Data Security H4: IT security: detectie

Inhoud

[(N)IDS 3](#_Toc466206283)

[IDS ontwijking 3](#_Toc466206284)

[Lokale malware-detectie 4](#_Toc466206285)

# (N)IDS

* Network Intrusion Detection Systems
* Inspectie van alle inkomend & uitgaand verkeer, op zoek naar verdachte patronen
* IDS vs IPS:
  + (N)IDS: Intrusion **Detection** System
    - **Detecteert** problemen & **rapporteert** ze
    - Vaak “offline”: de sensor wordt aan een poort gekoppeld om zo een “kopie” van het netwerkverkeerd te inspecteren
    - Voordeel: volledig onzichtbaar voor aanvallers
  + (N)IPS: Intrusion **Prevention** System
    - Kan zelf ingrijpen op netwerkverkeer (connecties sluiten, redirect,...)
    - **Verkeer moet door dit toestel**, en kan ook geblokkeerd worden
* Detectie binnen NIPS
  + Signature detectie
    - Bepaalde byte-patronen worden gelinkt aan bepaalde threats
    - Opletten voor false positives/negatives
  + Anomalie detectie
    - Afwijkend verkeer detecteren
      * VB: portscans, plotse verhoging bandbreedte, uitgaand verkeer, afwijkende pingpakketten, logs,...
    - Vaak voorafgegaan door een meting/inventarisatie van ‘normaal’ verkeer (=baseline)
  + Opmerking: het herkennen van malafide patronen is niet evident
    - VB: cryptolocker encrypteert alle bestanden, maar een goede encryptietool doet dat ook
    - VB: veel emails versturen op korte tijd kan verdacht zijn, maar het kan net zo goed een nieuwsbrief zijn
* Honeypot
  + =Een IT systeem dat is opgezet om aanvallers te lokken die het netwerk aanvallen
  + Zal...
    - Verkeer loggen
    - Alerts triggeren
    - Verleidelijk gemaakt worden door met lagere beveiliging te werken
    - Niet gekoppeld zijn met ‘echt’ belangrijke data

# IDS ontwijking

* Insertion technique
  + Aanvallert stuurt in een ‘aanval’ een specifiek pakker dat de bestemmeling niet doorlaat, maar de IDS wel doorlaat
  + Of omgekeerd: aanvaller stuurt in een ‘aanval’ een specifiek pakket dat de bestemmeling wel zou aanvaarden, maar de IDS niet doorlaat
* Obfuscation
  + Encoding van payloads (VB: naar unicode) zodat enkel nog de doelhost dit begrijpt
  + Polymorfe code ontwikkelen om signatured-based IDS systems te ontwijken
  + Afwijkende bestandsnamen/paden/...
  + Aanval uitvoeren over geëncrypteerde verbinding
  + False positives genereren om het slachtoffer te verwarren
  + Fragmentation
  + Session splicing
* Fragmentation attack
  + IP-pakketten kunnen opgesplitst worden als ze te groot zijn
  + Misbruik mogelijk door opzettelijk op te splitsen
  + Om te detecteren: IDS meot de fragmenten opnieuw samenstellen
  + Maar: aanvaller kan de timings vergroten tot de reassembly timeout van de IDS overschreden wordt
* Time-To-Live attack
  + Pakketten worden geïnjecteerd met een te lage TTL, om zo de IDS te verwarren
* Overlapping fragments attack
  + Maakt gebruik van de verschillende reassembly policies in toestellen
    - VB: Windows geeft voorkeur aan originele fragmenten, Cisco bewaart altijd de laatste versie van een bepaald fragment

# Lokale malware-detectie

* Host Intrusion Detection Systems
  + Auditing van specifieke host
  + Bevat vaak ook virusdetectie
  + Minder populair omdat fintuning complex is & een grote impact heeft op de performantie
  + Auditing van file system permissies, file integrity, registry....
    - Signature: verdachte bitpatronen definiëren
  + Anomalie detectie
    - * Parameters monitoren: tijd tussen aanmelden, gebruikte resources, grootte transfers
      * Threshold detectie: eenvoudig, maarveel false positives/negatives
      * Profile-based detection: gedrag uit het verleden in kaart brengen & afwijkingen detecteren
* Terminologie: malware
  + Virtus: malware die uitgevoerd moet worden
    - Infecteert andere bestanden
    - Trigger & payload
    - Soms polymorf (verandert bij elke infectie) of metamorf (herschrijft zichzelf)
  + Worm
    - Verspreidt zichzelf door actief op zoek te gaan naar slachtoffers
    - Multimorf/metamorf
  + Rootkit
    - Malware die zich in het OS zelf nestelt
    - Erg moeilijk te detecteren
  + Watering hole attack: hacker analiseert frequent bezochte sites van een slachtoffer & infecteert die sites
  + Spearphishing: heel persoonlijke vorm van phishing
  + Whaling: phishing die hooggeplaatste werknemers/bedrijfsleiders viseert