MI-PB-19

Behaviorální analýza provozu počítačových sítí, detekce a identifikace anomálního chování.

Data Mining

Proces automatického objevování užitečných informací ve velkém množství dat

Fáze:

- Příprava dat
- Selekce dat
- Čištění dat
- Začlenění předchozích znalostí
- Správná interpretace výsledků

Kategorie:

- Prediktivní: zkoumání dat za účelem předpovědi budoucího vývoje
- Deskriptivní: charakterizace společných vlastností dat a vztahů mezi nimi

Data mining v síťové bezpečnosti:

- Nepoužívají se signatury, ale usage patterns
- Též machine learning nebo behaviorální analýza
- Základní přístupy:
  - **Misuse detection:**
    - Normální vs. škodlivý datový tok
    - Modely škodlivého chování tvořeny automaticky
    - Často lepší pravidla, než manuálně vytvořené signatury
    - Dobrá detekce známých útoků
  - **Anomaly detection:**
    - Klasifikační algoritmy, prediktivní modely
    - Modely normálního chování vytvořeny automaticky
    - Odchylky z normálu automaticky detekovány
    - Teoreticky dokáže detekovat neznámé útoky

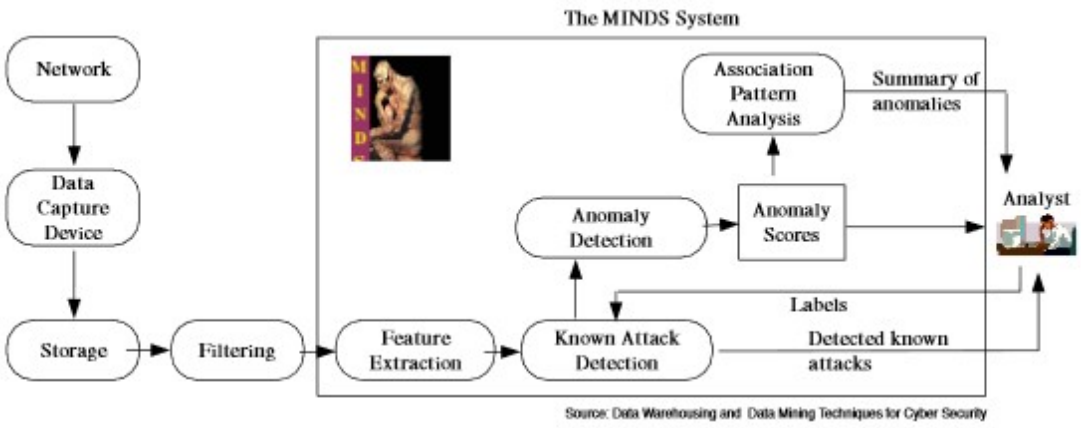
    - Teoreticky vysoký false alarm rate
    - **Trénink:**
        - **Supervised:** modely normálního chovány sestaveny z trénovacích dat
        - **Unsupervised:** žádná trénovací data, automatické učení o anomáliích (clustering, outlier detection)

Detekce založená na asociačních pravidlech:

- Jednoduchá metoda založená na počítání společných výskytů položek v transakčních databázích
- Unsupervised
- Asociační patterny: časté sady položek nebo asociačních pravidel
- Konstrukce profilu normálního provozu (např. HTTP dotaz: protokol=TCP, dstPort=80, numPackets=3...6: if port=80 and word3=HTTP/1.0 then word1=GET or POST)

Minnesota Intrusion Detection System (MINDS)

- Používá data mining k unsupervised detekci anomálií a analýze asociačních patternů



- **Operace:**
    - **Feature Extraction:**
        - Hlavní vlastnosti: src a dst IP a port, protokol, flagy, velikost, počet paketů
        - Odvozené vlastnosti pro časové okno T sekund: spojení s podobnými charakteristikami
        - Odvozené vlastnosti pro okno posledních N připojení: podobné charakteristiky spojení z různých zdrojů
    - **Signature-based detection for known attacks:**
        - Útoky detekované podle signatury nejsou již dále analyzovány
    - **Detekce anomálií:**
        - Outlier detection přiřadí anomální skóre tokům
        - Lidi analyzují jen nejvíc anomální toky
    - **Association pattern analysis:**
        - Seskupení nejanomálnějších spojení

        - Lidi rozhodují, jestli seskupení lze využít k tvorbě signatur pro prvotní detekce
- Local Outlier Factor:
    - Přirazen každému bodu
    - Lokální vůči sousedům
    - Výpočet: poměr hustoty okolí každého bodu k průměrné hustoté všech sousedů

IDS/ADS

IDS: intrusion detection system

- detekce podezřelého/škodlivého provozu
- host-based / network-based
- signature-based

ADS: anomaly detection system

- statistika, machine learning
- odchylky od normálního porovozu
- detekce známého a neznámého provozu

IPS: instrusion prevention system

- identifikace škodlivé aktivity, log, report, blokování
- zahazování paketů, reset spojení

Packet-based:

- Snort:
    - IDS/IPS
    - Stavový: detekce na základě pravidel s prahy pro sledování, kolikrát bylo pravidlo použito
    - Signature-, protocol-, anomaly-based
    - Sniffer, packet logger, intrusion detection
    - Součásti
        - Packet decoder: pakety z různých rozhraní
        - Preprocesory: modifikace paketů, sestavení fragmentovaných paketů, anomálie v hlavičkách
        - Detection Engine: aplikace pravidel na IP hlavičku, transportní hlavičku, apliakční hlavičku a data paketu
        - Output plugins: log, upozornění mailem, XML, ...

    - Pravidla:

      ```
      action protocol src_ip src_port direction dst_ip dst_port (options)
      ```

      Např.

      ```
      activate tcp any any -> 192.168.21.21 (content:"/bin/sh")
      ```

- Zeek:
    - Transformuje pakety na eventy
    - Eventy zpracovány script interpreterem (Turing kompletní skriptovací jazyk)
    - Application Layer decoding, detekce anomálií, signature amtching, analýza připojení
- Suricata:
    - IDS, IPS, Network Security Monitoring
    - TCP/IP engine, protocol parsing
    - Pravidla:

      ```
      action header options
      ```

      Např.

      ```
      drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN")
      ```

Flow-based:

- NEMEA: Network Measurements Analysis
    - Modulární -- propojené nezávislé NEMEA moduly
    - Application-aware
- FastNetMon:
    - Detekce DDoS během 2 sekund
    - Podpora BGP

Incident Response

Event: pozorovatelná událost v systému nebo na síti
Adverse event: event z negativními následky

Computer security incident: narušení nebo hrozba narušení politik počítačové bezpečnosti

- Úmysl způsobit škodu
- Proveden člověkem
- Zahrnuje výpočetní prostředek
- Např. krázež dat, neoprávněný přístup k PC, šíření malwaru

Incident Response:

- **Činnosti:**
  - Potvrzení, zda se projevil incident
  - Rychlá detekce a izolace
  - Určení a zdokumentování rozsahu incidentu
  - Minmalizace narušení chodu společnosti
  - Minimalizace škod
  - Obnovení normálních operací
  - Školení managementu
- **Kdy je potřeba:**
  - Dějí se incidenty
  - Efektivní reakce na incident může minimalizovat škody

Řešení incidentu:

- **Příprava**
  - Příprava na incident: Politiky, plány, procedury
  - Předcházení incidentům
  - Incident Respone Team (centrální vs. distribuovaný): interní zaměstnanci X částečně outsourcovaný X plně outsourcovaný
- **Detekce a analýza:**
  - Vektory útoku
  - Indikátory incidentu
  - Real-time monitoring
  - Uživatelé: phishing
  - SIEM: Security Information and Event Management:
    - Logování z HW a SW systémů
    - Analýza, souvislosti událostí
    - Log, report, alert
- **Zadržení, eradikace incidentu a obnovení:**
  - Činnosti nutné k tomu, aby se zabránilo dalším škodám (odpojení systému, odebrání uživatelského přístupu, změna hesel...)
  - Eradikace: identifikace, odstranění a oprava zranitelností, implementace dalších bezpečnostních kontrol
    Obnovení: pokračování v běžné činnosti
  - Tvorba chain of evidence: každé předání důkazu se loguje s podpisy
  - Sběr dat: offline/live -- forenzní nástroje
  - Analýza malwaru (statická/dynamická)
- **Post-incident activity:**

- Poučení z chyb, zlepšení