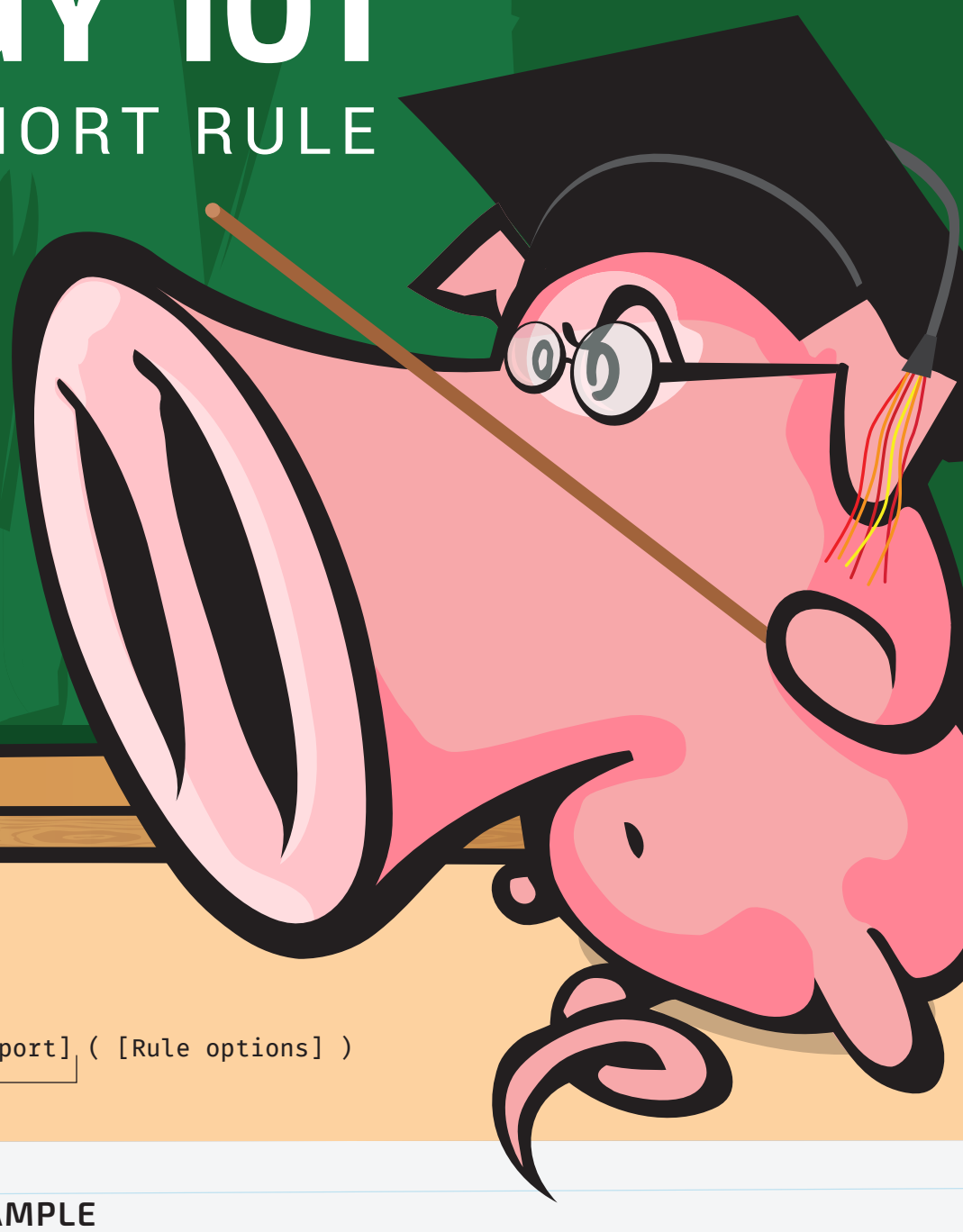
SNORTOLOGY 101

THE ANATOMY OF A SNORT RULE

WHAT IS SNORT?

Snort is an open source network intrusion prevention system (IPS) by Cisco. It is capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching and matching, and detect a variety of attacks and probes. Snort can be used as a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging), or as a full-blown network intrusion prevention system.



LET'S BREAK IT DOWN

BASIC OUTLINE OF A SNORT RULE

```
[action][protocol][sourceIP][sourceport] -> [destIP][destport] ( [Rule options] )
```

Rule Header

RULE HEADER

The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information.

`alert` **Action to take (option)** The first item in a rule is the rule action. The rule action tells Snort what to do when it finds a packet that matches the rule criteria (usually alert).

`tcp` **Type of traffic (protocol)** The next field in a rule is the protocol. There are four protocols that Snort currently analyzes for suspicious behavior - TCP, UDP, ICMP, and IP.

`$EXTERNAL_NET` **Source address(es)** variable or literal

`$HTTP_PORTS` **Source port(s)** variable or literal

`->` **Direction operator** The direction operator -> indicates the orientation of the traffic to which the rule applies.

`$HOME_NET` **Destination address(es)** variable or literal

`any` **Destination port(s)** variable or literal

EXAMPLE

Rule Header
```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
```

Message
```
msg: "BROWSER-IE Microsoft Internet Explorer CacheSize exploit attempt";
```

Flow
```
flow: to_client,established;
```

Detection
```
file_data;
    content:"recordset"; offset:14; depth:9;
    content:".CacheSize"; distance:0; within:100;
    pcre:"/CacheSize\s*=\s*/";
    byte_test:10,>,0x3ffffffe,0,relative,string;
```

Metadata
```
policy max-detect-ips drop, service http;
```

References
```
reference:cve,2016-8077;
```

Classification
```
classtype: attempted-user;
```

Signature ID
```
sid:65535;rev:1;
```

RULE OPTIONS

Rule options form the heart of Snort's intrusion detection engine combining ease of use with power and flexibility. All Snort rule options are separated from each other using a semicolon (;). Rule option keywords are separated from their arguments with a colon (:).

GENERAL RULE OPTIONS

Message A meaningful message typically includes what the rule is detecting. The msg rule option tells Snort what to output when the rule matches. It is a simple text string.

Flow For the rule to fire, specifies which direction the network traffic is going. The flow keyword is used in conjunction with TCP stream reassembly. It allows rules to only apply to certain directions of the traffic flow.

Reference The reference keyword allows rules to include references to external sources of information.

Classtype The classtype keyword is how Snort shares what the effect of a successful attack would be.

sid/rev The snort id is a unique identifier for each rule. This information allows output plugins to identify rules easily and should be used with the rev (revision) keyword.

DETECTION OPTIONS

Content This important feature allows the user to set rules that search for specific content in the packet payload and trigger response based on that data. The option data can contain mixed text and binary data.

- **distance/offset** These keywords allow the rule writer to specify where to start searching relative to the beginning of the payload or the beginning of a content match.
- **within/depth** These keywords allow the rule write to specify how far forward to search relative to the end of a previous content match and, once that content match is found, how far to search for it.

PCRE The pcre keyword allows rules to be written using perl compatible regular expressions which allows for more complex matches than simple content matches.

Byte test The byte_test options allows a rule to test a number of bytes against a specific value in binary.

SOURCE: SNORT.ORG *For more information about Snort and Snort rules, see additional documentation at snort.org.*