Evaluation of the Suricata NIDS
---Proposal---

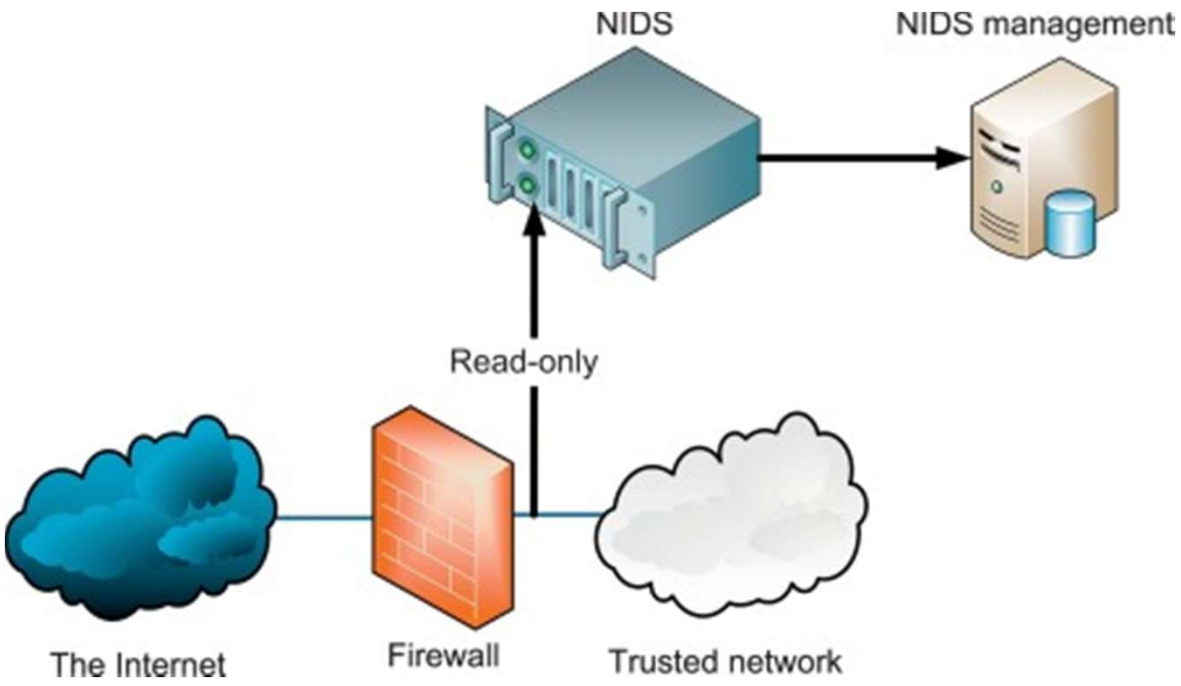
Jonathas Melo, Lucas Alcantara, **Marcelo d'Amorim**

IoT-Flows workshop, Michigan, May 24-25 2019
Funded by: NSF (US) and RNP (BR)

Network Intrusion Detection Systems (NIDS)

Software that monitors network traffic for attacks

Port scan
Spoofing(ARP,IP,DNS)
TCP SYN flood
Data modification
…



Variations of NIDS

- Signature-based (look for known issues)
- Anomaly-based (look for unknown issues)

Variations of NIDS

- **Signature-based (look for known issues)**
- Anomaly-based (look for unknown issues)

Our focus

Popular with several public alternatives available. E.g., Suricata, Snort, and Zeek.

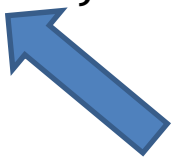
How it works?

- Security expert specifies attack pattern
- NIDS checks traffic
- The system or sys admin takes action

Basic Rule

Preventing SQL Injection Attack

```
alert tcp any any -> any 80 (msg: "Error Based SQL Injection Detected";
content: "%27" ; sid:100000011; )
```



Single quote

https://www.hackingarticles.in/detect-sql-injection-attack-using-snort-ids/

Rule Format

```
alert tcp any any -> any 80 (msg: "Error Based SQL Injection Detected";
content: "%27" ; sid:100000011; )
```

Action: pass, drop, reject, alert
Header: protocol source-address port [-> or <->] target-address port
Rule Options: …

https://suricata.readthedocs.io/en/suricata-4.1.4/rules/intro.html

Observations

- Rules are based on heuristics
- Hundreds of such rules exist
  (for Suricata: ~200 official, thousands non-official)
- They can get very confusing!

Observations

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sS window
2048"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:2048; threshold: type
both, track by_dst, count 1, seconds 60;
reference:url,doc.emergingthreats.net/2000537; classtype:attempted-recon;
sid:2000537; rev:8; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

https://security.stackexchange.com/questions/188021/suricata-nmap-scan-does-not-match-rules

- They can get very confusing

```
alert tcp $HOMEalert tcp $EXTERNAL_NET any -> $HOME_NET
[135,139,445,593,1024:]
(msg:"OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize path
canonicalization stack overflow attempt"; flow:to_server,established;
dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188; dce_opnum:31,32;
dce_stub_data;
pcre:"/^(\x00\x00\x00\x00|.{4}(\x00\x00\x00\x00|.{12}))/s";
byte_jump:4,-4,multiplier 2,relative,align,dce;
pcre:"/\x00\.\x00\.\x00[\x2f\x5c]/R"; metadata:policy balanced-ips
drop, policy connectivity-ips drop, policy max-detect-ips drop, policy
security-ips drop, service netbios-ssn;
reference:url,technet.microsoft.com/en-us/security/bulletin/MS08-067;
classtype:trojan-activity; sid:14782; rev:21;)_NET 3389 -> any any (msg:"ET
DOS Microsoft Remote Desktop (RDP) Syn/Ack Outbound Flowbit Set";
flow:from_server; flags:SA; flowbits:isnotset,ms.rdp.synack;
flowbits:set,ms.rdp.synack; flowbits:noalert; reference:cve,2012-0152;
classtype:not-suspicious; sid:2014385; rev:5; metadata:created_at
2012_03_15, updated_at 2012_03_15;)
https://redmine.openinfosecfoundation.org/issues/2559
```

Proposal

Detailed evaluation of Suricata

https://suricata-ids.org/

Why Suricata?

https://suricata-ids.org

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.

Why Evaluating Suricata?

- Impact of attacks is high
- Recent prior work exists [1], but results are preliminary (or complements our study)

[1] …, Open Source NIDS in a Production Environment. U. Lisbon MS dissertation, 2018.

Questions 1/2

- Can every mapped attack be detected by a rule?
- How often safe traffic is flagged?
- What happens under stress?
  - Many rules added
  - Intense traffic

Questions 2/2

- When a problem is detected (i.e., false pos/neg) …
  - Is it a misconfiguration?
  - Is it a bug in Suricata?
  - Is it a bug in the rule?

Method

- Consider both official and non-official rules
- Generate workloads
  - Benign and malicious workloads as per [1]
  - Create evading attacks from existing rules?

[1] Milenkoski et al., Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices. ACM Computing Surveys 2015.

(Some) Recent and Ongoing work

- Recent
  - Using Docker to assist StackOverflow users
  - Evaluating and Improving Parallel Test Execution
- Ongoing
  - Finding Bugs in JS engines with Differential Testing
  - Evaluating Seed Potential for Improved Fuzzing
  - Improving Random Sequence Generation
  - Evaluating Exploratory Testing in Practice (Motorola)

Evaluation of the Suricata NIDS
---Proposal---

Jonathas Melo, Lucas Alcantara, **Marcelo d'Amorim**

IoT-Flows workshop, Michigan, May 24-25 2019
Funded by: NSF (US) and RNP (BR)