Výpisky ze slajdů PV210

1. Přednáška

Kyberprostor

- digitální prostředí, jež umožňuje tvorbu, zpracování a výměnu informací v informačních systémech, službách, elektronických komunikačních sítích.

Kyberbezpečnost

- zabezpečení a akce, které jsou užívány k ochraně kyberprostoru
- schopnost chránit nebo bránit užívání kyberprostoru od kybernetických útoků

Bezpečnostní tým

CSIRT = **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam

- organizace, jež je zodpovědná za přijímání, zkoumání a reagování na reporty a aktivity, jež mohou býti bezpečnostním incidentem
- nabízí své služby pro danou konstituenci (firma, vláda, vzdělávací organizace, region atd.)
- lze připodobnit požárnímu oddělení

Bezpečnostní incident

- každá reálná podezřelá, nepřátelská aktivita související se zabezpečením počítačových sítí a systémů
- akt porušení bezpečnostní politiky
- složen z jednoho nebo více nechtěných informačních bezpečnostních událostí, které mohou narušit nebo oslabit informační bezpečnost
- porušení nebo hrozba porušení bezpečnostních politik

Konstituence

- může být dána národnostně, geograficky, technologicky, založena na poskytovateli.
- rozsah působnosti bezpečnostního týmu
- CSIRT-MU – studenti a zaměstnanci MU, IP adresy v adresním rozsahu muni.cz

Kooperace

- každý tým slouží svým uživatelům a interakuje s jinými týmy
- týmy jsou většinou podřízeny nějakému nadřazenému týmu (např. národnímu)
- týmy sdílí zkušenosti, znalost a udržují základnu

Ukázka hierarchie

MU (akademická organizace) – CESNET (akademický ISP) – CSIRT.CT (národní tým)

Proč je potřeba speciální tým?

- Abychom měli centralizovaného koordinátora pro IT bezpečnost
- Centralizované a specializované řešení bezpečnostních incidentů
- Mít po ruce odbornou znalost a asistovat uživatelům při obnově po BI
- Sledování vývoje v oblasti bezpečnosti
- Stimulace spolupráci uvnitř konstituence

2. přednáška

Služby bezpečnostního týmu

- tým poskytuje pouze vybrané služby, musí být jasně deklarovány

Typy služeb

- **reaktivní** - spuštěné žádostmi nebo událostmi, základní služby
- **proaktivní -** pomáhají chránit přes útoky a hrozbami, jejich cíl je snížit počet budoucích incidentů
- **služby kvality bezpečnosti** - nepřímo snižují počty budoucích incidentů, např. budování uživatelské znalosti

Reaktivní služby

Incident handling

- základní služba CSIRT, řešení bezpečnostních incidentů
- **analýza incidentu**
  - sběr dostupných informací a důkazů vztahujících se k incidentu,
  - cílem je zjistit rozsah útoku, rozsah škod, původ a řešení
- **řešení incidentu na místě**
  - přímý zásah tam, kde se stal incident
  - analýza
  - zotavení
- **podpora řešení incidentu**
  - poskytnutí obětem útoku pomoc se zotavením se z incidentu prostřednictví rad, dokumentace atd.
- **koordinace řešení incidentu**
  - snaha o efektivní rozdělení práce mezi všechny zúčastněné

Alerts and warnings

- upozorňování uživatelů na současné hrozby či útoky
- popis současných útoků zranitelností, doporučení, jak jim předcházet a snížt jejich dopad
- může podat CSIRT, nebo obdržet od jiného týmu

Vulnerability handling

- zpracovávání report ohledně zranitelností HW a SW,
- analýza počítačových systémů a obrana
- podobné jako *alerts and warnings*,
- Hlavní rozdíl v
  - Zahrnutí v analýze prostředí, funkc e a dopadu zranitelností
  - Více změřeno na detekci a zmírnění dopadu
- Tři fáze:
    - **Vulnerability analysis** – inspekce kódu
    - **Vunerability response** – poskytnutí varování, či opravy
    - **Vulnerability responose coordination** – komunikace s autory software
- Např. *Shellshock*

Proaktivní služby

- **Detekce vniknutí**
  - detekce bezpečnostních událostí a útoků
- **Audity a hodnocení**
  - Zkoumání infrastruktury, např. penetrační testování
  - Zhodnocení infrastruktury – konfigurace sítě
  - Zhodnocení best pratice – rozhovory se zaměstnanci ohledně jejich zvyků
  - Skenování – skenování sítě

    - Penetrační testování – prováděné útoky, simulující hackery

- **Vývoj bezpečnostních nástrojů**
    - Např. detekce útoků na autentizace SSH/RDP

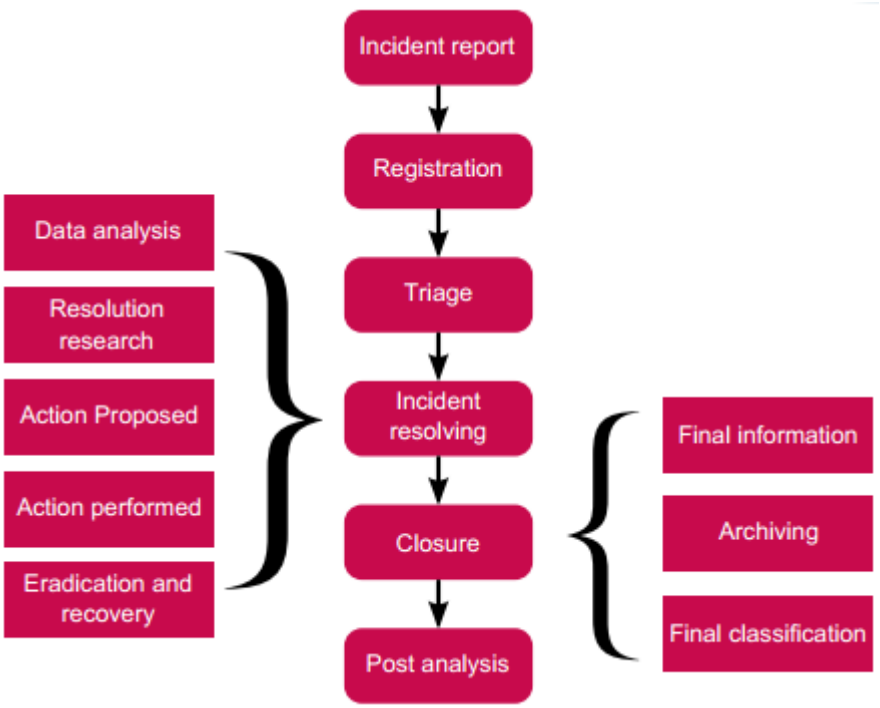
Služby kvality bezpečnosti

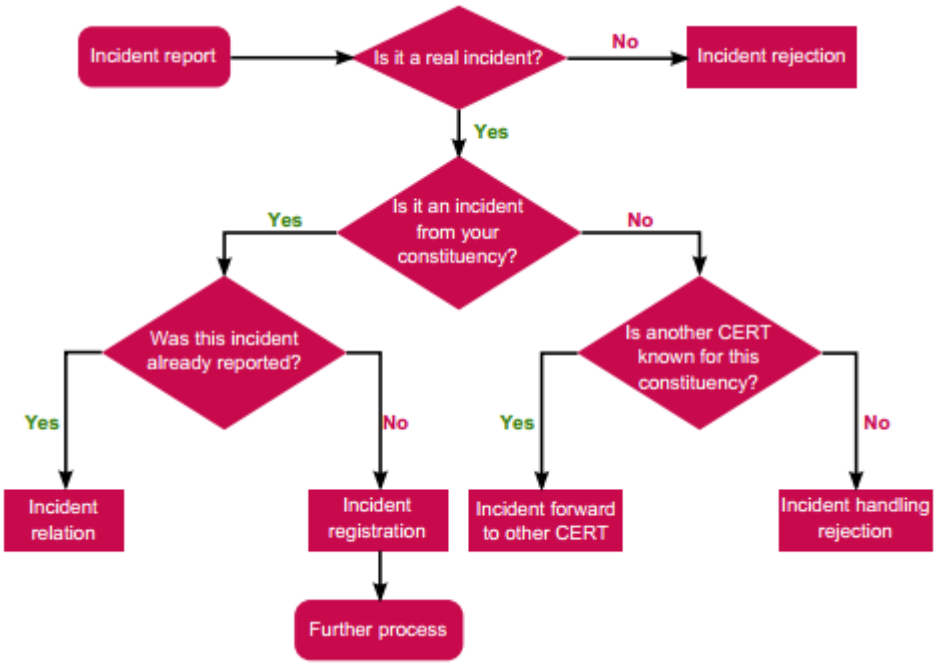
- **Awareness building**
    - zvyšování povědomí běžných uživatelů
    - Cílem je předcházet útokům a poskytnout návody, jak minimalizovat jejich dopad
    - Publikace článků, webu, videí, novinek či organizace seminářů a školení
    - Různé zaměření, např. pro běžné uživatel vs. specifecké uživatele
- **Education/training**
    - vzdělávání v oblasti bezpečnosti pro konkrétní uživatele (semináře workshopy, stáže, školení e-learning)
    - Zaměřeno na specifické problémy

3. Přednáška

Fáze řešení bezpečnostního incidentu

- **Obdržení hlášení o incidentu** Bezpečnostní tým obdrží zprávu o incidentu, která může pocházet od různých komunikačních zdrojů
  (email, telefon, osobně).
- **Registrace incidentu do tiketového systému** Incident je zaregistrován do systému a je mu přiřazen unikátní identifikátor.
- **Prioritizace** Kvůli limitovaným dostupným zdrojům, které lze vyhradit na řešení, je incidentu přiřazena priorita v závislosti na jeho
  závažnosti.
- **Vyřešení incidentu** Je tou nejdelší a nejsložitější fází, při které se
  zjišťují podrobné informace o incidentu jako zdroj či cíl útoku
  a jeho způsob.
- **Post analýza a poučení se** Získání zkušeností z vyřešeného incidentu.





Incident handling

- **Analysis**
  - Sběr dostupných informací a evidence
  - Cílem je zjistit
    - rozsah incidentu,
    - rozsah škod
    - způsob jakým byl útok podniknut
    - jak ho vyřešit
    - jak zmírnit dopad
- **On site**
  - zkoumání přímo tam, kde se incident stal
  - člen CSIRT provede analýzu a obnovu
- **Support**
  - asistence a vedení obětí zasažených útokem při zotavení se z incidentu
  - většinou pomocí mobilu, emailu nebo psaných instrukcí, dokumentace
  - obsahuje výklad nasbíraných dat, poskytuje kontaktní informace a instrukce jak zmírnit dopad incidentu

- **Koordinace**
  - Cílem je efektivní rozdělení práce mezi všechny zapojené
  - oběti, organizace zasažené, organizace odkud pochází útočník
  - může zahrnovat spolupráci po právní stránce, lidskými zdroji a PR, i se soudy

4. přednáška

CSIRT

Mission statement (programové prohlášení)

- definování cílů, priorit, a účelu
- základní pochopení toho, čeho chce tým dosáhnout
- tým musí mít podporu od managementu v organizaci

Typy CSIRTŮ

- Konstituence podle toho, kdo financuje
    - Stát
        - CERT.at
        - CSIRT.CZ
    - Státní správa, vláda
        - GOVCERT.CZ
    - Armáda
        - NATO Cyber Incident Response Centre
    - ISP
        - KPN-CERT,
        - BTCERTCC
    - Výrobci
        - Cisco PSIRT
        - Adobe PSIRT
    - Akademické
        - CSIRT-MU

Vznik prvního CSIRT, reakce na červa Morris

Nařízení CSIRTU

- Kvůli legální povinnosti – vyžádáno zákonem
- Jiné směrnice - (EU strategie, ENISA doporučení)
- Vnitřní směrnice organizace

Úrovně pravomocí

- **Plná** – ve své působnosti má csirt veškeré pravomoci
- **Sdílená** – csirt poskytuje plnou ppodporu, ale potřebuje souhlas při rozhodování
- **Žádné** – cisrt nemá žádné pravomoci

FIRST - Forum For **I**ncident **R**eponse and **S**ecurity **T**eams

- Organizace sdružující týmy
- Konference, technická kolokvia a setkávání týmů

TF-CSIRT Trusted Introducer

- Evropská komunita ale ne přímo vázáno na region
- Několik úrovní ověření týmu, podle jejich vyzrálosti
    - Known
    - Accredits
    - Certifies
- organizace setkání

Členové CSIRT týmů

Manažer, vedoucí týmu

- strategický směr
- umožňuje a usnadňuje práci členů
- dohlíží nad týmem
- reprezentuje
- nabírá nové pracovníky

Asistent manažera, dohlížitel, vedoucí skupiny

- poskytuje vedení pro tým
- podporuje strategický směr
- podporuje vedení, pokud je to potřeba
- poskytuje směr a mentorování členům týmu
- přiřazuje úkoly a povinnosti
- účastní se rozhovorů s novými členy
- při absence vedoucího řeší jeho povinnosti

Hotline

- řeší komunikace pro bezpečnostní reporty
- poskytuje asistenci, pokud na to má vědomosti

Handler

- analýza, sledování řešení incidentů
- koordinace reaktivní a proaktivních služeb
- šíří informace
- interakuje s jinými týmy, s experty atd.

Požadavky na pracovníky

- Nejdůležitější jdou dobé meziosobní a komunikační dovednosti
- Na niž závisí reputace týmu
- Selský rozum se efektivně a přijatelně rozhodovat, pokud nejsou dána pravidla
- Řešit problémy v nových situacích
- Dobré komunikační dovednosti
- Diplomatické jednání
- Schopnost dodržovat pravidla a procedury
- Ochota se učit
- Schopnost jednat pod tlakem
- Ochota přiznat vlastní chybu
- Být důvěryhodný a udržovat reputaci týmu
- Organizovat si čas, koncentrovat se na práci

ČR

- **CSIRT.CZ**
- **GovCERT.cz**
- **CESNET-CERTS**
- **CSIRT-MU**

5. přednáška

Penetrační testování

- metoda hodnocení počítače či počítačové sítě, která simuluje útok na daný systémem
- hlavní rozdíl mezi penetračním testerem a útočníkem je povolení
- Cíle
    - zvýšit zabezpečení
    - najít zranitelnosti, které by mohli využít útočníci
- Není to o tom najít nezáplatovaný systém, ale najít riziko, které je nebezpečné pro organizaci
- Interpretace
    - To, že se nenašla zranitelnost, neznamená, že tam žádná není
- Předpoklady pro úspěch
    - Je těžké dokázat, že neexistuje zranitelnost
    - Dovednosti, znalost a zkušenosti testera
    - Určit rozsah a cíle testování

Příklady penetračního testování

Síťové penetrační testování

- skenování sítě
- testování monitorovacího detekčního systému, firewalu
- testování výkonu (DDoS)
- rozsáhlé detekce zranitelností

Aplikační penetrační testování

- slovníkové a silové útoky
- SQL injekce a kód injekce
- Přetečení bufferu
- Directory traversal – průnik do jiného adresáře
- Input fuzzing - testování vstupů, které vyvolají neočekávanou chybu

Bezdrátová síť

- Umístění zlého zařízení
- Útoky na autentizace a šifrování

Sociální inženýrství

- Phishing

Fyzické zabezpečení

- Zabezpečení budov, fyzické přístupy k systémům

Nástroje

- Nmap
- Metasploit Framework
- Nessus – (vulnerability)
- OpenVAS – vulnerability
- Kali Linux, BackBox

Reporty pentestů

- **Pro manažera**
    - Cílový čtenář je manažer
    - Rozsah práce, identifikace systémů
    - Cíle testování

- Timeline
- Shrnutí nálezů, dopad na bezpečnostní politiky organizaci a doporučení

- **Pro člena bezpečnostního týmu**
  - Metody útoků
  - Hodnocení rizik

Pro systémového administrátora
- Specifikace testované infrastruktury
- Seznam zranitelností s hodnocením rizik

Common vulnerabilities and Exposures (CVE)

- Databáze veřejně známých zranitelností
- CV-2016-0001

Top 3 Attacks

- **Injection**
  - pokud jsou poslána data interpreteru, která obsahují další příkaz
  - např. SQL Injection
- **Porušení autentizace a session management**
  - Kompromitace hesel atd.
- **Cross-site scripting**
  - využití neostřených vstupů ve skriptech

Vzdělávání

- praktické ozkoušen
- je potřeba je nalákat
- vzdělání předchází incidentům
- mělo by být levnější než samotné řešení incidentů poté

6. přednáška

Definice síťového útoku

- pokus zničit, změnit, ukrást majetek nebo získat neoprávněný přístup či neautorizované použití majetku pomocí počítačové techniky a počítačové sítě

Typy útoků

- botnety
- DDoS
- Malware
- Útoky na získávání dat
- Útok na hesla
- Útoky na protokoly

Botnet

- Skupina kompromitovaných strojů
- řízená centrálním strojem útočníka
- využití pro
    - spam
    - DDoS útoky
    - propagaci malwaru.

DDoS

- Cílem je zabránit funkčnosti služeb
- Přehlcení požadavků
- ICMP , SYN flood, UDP flood

Information gathering attack

- Hlavním cílem je získat informace o síti (skenování)

Malware

- Červy, trojské koně, virusy, spyware, ransomware
- Může připojit do botnetu

Heslové útoky

- SSH, RDP
- Hádání hesel silou nebo slovníkovými útoky
- Po uhádnutí může být stroj připojen do botnetu

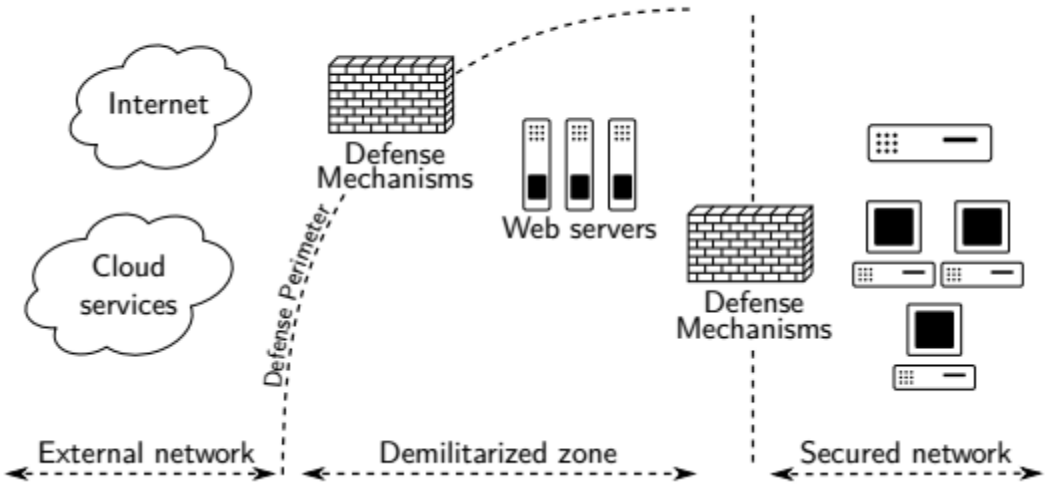
Útoky na protokoly

- DNS cache spoofing
- arp spoofing
- MIT
- session hickjaking (únos spojení http cookie)

Aktivní x pasivní
Vnější x vnitřní
4 rozměry

- Způsob
- Cíl
- Zranitelnost

- Vedlejší efekty



Firewall
Síťový x osobní
Transportní vrstva x aplikační x bezstavová

Proxy
Kontrola obsahu
URL DNS blacklist, MIME/URL regex filtrování

UTM
Jednotná správa hrozeb
Řešení UTM obvykle plní funkce antiviru, antispywaru, antispamu, síťové brány firewall, detekce a prevence vniknutí, filtrování obsahu a prevence úniku informací.

Systémy pro bezpečnost sítí
IDS – Intrusion detecion systém, Detekce průniků
IPS – Intrusion prevension systém, prevence průnik
ADS – Anomaly detetion systém
NBA – Network behavioral analysis

Flowmon
Monitorování toků v síti, přehled statistik

Bro
IDS

Aktivní monitorování

- Získávání informací z aktivně posílaných dotazů
- Výhody
  - Detailní informace
  - Mnoho možností jak monitorovat
- Nevýhody
  - Přidání další provozu do sítě
  - Monitorované objekty musí vědět, že jsou monitorovány
  - Časová a výpočetní složitost

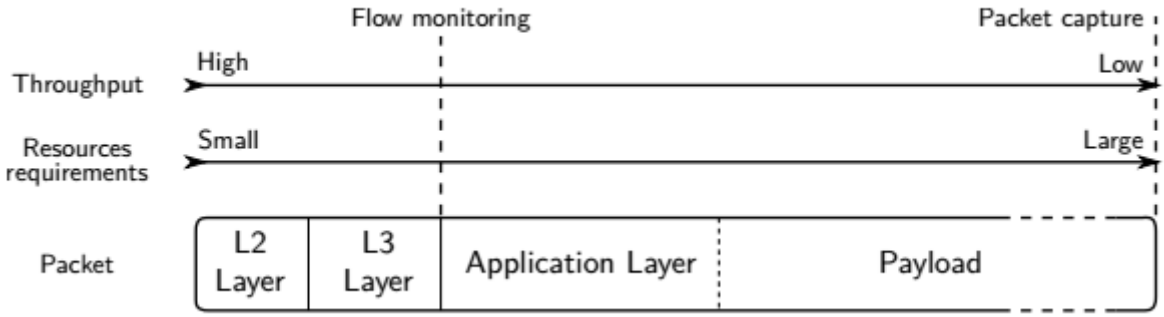
- Limitovaná oblast, nelze přes NAT, firewall

- Nástroje: nmap, zmap

Pasivní monitorování

- Pouze pozorování
- Výhody
  - Transparentní monitorování
  - Vhodné pro veliké vysokorychlostní sítě
  - Nezvyšuje provoz
  - Není limitováno firewallem, ani NAT
- Nevýhody
  - Limitované informace
  - Zašifrovaná data

Úrovně viditelnosti



Hloubková analýza paketů

- Zachytávají se celé pakety
- Výhody
  - Vysoká úroveň viditelnosti
  - Můžeme získat jakoukoli informaci
- Nevýhody
  - Problémy se soukromím
  - Výpočetně náročné
  - Pomalé, snižuje výkon
  - Nelze užít ve vysokorychlostních sítích

Sledování metadat

- Zachytávají se pouze metadata
- Výhody
  - Rychlé
  - Méně náročné než DPI
  - Vhodné pro vysokorychlostní
- Nevýhody
  - Nízká úroveň viditelnosti, méně dat pro analýzu
- Agregace metadat paketů se nazývají network flows.

7. přednáška

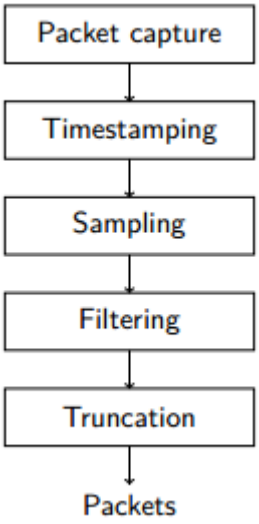
Framework

Motivace

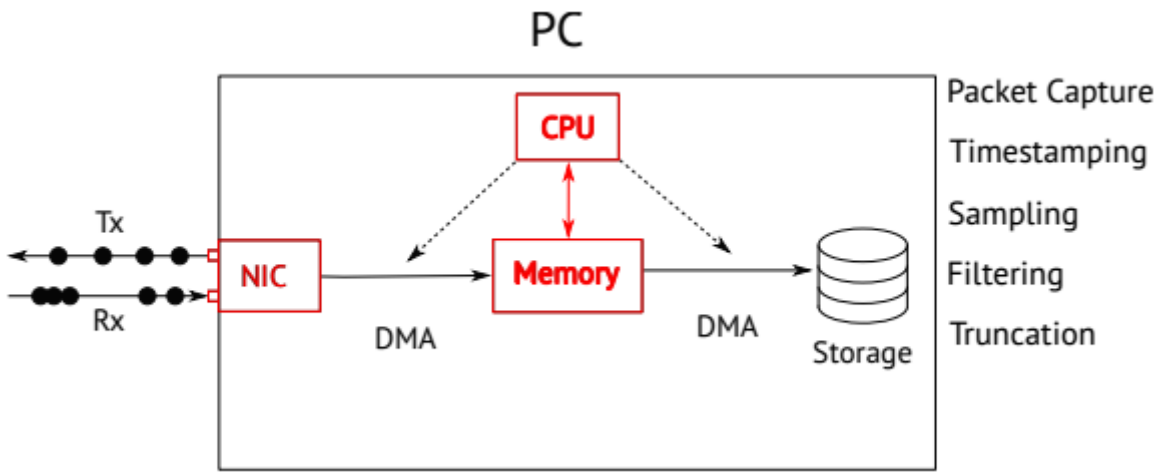
- Někdy jsou hlavičky paketů nedostačující
- Z celých paketů získání všechny informace

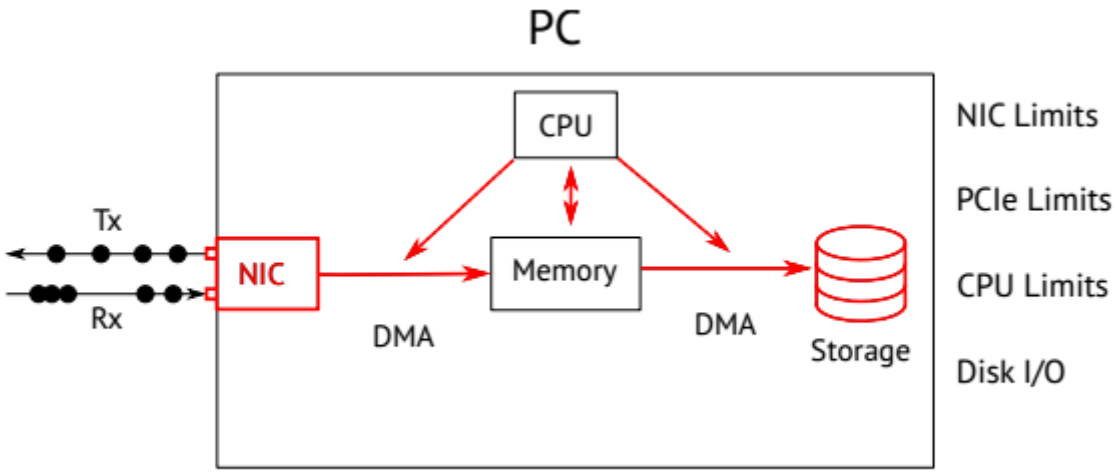
Požadavky

- Výpočetně náročně
- Velké množstní požadavků
- Propustnost limitovaná vstupem a výstupem zařízení



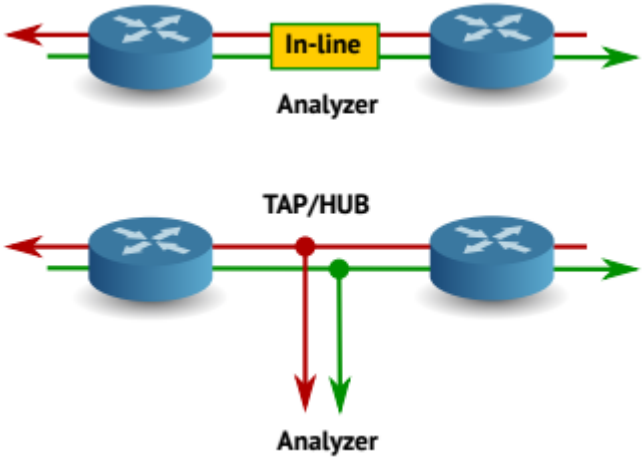
1. Zachycení
2. Označení známkami
3. Vzorkování
4. Filtrování
5. Oříznutí





Přístupové metody pasivního monitorování

- Zrcadlení
  - portů nebo span
- Přímá metoda
  - spojení pomocí tap/hub

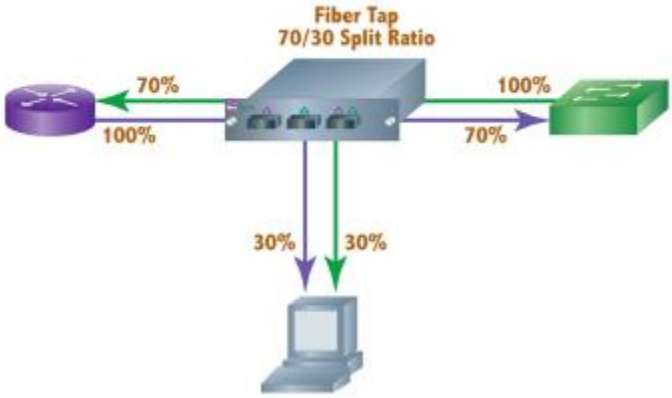


TAP - Test Access Port

- duplikace provozu pro monitorovací zařízení
- pasivní rozdělování nebo regenerační technologie

Optický TAP

- využívá refrakci
- aktivní regenerace signálu
- rozděluje intenzitu signálu (30:70, 50:50)



Metalický TAP

- musí být napájen
- porucha způsobí odpojení

Zachytávání paketů v bezdrátových sítích

- pasivní poslouchací monitorovací mód
- SSID a kanál k upřesnění
- Promiskuitní mód, všechny pakety v síti

Potřeba knihoven pro zachytávání paketů
Libpcap – univerzální knihovna

Filtrování paketů
Berkeley Paket Filter
BPF

Vzorkování
Vybírá se každý n-tý packet nebo náhodně
Může zkreslit data

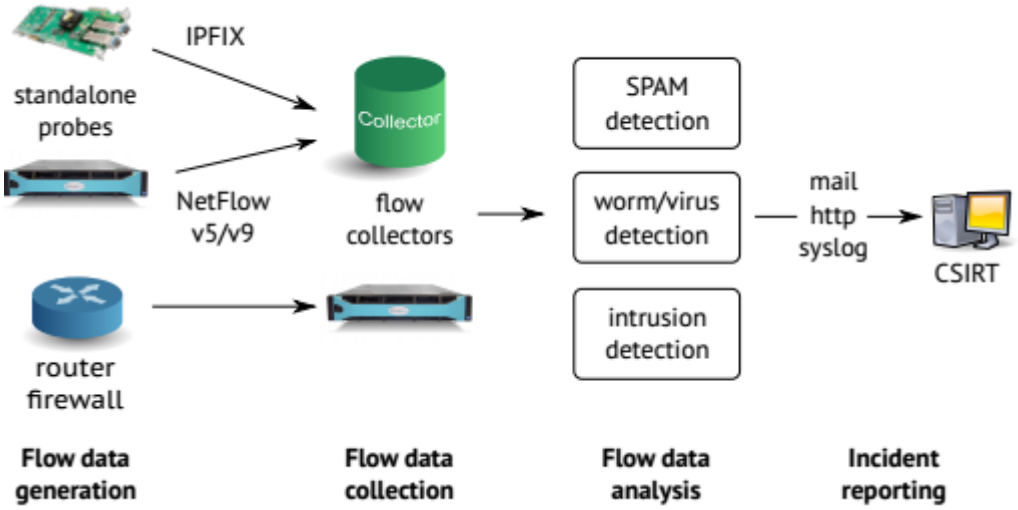
Analýzor paketů

- Software pro čtení informací ze síťového provozu
- Síťové problémy
- Průniky
- Statistiky
- Reverzní inženýrství protokolů
- Např. Tcpdump, Wireshark, tshark

8. přednáška

Měření toků

- Sdružování paketů podle podobných vlastností
- $F = (IP_{src}, IP_{dst}, P_{src}, P_{dst}, Prot, T_{start}, T_{dur}, Pckts, Octs, Flags)$



Flow mohou sbírat routery a firewally, ale ty jsou zaneprázdněny směrování atd a ne všechny to podporují

Samotné sondy

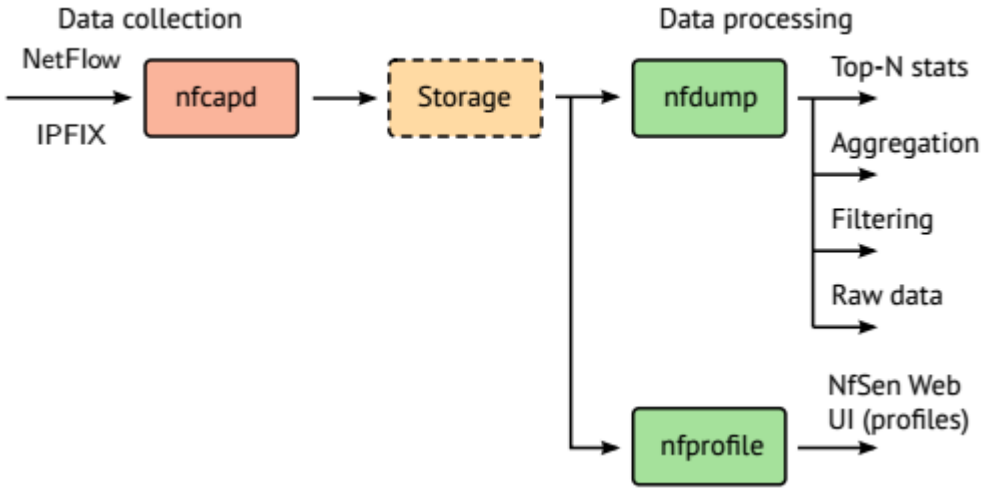
Důležité funkce

- Propustnost
- Flow cache
- Podpora (MAC, VLAN, MPLS, NBAR, http)

Výrobci Flowmon Probe,Cico

Protokoly

- NetFlow 5, 9
- IPFIX



Důležité funkce

- Výkon, kolik toků dokáže zpracuje za sekundu
- Podpora exportu

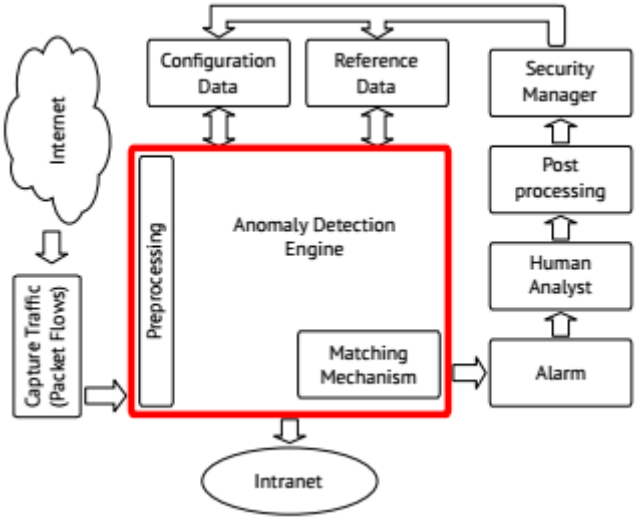
Nástroje NFDUMP, Flomon Collector

Standardní flow používá jen hlavičky paketů
Pakety jsou agregovány do flow a exportovány pro analýzu
Jsou méně citlivější na soukromí než pakety

Výhody

- Detailní přehled provozu sítě
- Top adresy, které komunikují a aplikace
- Díky viditelnosti vyšší zabezpečení sítě
- Detekce útoků

Analýza je manuální
Naivní, rychlé útoky se lehko detekují
Automatická řešení na detekování útoků
Detekce anomálií



9. Přednáška

Statistické metody detekce

Detekce anomálií Timeseries

1. předvídat
2. změřit
3. porovnat
4. při překročení hranice, označit jako anomálii

hranici nastavuje člověk podle zkušenosti

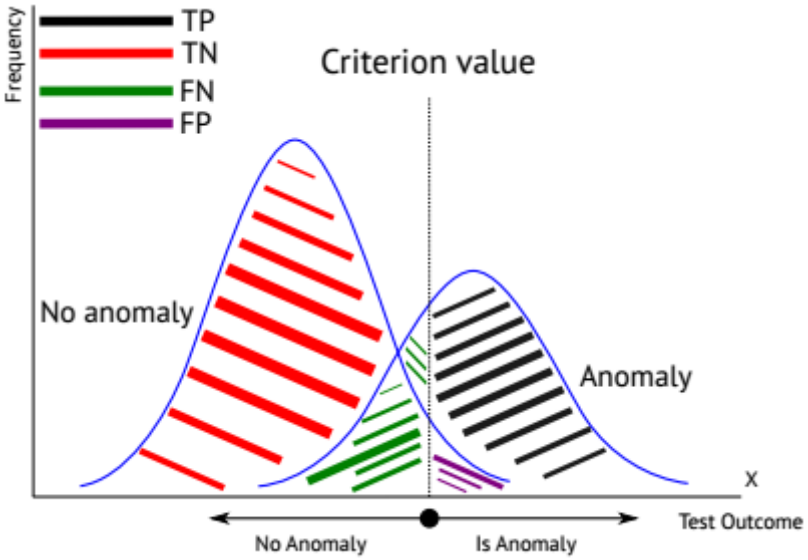
Odhadování hodnot

- Simple moving average
    - Další hodnota je vypočtena z průměru n předcházících
- Cumulative Moving Avereage
- Weighted Moving Average

Charakteristiky

Počet toků, paketů, bytů
Rychlost, b/s, p/s, t/s

Detekce anomálií



Detekce

- Detekce útoků na základě známých vzorů
- Detekce neznámých útoků na základě anomálií

10. přednáška

Digitální forenzní analýza

- Sbírání dat
- Prezentace výsledků
- Potvrzení hypotéz
- Reportování, které obstojí u soudu atd.

Rekonstrukce časové osy
Rekonstrukce dat
Odhaduje zneužití IT infrastruktury

Oblasti

- Počítačová (permanentní paměť)
- Síťová (provoz na síti))
- Softwarová (zkoumání škodlivého kódu)
- Živého systému (kompromitovaný host)

Důležité informace

- Napadený stroj
- Útočník
- Způsob útoku
- Cíl útočníka
- Jak omezit dopady

Digitální důkazy

Může být cokoliv

- Soubory
- Metadata
- Záznamy logů
- Zachycený provoz sítě, toky

Digitální důkazy jsou data

- Těžko sbíratelná
    - Mohou být dostupná jen po krátkou chvíli
    - Množství data je velké

- Jednoduše se poruší
    - Každý start změní časové známky v systému
    - Každý start procesu změní paměť
    - Při vypnutí přijde o paměť

Fáze

1. **získání dat**
2. **analýza a vyhodnocení**
3. **Reportování**

Sběr dat

1. Síťová konfigurace, procesy, paměť
2. Filesystem pevných disků a flash pamětí
3. Externí logy a síťové monitroing

4. Netechnické věci

Příklady

- Časové známky z filesystému
- Otisk paměti RAM? Hesla, šifrovací klíče
- Internetová spojení
- Netflow
- Logy z operačního systému a aplikací

Vždy pracovat s kopiemi dat
Všechny postupy musejí být pečlivě zaznamenány

Důležité i netechnické dovednosti

- Podpora managementu
- Komunikace v týmu
- Právní aspekty

11. přednáška

Typy incidentů z pohledu průběhu

- Útočník stále využívá
- Útočník přestal
- Jsou k dispozici jen artefakty

Komunikace

- Zabezpečené email, digitálně podepsané x.509
- IM
- Videokonference
- Kontakty na ostatní týmy

Sdílení dat

- Zabezpečené sdílené uložiště
- FLASH disky, HDD
- E2E šifrování
- Integrita, sdílí se i hashe

Časové známky

- **Mtime** (modifcation time) – změna obsahu souboru
- **Atime** (access time) – poslední část přístupu
- **Ctime** (change time) – změna metadat

Analýza podezřelých souborů

- **Statická**
  - Hledání stringů
  - Reverzní inženýrství
- **Dynamická**
  - Kontrolované spuštění v sandboxu a pozorování
  - Neprozkoumá všechny možné způsoby, které mohou nastat
  - Malware může detekovat že je analyzovaný

Spojené vztahy akcí, např. připojení přes SSH spustí tyto akce:

- Síťová komunikace přes TCP port 22
- Záznam v auth.log
- Vytvořena struktura v OS (běžící ssh process)
- Změna konfigurace uživatele, který přistoupil

12. přednáška

Digitální důkazy

- Striktní požadavky na sběr procesů
- Hashe
- Časové známky