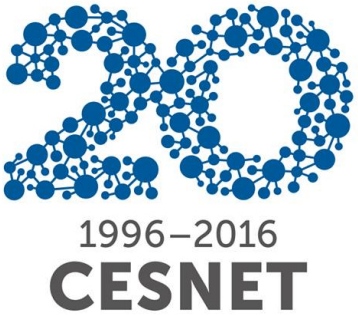

Tomáš Čejka
Petr Stehlík

{cejkat,stehlik}@cesnet.cz

Monitorování a bezpečnostní analýza

v počítačových sítích

installfest 2016 - workshop

Seznámení se systémem

- CentOS7.1, vytvořeno pomocí `packer.io`, na githubu zveřejníme skripty&šablony
- Nainstalováno spoustu užitečného SW mj.:
  - nmap
  - tcpdump
  - softflowd
  - nfdump
  - NEMEA systém
  - NEMEA Dashboard
- Instalováno většinou z RPM balíků

NEMEA: Kde se co najde?

- Spustitelné soubory (moduly, skripty): `/usr/bin/nemea`
- Konfigurační soubory: `/etc/nemea`
- Dokumentace a konfigurační části: `/usr/share/nemea*`
- Výstupní data, alerty: `/data/*`
- Komunikační soket a PID soubor supervisora: `/var/run/nemea-supervisor`
- Logy supervisora a std* modulů: `/var/log/nemea-supervisor`

Co bychom si tu měli/mohli vyzkoušet/ukázat:

- Kontrola nastavení a funkčnosti NEMEA
- Vygenerování vertikálního skenu a jeho detekce
- Ukázka práce s dodanými anonymizovanými daty (skripty + data v `/home/nemea`)
- NEMEA Dashboard

Kontrola nastavení a funkčnosti NEMEA

Služba nemea-supervisor běží jako služba (systemd):

```
service nemea-supervisor status
```

Systémovou službu (a tím všechny moduly NEMEA systému) je možné ovládat pomocí `/usr/bin/nemea/supervisor_cli`.
Viz. ikona na ploše...

V `/usr/share/nemea-supervisor` jsou části konfigurace, které se přegenerují do výsledného `/etc/nemea/supervisor_config.xml`. Pomocí `reload` se načte nová konfigurace.

Příp.:

```
/usr/bin/nemea/supervisor_cli -r
```

Vygenerování skenu

```
tcpdump -w vertical-scan.pcap
nmap -sS 192.168.1.101
tcpdump -x -nnn -r vertical-scan.pcap
nfcapd -p9995 -l ./netflow/
softflowd -n 127.0.0.1:9995 -r vertical-scan.pcap
nfdump -r `ls netflow/* | head -1` -o long
```

Použití NEMEA

Tam se nám to už měří (podle konfigurace by měl běžet `flow_meter` a `logger`).
Uložené flow:

```
tail -f /data/flow_meter/flows.csv
```

Alerty — spustit `vportscan2idea`, exportuje do DB.

Ukázka práce s dodanými anonymizovanými daty

- `csvfilter.sh`

  `./csvfilter.sh vportscan-anon DST_PORT '<=' 80`

- `generate-attacks-map.sh`
- `results.py`
- Kontrola výsledků (obrázků)

NEMEA Dashboard

- Úvod: architektura, technologie
- První přihlášení (localhost nebo 2280) + tvorba dashboardu
- Prohlédnutí detekovaných alertů, nahrazení dodanými daty

```
mongoimport --db nemeadb -c alerts_new \
    --file ~/data/mongo-alerts.json
```

- Úpravy a práce s dashboardem (drill-down)
- Dotazování se nad daty
- Future work & feedback

Závěr

Děkujeme za účast!