FSI LEI 2025/2026

Practical Exercises #4 Resolution examples

Goals

Network intrusion detection using Suricata (in Linux)

lo

Suricata in the packet sniffer mode

1. **Download** and **install** the suricata intrusion detection system with support for the "nfq" DAQ

   Seguir as instruções online (disponíveis no UCStudent)

   ```
   ##### Option 1: Install via YUM package manager
   yum install epel-release -y
   yum install suricata

   # Check that suricata has support for NFQ
   suricata --build-info | grep NFQ

   # Update rules
   suricata-update

   # Check configuration
   suricata -T -c /etc/suricata/suricata.yaml
   ```

2. Use suricata as a live packet capture mode to store captured packets (use pcap-logs)

   (ativar pcap-log em /etc/suricata/suricata.yaml)

   ```
   # Adaptar interface no comando seguinte
   suricata -i enp2s0 -c /usr/local/etc/suricata/suricata.yaml
   # (analisar logs em /var/log/suricata)

   # Testar com (acesso específico para testar IDS/IPS)
   curl http://testmyids.com

   # Em fast.log (alertas simples) confirmar registo do ataque detetado
   cat fast.log

   # Em eve.log (informação detalhado em JSON) confirmar mais detalhes:
   cat eve.json | jq 'select(.event_type=="alert")'| more
   ```

3. Check the contents of pcap files

   Usar o tcpdump -r para ler o ficheiro pcap

4. Run suricata in verbose mode.

   ```
   suricata -vvv -i enp2s0 -c /usr/local/etc/suricata/suricata.yaml
   ```

Suricata as a network intrusion detection system

5. Build a configuration file with rules for suricata/snort applicable to **the following types of communications**:

- Log all ICMP packets detected
- Alert when "POST" commands are detected in HTTP connections

Materials

- Suricata
- Suricata documentation

```
# Confirmar o rule-path que o suricata está a usar no ficheiro de
# configuração, adicionar o novo ficheiro de regras
```

```
##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - local.rules
```

```
cd /var/lib/suricata/rules/
# Criar ficheiro local.rules com regras.
```

```
alert icmp any any -> any any (msg:"ICMP Packet Detected";
sid:1000001; rev:1;)

alert http any any -> any any (msg:"HTTP POST detected";
content:"POST"; http_method; sid:1000002; rev:1;)
```

6. Run Suricata inline using the NFQ.

```
# Send packets to suricata via NFQUEUE (example)

iptables -A OUTPUT -j NFQUEUE --queue-num 0

iptables -A INPUT -j NFQUEUE --queue-num 0


# Run suricata in inline mode (queue 0)

suricata -q 0 -c /etc/suricata/suricata.yaml
```