Using The Host Attribute Table Feature in Snort

SOURCEfire®

KNOW MORE NETWORK RISKS
NO MORE GUESSING

The Snort Host Attribute Table

- Host Attribute Table
  - The Host Attribute Table is used to tell Snort® about the hosts in your environment.
  - Using this information, you can make Snort® configure itself to properly handle fragment and TCP data streams destined for these hosts.
  - You can also make Snort® aware of services running in your environment even if they are running over non-standard ports.
  - To use this feature, you must compile Snort with the `--enable-targetbased` compile-time flag

SOURCEfire®

The Snort Host Attribute Table

- Host Attribute Files
  - Host attributes are defined by way of an XML formatted file that you load at Snort®'s initialization time.
  - Syntax example

```
attribute_table filename <path to file>
```

  - The Snort distribution ships with a Document Type Definition (DTD) file that describes the structure of the XML document

The Snort Host Attribute Table

- About the DTD file
  - It lists all the valid elements and document structure
  - There are many possible attributes that you can use to define the attributes of a host as illustrated in the DTD file
  - Only the following elements are actually used by Snort®
    - For Host entries:
      - STREAM_POLICY
      - IP FRAG_POLICY
    - For service attributes:
      - PORT
      - IPPROTO
      - PROTOCOL

The Snort Host Attribute Table

- DTD File

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT SNORT_ATTRIBUTES ((ATTRIBUTE_MAP, ATTRIBUTE_TABLE))>
<!ELEMENT ATTRIBUTE_MAP ((ENTRY*))>
<!ELEMENT ENTRY ((ID, VALUE))>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!ELEMENT ATTRIBUTE_TABLE ((HOST*))>
<!ELEMENT HOST ((IP, OPERATING_SYSTEM, (SERVICES | CLIENTS)*))>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM ((NAME, VENDOR, VERSION, FRAG_POLICY, STREAM_POLICY))>
<!ELEMENT NAME (((ATTRIBUTE_VALUE | ATTRIBUTE_ID), CONFIDENCE?))>
<!ELEMENT VERSION (((ATTRIBUTE_VALUE | ATTRIBUTE_ID), CONFIDENCE?))>
<!ELEMENT VENDOR (((ATTRIBUTE_VALUE | ATTRIBUTE_ID), CONFIDENCE?))>
<!ELEMENT FRAG_POLICY (#PCDATA)>
<!ELEMENT STREAM_POLICY (#PCDATA)>
<!ELEMENT CLIENTS ((CLIENT*))>
<!ELEMENT CLIENT (((PROTOCOL | (IPPROTO, PROTOCOL)), APPLICATION))>
<!ELEMENT SERVICES ((SERVICE*))>
<!ELEMENT SERVICE ((PORT, IPPROTO, PROTOCOL, APPLICATION?))>
<!ELEMENT PORT (((ATTRIBUTE_VALUE | ATTRIBUTE_ID), CONFIDENCE?))>
<!ELEMENT PROTOCOL (((ATTRIBUTE_VALUE | ATTRIBUTE_ID), CONFIDENCE?))>
<!ELEMENT IPPROTO (((ATTRIBUTE_VALUE | ATTRIBUTE_ID), CONFIDENCE?))>
<!ELEMENT APPLICATION (((ATTRIBUTE_VALUE | ATTRIBUTE_ID), CONFIDENCE?),VERSION?)>
<!ELEMENT ATTRIBUTE_VALUE (#PCDATA)>
<!ELEMENT ATTRIBUTE_ID (#PCDATA)>
<!ELEMENT CONFIDENCE (#PCDATA)>
```

The Snort Host Attribute Table

- Defining Host Attributes
  - ATTRIBUTE_MAP Entry

```
<ATTRIBUTE_MAP>
      <ENTRY>
          <ID>1</ID>
          <VALUE>Windows</VALUE>
      </ENTRY>
</ATTRIBUTE_MAP>
```

SOURCEfire®

The Snort Host Attribute Table

KNOW MORE NETWORK RISKS
NO MORE GUESSING

- Defining Host Attributes
  - ATTRIBUTE_TABLE Entry

```
<ATTRIBUTE_TABLE>
     <HOST>
          <IP>192.168.10.90</IP>
               <OPERATING_SYSTEM>
                    <NAME>
                         <ATTRIBUTE_ID>1</ATTRIBUTE_ID>
                    </NAME>
                    <FRAG_POLICY>windows</FRAG_POLICY>
                    <STREAM_POLICY>windows</STREAM_POLICY>
               </OPERATING_SYSTEM>
     </HOST>
</ATTRIBUTE_TABLE>
```

SOURCEfire®

The Snort Host Attribute Table

- Valid Frag3 Policy Values:
  - BSD
  - BSD-Right
  - First
  - Last
  - Linux
- Valid Stream5 Policy Values:

• first	• Last	• Bsd
• Linux	• old-linux	• Windows
• Vista	• Solaris	• Hpux
• Hpux10	• Irix	• macos

SOURCEfire®

The Snort Host Attribute Table

KNOW MORE NETWORK RISKS
NO MORE GUESSING

- Defining Host Attributes
  - ATTRIBUTE_TABLE Entry (Host running a service)

```
<SERVICES>
     <SERVICE>
          <PORT>
               <ATTRIBUTE_VALUE>80</ATTRIBUTE_VALUE>
          </PORT>
          <IPPROTO>
               <ATTRIBUTE_VALUE>tcp</ATTRIBUTE_VALUE>
          </IPPROTO>
          <PROTOCOL>
               <ATTRIBUTE_VALUE>http</ATTRIBUTE_VALUE>
          </PROTOCOL>
     </SERVICE>
</SERVICES>
```

SOURCEfire®

The Snort Host Attribute Table

- Triggering Rules On Host Attribute Defined Services
  - You can write rules to trigger on service definitions rather than the port numbers in the rule header
  - See the rule example below:

```
alert tcp any any -> 192.168.10.0/24 80 \
   (msg:"Attribute table test"; \
    metadata: service http; sid:1001000;)
```

Sourcefire Education Program

KNOW MORE NETWORK RISKS
NO MORE GUESSING

Training & Certification

- Public Classes Worldwide
- Customer On-sites
- Sourcefire Guarantees

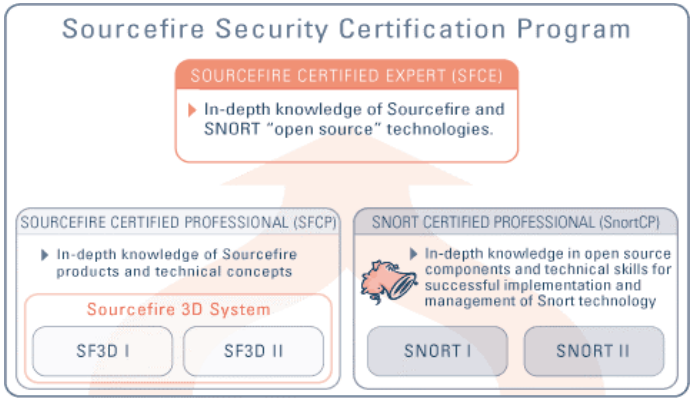
Training Courses Available

1. Rule Writing Best Practices
   - 2-Day Workshop
   - Snort® Rules Language and Rule Writing
2. Snort 1 & II (4-days)
   - Construct Solid & Secure Installations
   - Inner Workings of Snort

SnortCP Certification Exam

- 200 questions, 4 hours, 2 attempts

(ISC)² Trusted CPE Provider



Testimonials

Honestly, the best training I've been to. The course material and instructor were excellent. ***Education Industry***

This class answered all the questions and uncertainties I had with the product. The labs created an environment in which the students could experiment. It was an excellent course that I highly recommend.
Finance Industry

"The environment was extremely nice. The instructor was pleasant and knowledgeable. The content of the course exceeded my expectations."
Federal Government

SOURCEfire®

Thank You For Your Participation!
Q&A

SOURCEfire®

KNOW MORE NETWORK RISKS
NO MORE GUESSING