Prevencia a detekcia sieťových útokov 1 – zadanie č. 1

- **Úloha 1:**
  - Nastavte domácu sieť na IP adresu Vášho virtuálneho stroja.
  - Stiahnite voľne dostupné pravidlá "Emerging Threats Open" (ET Open).
  - Spustite suricatu ako službu v režime IDS.
  - Demonštrujte správnu funkčnosť pravidiel vygenerovaním testovacieho alarmu.
- Hodnotenie: 0.5 b

Prevencia a detekcia sieťových útokov 1 – zadanie č. 2

- **Úloha 1:**
  - Vytvorte pravidlo, ktoré vygeneruje upozornenie pri pokuse o komunikáciu z Vášho stroja na zvolenú cieľovú IP adresu a TCP port.
- **Úloha 2:**
  - Vytvorte pravidlo, ktoré vygeneruje upozornenie pri pokuse o HTTP komunikáciu z Vášho stroja v smere na server cez neštandardné porty.
  - Použite automatickú detekciu protokolov.
- Otestujte konfiguráciu a demonštrujte funkčnosť pravidiel v režime IDS.
- Vysvetlite význam monitorovania odchádzajúcej komunikácie zo siete.
- Hodnotenie: 1 b.

Prevencia a detekcia sieťových útokov 1 – zadanie č. 2 (pokr.)

- **Úloha 3:**
  - Spustite shell z predchádzajúcho cvičenia na Vami zvolenom porte a pripojte sa naň z iného (kolegovho) stroja.
  - Vytvorte pravidlo, ktoré zahodí pakety obsahujúce reťazec "/etc/shadow" vo vytvorenom spojení v smere na server cez zvolený port.
  - Otestujte konfiguráciu a demonštrujte funkčnosť pravidla v režime L3 inline IPS.
- Hodnotenie: 0.5 b.

Poznámky

- Vlastné pravidlá zapíšte do súboru */var/lib/suricata/rules/local.rules*.
- Pravidla testujte z iného stroja (napr. kolegovho) - premávka s rovnakou zdrojovou a cieľovou IP môže byť považovaná za podozrivú.
- V prípade, že suricata správne nedeteguje spojenia, môže byť chyba v nesprávnych kontrolných súčtoch paketov - použite prepínač `-k`.
- Podľa potreby upravte konfiguráciu firewall-u.
- Na simulovanie počúvajúcich služieb použite program netcat, prípadne python.

Zdroje

- man suricata
- https://suricata.readthedocs.io/en/suricata-6.0.8/rules/index.html
- https://suricata.readthedocs.io/en/suricata-6.0.8/rule-management/index.html
- https://suricata.readthedocs.io/en/suricata-6.0.8/setting-up-ipsinline-for-linux.html
- man iptables
- man nc
- https://docs.python.org/3/library/http.server.html