NFA Network/Internet Forensics Investigation and Intrusion Log Analysis

Course Introduction

Enterprises all over the globe are compromised remotely by malicious hackers each day. Credit card numbers, proprietary information, account usernames and passwords, and a wealth of other valuable data are surreptitiously transferred across the network. Insider attacks leverage cutting-edge covert tunneling techniques to export data from highly secured environments. Attackers' fingerprints remain throughout the network, in firewall logs, IDS/IPS, web proxies, traffic captures, and more.

Network Forensics will teach you to how to follow the attacker's footprints and analyze evidence from the network environment. Every student will receive a Network forensics tools, which is a fully-loaded, portable forensics virtual workstation, designed by network forensics experts and distributed exclusively Network Forensics students.

After completing this course, Attendees will gain knowledge on how to professionally investigate network/Internet security incident by using in-depth intrusion log analysis techniques.

Course Objectives

- To understand attacking methods and tools
- To identify a normal traffic behavior and attack traffic behavior
- To learn how to analyze traffic and payload characteristic
- To learn how to interpret TCP/IP traffic
- To understand behavior of current attacks to corporate network
- To experience a hands-on exercise of intrusion analysis
- To learn how to comply new Thailand ICT Law requirement

Course Highlights

- Windows and Linux Software and Network Forensic tools provided
- Network Forensic Workstation provided
- Free membership for ACIS Alumni
    - Access to the latest information related to the course subjects
    - A life-time class re-sit

Learning Level

- Expert

Course Duration

- 5 Days (30 Hours)

Prerequisites

- Digital Forensic

NFA Network/Internet Forensics Investigation and Intrusion Log Analysis

Target Group

- IT Security Officer
- Digital Forensic Investigator
- Cyber Cop/Law Enforcement

Course Outline

Module 1: Log Analysis

- Reporting Security Information to Management
- Combining Resources for an "Eye-in-the-Sky" View
- Blended Threats and Reporting
- Code Solutions
- Commercial Solutions
- Using Bro to Gather DNS and Web Traffic Data
- Using Bro for Blackholing Traffic to Malware-Infested Domains
- Using Bro to Identify Top E-Mail Senders/Receivers

Module 2: Network Threats

- Network Threats
  - Understand Network Attack
  - Denial-of-service (DoS) Attacks
  - Distributed denial-of-service (DDoS) Attacks
  - Back door Attacks
  - Spoofing Attacks
  - Man-in-the-Middle Attacks
  - Replay Attacks
  - Password Guessing Attacks
- TCP/IP Attacks
  - TCP SYN or TCP ACK Flood Attack
  - TCP Sequence Number Attack
  - TCP/IP Hijacking
  - ICMP Attacks
  - Smurf Attacks

Module 3: IDS Reporting

- Session Logging with Snort

- Session/Flow Logging with Argus
- Can You Determine When a DDoS/DoS Attack Is Occurring
- Using Snort for Bandwidth Monitoring
- Using Bro to Log and Capture Application-Level Protocols
- Tracking Users' Web Activities with Bro

Module 4: Security Log Management

- Log Source
- Log Management Function
- Log type
  - Windows Log
  - Linux Log
  - Switch and Router log
  - Firewall log
  - IDS / IPS log
  - E-mail log
  - Web server log
  - Proxy log
  - Anti-viruses log

Module 5: Log Analysis Tools

- Analyze log with Splunk
- Analyze log with Ntop
- Analyze log with MS-Excel
- Analyze log with Commercial Tools
- LAB: Analyze Log from Scenario and create Incident report

Module 6: SIM SEM and SIEM

- Understand SIM SEM and SIEM
- Analyze Log with SIM
- LAB: Install SIEM Open source tools

Module 7: Network Forensic and Security

- Analyzer Placement
  - Switch Environment and SPAN port
  - Hub and Network Tapping Device
  - Routed Network
  - Capturing in Stealth Mode

- Unusual Network Communications
- Reconnaissance Processes
- Analyzing ICMP Traffic
- TCP Security
- Address Spoofing
- Building Firewall ACL Rules
- Signatures of Attack

Module 8: Network Evidence Extraction

- Gather evidence from network devices
- Generate Packet Dump Metadata
- Create Network Event timeline
- Network Addressing and OS Fingerprint
- Extract Traffic Content(File Carving)
- Reconstruct Web histories and cached Web content
- Tools
    - Ngrep and TCPExtract
    - NetworkMiner

Module 9: Network Forensic Tools

- Network Forensic tools
    - Wireshark
    - Network Miner
    - CACE Pilot
    - Commercial Tools
- LAB: Network Forensic from Scenario

Recommended Course tracks

- MFI : Mobile forensics Investigation techniques
- CISSP : The Official CISSP CBK Review Seminar (Accredited Training by ISC^2)

NFA Network/Internet Forensics Investigation and Intrusion Log Analysis

สำรองที่นั่งและขอรับรายละเอียดเพิ่มเติมกรุณาติดต่อ (FOR MORE INFORMATION & REGISTRATION PLEASE CONTACT)	
คุณธนภัทร ไชยพิมล Mr. Tanapat Chaipimol Tel:(66) 2-650-5771 Ext.105 Fax: (66) 2-650 5776 Mobile: (66) 86-330-8532 Email: tanapat.ch@acisonline.net	คุณกิตมณี นิยมญาติ Ms. Kitmanee Niyomyat Tel:(66) 2-650-5771 ext. 108 Fax: (66) 2-650 5776 Mobile: (66) 86-325-7129 Email: kitmanee.ni@acisonline.net

ACIS Professional Center Co.Ltd.

2101, 21 Fl., 62 The Millennia Building, Lungsuan Rd., Lumpini, Pathumwan, Bangkok 10330
Tel: +(66)2-650-5771 Fax: +(66)2-650-5776 Hotline: +(66)86-352-7129 Email: registration@acisonline.net
Website: www.acisonline.net