Publication date : 08/01/2024

Course : Wireshark - Audit and performance

Practical course - 3d - 21h00 - Ref. RUE
Price : 2370 CHF E.T.

★★★★⯪ 4,1 / 5

Wireshark enables regular, in-depth analysis of networks to identify potential problems. In this course, you'll learn how to use Wireshark to check protocols. Once the information has been captured, it can be consulted on the program's graphical interface or via the ATS tshark mode.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Understanding network flow analysis
- ✓ Filter and analyze network activity
- ✓ How to produce reports
- ✓ Use Wireshark to diagnose network performance problems

Intended audience

System administrators, network administrators and developers.

Prerequisites

Basic knowledge of TCP/IP.

Practical details

Teaching methods

Training alternates theory and practice. A great deal of practical work is carried out throughout the course.

Course schedule

PARTICIPANTS

System administrators, network administrators and developers.

PREREQUISITES

Basic knowledge of TCP/IP.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant’s academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they’ve developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

1 A reminder of the basics

- Communication methods (unicast, multicast, broadcast).
- Topologies and access control. OSI model.
- Ethernet frame format. Size and meaning (Runt, Giant...) and the ARP protocol.returnchariot
- Layer 2 protocols (802.3, 802.1p, 802.1q, 802.1ad). Layer 2 multicast.
- IP packet format.
- Special addresses (loopback). Multicast addresses (known addresses), broadcast method.returnchariot
- ICMP protocol (role and response analysis).

2 The Wireshark screen

- Toolbar.
- Filter zone.
- Package display area.
- Area displaying the contents of the selected package in hexadecimal.
- Status bar (accesses expert mode, annotations, displays number of packets captured and current profile).

3 Analysis tasks with Wireshark

- Capture network communications in "clear text" (e.g. Telnet, HTTP).
- Check which applications are used by which hosts.
- Define a reference point for network communication.
- Check that certain network services are working properly.
- Identify who wants to connect to the wireless network.
- Capture unexpected traffic. Capture and analyze host or network traffic.
- View and reassemble files transferred via FTP or HTTP. View and listen to VoIP communications.

4 Troubleshooting with Wireshark

- Identify abnormal delays.
- Identify TCP problems.
- Detect HTTP problems.
- Detect application errors.
- Generate graphs.
- Identify saturated buffer problems.
- Detect duplicate IP address problems.
- Identify problems with the DHCP protocol or DHCP relay.

5 Security analysis tasks

- Detect applications using non-standard ports.
- Identify traffic coming from or going to a suspect host.
- Identify machines trying to obtain an IP address.
- Identify a recognition process on the network.
- Locate and map external addresses.
- Examine a TCP or UDP conversation between a client and a server.
- Locate known attack signatures on your network.

Dates and locations

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

REMOTE CLASS

2026 : 4 May, 29 June, 9 Sep., 16 Nov.