Network Forensic Analysis

The NFA course is a lab-intensive course designed for technicians involved with incident response, traffic analysis or security auditing. The certification exam is an actual practical lab requiring candidates to follow procedures and apply industry standard methods to detect and identify attacks.

NFA was designed to partner with courses like CEH in mind in order to provide experience detecting the attacks a student may have seen or read about in the past. By no means is CEH a requirement for NFA, but the two go very well together: attack in one course, detect in the other.

NFA is a continuously evolving course, rarely repeating the exact same captures or attacks. Many courses update their curriculum only after a large period of time, perhaps even years. NFA is committed to using the most recent attacks that real-world analysts are currently experiencing. While certain “historical” attacks are discussed in the course, students will analyze captures of attacks that are as current as a few weeks. Freewater Technologies keeps the focus on cutting edge technology, providing students with tangible information that can immediately be applied to job skills.

The GCIA exam, like all SANS Certifications, does not require a specific training course – it is designed for any qualified individual to “challenge” the test. NFA maps clearly to the objectives of GCIA and could be used for the preparation of the certification. The NFA courseware is also an excellent resource for a candidate to use during the actual exam (GCIA is open book). While NFA is not an official SANS course, the same content is covered, including:

- Network Fundamentals/Operations/Architecture
- TCP
- UDP
- ICMP
- IPv6
- Detailed Link-Layer operation
- Application Protocols
- Detailed DNS operation
- HTTP
- SMTP
- FTP
- In-depth Snort (Configuration and Advanced usage)
- Pcap filtering
- Wireshark
- tcpdump
- Analysis and Forensics
- Handling and reporting
- Evidence gathering
- Incident and event types
- Attack identification
- Evasion
- Packet crafting
- Fragmentation

- Firewall operations
- ISA
- TMG
- ASA
- Juniper

- Tool selection
  - Detailed experience with toolkits and their usage

The hands-on portion of NFA is second to none. Freewater utilizes a custom environment where EACH STUDENT has a self contained Internet that includes:

1) A Windows Domain containing
   - DC with detailed Active Directory (Multiple OUs and GPOs)
   - Exchange Server
   - Client machine(XP and Windows 8)
   - Wordpress Website
   - SQL-Injection vulnerable Website
   - XSS-vulnerable website
   - FTP server
   - ISA firewall (also substituted with a Microsoft TMG firewall)
   - Internal Snort sensor “tapped” for all traffic to and from the firewall

2) Linux machine as an Internet server containing
   - Apache2 with multiple websites
   - Postfix/dovecot/roundcube/thunderbird as a fully functional email server
   - Nmap
   - Wireshark
   - Metasploit
   - JTR
   - Hydra
   - Zap
   - Snort
   - XSSer
   - And many more...

3) Internet client machines
   - Windows 7
   - BT53
   - Kali
4) ISP server
- Windows Server 2008 R2
- DNS for the entire “Pod”
- SMTP relay
- 3 fully functional sites (one wordpress, the others designed as vulnerable to common web application attacks)

This highly customized proprietary configuration contains three companies (the internal domain, the ISP and the Linux system) that fully simulates a live Internet. There is no attack that cannot be physically created or inspected. For example:

Sitting at the Linux box, a student could craft an HTML formatted email with a Cross-Site Scripting attack and email it to a user of the Windows domain. The student could then open that email on the Windows XP box and the Windows 8 box to observe the results. The email would route through the ISP and travel through the firewall, which gives the student a chance to actually see what occurs with different rules or application inspection at the firewall. Traffic can be captured on both the “Internet” and the “Internal” domain side at the same time with Wireshark, tcpdump or Snort. After analysis, a student would then be able to write a Snort signature to detect the attack and immediately see if their rule was correct. No other course offers this much flexibility and real-world experience.

NFA is a great choice for anyone who:
- Is looking to prepare for GCIA
- Has taken CEH or will take CEH
- Has an employer that would benefit from a certification that proves they can actually perform the tasks associated with incident analysis