Ducara Info Solutions (P) Ltd.

CIIDS

Certified Intrusion Detection Specialist

OverView

Protecting investors by improving the accuracy & reliability of corporate disclosures

The **CIIDS** Specialist Certification delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of **TCP/IP** and the most used application protocols, such as **DNS** and **HTTP**, so that you can intelligently examine network traffic for signs of an intrusion.
You will get plenty of practice learning to master different open source tools like **tcpdump**, **Wireshark**, **Snort**, **Bro**, **tshark,** and **SiLK**. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer Knowledge to execution.

TarGeT AuDienCe

Primary Audience

- ✓ IPS/IDS Managers
- ✓ System Engineers
- ✓ Security Analysts
- ✓ IT Operations Managers
- ✓ Network Security Engineers
- ✓ Business Associates

Secondary Audience

- ✓ Analysts and Administrators responsible for configuring IPS/IDS sensors
- ✓ Individuals responsible for network and host monitoring, traffic analysis and Intrusion Detection

ObjecTive

The objective of the **CIIDS** training module is to maximize the return on your investment with hands-on and real world training on **IDS Network Security** products and technologies, security best practices and other IDS Security Service offerings. Analysts will be introduced to or become more proficient in the use of traffic analysis tools for signs of intrusions.

You will be able to understand the importance of optimal placement of **IDS sensors** and how the use of **Network Forensics** such as log data and network flow data can enhance the capability to identify Intrusions. Hands-on security managers will understand the complexities of Intrusion Detection and assist analysts by providing them with the resources necessary for success.

CouRse OuTline

Course Duration: 24 Hrs

1. Basics of Traffic Analysis
2. Application Protocols
3. Fundamentals of Traffic Analysis
4. Application Protocols and Traffic Analysis In Depth
5. Network Monitoring: Snort and Bro
6. Network Monitoring: Signatures vs. Behaviors
7. Network Traffic Forensics

Module 1
Basics of Traffic Analysis

- Why is it necessary to understand packet headers and data?
- TCP/IP communications model
- Data encapsulation/de-encapsulation
- Discussion of bits, bytes, binary, and hex
- Introduction to Wireshark
- Navigating around Wireshark
- Examination of Wireshark statistics
- Stream reassembly
- Finding content in packets
- Why should you capture and be able to analyze packets
- Understanding bits, bytes, binary, and hexadecimal
- Using tcpdump and Wireshark and their filtering techniques
- Link layer, IPv4, IPv6, and fragmentation
- Transport layers TCP, UDP, and ICMP

Module 2
Application Protocols

DNS
- DNS architecture and function
- Caching
- DNSSEC
- Malicious DNS, including cache poisoning

Microsoft Protocols
- SMB/CIFS
- MSRPC
- Detection challenges
- Practical Wireshark application

Modern HTTP and TLS
- Protocol format
- Why and how this protocol is evolving
- Detection challenges

SMTP
- Protocol format
- STARTTLS
- Sample of attacks
- Detection challenges

IDS/IPS Evasion Theory
- Theory and implications of evasions at different protocol layers
- Sampling of evasions
- Necessity for target-based detection

Module 3

Fundamentals of Traffic Analysis

- Concepts of TCP/IP
- Network Access/Link Layer: Layer 2
- IP Layer: Layer 3 IPv4 IPv6
- Introduction to 802.x link layer
- Address resolution protocol
- ARP spoofing
- Checksums and their importance, especially for an IDS/IPS
- Fragmentation: IP header fields involved in fragmentation, composition of the fragments, fragmentation attacks
- Introduction to Wireshark
- Wireshark Display Filters
- Writing BPF Filters
- Real World Analysis-Command Line Tools
- Regular Expressions fundamentals
- Rapid processing using command line tools
- Rapid identification of events of interest

Module 4

Basics Traffic Analysis

- Scapy
- Advanced Wireshark
- Detection Methods for Application Protocols
- Modern HTTP and TLS
- IDS/IPS Evasion Theory
- Identifying Traffic of Interest
- Advanced Wireshark
- Tshark
- Detection Methods for Application Protocols
- Detection challenges
- STARTTLS
- Sample of attacks
- Detection challenges
- Theory and implications of evasions at different protocol layers
- Necessity for target-based detection
- Finding anomalous application data within large packet repositories
- Extraction of relevant records
- Application research and analysis

Module 5

Network Monitoring: Snort and Bro

- Running, installing, configuring, and customizing Snort
- Writing Snort rules
- Running, installing, configuring, and customizing Bro
- Writing Bro scripts and signatures, and raising Bro notices

Module 6

Network Monitoring: Signatures v/s Behaviors

1. Network Architecture
2. Instrumenting the network for traffic collection
3. IDS/IPS deployment strategies
4. Hardware to capture traffic
5. Introduction to IDS/IPS Analysis and their functions
6. The analyst's role in detection
7. Introduction to Snort
8. Differences between Snort & Bro
9. Flow process for Snort and Bro
10. Running Snort & Writing Snort rules
11. Solutions for dealing with false negatives and positives
12. Introduction to Zeek
13. Zeek Operational modes
14. Zeek output logs and how to use them
15. Practical threat analysis
16. Zeek scripting
17. Using Zeek to monitor and correlate related behaviors
18. Hands-on exercises, one after each major topic, offer students the opportunity to reinforce what they just learned.

Module 7

Network Traffic Forensics

1. Introduction to Network Forensics Analysis
2. Theory of network forensics analysis
3. Phases of exploitation
4. Data-driven analysis vs. Alert-driven analysis
5. Hypothesis-driven visualization
6. Using Network Flow Records
7. NetFlow and IPFIX metadata analysis
8. Using SiLK to find events of interest
9. Identification of lateral movement via NetFlow data
10. Examining Command and Control Traffic
11. Introduction to command and control traffic
12. TLS interception and analysis & profiling
13. Covert DNS C2 channels: dnscat2 and Ionic
14. Other covert tunneling, including The Onion Router (TOR)
15. Analysis of Large pcaps
16. The challenge of analyzing large pcaps
17. Students analyze three separate incident scenarios
18. Hands-on experience analyzing incident scenarios

Connect Us!

Ducara help harnessing latest security trends & enhancing skills to simplify IT security complexity efficiently.

info@ducarainfo.com

www.ducarainfo.com

DUCARA