Detekcia a prevencia sieťových prienikov

- Motivácia
- Základné pojmy
- Scenáre nasadenia NIDS
- Suricata NIDS
  - Základné prepínače
  - Režimy
  - Konfigurácia
  - Pokročilá funkcionalita
  - Pravidlá

Motivácia

- Firewall je efektívny nástroj na filtrovanie sieťovej premávky, preklad adries (NAT), prípadne “traffic shaping”
- Nevýhodou je, že robí rozhodnutia iba na základe dát v hlavičkách správ a neberie do úvahy obsah paketu - aplikačné dáta
- Príklad:

```
# allow established connections
iptables –A INPUT –m state --state RELATED,ESTABLISHED \
–j ACCEPT
# allow connection requests to web server
iptables –A INPUT –p tcp –dport 80 –m state –state NEW \
–j ACCEPT
# drop everything else
iptables –A INPUT –j DROP
```

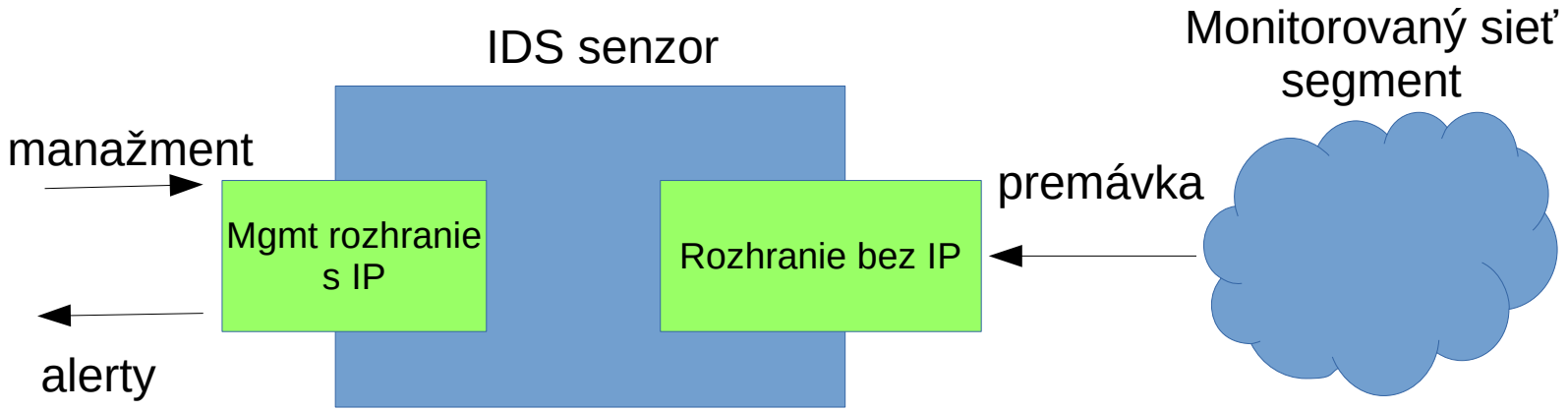
Čo ak niekto pošle paket, s cieľom zneužiť zraniteľnosti webového servera?

Basic Terms

- IDS (Intrusion Detection System) – monitoruje sieťovú premávku, analyzuje celý obsah paketov (hlavičky + dáta) a v prípade, že paket zodpovedá konkrétnym kritériám vygeneruje upozornenie (alert) pre bezpečnostného analytika. Vyžaduje, aby analytik konštantne sledoval alerty.
- IPS (Intrusion Prevention System) – je umiestnený tak, aby cez neho pretekala sieťová premávka, analyzuje prichádzajúce pakety a zahadzuje tie, ktoré zodpovedajú konkrétnym kritériám. Vyžaduje kvalitné a presné detekčné kritériá (nízka miera “false positive”).

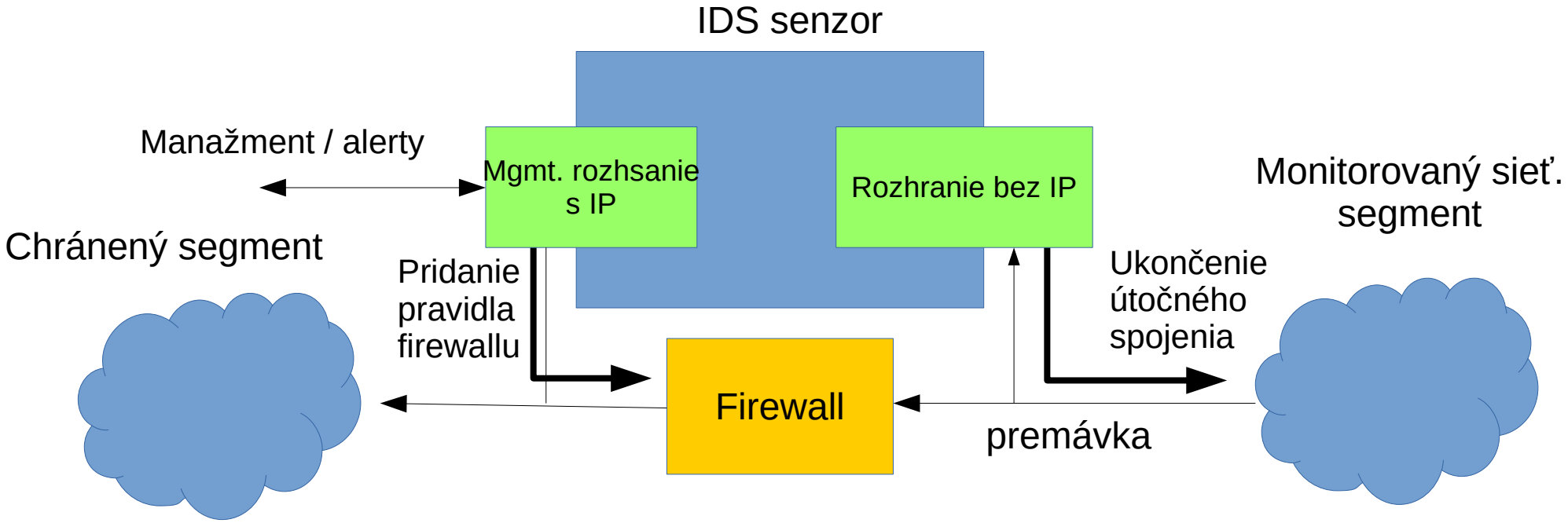
Nasadenie – IDS režim

- Režim IDS – pasívny
  - Monitorovanie komunikácie
  - Pripojenie cez hub / span port / network tap



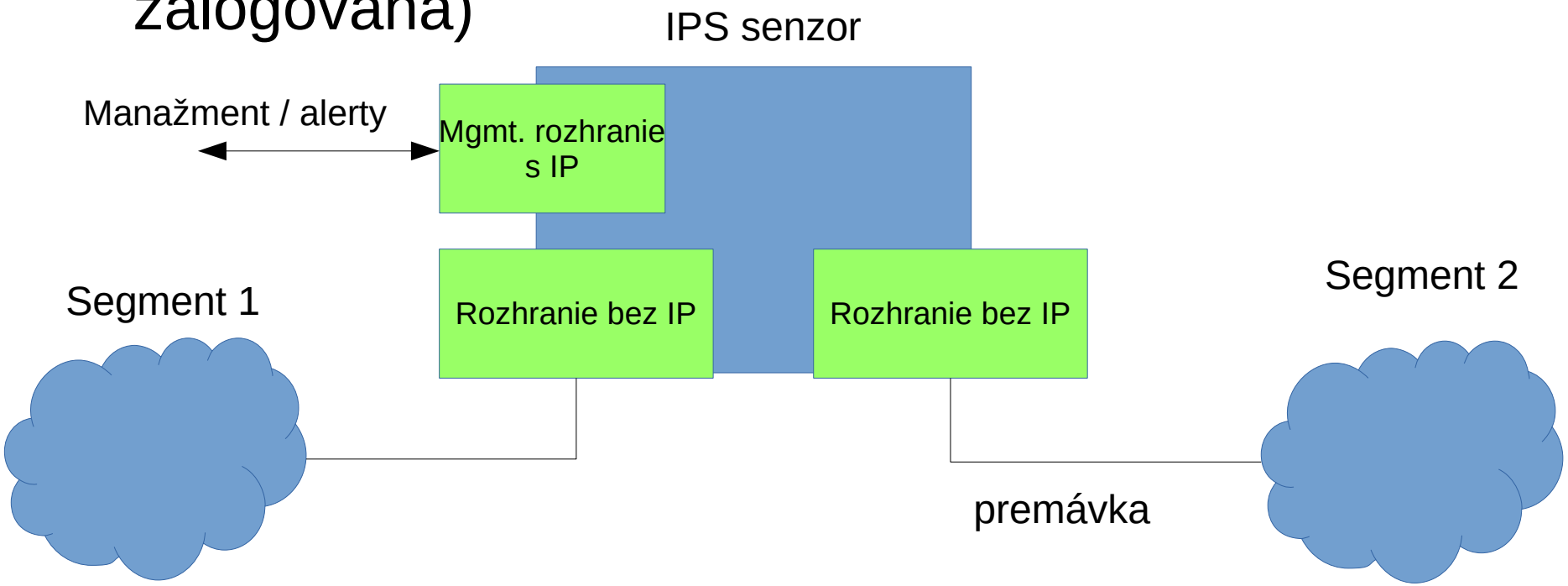
Nasadenie – IDS s aktívnou odozvou

- Režim IDS s aktívnou odozvou
  - Monitorovanie komunikácie
  - Pri útoku možnosť ukončiť útočné spojenie / upraviť pravidlá firewallu



Nasadenie – IPS režim

- IPS režim - inline
  - Premávka prechádza cez IPS senzor
  - Ak zodpovedá pravidlu je zahodená (prípadne zalogovaná)



Suricata

- “High performance Network IDS, IPS and Network Security Monitoring engine.”[1]
- Open Source.
- Vyvíjaná Open Information Security Foundation (OISF).
- Používa formát pravidiel snort.

[1] https://suricata.readthedocs.io/en/suricata-6.0.8/what-is-suricata.html

Suricata – Dôležité prepínače

`-h` – výpis help-u.

`-c <path>` – cesta ku konfiguračnému súboru.

`-T` – otestovanie konfigurácie.

`-v` – zvýšenie podrobnosti logovania.

`-i` <interface> - analýza paketov na rozhraní <interface>. Táto možnosť sa pokúsi použiť najvhodnejšiu metódu získavania paketov.

`-l` <directory> - logovanie alertov a paketov do adresára <directory> (default */var/log/suricata*).

`-k [all | none]` – Zapnutie (all) alebo vypnutie (none) kontroly kontrolných súčtov.

`man suricata`

Suricata – Runmodes (1)

- Dva hlavné režimy
  - IDS – iba detekcia,
  - IPS – detekcia aj prevencia.
- Každý režim môže ďalej bežať v **jednom** režime z *runmodes*.
- Runmode je špecifická kombinácia
  - modulov (module)– časti funkcionality, napr. decode-module,
  - vlákien (thread)– inštancie modulov, ktoré spracovávajú pakety (multi-threading),
  - fronty (queue) – posunutie paketu ďalšiemu vláknu.
- Režimy runmodes môžu byť: single, workers, autofp.
- Typicky previazané s výberom metódy odchytávania paketov.

Suricata – Runmodes (2)

- PCAP_DEV (pcap live mode) – odchytávanie premávky prostredníctvom knižnice libpcap library. Suricata beží v režime IDS.
- PCAP_FILE (pcap file mode) – analýza PCAP súboru.
- AF_PACKET_DEV (af_packet IPS mode) – podporuje IPS/tap režim, premostenie a monitorovanie premávky medzi sieťovými rozhraniami.
- NFQ (L3 IPS mode) – odchytánie premávky z iptables firewall-u prostredníctvom NFQUEUE. Suricata beží v IPS režime.
- Zobrazenie dostupných *runmodes*
  - `suricata --list-runmodes`

Suricata – IDS režim

- Predvolený režim.
- `-i` pre výber sieť. rozhrania, z ktorého chcete odchytávať premávku.
- Suricata sa pokúsi použiť najvhodnejšiu dostupnú metódu získavania paketov.
- Monitorovanie premávky na rozhraní eth0
  - `suricata -c \ /etc/suricata/suricata.yaml -i eth0`

Suricata – IPS s použitím Netfilter (1)

- **Layer 3 inline IPS režim**, suricata číta pakety z iptables NFQUEUE (NFQ).
  - Scenár 1: ochrana lokálnej siete,
  - Scenár 2: ochrana lokálneho hosta.

https://suricata.readthedocs.io/en/suricata-6.0.8/setting-up-ipsinline-for-linux.html#setting-up-ips-with-netfilter

Suricata – IPS s použitím Netfilter (2)

- Monitorovaná premávka v oboch smeroch musí byť presmerovaná do *nfqueue*, (vrátane. RELATED,ESTABLISHED ak sa používa) inak nefunguje detekcia relácií ani samotná komunikácia.
- Príklad: monitorovanie HTTP premávky na porte 80
  - `iptables -I INPUT -p tcp --dport 80 -j NFQUEUE`
  - `iptables -I OUTPUT -p tcp --sport 80 -j NFQUEUE`
  - `suricata -c /etc/suricata/suricata.yaml -q 0`
- V prípade, že na NFQ nepočúva žiaden používateľský program, všetky pakety sa ukladajú do fronty a zahadzujú.
  - --`bypass` zmena tohto správania na ACCEPT pre dôležitú premávku (napr. SSH).

Suricata – AF_PACKET IPS režim

- **Layer 2 inline IPS režim**, suricata preposiela pakety medzi rozhraniami a funguje ako IPS medzi nimi.
- Časť `af-packet` v konfiguračnom súbore.
- .Potrebné dve sieťové rozhrania
  - Obe rozhrania vyžadujú povolenie zero copy režimu (`use-mmap: yes`).
  - Obe rozhrania vyžadujú rovnakú hodnotu MTU.
- Metóda odchytávania AF_PACKET podporuje 2 režimy
  - `copy-mode: ips` (akcia drop sa použije),
  - `copy-mode: tap` (žiadne zahadzovanie).

Suricata – Konfigurácia (1)

- Predvolený konnfiguračný súbor */etc/suricata/suricata.yaml*
- Premenné
  - `HOME_NET, EXTERNAL_NET`, etc. - domáca/chránená sieť, externá sieť
  - `HTTP_SERVERS, SMTP_SERVERS`*, etc.* - adresy rôznych serverov na sieti
  - `HTTP_PORTS, FTP_PORTS` – štandardné porty používané službami na sieti
- Výstupy (logy)
  - *fast.log*, jednoriadkové upozornenia (podobne, ako snort fast.log).
  - *eve.log*, eve-log vo formáte JSON, vhodné, ak sa suricata používa v kombinácii s inými nástrojmi.
    - Použitie `jq` na zobrazenie / filtrovanie upozornení.
  - *suricata.log*, správy ohľadom fungovania suricaty.
  - *stats.log*, štatistiky o premávke a filtrovaní.
  - ...

Suricata – Configuration (2)

- Nastavenia odchytávania (Capture settings)
  - Metódy, ktoré budú použité na získavanie sieťovej premávky.
- Konfigurácia aplikačných protokolov (App Layer Protocol configuration)
  - Parsre/dekódery protokolov aplikačnej úrovne.
- Načítavanie pravidiel (Rule loading)
  - Predvolene načítané pravidlá získané použitím `suricata-update`.
  - Definovanie vlastných pravidiel pomocou `rule-files`.
- Ďalšie nastavenia
  - Nastavenia detečného modulu, pokročilé nastavenia, pokročilé sledovanie premávky, modul Defrag, ...

Suricata – Ovládanie

- Manuálne
  - `sudo suricata -c <config> ...`
- Ako služba
  - `sudo systemctl start suricata`
  - Konfigurácia parametrov a prepínačov
    - */etc/sysconfig/suricata* (RedHat-based distros)
    - */etc/default/suricata* (Debian-based distros)

Suricata – Pokročilá funkcionalita

- Automatická detekcia protokolov,
- Analýza PCAP súborov,
- Logovanie protokolových transakcií,
- Sieťové toky,
- Zaznamenávanie premávky do PCAP,
- Extraakcia súborov.

Suricata – Pravidlá

- Definície škodlivého/podozrivého obsahu, ktorý je hľadaný v sieťovej premávke (signatúry).
- Najdôležitejšia časť IDS/IPS.
- Potrebná častá aktualizácia (aj viackrát / deň).
- Voľné aj platené zoznamy pravidiel.
- Možnosť definovať vlastné pravidlá.

Suricata – manažovanie pravidiel

- nástroj `suricata-update`
- Download/update pravidiel
  - `suricata-update`
  - Predvolene stiahne pravidlá Emerging Threats (ET) Open ruleset.
  - Predvolená cesta k stiahnutým pravidlám: */var/lib/suricata/rules.*
- Dostupné viaceré sady pravidiel (rulesets)
  - `suricata-update list-sources`
  - `suricata-update enable-source <source>`
- Vlastné pravidlá
  - `local.rules`
  - reštart pre aplikovanie nových pravidiel.

Suricata – formát pravidiel

alert tcp $HOME_NET 2589 -> $EXTERNAL_NET any
(msg:"MALWARE-BACKDOOR..."; flow:to_client,established;
content:"2|00 00 00 06 00 00 00|Drives|24 00|"; depth:16;
metadata:ruleset community; classtype:misc-activity; sid:105; rev:14;)

- Akcia – vykonaná pri zhode (alert, drop, reject, pass, etc.)
- Protokol – tcp, udp, ip, icmp, ftp, ssh, http, tls, ...
- IP addresy – premenná, IP adresa, IP rozsah (IP/maska, [IP1, IP2]), negácia (!IP), any
- Port – premenná, port, rozsah, negácia, any
- **Smer** – zdroj **->** cieľ, **<>** obojsmerná komunikácia
- Možnosti (*options*) – message (loguje sa), podmienky vyhľadávania, klasifikácia pravidla, ID, ...

Suricata – vybrané možnosti pravidiel

- `content` – Hľadanie v obsahu paketu
  - `content:“text”;` - textové data
  - `content:”|0a0d|”;` - binárne data
  - `content:”text”; nocase;` – nezáleží na veľkosti písmen
  - `content:”/index.html”; http_uri;` – hľadanie v request URI bufferi
- `flow` – smer a stav toku (spojenia)
  - stav: established/not_established, only_stream/no_stream, only_frag/no_frag, ...
  - smer: to_server,to_client,from_server,from_client
  - `flow:established,to_server;`

Suricata – vybrané možnosti pravidiel (pokr.)

- `classtype` – klasifikácia pravidiel a alertov
  - na základe definícií v */etc/suricata/classification.config*
  - `classtype:trojan-activity;`
- `sid: n;` – signature ID
  - ID pravidla by malo byť unikátne
- `rev: n;` – číslo revízie pravidla

Zdroje

- man suricata
- https://suricata.io/
- https://suricata.readthedocs.io/en/suricata-6.0.8/
- https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_Developers_Guide