

Firewalls, Proxies und IDS Technologien & Produkte

Ein zentraler Baustein zur Umsetzung einer Security Policy ist die Firewall, die das interne Netz vor Angriffen aus dem Internet schützen soll. Die Funktionalität moderner Firewall-Systeme geht weit über einfache Filtertechniken hinaus und verschmilzt oft mit den Tätigkeiten von Proxies. Intrusion Prevention Systeme (IPS) sollen den Verkehr im Netzwerk analysieren, Angriffe entdecken und Gegenmaßnahmen ergreifen. Dieser Kurs beschäftigt sich mit den grundlegenden Technologien und Arbeitsweisen, auf denen Firewalls und IPS basieren. Die Implementierung dieser Systeme in ein bestehendes Netzwerk und die Interaktion mit anderen Komponenten bilden weitere Schwerpunkte.

Kursinhalt

- Arbeitsweise von Firewall und IPS
- Abwehr von Spoofing- und Flooding-Angriffen
- Statische Paketfilter, Access-Listen
- Dynamische Paketfilter, Stateful Firewalls
- Personal Firewalls
- Generische Proxies und Application Layer Gateways
- Authentisierung, URL Filtering und zentrales Virenschanning
- Data Loss Prevention (DLP)
- Applikations-Firewalls
- DMZ-Konzepte
- Hochverfügbarkeit und Lastverteilung
- Intrusion Detection (IDS) vs. Intrusion Prevention (IPS)
- IPS-Techniken (HIPS, NIPS, PIPS)
- Muster- und Anomalieerkennung
- Event Correlation
- Zusammenspiel von Firewall und IPS

Jeder Teilnehmer erhält ausführliche Kursunterlagen aus der Reihe ExperTeach Networking in deutscher Sprache.

Zielgruppe

Netzwerkdesigner und Projektmanager erlernen die Planung und Umsetzung einer Security-Lösung am Perimeter. Techniker erwerben das technologische Know-how für den Betrieb von Firewalls und IPS, auch als Basis für nachfolgende Produktschulungen.

Voraussetzungen

Basiswissen im Umgang mit der Internetworking-Terminologie sowie Kenntnisse des IP-Protokolls sind erforderlich.



Vormerkung und Buchung

Gerne merken wir für Sie für die Dauer von zwei Wochen kostenfrei und unverbindlich einen Kursplatz vor. Auf www.experteach.at können Sie unter *Anmeldung* bequem Vormerkung, Buchung und Hotelreservierung vornehmen. Oder rufen Sie uns einfach an unter 06074-4868-0.

Für geschlossene Teilnehmergruppen modifizieren wir diesen Kursinhalt gerne entsprechend Ihren Anforderungen. Bitte sprechen Sie uns an!



Auf Wunsch senden wir Ihnen gerne unseren kompletten Katalog zu, der Sie über alle Trainings und andere Dienstleistungen informiert.

3 Tage €1.545,00 zzgl. MwSt.

Termin/Kursort

18.06.-20.06.12	Frankfurt	05.09.-07.09.12	Düsseldorf
23.07.-25.07.12	München	24.10.-26.10.12	Hamburg
23.07.-25.07.12	Wien	03.12.-05.12.12	Frankfurt

Aktuelle Informationen finden Sie auf www.experteach.at FWA



EXPERTeTeach





Firewalls, Proxies und IDS – Technologien & Produkte

1 Einführung und Motivation

- 1.1 Eine Barriere zwischen Netzen
 - 1.1.1 Aufgaben der Firewall
 - 1.1.2 Die DMZ
 - 1.1.3 Die Firewall im ISO/OSI-Modell
 - 1.1.4 Zusammenspiel mit anderen Netzkomponenten
- 1.2 Das Internet Protocol
 - 1.2.1 Der IP-Header – Format und Funktionen
 - 1.2.2 UDP – Verbindungslos und ungesichert
 - 1.2.3 TCP – verbindungsorientiert und gesichert
- 1.3 Die Firewall im Zentrum des Angriffs
 - 1.3.1 Informationsbeschaffung
 - 1.3.2 IP Spoofing
 - 1.3.3 Denial of Service
- 1.4 Kontrolle der Applikationsschichten
 - 1.4.1 Firewalls und Proxies
 - 1.4.2 Protokoll-Verständnis der Firewall
 - 1.4.3 Applikationskontrolle durch Proxies
- 1.5 Angriffe auf Programme

2 Paketfilter

- 2.1 Das Regelwerk einer Firewall
 - 2.1.1 Trigger
 - 2.1.2 Aktionen
 - 2.1.3 Abarbeiten des Regelwerkes
- 2.2 Statische Paketfilter – Access-Listen
 - 2.2.1 Funktionsweise statischer Paketfilter
 - 2.2.2 Statische Paketfilter – Schwächen und Grenzen
 - 2.2.3 Problem: Dynamische Ports
 - 2.2.4 Problem: UDP
 - 2.2.5 Fragmentierung
 - 2.2.6 Problem: Applikationsschicht
 - 2.2.7 Fazit
- 2.3 Dynamische Paketfilter – Stateful Firewalls
 - 2.3.1 Das Konzept der State Table
 - 2.3.2 Das Regelwerk einer Stateful Firewall
 - 2.3.3 Dynamische Paketfilter – Stärken und Schwächen
- 2.4 Personal Firewalls

3 Proxies – Applikationskontrolle im Visier

- 3.1 Der Begriff des Proxies
 - 3.1.1 Explizite Proxies
 - 3.1.2 Transparente Proxies
 - 3.1.3 Reverse Proxies
- 3.2 Generische Proxies
 - 3.2.1 Forwarding
 - 3.2.2 SOCKS
- 3.3 Applikation Layer Gateways
 - 3.3.1 Arbeitsweise
 - 3.3.2 Limitierungen
- 3.4 Web Proxies

- 3.4.1 HTTP-Grundlagen
- 3.4.2 URL-Filtering
- 3.4.3 Header-Manipulationen
- 3.4.4 Aktive Inhalte
- 3.4.5 Caching
- 3.4.6 Proxies und Virenschanning
- 3.4.7 SSL Proxies
- 3.5 Authentisierung an der Firewall
 - 3.5.1 Die Server-Seite
 - 3.5.2 Die Client-Seite
 - 3.5.3 Beispiel 1: HTTP an einem expliziten Proxy
 - 3.5.4 Beispiel 2: HTTP an einem transparenten Proxy
 - 3.5.5 Ersatz-Authentisierung
 - 3.5.6 Single Sign-On
 - 3.5.7 Weitere Aspekte
- 3.6 Mail Relays
- 3.7 Voice over IP
 - 3.7.1 Komponenten von VoIP
 - 3.7.2 Architektur
 - 3.7.3 VoIP und Firewalls
 - 3.7.4 Session Border Controller

4 Netzdesign

- 4.1 Planung und Netzdesign – Der richtige Standort
- 4.2 DMZ-Konzepte – Ein Überblick
- 4.3 Network Address Translation (NAT) und Firewalls
 - 4.3.1 Die NAT-Terminologie
 - 4.3.2 NAT – Ohne Probleme?
 - 4.3.3 Ein Beispiel – NAT und aktives FTP
- 4.4 Firewalls und VPN
 - 4.4.1 Separates Gateway
 - 4.4.2 Firewall als VPN-Gateway
- 4.4.3 Firewalls und Außenstellen
- 4.5 Firewall-Cluster
 - 4.5.1 Der Cluster im OSI-Modell
 - 4.5.2 Redundanz mit VRRP
 - 4.5.3 Load Sharing mit Multicasts
 - 4.5.4 Load Sharing mit Pivot Firewall
 - 4.5.5 Load Sharing durch IP Routing
 - 4.5.6 Load Sharing mit Content Switches
 - 4.5.7 Bewertung der Methoden
 - 4.5.8 Die DMZ

5 Intrusion Detection und Prevention

- 5.1 Grundlagen
 - 5.1.1 Network-based IDS
 - 5.1.2 Host-based Intrusion-Detection-Systeme
- 5.2 Angriffserkennung
 - 5.2.1 Mustererkennung
 - 5.2.2 Protokollanalyse
 - 5.2.3 Anomalieerkennung

- 5.2.4 Policy-based IDS
- 5.2.5 HIDS-Techniken
- 5.2.6 Korrelationen
- 5.2.7 Weitere Methoden
- 5.2.8 Umgehen von IDS
- 5.3 Maßnahmen
- 6 Bestandsaufnahme, Planung und Security Policy
 - 6.1 Bestandsaufnahme mit System
 - 6.2 Security Policy – Wer darf was?
 - 6.3 Der Preis der Sicherheit – Finanz- und Zeitaufwand
 - 6.3.1 Hard- und Software-Kosten
 - 6.3.2 Installationsaufwand
 - 6.3.3 Administrative Kosten
 - 6.3.4 Update-Planung – Der Hacker schläft nicht
- 7 Firewall-Produkte
 - 7.1 Check Point Firewall
 - 7.2 ASA – Cisco Systems
 - 7.3 Juniper/NetScreen
 - 7.4 Astaro Security Gateway
 - 7.5 Blue Coat Proxy Appliance
 - 7.6 Weitere Anbieter
 - 7.7 Open Source Firewalls
 - 7.8 Squid Proxy-Server



ExperTeach GmbH Training Center Wien

Millennium Tower, 24. Etage
Handelskai 94-96 • A-1200 Wien
Telefon +43 66 43 45 39 64
info@experteach.at • www.experteach.at

© ExperTeach GmbH, alle Angaben ohne Gewähr

Stand 05.05.2012