Forschungsprojekt: Snort Integration

Integration von Snort in der Laborumgebung für praktische Übungen

Fakultät für Ingenieurwissenschaften

Paul Brandt

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES TECHNOLOGY, BUSINESS AND DESIGN

Gliederung

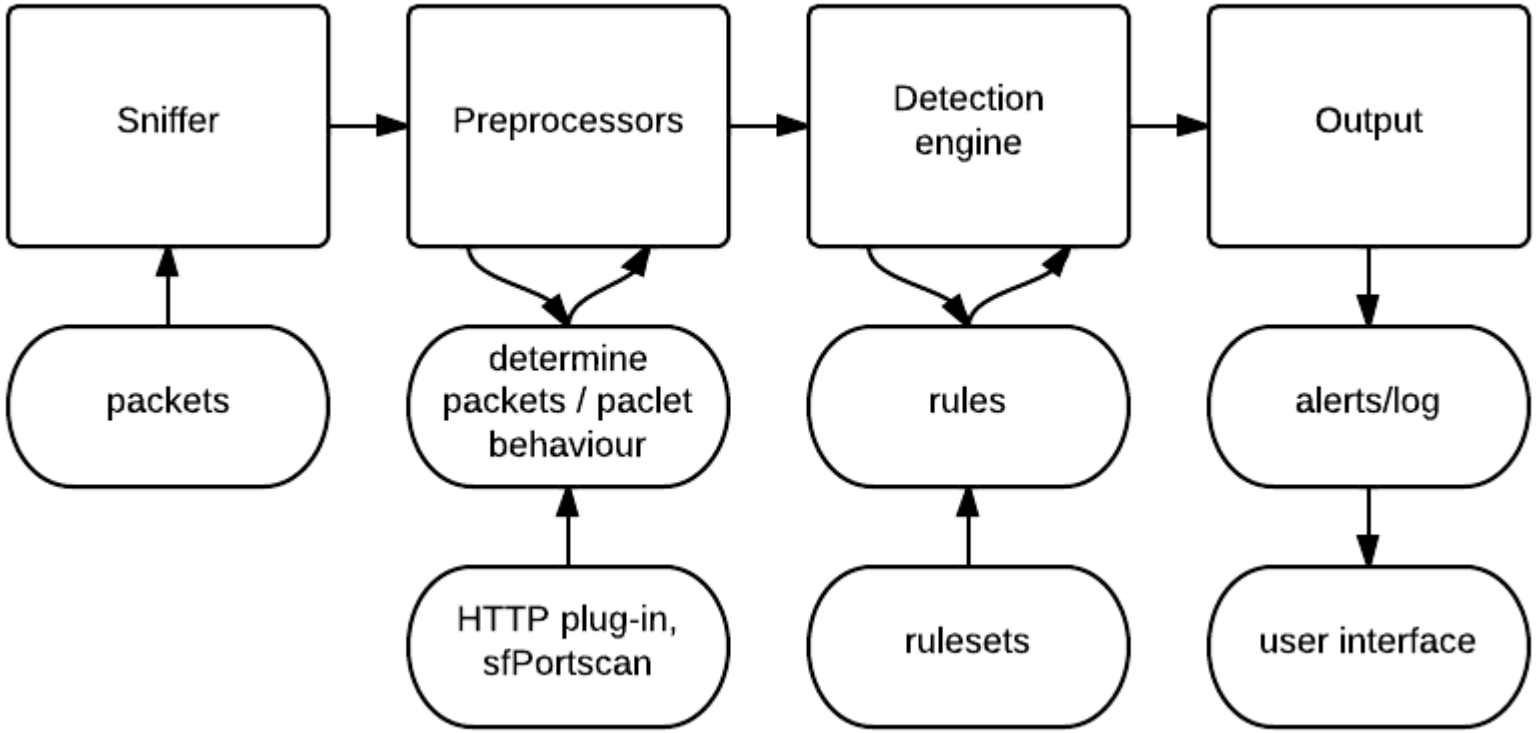
1. Aufgabenstellung
2. Snort
    1. Regeln
    2. Modi
3. Limitierungen der Laborumgebung
4. Livedemo

1. Aufgabenstellung

- Detaillierte Aufbereitung der theoretischen Grundlagen für einen Laborversuch auf Basis der bestehenden Laborkonfiguration
- Untersuchungen möglicher Angriffe und deren Erkennung im Zusammenspiel von Paketfiltern und IDS/IPS
- Umsetzung der Laborunterlagen in ein vorgegebenes Web-Template in englischer Sprache mit Aufbereitung von Demonstrations- und Laboraufgaben
- Implementierung, Testung und Aufbereitung der Ergebnisse des Laborversuches in der virtuellen Laborumgebung

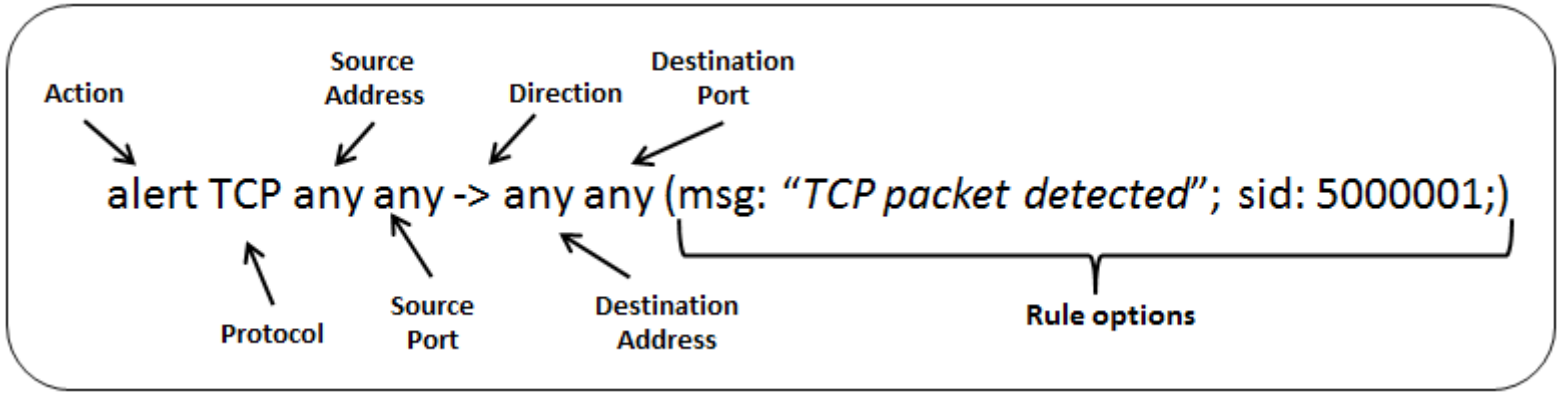
2. Snort

- Snort vorhanden (Scanner)
- Stellt IDS und IPS Funktionalitäten bereit
- Exploiterkennung via Rulesets möglich



2.1 Regeln

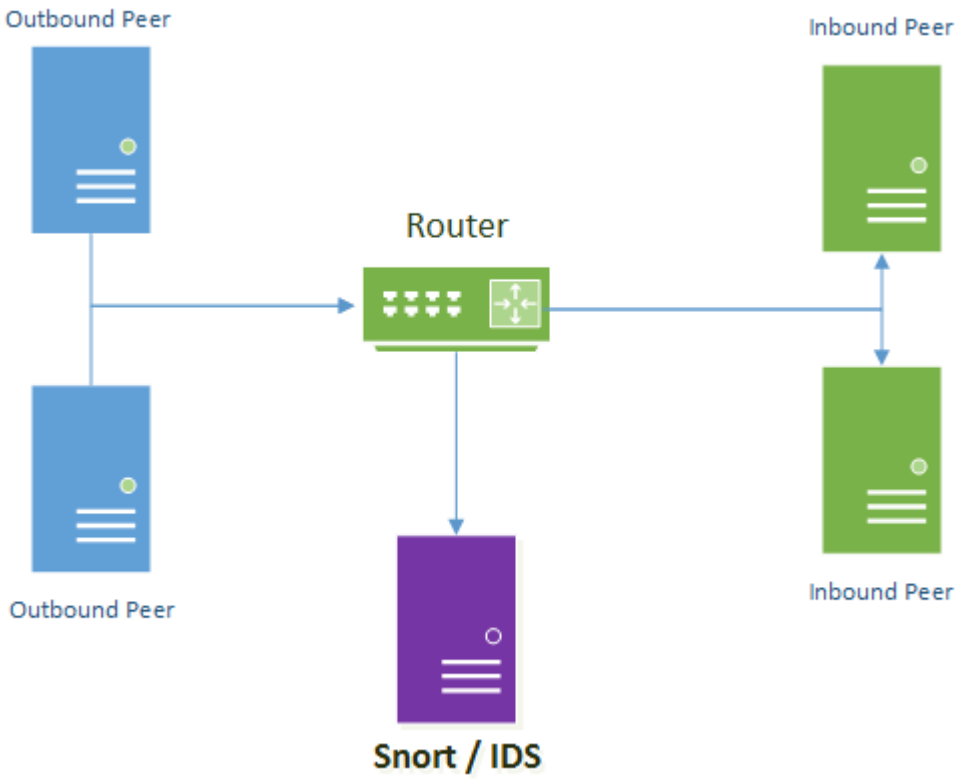
- Snort arbeitet auf Basis von Regelsätzen
- Beispiel:

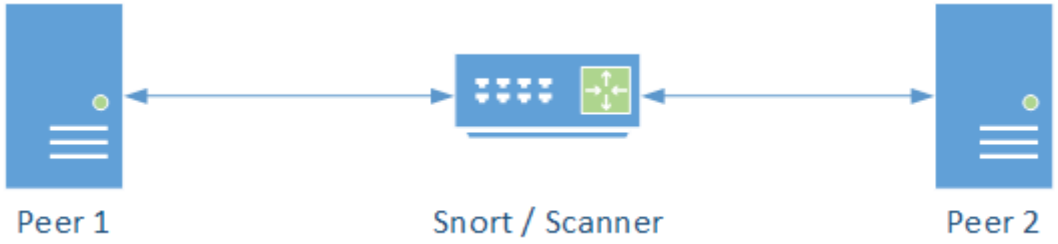


2.2 Modi

- Snort bietet 3 Betriebsmodi: passive, inline, inline-test
- Passive: IDS (nur alert / logging)
  - Beeinflusst Netzwerkperformance kaum
- Inline: IPS (Kann traffic blockieren)
  - Benötigt zwei NICs
  - Hat maßgeblichen Einfluss auf die Netzwerkperformance
  - Bei Ausfall: Keine Kommunikation zwischen angeschlossenen Netzen möglich
- Inline-test: simuliert inline ohne drops auszuführen
  - Verhält sich ähnlich wie passive bzgl. Netzwerkperformance

2.2 Modi





IDS Mode

IPS Mode

3. Limitierung der Laborumgebung

- Packet MTU scheinbar > 1514 Bytes
  - Führt ggf. zum nicht triggern von Regeln
- Scanner hat keine “Man in the middle” Position / Routeraufgaben
  - IPS Mode ist damit nur eingeschränkt simulierbar

4. Livedemo

- Dokumentation
- IDS Mode
  - Einfache und komplexe Regeln
- IPS Mode
  - Konfiguration und Start

Quellen

- https://www.snort.org/faq/what-is-snort (Stand: 16.06.2019)
- https://truica-victor.com/snort-architecture/ (Stand: 16.06.2019)
- http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node32.html (Stand: 16.06.2019)