KRESTEN JACOBSEN

IDS / IPS

Hvad: Intrusion Detection System & Intrusion Protection System

Hvorfor:*IDS* - Opdage angreb (alarmer) for efterfølgende at kunne rette services / firewalls til og evt. genoprette "normal drift".

IPS - Opdage og blokere angreb direkte i netværket.

OVERBLIK: IDS / IPS

	Type	Description
Deployment options	Network based	Network sensors scan traffic that is destined to many hosts.
	Host based	Host agent monitors all operations within an operating system.
Approaches to Identifying Malicious Traffic	Signature based	A vendor provides a customizable signature database.
	Policy based	Policy definition and description is created.
	Anomaly based	"Normal" and "abnormal" traffic is defined.
	Honeypot based	Sacrificial host is set up to lure the attacker.

Network based: *NIDS & NIPS*

Fordele: Kan se trafik til mange hosts.

Ulemper: Kan ikke se hvad der foregår, hvis trafikken er krypteret.

Host Based: *HIDS & HIPS*

Fordele: Kan se trafikken *efter* dekryptering.

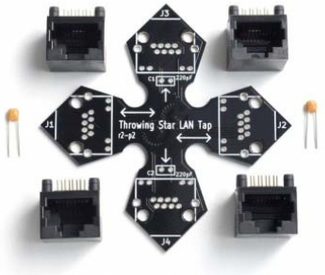
Kan principielt også overvåge aktivitet på hosten; processer, buffer overflow ol. (ude af scope på dette kursus)

Ulemper: Skal installeres på *hver* host (kan kun se en).

Man bør bruge en kombination af de forskellige typer, for bedst mulig dækning.

ARKITEKTUR: IDS / IPS – DATA COLLECTION + SOFTWARE STACK

	Hardware tap	Switch port mirroring
Pro	Kan skaleres nemt	Kræver (sikkert) ikke ekstra udstyr
Con	Kan være rigtig dyrt	Hastighed på porten begrænser



+

"Ninja stjernen" er et eksempel på en billig hardware network tap, men den kører altså også maksimalt 100MBIT.

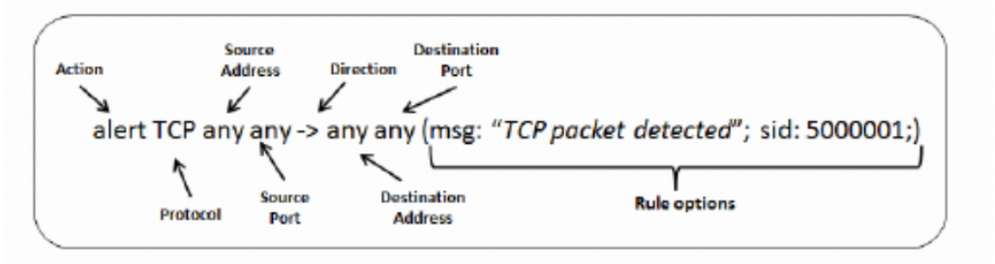
Snort bruges af en IDS / IPS til at "sniffe" trafik.

squil er et "Management interface", som kan rapportere på snort-regler.

EKSEMPEL: SYN-FLOOD DETECTION MED SNORT

- IDS / IPS'er kan bruges til at opdage og forhindre eks. syn-flooding.
- Eks. på snort-regel :

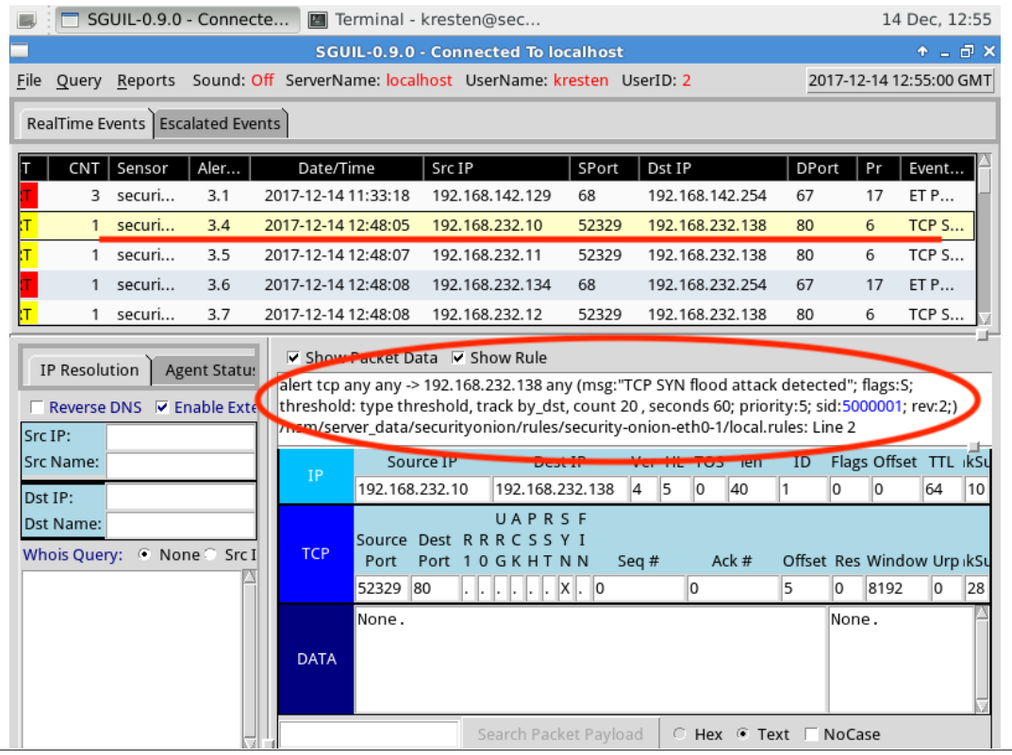
```
alert tcp any any -> 192.168.65.132 any (msg:"TCP SYN flood attack
detected"; flags:S; threshold: type threshold, track by_dst, count 20,
seconds 60; classtype:denial-of-service; priority:5; sid:5000001; rev:1;)
```



Snort-reglen sættes i `/etc/nsm/rules/local.rules`

Classtype overstreget, da jeg simpelthen ikke kunne få det til at virke med den sat og den derfor er pillet ud i reglen på næste side...

RELATEREDE EMNER: IDS / IPS



Screenshot fra SGUIL (administrationsmodul som kører oven på Snort) af capture fra foregående snort-regel.