

Snort® Operation:

- ▶ Know the various modes of Snort® operation
- ▶ Know the various command line switches for starting Snort®, reading and processing alert data, applying filters and producing output
- ▶ Be familiar with Berkeley Packet Filter syntax
- ▶ Know the directory locations for where Snort® stores log and alert data by default
- ▶ Know how to access and read Snort® log and alert data
- ▶ Be familiar with the basic operation and configuration of Snort® startup scripts

Snort® Preprocessors:

- ▶ Know the general operation and functionality of Snort® preprocessors
- ▶ Understand how preprocessors play a role in defending the sensor against attacks and evasions
- ▶ Know how frag3 address IP fragment reassembly
- ▶ Understand the concepts behind normalization
- ▶ Understand how encodings apply to protocols such as HTTP
- ▶ Be familiar with common encoding types
- ▶ Be prepared to work through some encoding examples
- ▶ Be familiar with how portscan detection is handled in Snort® preprocessor technology
- ▶ Know the latest dynamic preprocessors such as DCE/RPC, SSH and DNS
- ▶ Understand the updates to the stream processing engine: stream5
- ▶ Know how to configure preprocessor alerting options

Snort® Configuration:

- ▶ Know the general syntax of runtime directives
- ▶ Know the general syntax for configuring variables and how to associate values to variables
- ▶ Be familiar with the general structure of the primary Snort® configuration file
- ▶ Have a general knowledge of the default settings within the primary Snort® configuration file
- ▶ Know the general syntax for configuring preprocessors
- ▶ Be familiar with the structure and significance of SIDs and GIDs
- ▶ Know the various preprocessor settings for the major preprocessors and what they do
- ▶ Understand how to configure preprocessors that use global and instance configuration schemes
- ▶ Know the syntax for configuring output plug-ins
- ▶ Know the configuration specifics for portscan detection
- ▶ Understand the concepts behind the Host Attribute Table
- ▶ Know the Host Attribute Table file structure

Barnyard:

- ▶ Understand what is required to implement Barnyard in your Snort® deployment
- ▶ Understand the benefits of incorporating Barnyard in your Snort® deployment
- ▶ Know the configuration and functionality of the Unified output format
- ▶ Be familiar with the various output options you can use with Barnyard
- ▶ Understand the general Barnyard architecture
- ▶ Know the significance and syntax of the SID map file and the GID map file
- ▶ Know the various command line options associated with Barnyard
- ▶ Know the general configuration syntax and structure of the primary Barnyard configuration file
- ▶ Know the various operating modes of Barnyard
- ▶ Know the structure, syntax and significance of the write-ahead lookup file

Rule Usage:

- ▶ Be familiar with the various rule options
- ▶ Know the general set of rule options that should be used in every rule
- ▶ Know the various files associated with specific rule options and their structures
- ▶ Know the ways in which priority is assigned to rules
- ▶ Be familiar with the options for applying thresholds and alert suppression
- ▶ Know rule structure and syntax
- ▶ Be familiar with the various post-detection rule options and what they do
- ▶ Know how to search for content in network traffic through the content option and its modifiers
- ▶ Be prepared to work through content search examples
- ▶ Have a basic understanding of PCRE and how it is applied in rules
- ▶ Be prepared to work through byte_jump/byte_test rule option examples

Rules, General:

- ▶ Be familiar with good rule writing practices
- ▶ Understand the implications of poorly written rules
- ▶ Know where to obtain rules
- ▶ Understand the types of available rules and the implications related to VRT rule sets
- ▶ Understand general rule tuning and troubleshooting practices
- ▶ Understand the implications of automated rule updates
- ▶ Be familiar with the configuration and usage of the Oinkmaster rule update tool
- ▶ Be familiar with the various rule actions and what they do

General Knowledge and Skills:

- ▶ Be prepared to demonstrate knowledge of general command line usage and syntax for both Linux and Windows environments
- ▶ Know common commands for managing both Linux and Windows based installations
- ▶ Be familiar with general networking concepts
- ▶ Be familiar with the general directory structure of Unix-like OSs
- ▶ Be familiar with the names and functions of common network protocols
- ▶ Know some techniques for achieving active response in Snort® installations

Sample Questions:

1. It is important to understand the affect/impact of networking devices in order to have a successful IDS/IPS deployment. Which of the following is NOT true about network devices:
 - a. Switches only present a datagram to a port for which it is destined
 - b. Hubs only present a datagram to a port for which it is destined
 - c. Routers forward datagrams based on the destination IP address
 - d. Taps replicate data right off the wire

2. In a typical Linux installation, the portion of the directory tree usually reserved for configuration files is ...
 - a. /var
 - b. /etc
 - c. /conf
 - d. /usr

3. Which of the following preprocessors is best at resolving ambiguities that may result from different implementations of IP networking stacks?
 - a. flow
 - b. frag3
 - c. HTTP_Inspect
 - d. telnet_decode

4. Running Snort from the command line gives you the ability to read PCAP formatted files. Which of the items below does **NOT** correctly represent how you could read PCAPs in from the command line?
 - a. --pcap-file=<file>
 - b. --pcap-xml=<XML file>
 - c. --pcap-list=<list>
 - d. --pcap-dir=<directory>

5. There are four primary components of Snort. Which of the following is NOT one of them:
- a. Sniffer
 - b. Postprocessors
 - c. Detection engine
 - d. Output module

Answer Key:

1. B | 2. B | 3. B | 4. B | 5. B