Systems & Network Training

Definitive network forensics for engineers

A 3 day Hands on training course

Save on expenses. This course is also available on your premises.

Description

This course studies network forensics—monitoring and analysis of network traffic for information gathering, intrusion detection and legal evidence. We focus on the technical aspects of network forensics rather than other skills such as incident response procedures etc.. Hands on sessions follow all the major sections.

Key outcomes

By the end of the course delegates will be able to:

- ✔ Recognise network forensic data sources.
- ✔ Perform network forensics using:
  - Wireshark
  - NetFlow
  - Log analysis.
- ✔ Describe issues such as encryption.

Training Approach

This structured course uses Instructor Led Training to provide the best possible learning experience. Small class sizes ensure students benefit from our engaging and interactive style of teaching with delegates encouraged to ask questions throughout the course. Quizzes follow each major section allowing checking of learning. Hands on sessions are used throughout to allow delegates to consolidate their new skills.

Details

Who will benefit?
Technical network and/or security staff.

Prerequisites
TCP/IP foundation for engineers.

Duration: 3 days

Overall rating: **New course**

Generic Training	Small Class Sizes	Hands On Training	Our Courseware	Customise Your Course
Generic training complements product specific courses covering the complete picture of all relevant devices including the protocols “on the wire”.	We limit our maximum class size to 8 delegates; often we have less than this. This ensures optimal interactivity between delegates and instructor.	The majority of our courses use hands on sessions to reinforce the theory.	We write our own courses; courseware does not just consist of slides and our slides are diagrams not bullet point text.	Please contact us if you would like a course to be customised to meet your specific requirements. Have the course your way.
“*Friendly environment with expert teaching that teaches the why before the how.*” G.C. Fasthosts	*“Excellent course. The small class size was a great benefit...”* M.B. IBM	*“Not many courses have practice added to it. Normally just the theoretical stuff is covered.”* J.W. Vodafone	*“Comprehensive materials that made the course easy to follow and will be used as a reference point.”* V.B. Rockwell Collins	*“I was very impressed by the combination of practical and theory. Very informative. Friendly approachable environment, lots of hands on.”* S.R. Qinetiq

Definitive network forensics for engineers

Course Content

What is network forensics?
What it is, host vs network forensics, purposes, legal implications, network devices, network data sources, investigation tools. Hands on: whois, DNS queries.

Host side network forensics
Services, connections tools. Hands on: Windows services, Linux daemons, netstat, ifoconfig/ipconfig, ps and Process explorer, ntop, arp, resource monitor.

Packet capture and analysis
Network forensics with Wireshark, Taps, NetworkMiner. Hands on: Performing Network Traffic Analysis using NetworkMiner and Wireshark.

Attacks
DOS attacks, SYN floods, vulnerability exploits, ARP and DNS poisoning, application attacks, DNS ANY requests, buffer overflow attacks, SQL injection attack, attack evasion with fragmentation. Hands on: Detecting scans, using nmap, identifying attack tools.

Calculating location
Timezones, whois, traceroute, geolocation. Wifi positioning. Hands on: Wireshark with GeoIP lookup.

Data collection
NetFlow, sflow, logging, splunk, splunk patterns, GRR. HTTP proxies. Hands on: NetFlow configuration, NetFlow analysis.

The role of IDS, firewalls and logs
Host based vs network based, IDS detection styles, IDS architectures, alerting. Snort. syslog-ng. Microsoft log parser. Hands on: syslog, Windows Event viewer.

Correlation
Time synchronisation, capture times, log aggregation and management, timelines. Hands on: Wireshark conversations.

Other considerations
Tunnelling, encryption, cloud computing, TOR. Hands on: TLS handshake in Wireshark.

What our customers say

"Absolutely brilliant, very knowledgeable and helpful trainer would recommend to teach anyone. Kept me interested 100% of the time which is very impressive as this does not happen often, if at all!"

O. B. Network Rail

"The best technical course I've been on!."

L. W. Fujitsu Telecoms Europe

"Very well thought out and structured course. Would recommend 100%. Lots of equipment, good quality."

A.R. Unipart

"Course content is interesting. Relevant to current systems and presented well."

S.S-T. Arqiva