémoch, ktoré následne nahlásia výrobcovi so snahou získať finančnú odmenu.
- **Hacktivists**: Gray Hat, ktorí sa snažia poukázať na existujúce problémy v spoločnosti v podobe protestov, zverejňovania usvedčujúcich informácií a pod.
- **Cybercriminals**: Black Hat, ktorý vykonávajú kriminálnu činnosť s cieľom sa obohatiť. Porušujú zákon.
- **State-sponsored**: Štátom sponzorovaný útočníci s cieľom získavania informácií a špionáže smerom k iným konkurenčným krajinám a pod.
- **IOC (Indicators of Compromise)**: Záznamy o uskutočnenom útoku. Obsahujú identifikátor škodlivého kódu, IP adresy serverov, názvy súborov, charakteristiku vykonaných zmien v systéme. Slúži ako dokumentácia toho, čo sa udialo počas útoku.
- **IOA (Indicators of Attack)**: Záznam obsahujúci motív a stratégie na pozadí útoku spolu s identifikáciou útočníka. Pomáhajú vytvárať proaktívne bezpečnostné prístupy.
- **Security Tools**: Nástroje pre vykonávanie penetračných testov s cieľom odhalenia existujúcich zraniteľností.
    - **Password Crackers**: Nástroje na prelomenie hesiel.

    - **Wireless Hacking Tools**: Nástroje na vniknutie do bezdrôtových sietí a nájdenie ich zraniteľností.
    - **Network Scanning and Hacking Tools**: Nástroje na detekciu aktívnych zariadení, povolených portov, ...
    - **Packet Crafting Tools**: Nástroje na tvorbu vlastných dátových jednotiek s cieľom testovania dier vo Firewall-och.
    - **Packet Sniffers**: Nástroje na odchytávanie sieťovej prevádzky a analýzu odchytených dát.
    - **Rootkit Detectors**: Nástroje na kontrolu integrity súborov a adresárov s cieľom objavenia existencie rootkit škodlivého kódu.
    - **Fuzzers to Search Vulnerabilities**: Nástroje na objavenie zraniteľností v počítačových systémoch.
    - **Forensic Tools**: Nástroje na nájdenie a zaznamenanie evidencie dôkazov z informačných systémov.
    - **Debuggers**: Používané Black Hat na vykonávanie reverzného inžinierstva a na písanie exploitov. Používané tiež White Hat hackermi na analýzu škodlivého kódu.
    - **Hacking OS**: Operačné systémy s predinštalovanými nástrojmi na penetračné testovanie – napr. Kali Linux.
    - **Encryption Tools**: Nástroje na šifrovanie dát.
    - **Vulnerability Exploitation Tools**: Nástroje na testovanie zraniteľností na cieľových systémoch – napr. Metasploit.
    - **Vulnerability Scanners**: Nástroje na skenovanie siete a identifikáciu otvorených portov.
- **Eavesdropping Attack**: Odpočívacie útoky, kedy útočník odchytáva komunikáciu a snaží sa z nej získať dôverné informácie.
- **Data Modification Attack**: Útok, kedy útočník odchytí prenášané dáta, pozmení ich a odošle na cieľový systém.
- **IP Address Spoofing Attack**: Útoky, v ktorých útočník nahrádza štandardne zdrojovú adresu v prenášaných paketoch tak, aby sa javili, že pochádzajú od dôveryhodného zdroja.
- **Password-based Attacks**: Útoky cielené na lámanie hesiel s cieľom získania neautorizovaného prístupu do systému.
- **DoS (Denial-of-Service) Attack**: Útok snažiaci sa zahltiť cieľový systém tak, aby nedokázal poskytovať svoje služby bežným používateľom.
- **MiTM (Man-in-the-Middle) Attack**: Útok, kedy sa útočník snaží presmerovať komunikáciu tak, aby prechádzala cez neho. V komunikácií sa teda útočník dostane medzi reálny zdroj a cieľ komunikácie.
- **Compromised Key Attack**: Útok spočívajúci v získaní tajného kľúča, ktorý sa používa napr. na šifrovanie prenášanej komunikácie. V takom prípade môže útočník získať prístup k dátam, ktoré sa prenášanú v šifrovanej podobe a tým narušiť dôvernosť komunikácie.
- **Sniffer Attack**: Útok s cieľom odchytiť, prečítať a uložiť prenášané dáta s možnosťou ich analýzy.

Kapitola 14 – Common Threats and Attacks

- **Viruses**: Vírus – škodlivý kód, ktorý potrebuje k svojej existencii hostiteľský súbor, po spustení ktorého dokáže vykonávať vlastnú škodlivú činnosť.

- **Trojan Horses**: Trójsky kôň, je softvér, ktorý sa tvári ako užitočná aplikácia, no má v sebe skrytú funkcionalitu, ktorá dokáže vykonať škodlivú činnosť (umožniť vzdialený prístup, odosielať dáta, mazať súbory, vypnúť bezpečnostný softvér, vykonať DoS, odchytávať stlačené klávesy, ...).
- **Worms**: Červ je škodlivý kód, ktorý dokáže existovať ako samostatná jednotka a je prispôsobený tak, aby sa dokázal veľmi rýchlo šíriť využitím počítačovej siete.
- **Ransomware**: Škodlivý kód, ktorý zašifruje používateľské dáta a následne žiada od používateľa výkupné (často v podobe kryptomien), po zaplatení ktorého by mala dostať obeť kľúč na dešifrovanie svojich dát.
- **Malware**: Všeobecné pomenovanie pre škodlivý kód.
    - **Scareware**: Škodlivý kód, ktorý sa snaží vystrašiť obeť – napr. výhražnou správou, že pokiaľ nevykoná nejakú činnosť do pár sekúnd, tak sa vykoná činnosť, ktorá by poškodila dobré meno obete, alebo nejakým spôsobom poškodí počítač a pod.
    - **Phishing**: Snaha získať od používateľa citlivé informácie. Štandardná forma je, že obeť útoku dostane email zo „svojej" banky, v ktorom je požiadaná o overenie svojej totožnosti zaslaním svojich prihlasovacích údajov.
    - **Rootkits**: Škodlivý kód, ktorý po svojej inštalácií dokáže skrývať svoju existenciu – maže logy, upravuje výpisy tak, aby ho nebolo vidieť. Veľmi náročné na nájdenie a odstránenie.
    - **Spyware**: Škodlivý kód, ktorý sleduje používateľskú aktivitu. Odchytáva stlačené klávesy, odosiela históriu prehľadávania, kradne cookies, ...
    - **Adware**: Škodlivý kód, ktorý zobrazuje neúmerné množstvo reklamných správ, s cieľom zistenia používateľských záujmov, ...
- **Reconnaissance Attacks**: Prieskumnícky útok, ktorým sa útočník snaží získať čo možno najviac informácií o cieľovom systéme.
    - **Internet Information Queries**: Na získavanie informácií použije útočník internet. Získanie informácií ako registrovaná doména, IP adresy serverov, email kontakty na zamestnancov firmy, ...
    - **Ping Sweep**: Útok, kedy útočník vykoná odoslanie Ping požiadavky na celú sieť. IP adresy, z ktorých mu príde odpoveď znamenajú identifikáciu aktívnych zariadení, na ktoré je možné následne cielene útočiť.
    - **Port Scan**: Útok na zistenie, aké služby sú spustené na aktívnych zariadeniach.
- **Access Attacks**: Útoky pre získanie prístupu do systému.
    - **Password Attacks**: Umožňujú získať prístup do systému prelomením hesiel.
    - **Spoofing Attacks**: Útočník sa do systému snaží dostať falšovaním údajov ako sú IP adresy, MAC adresy, falošné ARP záznamy, ...
    - **Trust Exploitation**: Útok založený na zneužití toho, že je v sieti zariadenie, ktorému dôverujú iné zariadenia (ciel útoku). Ak sa podarí útočníkovi získať prístup na menej zabezpečené zariadenie, ktorému dôverujú ďalšie zariadenia, tak to útočníkovi následne umožní jednoduchší prístup k viac zabezpečeným zariadeniam (primárny cieľ útoku).
    - **Port Redirection**: Presmerovanie portov, kedy sa najskôr útočník napr. využitím protokolu SSH dostane na kompromitované zariadenie, z ktorého mu je následne povolený prístup na ďalšie zariadenia už napr. protokolom Telnet.
    - **Buffer overflow**: Útok využívajúci pretečenie zásobníka, ktorý umožní prepísať pamäť zariadenia tak, že prepíše návratovú hodnotu funkcie na hodnotu v pamäti, kde je uložený škodlivý kód.

- **Social Engineering**: Prístupový útok snažiaci sa manipulovať obete využitím rôznych psychologických trikov.
  - **Pretexting**: Útok formou správy, kedy útočník žiada potvrdenie identity používateľa na základe jeho prihlasovacích údajov.
  - **Phishing**: Snaha získať od používateľa citlivé informácie. Štandardná forma je, že obeť útoku dostane email zo „svojej" banky, v ktorom je požiadaná o overenie svojej totožnosti zaslaním svojich prihlasovacích údajov.
  - **Spear Phishing**: Email odosielaný obeti je „ušitý na mieru" prispôsobený obeti tak, aby ju v čo najväčšej miere zaujal a pripadal čo najmenej podozrivý.
  - **Spam**: Nevyžiadaná emailová správa obsahujúca škodlivé linky, škodlivý kód, prípadne nevhodný obsah.
  - **Something for Something**: Útočník ponúka obeti výhru „stal sa 10 000 používateľom", no na jej doručenie potrebuje od používateľa informácie ako email, číslo účtu a pod.
  - **Baiting**: Útočník nechá pohodené USB, ktoré obsahuje škodlivý kód, na verejne dostupnom mieste, z ktorého si ho väčšina ľudí zoberie a po pripojení do svojho PC umožní útočníkovi vykonávať jeho aktivitu.
  - **Impersonation**: Útočník sa tvári, že je niekto iný, aby si získal dôveru obete. Môže napr. prísť ako údržbár do firmy, prípadne telefonovať obeti ako jej rodinný príslušník a pod.
  - **Tailgaiting**: Útočník rýchlo nasleduje dôveryhodnú osobu tak, aby sa napr. vyhol kamerovým systémom, prešiel turniketom a pod.
  - **Shoulder Surfing**: Útočník pozerá obeti cez plece so snahou zapamätať si zadávané heslá a pod.
  - **Dumpster Diving**: Útočník prehľadáva smetné koše s cieľom nájsť papieriky s heslami, emailovými adresami a pod.
- **DoS (Denial of Service) Attack**: Útok s cieľom zamedziť prístup k službám obete.
  - **Overwhelming Quantity of Traffic**: Útočník generuje neúmerné množstvo dát, ktorým sa snaží zahltiť zariadenie obete.
  - **Maliciously Formatted Packets**: Útočník odošle na zariadenie obete škodlivo upravenú dátovú jednotku s cieľom spôsobenia neštandardného správania sa cieľového zariadenia (nevie, čo s prijatými dátami spraviť), prípadne jeho úplné znefunkčnenie.
  - **Ping of Death**: Útočník pošle na cieľové zariadenie ICMP správu, v ktorej bude paket, ktorého veľkosť je väčšia ako maximálna možná.
- **DDoS (Distributed Denial of Service) Attack**: Útok ako DoS, ktorý ale prichádza z veľkého množstva zariadení.
  - **Zombies**: Skupina kompromitovaných zariadení – sú pod kontrolou útočníka.
  - **Bots**: Škodlivý kód navrhnutý tak, aby infikoval cieľové zariadenia a umožnil ich ovládať.
  - **Botnet**: Skupina infikovaných zariadení (Zombies).
  - **Handlers**: C&C (Command and Control) systém, z ktorého môže útočník komunikovať s každým infikovaným zariadením a odosielať mu riadiace príkazy.
  - **Botmaster**: Útočník riadiaci útok.
- **Evasion Methods**: Metódy, ktorými sa útočník snaží skryť svoju škodlivú aktivitu.

- **Encryption**: Šifrovaním môže útočník skryť čo prenáša, či sa jedná o škodlivý kód, alebo o ukradnuté citlivé dáta.
- **Tunneling**: Zabalením škodlivého obsahu napr. do protokolov ICMP, DNS a pod., ktoré sú bežné sieťové protokoly, môže útočník bez pozorovania preniesť dáta do alebo von z chránenej zóny.
- **Resource Exhaustion**: Útočník vykoná útok a zahltí bezpečnostné systémy tak, aby následne mohol vykonať svoj útok bez toho, aby bol spozorovaný.
- **Traffic Fragmentation**: Útočník rozdelí obsah, ktorý chce preniesť do veľkého množstva malých dátových jednotiek, ktoré nezávisle od seba prenesie sieťou.
- **Protocol-level Misinterpretation**: Útočník pozmení isté polia v hlavičkách dátových jednotiek (kontrolný súčet, TTL, ...) tak, aby spôsobil, že firewall bude tieto dáta ignorovať.
- **Traffic Substitution**: Snaha oklamať IPS systémy obfuskáciou – napr. zakódovať prenášaný obsah iným formátom (Unicode – ASCII, ...).
- **Traffic Insertion**: Útočník vloží medzi škodlivý obsah niekoľko bajtov navyše tak, aby zmenil vzor prenášaných dát a tým sa vyhol zhode s detekčnými pravidlami.
- **Pivoting**: Útočník infikuje zariadenie nachádzajúce sa vo vnútornej (dôveryhodnej) zóne. Z týchto zariadení následne vykonáva svoje útoky ďalej. Ako zdroj útoku sa následne javí infikované zariadenie a nie pôvodný útočník.
- **Rootkits**: Komplexný nástroj navrhnutý tak, aby za sebou automaticky skrýval všetky stopy a zmeny, ktoré vyvolal v OS.
- **Proxies**: Útok založený na využití proxy zariadenia, cez ktoré útočník prenáša svoje dáta a tým skrýva svoju skutočnú identitu.

Kapitola 15 – Network Monitoring and Tools

- **TAP (Test Access Point)**: Hardvérové zariadenie pracujúce na 1. vrstve OSI modelu umožňujúce kopírovanie prevádzky prichádzajúce jedným rozhraním a ich odosielanie iným rozhraním. Výhodou oproti SPAN (Switch Port Analyzer) prístupu je, že dokáže mirorovať aj poškodené dáta, ktorým nesedí kontrolný súčet, prípadne majú iné poškodenie.
- **ELK (Elasticsearch, Logstash, Kibana)**: Je trojica nástrojov umožňujúca rýchle vyhľadávanie, prácu s dátami a ich vizualizáciu.
- **Flow Stitching**: Zoskupovanie individuálnych záznamov do dátových tokov.
- **Flow Deduplication**: Filtrovanie duplicitných vstupných záznamov prichádzajúcich od viacerých NetFlow klientov.
- **NAT Stitching**: Zjednodušovanie tokov obsahujúcich NAT záznamy.