


Ducara Info Solutions (P) Ltd.

C|SIDS


**Certified Snort Intrusion
Detection Specialist**





Most security practitioners have heard of the open source network intrusion detection system, Snort is for those who haven't, however, its ability to monitor traffic, log packets and analyze protocols.

See how Snort can protect your network from buffer overflows and a wide variety of attacks and probes.



Why C|SIDS?



Trends Today

Snort Intrusion detection can be a confusing issue for system administrators. When an intrusion detection system is developed, there are several issues to deal with, including:

- How to monitor the system for intrusion attempts
- What traffic should be monitored
- How to log intrusion attempts
- What to do when an intrusion attempt is detected



Objective

The overall objective of this course is to learn about the **Intrusion Detection System (IDS)** and how it monitors the network traffic for suspicious activity and issues alerts when such activity is discovered.

While the anomaly detection and reporting which is the primary function and there are some **Intrusion Detection Systems** which are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.

Who's for this course?

- An Snort IDS is capable of distinguishing different types of network traffic, such as a **Hypertext Transfer Protocol (HTTP)** request over port **80** from some other application such as **Simple Mail Transfer Protocol (SMTP)** being run over port **80**.
- We see here that an IDS understands which TCP/IP Applications run over preassigned port numbers, and therefore falsifying port numbers would be trivially detectable.



Target Audience

Course Outline

Topics Covered in Course

1.

- Setting up Security Onion with VirtualBox

2.

- Boletto Malware Snort Rule Writing and PCAP Analysis

3.

- Vetting Snort Rule Quality with Dumbpig

4.

- Utilizing Offset and Depth in a Snort Rule

5.

- Kali Linux Setup with VirtualBox

6.

- Snort Rule Writing (SSH and FTP)

Course Outline

Topics Covered in Course

7.

- Windows 7 Eternalblue Vulnerable VM VirtualBox Setup

8.

- Windows 7 Eternalblue Exploitation and Snort/PCAP Analysis

9.

- Eternalblue PCAP Analysis and Snort Rule Writing

10.

- Ubuntu Server 12.04 Vulnerable VM VirtualBox Setup

11.

- Ubuntu Server 12.04 Heartbleed Exploitation and Snort/PCAP Analysis

12.

- Heartbleed PCAP Analysis and Snort Rule Writing



Ducara Info Solutions (P) Ltd.

Discover More

info@ducarainfo.com

www.ducarainfo.com

With our live and online training solutions, we can help you get the skills you need to succeed in the Cyber Security domain.