

Course summary sheet (2011-12-05)

UTM Expert Plus v9 (NT-FWXP+-V9)

NETASQ approved training organization #31.59.05307.59

1. Introduction

The aim of this training course is to provide tools and methods to gather relevant information, to study and troubleshoot problems using the CLI. This course is suitable for companies who want to become NSCS or NCTC (for people who aim at becoming a support engineer or expert trainer on our UTM product)

2. Venue, duration and registration

This course is only provided by NETASQ Trainers or Support members teams.

NETASQ can suggest you training courses in Villeneuve d'Ascq (France), or in Boulogne Billancourt (France). Our trainers are willing to move abroad so as to provide you with the training.

The Expert Plus training course takes place over three days. The training starts at 9.30 am on the first day, and at 9.00 am the second and third days. All registration requests have to be sent to NETASQ's training department (training@netasq.com). The maximum class size is 4 trainees per session. Training material will be provided for each trainee.

3. Pre-requisites and hardware

Deep TCP/IP and good UNIX shell knowledge. Trainees must be CNE V9 certified and should be equipped with a laptop running a Windows operating system (or any other OS with a Virtualization software and a virtual Windows) to conduct the exercises suggested in the training course and also VirtualBox in version 3.1.x at least (<http://www.virtualbox.org/>) or VMPlayer 3.0.x.

4. Detailed description

4.1 Day 1

- Introduction
- Operating System and related UNIX commands
 - o Access methods to the SHELL and related settings
 - o SSH : Related features
 - o File systems and related commands
 - o Directories and related commands
 - o System and user environment

- Files and related commands
- Logs
 - Local logs : location, categories, indexation, nomenclature and syntax
 - Related commands
 - Configuration files
 - Settings for export to external syslog
 - logd : the logs daemon; verbose and synoptic
 - logctl : interacting with logd
- Configuration Files and backup file
 - Directory location and general syntax
 - Related commands : setconf, decbackup, encbackup, nsrpc, tar, defaultconfig
- Network and Routing
 - Network configuration file: interfaces settings samples (advanced, bridged, protected)
 - the Bridge : behavior, peculiar settings
 - Network related commands
 - Routing : reminders (general needs and purposes, priorities)
 - Routing configuration files and settings
 - Gatemon settings
 - Routing related commands
 - Interaction with the protected addresses table
 - Gatemon verbose
- Traffic captures and analysis with tcpdump
 - Introduction and advises
 - General syntax
 - Usual filters
 - Commented examples
 - Advises to perform relevant captures
 - Analysis on tcpdump outputs (TCP stream, UDP/icmp)

4.2 Day 2

- Daemons and Processes
 - List and role
 - Launched supervisor
 - Related commands
- Objects
 - Configuration files and related UNIX files
 - Related commands
- ASQ : analysis
 - Step-by-step analysis of network layers

- Related command : sfctl
- Peculiar global settings
- Location and structure of profiles
- Noteworthy settings of protocol analysis
- Asynchronous ASQ : cases, packet "watermarking"
- ASQ verbose mode
- ASQ : Security Policy
 - Configuration files and syntax
 - Filter : related commands
 - Filter : samples of loaded rules (action, inspection level, plugin, PBR, QoS, interfaces, proxy)
 - Filter : translation of objects groups and lists (tables), and operators
 - NAT : reminders (Dynamic NAT, Static NAT by port, Static NAT/Bimap, No NAT)
 - NAT : related commands
 - NAT : samples of loaded NAT rules and ARP related mechanism
- ASQ : Stateful and state tables
 - Protected addresses table
 - Hosts table
 - Connections table : samples of connections states (NAT, vconn, FTP plugin, async, lite...)
- FTP concepts and mechanism
 - Mechanisms for passive and active modes
 - Needed and useless filter rules

4.3 Day 3

- Eventd : events scheduler daemon
 - Use and syntax
 - Examples
- IPsec VPN
 - NETASQ IPsec/IKE implementation
 - Synoptic
 - IKE negotiations and derived keys
 - NAT-T, DPD, Keepalive, SharedSA, Policy None, SPD Cache
 - Related commands
 - Analysis of an IPsec-SA
 - Logs and troubleshooting
 - Verbose mode

5. Certification

Within two months after the training, each trainee can attend the Expert Plus exam. This exam will last 2h00 and permits to validate the CNEP certification.

This exam is composed of two parts:

- a theoretical purpose, with question MCQ and Open Questions related to either general TCP/IP network knowledge and NETASQ UTM features, settings and troubleshooting methods.
- a practical purpose, where you'll have to answer some problems reports issued by a customer; explaining your ideas and methods, and describing in details any action you'd like the customer to perform in case you'd ask more information.