Uma Introdução a Detecção de Intrusão utilizando Suricata

Caio Vargas

Detecção e prevenção de Intrusão: Por quê?

- **Cenário:**
  - Datacenter com diversos servidores
  - Estações de trabalho
  - IoT
  - Dispositivos móveis
  - Complexidade sempre aumentando
- **Necessidade de identificar atividade maliciosa no ambiente**
- **Número grande de hosts requer solução automatizada**
- **Solução: IDS**

HIDS vs NIDS

- **Host-based IDS (HIDS):**
  - Executa em cada host
  - Banco de dados com checksums de binários
  - Análise de regiões de memória de alta criticidade
  - Alto nível de acesso ao host
  - Host comprometido → IDS comprometido
  - Compatibilidade e escalabilidade
  - Exemplos: OSSEC, AIDE

HIDS vs NIDS

- **Network-based IDS:**
  - Executa em ponto central na rede
  - Análise de tráfego para detecção de ataques
  - Visão geral da rede
  - Escalável
  - Detecção de anomalias
  - Alto número de falso positivos
  - Criptografia impossibilita análise de tráfego
  - Exemplos: Snort, Suricata, Bro

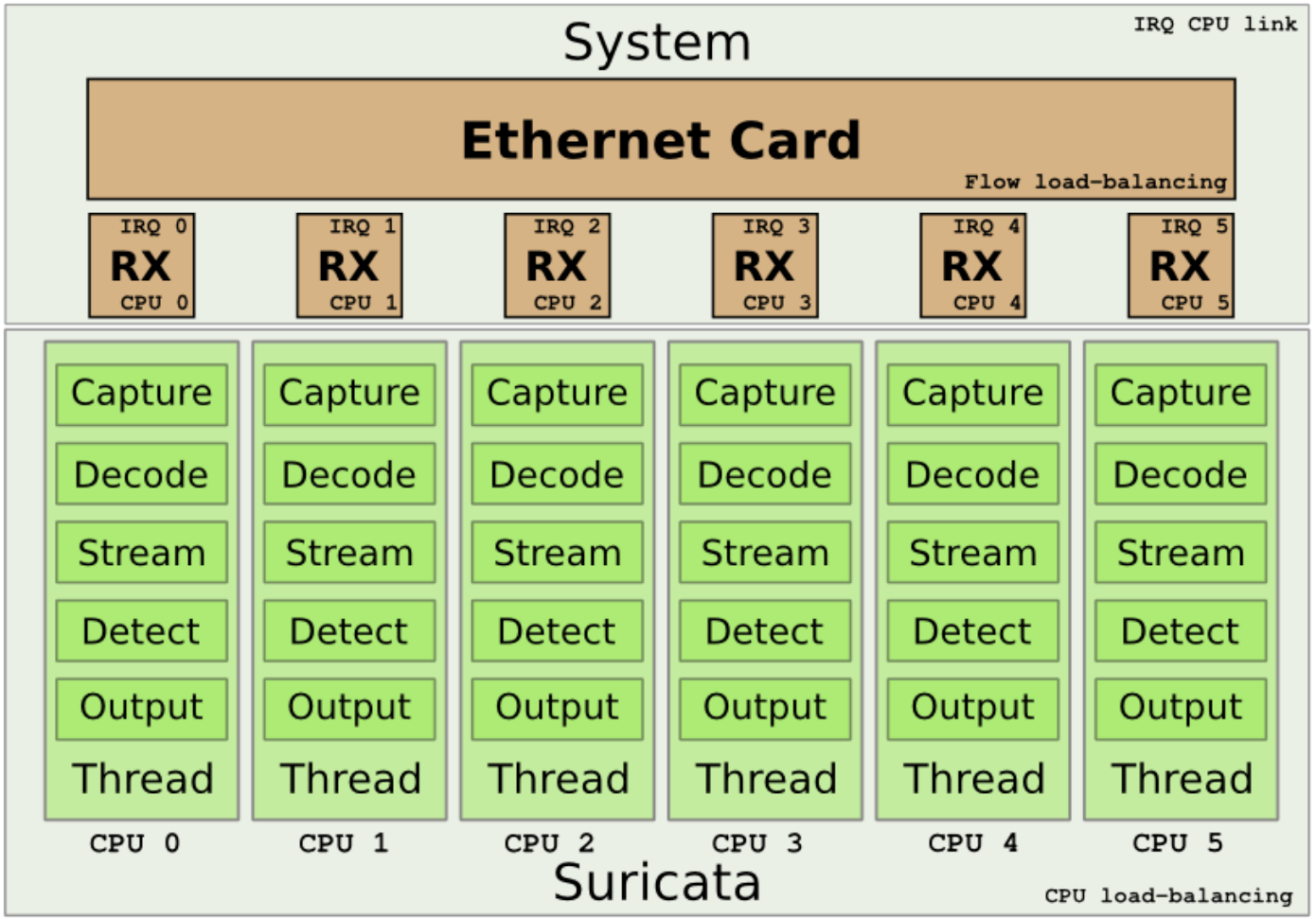
Suricata: O que é?

- Sistema de detecção e prevenção de intrusão baseado em rede (NIDS)
- Open Source
- Desenvolvido pela OISF como alternativa ao Snort (performance ruim)
- Baseado principalmente em assinaturas

Suricata: Como funciona?

- **Sensores posicionados onde possam inspecionar tráfego na rede (IDS) ou no meio do tráfego (IPS)**
  - Decodificação de pacotes
  - Reconstrução (desfragmentação e streams TCP)
  - Casamento de pacotes com assinaturas
  - Realiza ação (alert, drop, pass)

Suricata: Arquitetura



Suricata: Features

- **Detecção de protocolos**
  - DNS, HTTP, TLS, SMTP
- **Captura de arquivos**
- **Armazenamento de tráfego**
- **Log de flows (similar ao NetFlow)**
- **Log unificado em JSON**

Regras

- **Principal característica do Suricata:**
  - Permite customização do tráfego a ser detectado e das ações a serem tomadas
- **Baseadas na sintaxe de regras do Snort**
- **Conjunto de regras padrão com**

Regras: sintaxe

- **Compostas de três partes:**
  - Action
  - Header
  - Options

```
alert tcp 10.0.0.31 any -> any 80
(msg:"HTTP Google Access";
content:"google.com"; http_uri;
classtype:web-access; sid:1; rev:1;)
```

Regras: Actions

- **Action:**
  - Define qual ação a ser tomada quando a regra é ativada

alert

pass

drop (IPS)

Regras: Headers

- **Header:**
  - Define protocolo, endereços, portas e direção dos pacotes que ativam a regra

```
tcp 10.0.0.31 any -> any 80
proto ip port direction ip port
```

Regra: Options

- **Options:**
  - Fornece opções para logs e filtros para ativamento de regras

```
(msg: "HTTP Google Access";
content: "google.com"; http_uri;
classtype: web-access;
sid: 1;
rev: 1;)
```

Regras: Exemplos

```
alert http any any -> any !80 ( \¬
msg: "HTTP protocol on non-default port"; \¬
flow: to_server, established; classtype: policy-violation; \¬
sid: 1010100; gid: 1;)¬

alert tcp $HOME_NET 23 -> $EXTERNAL_NET any ( \¬
msg: "TELNET reply to external network"; \¬
flow: from_server,established; classtype: attempted-user; \¬
sid: 1010101; gid: 1;)¬

alert tcp $HOME_NET any -> $EXTERNAL_NET any ( \¬
msg: "PASSWD file detected"; flow: to_client,established; \¬
content: "root:x:0:0:root:/root:/"; classtype: policy-violation; \¬
sid: 1010102; gid: 1;)¬
```

Logs

- **Alertas e eventos geram logs**
  - Tentativas de ataque
  - Consultas DNS
  - Certificados X.509
- **Facilmente integrados com ELK**
  - Representação visual dos ataques ocorrendo na rede

Logs: alerta


```
{
    "timestamp": "2009-11-24T21:27:09.534255",
    "event_type": "alert",
    "src_ip": "192.168.2.7",
    "src_port": 1041,
    "dest_ip": "x.x.250.50",
    "dest_port": 80,
    "proto": "TCP",
    "alert": {
        "action": "allowed",
        "gid": 1,
        "signature_id" :2001999,
        "rev": 9,
        "signature": "ET MALWARE BTGrab.com Spyware Downloading Ads",
        "category": "A Network Trojan was detected",
        "severity": 1
    }
}
```

Logs: DNS query


```
{
   "timestamp":"2017-02-17T00:48:03.332510-0300",
   "flow_id":396785088,
   "in_iface":"eth0",
   "event_type":"dns",
   "src_ip":"192.168.122.217",
   "src_port":58939,
   "dest_ip":"192.168.122.1",
   "dest_port":53,
   "proto":"UDP",
   "dns":{
      "type":"query",
      "id":9013,
      "rrname":"google.com",
      "rrtype":"AAAA",
      "tx_id":1
   }
}
```

Demonstração

Perguntas?