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 16 – Attacking the Foundation

- **Amplification Attack**: Útok kedy útočník odošle správu veľkému množstvu zariadení (správu ktorá vyžaduje odpoveď – napr. echo request), pričom ako zdrojovú adresu uvedie adresu obete. Výsledkom útoku je, že malou dátovou jednotkou útočník podmieni vznik veľkého množstva dát.
- **Reflection Attack**: Veľké množstvo zariadení odpovedá (odrazí) zariadeniu obete.
- **Spoofing Attack**: Útok, pri ktorom dochádza k falšovaniu – štandardne zdrojovej/cieľovej IP adresy.
    - **Non-blind Spoofing**: Falšovanie adresy, kedy útočník chce, aby mu prišla odpoveď na ním inicializovanú komunikáciu. Štandardne falšujeme cieľovú adresu – napr. pri testovaní pravidiel firewall-u a pod.
    - **Blind Spoofing**: Útočník nechce prijímať odpovede na ním inicializovanú komunikáciu. Štandardne falšuje zdrojovú adresu, na ktorú chce, aby prichádzali odpovede – adresa obete. Používané pri DoS útokoch.
- **TCP SYN Flood Attack**: Útočník odosiela dátové jednotky s nastaveným SYN flagom s cieľom vyžiadania procesu pre nadviazanie TCP 3-way handshake-u. Cieľom je vyčerpať zdroje cieľa a zabrániť vytváraniu TCP spojení s reálnymi používateľmi.
- **TCP Reset Attack**: Útočník odosiela dátové jednotky s nastaveným RST flagom s cieľom ukončovať aktívne vytvorené TCP spojenia, čím spôsobí dočasný výpadok služieb, potrebu opätovného vytvárania TCP spojenia a tým zvýšenie vyťaženia systémových prostriedkov cieľového servera.
- **TCP Session Hijacking**: Útok s cieľom zapojiť sa do existujúcej komunikácie a odosielať dáta na server využitím aktívneho TCP spojenia ako autentifikovaný používateľ. K tomuto útoku potrebuje útočník sfalšovať IP adresu niektorého z hostov, odhadnúť nasledujúce sekvenčné číslo a odoslať ACK ďalším hostom. Po úspešnej realizácií dokáže útočník odosielať dáta na server, no nedokáže prijímať odpovede.
- **UDP Flood Attacks**: Odosielanie veľkého množstva UDP správ na čo možno najväčšie množstvo cieľových zariadení. Využíva sa pri DoS útokoch.

Kapitola 17 – Attacking What We Do

- **ARP Cache Poisoning Attack**: Útok, ktorého cieľom je otráviť ARP tabuľku obete falošným ARP záznamom.
- **DNS Open Resolver Attacks**: Útoky na Open DNS Resolver zariadenia (poskytujú služby okolitému svetu – nie len svojej doméne) – napr. Google DNS.
    - **DNS Cache Poisoning Attack**: Útok, ktorého cieľom je otráviť DNS tabuľku DNS resolvera, ktorý následne odošle používateľovi falošný DNS záznam, ktorý ho presmeruje napr. na IP adresu servera s škodlivým obsahom.
    - **DNS Amplification and Reflection Attack**: Útočník odošle DNS požiadavku DNS resolveru, pričom ako zdrojovú IP adresu použije adresu obete. DNS odpoveď je niekoľko násobne väčšia ako DNS požiadavka, čím sa niekoľko krát znásobí sila útoku.
    - **DNS Resource Utilization Attack**: Útočník zahltí DNS resolver množstvom správ, čím znemožní jeho funkčnosť, vzhľadom k čomu ani používatelia nedostanú odpovede na svoje požiadavky.
- **DNS Stealth Attacks**: Útoky, vďaka ktorým sa útočníci snažia skryť svoju aktivitu, aby neboli vystopovateľní.
    - **Fast Flux**: Útok na skrývanie pozície (adresy) zariadenia, z ktorého útočník doručuje phishingové maily / škodlivý kód. Útočník veľmi často mení DNS záznamy – k jednej DNS doméne je priradené veľké množstvo IP adries, ktoré sa často menia.
    - **Double IP Flux**: Útočník často mení mapovanie domény k IP adrese, pričom zároveň mení aj autoritatívny DNS server.
    - **Domain Generation Algorithms**: Technika využívajúca v škodlivom kóde, ktorá umožňuje náhodne generovať názvy domén, ktoré sú následne použité ako randezvous point k ich C&C serverom.
- **DNS Domain Shadowing Attacks**: Útočník získa prístupové údaje vlastníka nejakej domény. Následne využitím týchto údajov vytvorí množstvo sub-domén, ktoré budú ukazovať na servery s škodlivým obsahom, pričom nijakým spôsobom nezmenia údaje v rodičovskej doméne.
- **DNS Tunneling**: Útočník odosiela DNS požiadavky z vnútra napadnutej siete smerom von, pričom v DNS požiadavkách upraví hodnoty v DNS záznamoch tak, že v nich prenesie smerom von citlivé informácie. Útoku sa dá zabrániť tak, že v čase útoku bude blokované odosielanie DNS požiadaviek, alebo tak, že bude kontrolovaný až samotný obsah DNS požiadaviek.
- **DHCP Spoofing Attacks**: Útok, počas ktorého útočník urobí zo seba DHCP server a odosiela používateľom DHCP odpovede s falošnými údajmi (falošná brána, falošný DNS server, falošná IP adresa).
- **Common HTTP Exploits**: Bežné nástroje, využívajúce útočníkom, založené na HTTP protokole.
    - **Malicious iFrame**: iFrame je HTML element, ktorý umožňuje načítať prehliadaču z danej zobrazenej stránky inú, škodlivú stránku, čo môže spôsobiť stiahnutie škodlivého kódu.
    - **HTTP 302 Cushioning**: Útočník zneužije návratovú hodnotu Status kód 302, ktorá umožní presmerovať požiadavku na načítanie stránky na inú adresu. Tento proces sa môže opakovať viac krát, kde finálna URL adresa bude predstavovať stránku s škodlivým obsahom.
    - **Domain Shadowing**: Útočník získa prístupové údaje vlastníka nejakej domény. Následne využitím týchto údajov vytvorí množstvo sub-domén, ktoré budú ukazovať na servery

s škodlivým obsahom, pričom nijakým spôsobom nezmenia údaje v rodičovskej doméne. Po označení danej domény ako škodlivej útočník jednoducho vytvorí ďalšie subdomény.

- **Email attacks**: Útoky využívajúce email-ovú komunikáciu.
  - **Attachment-based Attacks**: Útočník pridá škodlivý obsah do prílohy emailu.
  - **Email Spoofing**: Útočník sfalšuje zdroj (odosielateľa) emailu s cieľom získania citlivých informácií od obete (príjemca).
  - **Spam Email**: Útočník odošle nevyžiadaný email obsahujúci reklamy / škodlivú prílohu / odkazy na škodlivé stránky.
  - **Open Mail Relay Server**: Sú to SMTP servery, ktoré umožňujú komukoľvek odosielať emaily, čo môžu zneužívať aj útočníci na skrytie svojej identity.
- **Code Injection**: Útočník vloží na webovú stránku škodlivý kód, ktorý sa u obete vykoná s právami, aké má webová aplikácia. Útok je možný kvôli slabej validácií vstupu.
- **SQL Injection**: Útočník zadá do prihlasovacieho formulára škodlivo upravený SQL dotaz, ktorého výsledkom pri slabej validácií vstupu môže byť zobrazenie celého obsahu databázy (mená, heslá, emaily, ...) používanej daným webom.
- **XSS (Cross Site Scripting)**: Útok kedy útočník zadá napr. do časti komentáre na webovom portály škodlivý vstup v podobe JavaScriptu. Následne obeť keď sa pripojí k danej stránke, stiahne si obsah komentárov, čo môže na strane klienta spôsobiť vykonanie škodlivého skriptu. Tento typ útoku je znova možné ošetriť dôslednou validáciou vstupu a neumožniť vloženie vykonateľného kódu ako komentár na stránku.

Kapitola 18 – Understanding Defense

- **Defence in Depth**: Prístup, kedy zabezpečenie systému nie je založené len na jednom bezpečnostnom mechanizme, ale na viacerých na seba nadväzujúcich.
  - **Security Onion**: Platí, že ak sa chce útočník dostať k chráneným zdrojom, tak musí postupne prelomiť všetky bezpečnostné mechanizmy. Platné skôr v minulosti.
  - **Security Artichoke**: Platí, že ak sa chce útočník dostať k chráneným zdrojom, tak mu stačí prelomiť len niektoré z bezpečnostných mechanizmov.
- **MDM (Mobile Device Management)**: Softvér umožňuje implementovať bezpečnostné nastavenia a konfiguráciu pre všetky zariadenia, ktoré sa pripájajú do firemnej siete.

Kapitola 19 – Access Control

- **Confidentiality**: Dôvernosť = dáta budú prístupné len autorizovaným entitám. Na zabezpečenie tejto vlastnosti sa používa šifrovanie.
- **Integrity**: Celistvosť = nedôjde k pozmeneniu obsahu dát. Ak áno, tak o tom budeme vedieť. Na zabezpečenie tejto vlastnosti sa používajú Hash mechanizmy.
- **Availability**: Dostupnosť = služby a dáta budú neustále dostupné. Nestane sa, že autorizovaný používateľ nebude vedieť pristupovať k službám alebo dátam. Na zabezpečenie tejto vlastnosti sa používa redundancia a zálohovanie.

- **Zero Trust Security**: Prístup kontroly založený na tom, že nedôverujeme vôbec ničomu a všetko sa kontroluje. Nevýhodou je, nepohodlnosť pre používateľov. Výhodou je, plné zabezpečenie každého aspektu systému.
- **Access Control Models**: Modely kontroly prístupu opisujúce spôsob kontroly, obmedzenia a priradzovanie prístupu entitám.
    - **DAC (Discretionary Access Control)**: Najmenej obmedzujúci model, umožňujúci vlastníkovi definovať prístupové práva k jeho zdrojom. Na definovanie prístupových práv sa používajú prístupové zoznamy.
    - **MAC (Mandatory Access Control)**: Najprísnejší model prístupu používaný v armáde. Každému zdroju je priradený bezpečnostný level a každý používateľ má priradenú bezpečnostnú previerku, na základe ktorej má oprávnenie pristupovať k danému zdroju alebo nie.
    - **RBAC (Role-based Access Control)**: Prístup k zdrojom je priradzovaný rolám. Následne používatelia majú prístup k takým zdrojom, v akých rolách sa nachádzajú.
    - **ABAC (Attribute-based Access Control)**: Zdrojom sú priradzované atribúty, na základe ktorých majú následne používatelia povolený/zakázaný prístup. Je to závislé od aktuálneho nastavenia prostredia.
    - **RBAC (Rule-based Access Control)**: Sieťový špecialisti definujú sériu pravidiel, ktoré ak sú splnené, tak daný používateľ má prístup k daným zdrojom, v opačnom prípade nie. Pravidlá štandardne definujú povolené/zakázané IP adresy, protokoly a pod.
    - **TAC (Time-based Access Control)**: Priradzovanie prístupu je na základe času.
- **Authentication**: Autentifikácia je proces na overenie identity používateľov. Kto používateľ je.
- **Authorization**: Autorizácia je proces na priradzovanie práv používateľom. Čo používateľ môže.
- **Accounting**: Účtovanie je proces na robenie záznamov o činnosti. Čo používateľ v systéme vykonal.

Kapitola 20 – Threat Intelligence

- **AIS (Automated Indicator Sharing)**: Služba umožňujúca výmenu indikátorov kybernetických hrozieb v reálnom čase. Po zdetegovaní hrozby, sa o nej vygeneruje záznam, ktorý sa následne vyzdieľa komunite, aby sa mohla chrániť.
- **CVE (Common Vulnerability and Exposure Database)**: Databáza obsahujúca známe bezpečnostné hrozby. CVE poskytuje zoznam CVE identifikátorov pre verejne známe zraniteľnosti spolu s ich opisom.
- **Threat Intelligence Communication Standards**: Štandardy umožňujúce bezpečné prenášanie a zdieľanie informácií o kybernetických hrozbách.
    - **STIX (Structured Threat Information Expression)**: Predstavuje množinu špecifikácií pre výmenu informácií o kybernetických hrozbách medzi organizáciami.
    - **TAXII (Trusted Automated Exchange of Indicator)**: Definícia protokolu aplikačnej vrstvy, ktorý umožňuje komunikáciu / prenos dát špecifikovaných v STIX špecifikácií využitím HTTPS protokolu.
    - **CybOX**: je štandardizovaná schéma na špecifikáciu, zachytávanie, charakterizáciu a komunikáciu udalostí a vlastností sieťových procesov, ktoré podporujú rôzne funkcie

súvisiace s kyberbezpečnosťou. Jednoducho povedané sa jedná o množinu schém na opis udalostí a vlastností súvisiacich s kyberbezpečnosťou.

Kapitola 21 – Cryptography

- **Data Integrity**: Zabezpečenie celistvosti dát. Mechanizmus pre overenie, že nedošlo k zmene prenášaných dát, či už neautorizovaným spôsobom, alebo chybou pri prenose.
- **Hash**: Je jednosmerná šifra. Umožňuje vytvoriť odtlačok pôvodnej správy. Z akokoľvek veľkého vstupu vygeneruje reťazec o fixnej veľkosti, pričom platí, že pri malej zmene v pôvodnej správe dôjde k radikálnej zmene vo vygenerovanej Hash hodnote. Zároveň sa nemôže stať, že dva rôzne vstupy budú mať za dôsledok vygenerovanie rovnakej Hash hodnoty.
- **Origin Authentication**: Mechanizmus pre overenie pôvodu správy.
    - **HMAC (Keyed-hash Message Authentication Code)**: Kód generovaný tak, že k obsahu pôvodnej správy sa pridá aj tajný kľúč a až následne sa vypočíta Hash.
- **Data Confidentiality**: Mechanizmus pre zabezpečenie dôvernosti dát. Pri prenose/ukladaní sa pracuje s dátami v šifrovanej podobe, aby ich nebolo možné čítať neautorizovanými entitami.
- **Data Non-Repudiation**: Mechanizmus zabezpečujúci, že iniciátor komunikácie/odosielateľ správy/požiadavky nebude môcť poprieť, že vykonal danú aktivitu.
- **Symmetric Encryption**: Šifrovanie využívajúce ten istý kľúč na šifrovanie dát aj ich dešifrovanie.
- **Asymmetric Encryption**: Šifrovanie využívajúce dvojicu kľúčov, pričom jedným kľúčom sa dáta šifrujú a druhým dešifrujú.
- **Block Ciphers**: Bloková šifra. Šifrované dáta sú rozdelené do blokov o fixnej veľkosti a tieto bloky sú šifrované samostatne.
- **Stream Ciphers**: Prúdová šifra. K šifrovaniu dochádza bit po bite / bajt po bajte.
- **Code Signing**: Podpisovanie kódu. Slúži na overenie, že kód, ktorý si stiahneme do zariadenia je ten istý, aký bol vyrobený výrobcom = nebol pozmenený neautorizovaným spôsobom.
- **Digital Certificates**: Slúži na preukázanie / overenie identity. Je vydávaný certifikačnou autoritou. Jedná sa o verejný kľúč spolu s údajmi o používateľovi podpísaný certifikačnou autoritou.
- **PKI (Public Key Infrastructure)**: Množina špecifikácií, systémov a nástrojov umožňujúcich generovanie, správu, distribúciu, používanie, ukladanie a zbavovanie platnosti digitálnych certifikátov.
- **CA (Certificate Authority)**: Certifikačná autorita, ktorá umožňuje na základe požiadavky overiť identitu používateľa a vygenerovať pre neho certifikát.

Kapitola 22 – Endpoint Protection

- **Detection Approaches**: Prístupy na detekciu škodlivého kódu:
    - **Signature-based**: Škodlivý kód je identifikovaný na základe charakteristík jeho súborov, zdrojového kódu a pod. Porovnávajú sa napr. Hash hodnoty súborov, kódov a pod.
    - **Heuristics-based**: Škodlivý kód je identifikovaný na základe pozorovania všeobecných vlastností, ktoré je možné vidieť aj u iných typov škodlivého kódu.
    - **Behavior-based**: Škodlivý kód je identifikovaný na základe jeho správania.

- **Host-based Malware Protection**: Mechanizmy na ochranu koncových zariadení implementované priamo na koncových zariadeniach v podobe antimalware softvéru.
- **Network-based Malware Protection**: Mechanizmy na ochranu koncových zariadení implementované na sieťových zariadeniach (NG-FW, IPS, NAC, ...).
- **AMP (Cisco Advanced Malware Protection)**: Riešenie pre pokročilú analýzu softvéru a tvorbu ochranných systémov. Obsahuje funkcionality potrebné pred, počas a po 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.
- **NAC (Network Admission Control)**: Slúži na riadenie prístupu do siete. Jedná sa o rôzne autentifikačné servery a riešenia ako RADIUS, ISE a pod.
- **HIDS (Host-based Intrusion Detection)**: Riešenia umožňujúce detekciu vniknutí. Pracujú na základe detailného monitorovania systémovej konfigurácie a aktivity aplikácií.
    - **Anomaly based**: Detekcia je založená na porovnávaní systémovej aktivity vzhľadom k jej štandardnému profilu.
    - **Policy based**: Detekcia je založená na porovnávaní aktivít systému s definovanými pravidlami.
- **OSSEC (Open Source HIDS SECurity)**: Systém monitorujúci systémové logy na koncových zariadeniach, pričom vykonáva kontrolu integrity súborov. Architektonicky pozostáva z riadiaceho servera a agentov nainštalovaných na zariadeniach koncových používateľov.
- **Attack Surface**: Predstavuje celkovú množinu zraniteľností systému (vstupy pre útočníka).
    - **Network**: Útočník zneužíva zraniteľnosti v počítačovej sieti.
    - **Software**: Útočník zneužíva zraniteľnosti vo web-e, cloud-e a aplikáciách.
    - **Human**: Útočník zneužíva slabé stránky v správaní používateľov.
- **Application Blacklisting**: Zoznam pravidiel, ktorý zakáže špecifické aplikácie a všetko ostatné povolí. Menej bezpečné.
- **Application Whitelisting**: Zoznam pravidiel, ktorý povolí špecifické aplikácie a všetko ostatné zakáže. Viac bezpečné.
- **Sandbox**: Jedná sa o izolované prostredie spustené na zariadení, ktoré sa tvári ako reálne zariadenie. Izolácia tohto prostredia umožňuje pozorovanie správania škodlivého kódu bez ohrozenia reálneho OS.

Kapitola 23 – Endpoint Vulnerability Assessment

- **Risk Analysis**: Analýza možných dopadov na systémové zdroje, z čoho je možné vyvodiť záver ohľadom závažnosti rizík.
- **Vulnerability Assessment**: Testovanie zraniteľností využitím skenovania zariadení, otvorených portov a spustených služieb.
- **Penetration Testing**: Využitie nástrojov útočníkov pre simulovanie rôznych útokov s cieľom nájdenia zraniteľných miest.
- **CVSS (Common Vulnerability Scoring System)**: Nástroj na ohodnotenie a výpočet závažnosti zraniteľnosti. Hodnota CVSS pomáha priradiť prioritu jednotlivým rizikám.

    - **Base Metric**: Množina charakteristík zraniteľnosti, ktoré sú konštantné v čase.
    - **Temporal Metric**: Množina charakteristík zraniteľností, ktoré sa môžu v čase meniť, no nijak neovplyvňujú vlastnosti prostredia.
    - **Environmental Metric**: Množina charakteristík zraniteľností, ktoré súvisia s prostredím organizácie.
- **Patch Management**: Riadenie „záplat". Definuje postupy, ktoré je potrebné vykonať na dočasné vyriešenie objavenej zraniteľnosti. Jedná sa o dočasné riešenia, kým od výrobcu nepríde aktualizácia.
    - **Agent-based**: Vyžaduje agenta, ktorý je spustený na monitorovanom zariadení. Agent kontroluje aktuálny stav a v prípade nájdenia zraniteľnej aplikácie si vyžiada od riadiaceho servera Path a nainštaluje ho. Vhodné pri správe mobilných zariadení.
    - **Agentless Scanning**: Riadiaci server skenuje koncové zariadenia a v prípade nájdenia zraniteľnosti vykoná inštaláciu záplaty. Skenovanie možné len pre zariadenia v sieti pod našou správou. Problém pri mobilných zariadeniach.
    - **Passive Network Monitoring**: Zariadenia vyžadujúce záplatu sú identifikovaná na základe prenášanej sieťovej prevádzky. Efektívne len pre aplikácie, ktoré pri komunikácii prenášajú číslo svojej verzie.
- **ISMS (Information Security Management System)**: Jedná sa o riadiaci rámec na identifikáciu, analýzu a vyriešenie bezpečnostných rizík. Obsahuje model, ktorý je možné použiť ako návod na plánovanie, implementáciu a vyhodnocovanie bezpečnostných programov.

Kapitola 24 – Technologies and Protocols

- **Tor Network**: Sieť umožňujúca anonymnú komunikáciu v rámci internetu, pričom využíva množstvo relay zariadení, ktoré viacnásobne šifrujú komunikáciu a tým znemožňujú stopovať komunikujúcich používateľov. Vyžaduje ale používanie špeciálneho webového prehliadača.

Kapitola 25 – Network Security Data

- **Session Data**: Záznam o komunikácii medzi dvoma komunikujúcimi bodmi, ktorý pozostáva z 5 údajov a to zdrojová/cieľová IP adresa, zdrojový/cieľový port a číslo protokolu. V rámci záznamu o komunikácii sa tiež uvádza doba trvania, množstvo prenesených dát a ID.
- **Transaction Data**: Jedná sa o dáta, ktoré boli komunikáciou prenesené. Možné vidieť napr. po odchytení. Môže sa jednať napr. o HTTP požiadavku, odpoveď a pod.
- **Statistical Data**: Dáta o sieťovej prevádzke, ktoré je možné použiť na vytvorenie štandardného profilu, vzhľadom ku ktorému je následne možné porovnávanie analyzovaných dát a možných vniknutí.
- **SIEM and Log Collection**: SIEM umožňuje zbierať a analyzovať dáta z rôznych zdrojov.
    - **Log Collection**: Zber logov z rôznych zdrojov.
    - **Normalization**: Prepísanie zozbieraných logov do spoločného formátu – pre lepšie neskoršie spracovanie.
    - **Correlation**: Priradenie logov k vzniknutým udalostiam a hláseniam v systéme.
    - **Aggregation**: Redukovanie množstva zozbieraných dát odstránením duplicitných dát o tej istej udalosti z rôznych zdrojov.

    - **Reporting**: Štandardne poskytuje grafické rozhranie a vizualizáciu analyzovaných a historických dát.
    - **Compliance**: Generovanie záznamov pre splnenie právnych predpisov a regulácií.
- **AVC (Cisco Application Visibility and Control)**: Systém, ktorý dokáže rozoznať a analyzovať viac ako 1000 rôznych aplikácií, na základe čoho je následne možné generovať štatistiky a vytvárať pravidlá pre povolenie / zakázanie používania daných aplikácií. Na rozoznávanie využíva NBAR2.
- **NBAR2 (Cisco Next-generation Network-based Application Recognition version 2)**: Mechanizmus pre klasifikáciu dát na základe DPI.
- **DPI (Deep Packet Inspection)**: Mechanizmus vykonávajúci hĺbkovú inšpekciu paketov, kedy dochádza k analýze až samotných prenášaných dát.
- **DLP (Data Loss Prevention)**: Mechanizmus skenujúci odchádzajúcu prevádzku s cieľom zamedzenia odoslania citlivých dát z vnútornej siete do nechránenej oblasti.

Kapitola 26 – Evaluating Alerts

- **Detection Tools for Collectiong Alert Data**: Detekčné nástroje umožňujúce zber dát o hláseniach.
    - **CapME**: Webová aplikácia umožňujúca zobrazovanie .pcap súborov.
    - **Snort**: Sieťový detekčný systém vniknutí.
    - **Zeek**: Podobne ako Snort, avšak na analýzu vniknutí používa vzory správania.
    - **OSSEC**: Detekčný systém vniknutí pre koncové zariadenia.
    - **Wazuh**: Plne vybavené riešenie na ochranu koncových zariadení. Vykonáva analýzu súborov, kontrolu integrity, hľadanie zraniteľností, ohodnocuje konfiguráciu zabezpečenia a dokáže reagovať na vzniknuté incidenty.
    - **Suricata**: Kombinácia sieťového detekčného systému a prevenčného systému. Detekcia je vykonávaná na základe signatúr = podpisov = Hash hodnôt.
- **Analysis Tools**: Nástroje umožňujúce analýzu zozbieraných dát.
    - **Sguil**: Konzola umožňujúca vyšetrovanie bezpečnostných hlásení získaných z veľkého množstva zdrojov. Predstavuje štartovací bod analýzy incidentov a umožňuje priamy prechod k množstvu ďalších nástrojov – otvorenie Wiresharku, ...
    - **Kibana**: Grafické rozhranie pre zobrazovanie dát.
    - **Wireshark**: Nástroj na odchytávanie dát.
    - **Zeek**: Analyzátor sieťovej prevádzky – dokáže vykonať hĺbkovú analýzu. Možné získať prístup k transakčným dátam a obsahu prenášaných súborov.
- **Evaluating Alerts**: Proces vyhodnocovania hlásení.
    - **True Positives**: Požadovaný typ hlásenia. Jedná sa o detekciu reálneho útoku.
    - **False Positives**: Nežiadúci typ hlásenia. Jedná sa a detegovanie útoku, ktorý ale nenastal. Potreba eliminovať na minimum úpravou detekčných pravidiel. Stojí to zbytočný čas analytikov, ktorý musia preverovať falošné hlásenia.
    - **True Negatives**: Požadovaný typ hlásení. Predstavuje štandardnú neškodnú prevádzku.
    - **False Negatives**: Nežiadúci typ hlásení a veľmi nebezpečný. Znamená, že reálny útok nebol detegovaný a náš detekčný systém to vnímal ako korektnú prevádzku.
- **Deterministic Analysis**: Analýza, kedy sa pozoruje presný postup a správanie exploit-u. Predpokladá sa presný postup krok po kroku a až vykonaním finálneho kroku dochádza k realizácii útoku/vniknutia. Vyhodnotenie rizík je na základe známych zraniteľností.

- **Probabilistic Analysis**: Štatistická analýza na určenie pravdepodobnosti úspešného dokončenia útoku, na základe pravdepodobnosti úspešnosti vykonania jednotlivých krokov. Vyhodnotenie rizík je na úrovni odhadu úspešnosti vykonávania jednotlivých krokov útoku.

Kapitola 27 – Working with Network Security Data

Kapitola neobsahuje nové pojmy súvisiace s kyberbezpečnosťou. Ukazuje prácu s rôznymi nástrojmi, ktoré umožňujú analýzu hlásení a vyšetrovanie incidentov.

Kapitola 28 – Digital Forensics and Incident Analysis and Response

- **Digital Forensics Process**: Procesy práce s digitálnymi dátami pre účely súdnych procesov
    - **Collection**: Identifikácia dôležitých dát a ich zber – bezpečné odobratie z médií.
    - **Examination**: Prieskum zozbieraných dát a oddelenie relevantných (dôležitých) dát.
    - **Analysis**: Získanie informačnej hodnoty. Vyvodenie záverov na základe dôkladnej analýzy na dátach z rôznych zdrojov.
    - **Reporting**: Vytvorenie záznamov pre súdne procesy.
- **Types of Evidence**: Typy dôkazov.
    - **Direct Evidence**: Priame dôkazy. Očití vedkovia a pod.
    - **Indirect Evidence**: Nepriame dôkazy. Dôkazy, ktoré len naznačujú možné hypotézy na základe iných podporných dôkazov.
    - **Best Evidence**: Najlepší dôkaz. Napríklad úložisko dát, ktoré používal obvinený, prípadne archivované súbory, u ktorých máme istotu, že neboli pozmenené.
    - **Corroborating Evidence**: Potvrdzujúce dôkazy, ktoré podporujú tvrdenia vyplývajúce z najlepších dôkazov.
- **Chain of Custody**: Reťaz spracovania, predstavuje množinu procesov a zainteresovaných ľudí súvisiacu so zberom, držaním a bezpečným uložením dôkazov.
- **TTP (Tactics, Techniques, and Procedures)**: Záznamy o taktike, použitých technikách a procesoch počas vykonávania útoku.
- **Cyber Kill Chain Model**: Model znázorňujúci postupnosť krokov útoku. Cieľom je útok zastaviť v čo možno najskoršej fáze tohto modelu.
    - **Reconnaisance**: Získavanie informácií o obeti a cieľovom systéme.
    - **Weaponization**: Na základe zozbieraných dát vytvorenie nástroja pre vniknutie na cieľový systém.
    - **Delivery**: Doručenie vytvoreného nástroja (napr. email-om) na cieľové zariadenie.
    - **Exploitation**: Spustenie doručeného nástroja na zneužitie zraniteľnosti pre získanie väčšej kontroly pre umožnenie doručenia reálneho škodlivého kódu.
    - **Installation**: Inštalácia škodlivého kódu – napr. vytvorenie backdoor (zadné vráta) pre umožnenie vzdialeného prístupu na zariadenie obete.
    - **Command & Control**: Vytvorenie komunikačného kanála medzi útočníkom a obeťou s cieľom prenosu riadiacich inštrukcií pre ovládanie obete.
    - **Actions on Objectives**: Útočník začne vykonávať úkony podľa svojich požiadaviek pre získanie zdrojov, informácií, citlivých dát a pod.

- **Diamond Model**: Model opisujúci tok procesov/komunikácie/interakcie počas útoku.
    - **Adversary**: Osoby zodpovedné za vniknutie do systému = Útočníci.
    - **Capability**: Nástroje, zraniteľnosti a techniky umožňujúce útočníkovi útočiť na obeť.
    - **Infrastructure**: Množina sieťových zariadení umožňujúca komunikáciu.
    - **Victim**: Cieľ útoku = Obeť.
- **Incident Response Life Cycle**: Životný cyklus definujúci postupnosť krokov, ktorú je potrebné vykonávať od fázy pred začatím útoku, cez jeho vykonanie až po jeho ukončenie a zotavenie poškodeného systému.
    - **Preparation**: Zamestnanci sú trénovaní ako reagovať a odpovedať na možné incidenty.
    - **Detection and Analysis**: Proces detekcie a analýzy detegovaného útoku.
    - **Containment, Eradication and Recovery**: Postupy ako ohraničiť detegované vniknutie, aby sa ďalej nešírilo, eliminovať jeho vplyv na naše zdroje a citlivé dáta a zotaviť naše prostredie tak, aby mohlo fungovať ako pred útokom (použitie zálohy na obnovu dát a softvéru).
    - **Post-Incident Activities**: Vytvorenie dokumentácie, ako bol útok detegovaný, ako sa postupovalo pri jeho odstránení a aké opatrenia boli vykonané pre zabránenie jeho šíreniu a ďalším škodám. Táto dokumentácia má pomôcť v budúcnosti pri riešení ďalších podobných útokov.