

Packet Generation Tool for Testing a Network Intrusion Detection System

Author: Johnson Fong

Supervisor: Dr. Peter Sutton

Introduction: Network Intrusion detection System (NIDS) is a system designed to detect the evidence of computer network intrusion. It resides on a computer connected to a segment of a network and monitors network traffic on that network segment, looking for indications of ongoing or successful attack.

Aim: Snort is an example of an open source software implementation of a NIDS. Research and experience have shown that no NIDS is perfect; it may miss attacks (false negative) or report false alarms for legitimate traffic (false positive). This project aims to develop a highly configurable and flexible testing tool that is able to generate different streams of network packets based on set of parameters user provides.

Result: A testing tool has been developed which can analyse Snort rules and automatically generates series of alert-triggering traffic that conform to the rules.

It is capable of handling most aspects of rule options including the Perl compatible regular expression and flow option, which are only available to recent versions of Snort (2.0.0 onwards).

Furthermore, based on parameters the user specifies into the tool, a combination of alert-free and alert-triggering network traffic can be generated in an attempt to emulate a more realistic workload for NIDS performance evaluation.

Snort Output (260 Alert):

```

C:\WINDOWS\system32\cmd.exe
04/25[**] BAD-TRAFFIC TCP[**] 192.xx -> 10.xx
04/25[**] BAD-TRAFFIC TCP[**] 192.xx -> 10.xx
04/25[**] ICMP PING NMAP[**] 192.xx -> 10.xx
04/25[**] ICMP PING NMAP[**] 192.xx -> 10.xx
    
```

Snort Rule File:

```

Alert tcp any any -> any any
(msg:"BAD-TRAFFIC TCP"; flow:
established, ttl:=3; flags: SF,12;
window:!15;)
... ..
    
```

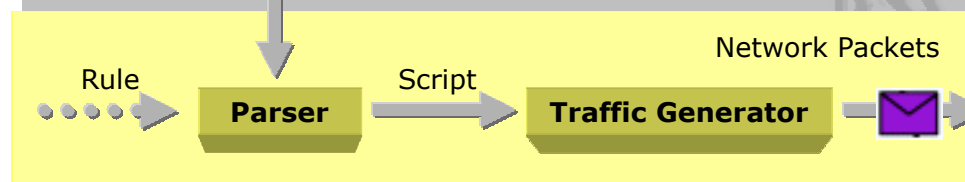
250 Bad Rules



TestingTool

```

C:\WINDOWS\system32\cmd.exe
./Testing Tool - TCP 500 - BAD 50% - portscan 10
    
```



EMBEDDED SYSTEMS

Innovation Expo