Systems & Network Training

SIP security for engineers

A 2 day Hands on training course

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

Description

A hands-on course covering SIP security. It is assumed that delegates already know SIP as this course focuses purely on the security issues in SIP IP telephony networks. Hands-on practicals follow each major theory session and include use of various SIP security tools such as vomit, sipp, sipsak and sivus amongst others.

Key outcomes

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

- ✔ Secure SIP networks.
- ✔ Use various SIP security tools.

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 staff working with SIP.
Technical security staff.

Prerequisites
Definitive SIP for Engineers.

Duration: 2 days

Customer rating: ★★★★★

Generic training	Small class sizes	Hands On training	Our courseware	Customise your course
Generic training compliments 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

SIP security for engineers

Course content

SIP review
SIP infrastructure and entities, example SIP session. Hands on: Simple SIP network with and without authentication.

SIP security attacks
DOS attacks, infrastructure attacks, eavesdropping, spoofing, replay, message integrity. Hands on: Basic SIP packet capture, infrastructure attacks.

SIP tools
SIP packet creation: Sivus, SIPsak, PROTOS, SFTF, SIP bomber, SIPp, Seagull, Nastysip. SIP packet generators: SIPNess, NetDude. Monitoring: Wireshark, Cain & Abel, Vomit, Oreka, VoiPong. Scripts and tools: SIP-Fun, Skora.net, kphone-ddos, sip-scan, sip-kill, sip-redirectrtp. Health of different tools. Hands on: Generating SIP packets, rebuilding conversations from captured packets, password cracking.

VPNs and SIP
IPSec, AH, ESP, transport mode, tunnel mode, Pre Shared Keys, Public keys. Hands on: SIP calls over IPSec.

Secure SIP signaling
SIP relationship with HTTP, Deprecated HTTP 1.0 basic authentication, HTTP 1.1 Digest authentication, S/MIME, SIPS, SIPS URI, TLS, DTLS, PKI infrastructures. Hands on: SIP with TLS.

Secure media streams
SRTP, features, packet format, default encryption, default authentication, key distribution. S/MIME, MIKEY, SDP security descriptions. SIP security agreements. Hands on: Analysing SRTP packets.

Firewalls
NAT traversal. Impact of firewall on infrastructure attacks. TLS and firewalls. SIP specific firewalls. Hands on: SIP calls through a firewall.