

## Security in IP Networks Recognizing and Closing Security Gaps

Recent years have given rise to an abundance of new methods of attack. The providers of protective measures, however, have not been idle, either. As a result, the topic of network security has become increasingly complex compared to earlier days. The know-how imparted in this course is the basis for taking over tasks in security planning and administration of IP-based networks, which the participants will be able to perform on their own account.

### Course Contents

- Attacks on the Protocol Layer, e.g. ARP Cache Poisoning and IP Spoofing
- Attacks on Applications and Operating Systems
- Scanning and OS Fingerprinting
- Basic Protection According to the BSI (Federal Office for Information Security)
- Symmetrical and Asymmetrical Encryption (AES, 3DES, RSA, ECC, ...)
- Data Integrity and Keyed Hash (MD5, SHA-1)
- Authentication, Signatures, and Certificates
- IPsec and SSL and their Application in VPNs
- Applications: SSH, PGP, EFS, and Blackberry
- Firewalls and DMZ
- Intrusion Detection and Prevention
- Hands-On Exercises at the Test Network

In this course of the ExperTeach Networking series, each student will receive the comprehensive ExperTeach course documentation.

### Target Group

Networkers who require detailed knowledge regarding the security problems in the TCP/IP world and who are looking for adequate solutions can find them in this course. The course is designed for administrators, planners, and consultants.

### Knowledge Prerequisites

Optimum prerequisites for participation in the course are profound basic know-how of the LAN, router, and Internet environment, as well as a deeper knowledge of the IP protocol.



### Reservation and Registration

We will be glad to make a free and non-binding course reservation for you for the duration of two weeks. On [www.experteach-training.com](http://www.experteach-training.com) under *Registration*, you can conveniently make course reservations, registrations, and hotel reservations. Alternatively, call us under +49 6074 4868-0.

For closed groups of participants, we can modify the course contents according to your requirements. Do not hesitate to contact us!



**3 days** €1,395 exclusive of V.A.T.

### Course date (mm/dd/yy)/Location

02/21-02/24/12	Frankfurt	08/27-08/30/12	Frankfurt
03/13-03/16/12	Düsseldorf	09/18-09/21/12	Düsseldorf
04/10-04/13/12	Berlin	10/16-10/19/12	Berlin
04/10-04/13/12	Hamburg	10/16-10/19/12	Hamburg
04/24-04/27/12	München	11/05-11/08/12	Stuttgart
04/24-04/27/12	Stuttgart	11/05-11/08/12	München
05/29-06/01/12	Frankfurt	12/03-12/06/12	Zürich
05/29-06/01/12	Zürich	12/03-12/06/12	Frankfurt
07/30-08/02/12	Wien	01/21-01/24/13	München
07/30-08/02/12	München	02/18-02/21/13	Frankfurt

Up-to-date information: [www.experteach-training.com](http://www.experteach-training.com) SECU



EXPERTeach





<p><b>1 Motivation for Network Security</b></p> <p><b>1.1 Aims of Network Security</b></p> <p>1.1.1 Confidentiality</p> <p>1.1.2 Unalterability</p> <p>1.1.3 Traceability</p> <p>1.1.4 Availability</p> <p><b>1.2 Fundamental Threats</b></p> <p>1.2.1 Spoofing</p> <p>1.2.2 Bugging</p> <p>1.2.3 Denial of Service</p> <p>1.2.4 Source of Information</p> <p><b>1.3 The Basic Protection Manual of the BSI (Federal Office for Information Security)</b></p> <p><b>1.4 Current Threats</b></p> <p>1.4.1 Attacks on Browsers</p> <p>1.4.2 Phishing</p> <p>1.4.3 WLANs</p> <p><b>2 Weak Points of the IP Protocol Family</b></p> <p><b>2.1 ARP Spoofing</b></p> <p>2.1.1 ARP Cache Poisoning</p> <p>2.1.2 Flooding the Switching Table</p> <p><b>2.2 Attacks on IP</b></p> <p><b>2.3 Attacks on TCP</b></p> <p>2.3.1 SYN Flooding</p> <p>2.3.2 Sequence Number Attack</p> <p>2.3.3 Blind Spoofing</p> <p><b>2.4 DNS</b></p> <p>2.4.1 Forged Host File</p> <p>2.4.2 Spoofing of DNS Replies</p> <p>2.4.3 Attacks on the Servers</p> <p><b>2.5 Routing</b></p> <p>2.5.1 Denial of Service on BGP-4</p> <p>2.5.2 Data Rerouting</p> <p><b>2.6 Attacks on Applications</b></p> <p><b>2.7 Typical Methods and Tools</b></p> <p>2.7.1 Search Engines</p> <p>2.7.2 The whois Service</p> <p>2.7.3 DNS-nslookup and dig</p> <p>2.7.4 Scanning</p> <p>2.7.5 Phishing</p> <p><b>3 Data Protection via Encryption</b></p> <p><b>3.1 The Beginnings of Cryptography</b></p> <p><b>3.2 Symmetrical Encryption</b></p> <p><b>3.3 Lifetime and Distribution of the Keys</b></p> <p><b>3.4 Generation of Keys</b></p> <p>3.4.1 Diffie-Hellman</p> <p>3.4.2 SPEKE</p> <p><b>3.5 Asymmetrical Encryption</b></p> <p>3.5.1 RSA</p> <p>3.5.2 El Gamal</p>	<p><b>4 Data Integrity and Authentication</b></p> <p><b>4.1 Data Integrity: Hash Values</b></p> <p>4.1.1 Typical Features</p> <p>4.1.2 Keyed Hash</p> <p>4.1.3 Replay Attacks</p> <p><b>4.2 Data Origin Authentication</b></p> <p>4.2.1 Pre-Shared Key</p> <p>4.2.2 Keyed Hash</p> <p>4.2.3 Digital Signature</p> <p><b>4.3 Authentication of the Communication Partner</b></p> <p>4.3.1 Man in the Middle</p> <p>4.3.2 Certificates</p> <p>4.3.3 PKI and CA</p> <p>4.3.4 Single Sign-On and Kerberos</p> <p>4.3.5 Smart Token Systems</p> <p>4.3.6 Biometrics</p> <p>4.3.7 Authentication with RADIUS</p> <p><b>5 Application Examples</b></p> <p><b>5.1 OSI Model and Encryption</b></p> <p><b>5.2 IPsec VPNs</b></p> <p>5.2.1 IPsec Modes</p> <p>5.2.2 IPsec Protocols</p> <p>5.2.3 Example: IPsec VPN and VoIP</p> <p><b>5.3 SSL VPNs</b></p> <p>5.3.1 Architecture of SSL VPNs</p> <p>5.3.2 The Browser as a Universal Client</p> <p>5.3.3 OpenSSL</p> <p><b>5.4 PGP and GNU PG</b></p> <p><b>5.5 Secure Shell</b></p> <p><b>5.6 Blackberry</b></p> <p>5.6.1 Blackberry and Security</p> <p>5.6.2 Payload Data Transport</p> <p><b>5.7 Encrypted File System</b></p> <p><b>6 Firewalls</b></p> <p><b>6.1 The Role of the Firewall in the Network</b></p> <p><b>6.2 Static Packet Filters</b></p> <p>6.2.1 Working Mode of Static Packet Filters</p> <p>6.2.2 Static Packet Filters-Weak Points and Limits</p> <p><b>6.3 Dynamic Packet Filters-Stateful Firewalls</b></p> <p>6.3.1 Working Mode of Dynamic Packet Filters</p> <p>6.3.2 Dynamic Packet Filters-Strong and Weak Points</p> <p><b>6.4 Proxy Firewalls</b></p> <p>6.4.1 Application Layer Gateways</p> <p>6.4.2 Circuit Relays-Generic Proxies</p> <p><b>6.5 Network Design</b></p> <p>6.5.1 Network Address Translation (NAT) and Firewalls</p> <p>6.5.2 DMZ Concepts-An Overview</p> <p>6.5.3 Firewalls and VPNs</p>	<p><b>6.5.4 Redundancy and Load Sharing</b></p> <p><b>7 Behind the Firewall-IDS and IPS</b></p> <p><b>7.1 What is IDS?</b></p> <p><b>7.2 Threat Detection via IDS</b></p> <p>7.2.1 Sample Identification</p> <p>7.2.2 Detection of Anomalies</p> <p>7.2.3 Protocol Evaluation</p> <p><b>7.3 Network-Based IDS</b></p> <p>7.3.1 The Advantages of NIDS</p> <p>7.3.2 The Disadvantages of NIDS</p> <p><b>7.4 Host-Based Intrusion-Detection-Systems</b></p> <p>7.4.1 The Advantages of HIDS</p> <p>7.4.2 The Disadvantages of HIDS</p> <p><b>7.5 NNIDS-IDS on Network Components</b></p> <p><b>7.6 Intrusion Prevention Systems</b></p> <p><b>7.7 The Computer Security Incident Response Team</b></p> <p>7.7.1 Detecting a Burglary</p> <p>7.7.2 Limiting the Damage-A Case Study</p> <p><b>7.8 Legal Background</b></p> <p>7.8.1 The Bundesdatenschutzgesetz (BDSG) (Federal Law on Data Protection)</p> <p>7.8.2 The Betriebsverfassungsgesetz (BetrVG) (Works Constitution Act)</p> <p>7.8.3 Right of Access to Personal Data</p>
--	---	---



**ExperTeach Gesellschaft für Netzwerkkompetenz mbH**

Waldstr. 94 • D-63128 Dietzenbach  
Phone +49 6074 4868-0 • Fax +49 6074 4868-109  
info@experteach.de • www.experteach.de

© ExperTeach GmbH, all specifications made are exempted from liability.

Status 02/04/2012