



Turris Omnia a Suricata

Když iptables nestačí

Michal Hrušecký • Michal.Hrusecky@nic.cz

2018-03-27 14:00:00 UTC



Turris Omnia

Omnia je "jen" odlehčený linuxový server

- normalní linuxové prostředí
- všechny běžné nástroje
- množství síťových interface
- spousta software v repozitářích
- je na rozhraní LAN/WAN

⇒ Ideální místo pro filtrování provozu



Firewall - iptables

- plné iptables
- jednoduše nastavitelné přes LuCI
- lze NATovat, blokovat, povolovat
- funguje spolehlivě a rychle
- omezuje se na low level - do čtvrté vrstvy
 - filtrování podle mac, ip, tcp/udp
- umí i nějaké stavové informace



Suricata

Když firewall nestačí...



Co je Suricata

- IDS/IPS systém
- umí pracovat s flow
- pracuje s daty uvnitř packetů
- mnoho pravidel na detekci různých aktivit
 - dobrý zdroj <http://doc.emergingthreats.net/>
- lze dopsat vlastní pravidla
- lze i blokovat
- lze propojit s dalším SW
- open source a dostupná v repozitářích pro Turris



Co je to flow

- packety které mají stejné:
 - zdrojová IP
 - cílová IP
 - protokol
 - zdrojový port
 - cílový port



Co se dá najít v datech

Pokud nešifrujete

- url webu
- obsah mailu
- odeslaný soubor
- co je na webu který si kdo prohlíží
 - známe konkrétní obsah, můžeme hledat klíčová slova
- ...
- prostě všechno

Dnes ale všichni šifrují (jen někteří o tom neví)!

Ne ale všechno je šifrované...



Co se dá najít pokud člověk šifruje

Pořád překvapivě hodně

Hlavně než se naváže šifrované spojení

A DNS je nešifrované

Při navazování se server prezentuje svým certifikátem

- víme společnost která certifikát vydala
- víme pro jaký/jaké servery ho vydala

Neznáme obsah komunikace, ale víme kdo s kým, kolik a jak dlouho



Ukázka dat - DNS

```
"dns": {  
  "type": "answer",  
  "id": 5146,  
  "rcode": "NOERROR",  
  "rrname": "www.turris.cz",  
  "rrtype": "A",  
  "ttl": 60,  
  "rdata": "217.31.192.105"  
}
```



Ukázka dat - TLS

```
"tls": {  
  "subject": "CN=forum.turris.cz",  
  "issuerdn": "C=US, O=Let's Encrypt, CN=Let's Encrypt  
Authority X3",  
  "serial":  
"03:99:E7:11:A0:3A:BC:AA:6F:5E:4A:AE:10:05:E5:02:7D:C1",  
  "fingerprint":  
"f2:14:91:48:ba:ad:3b:91:22:7c:1d:0d:b9:f9:a3:2f:dd:1a:f8:5c",  
  "sni": "forum.turris.cz",  
  "version": "TLS 1.2",  
  "notbefore": "2017-11-02T22:01:36",  
  "notafter": "2018-01-31T22:01:36"  
}
```



Pravidla pro Suricatu

- trojce ACTION HEADER RULE
- ACTION
 - pass, drop, reject, alert
- HEADER
 - PROTOCOL SRC_IP SRC_PORT -> DST_IP DST_PORT
 - tls \$HOME_NET any -> \$EXTERNAL_NET any
- RULE
 - Podle čeho vlastně matchujeme
 - (tls_sni;content:"fbcdn.net";sid:10123;rev:1;)
 - sid a rev jsou povinné, sid by mělo být unikátní



Blokování provozu

Lze blokovat podle různých pokročilých kritérií

```
drop tls $HOME_NET any -> $EXTERNAL_NET any ( \  
  msg:"Hazard detected"; \  
  tls_sni; content:"uctenkovka.cz"; \  
  sid: 11234; rev:1; )
```

Lze si i poznamenat dodatečné informace a hledat posloupnost stavů



Suricata a Turrís

- je v repozitářích
- má modulární konfigurační soubor
- máme zabalena i Emerging threads rules
- pracujeme na integraci
 - počátky budou v 3.9
 - balíček pakon



Pakoň

- démon co sbírá data o provozu
- poslouchá na br-lan
- ukládá si informace
- stačí nainstalovat balíček pakon a zapnout suricatu
- aktuálně pouze CLI
- lze se na výsledky dotazovat



Příklad

Kdo lezl za poslední týden na Facebook?

```
# pakon-show -s -7d -H facebook.com
|datetime          | dur.  | src MAC          | hostname
| dst port | proto | send  | recvd |
|
|
|2017-11-19 22:55:11 | 185s  | 0c:98:38:01:27:de | facebook.com
| https      | ?     | 4KiB | 1KiB|
|2017-11-20 00:04:34 | <1s  | 0c:98:38:02:a4:fe | facebook.com
| https      | tls   | 4MiB | 21MiB|
...

```



Příklad

Kam lezla moje televize za poslední týden?

```
# pakon-show -s -7d -m 1c:5a:6c:34:2c:19
|datetime          | dur.  | src MAC | hostname
  | dst port | proto | send   | recvd |
  |          |      |       |       |       |
|2017-11-22 06:01:55 | 292s  | ...    | google.com
  | https    | tls   | 105KiB | 338KiB|
|2017-11-22 06:02:50 | 33s   | ...    | hmma.baidu.com
  | https    | tls   | 665B   | 11KiB |
|2017-11-22 19:49:51 | 933s  | ...    | prima-ott-
sec.ssl.cdn.cra.cz
  | http     | http  | 3MiB   | 204MiB|
...

```



Srovnání Pakoně s Majordomo

Majordomo monitoruje IP a je schopný se dotázat na reverzní záznamy.

Problém jsou CDN, webhostingy a servery bez reverzu

Čili dostanete záznamy typu:

- slunce.srv.wz.cz
- edge-star-mini-shv-01-vie1.facebook.com

Pakoň dokáže rozlišit jednotlivé služby a kam opravdu člověk šel.

Pakoň nahradí Majordomo.



Budoucnost?

Pakoň bude mít i web inteface.

Rozvoj Pakoně a integrace Suricaty bude pokračovat.

Mezitím si můžete zkoušet co všechno Suricata umí.

Děkuji za pozornost

Otázky?

