



OpenSource Training Ralf Spenneberg

Schulungen direkt vom Autor

Intrusion Detection und Incident Handling

Erkennen Sie Angriffe mit Snort & Co.

Kursnummer:

1005

Zielgruppe:

Linux Systemadministratoren,
Firewall Administratoren
Sicherheitsbeauftragte

Dauer:

5 Tage

Preis:

1.500,00 EUR zzgl. MwSt.

Inhouse:

7.500,00 EUR zzgl. MwSt.
Termine nach Absprache

Termine:

20.10. - 24.10.2008
16.02. - 20.02.2009
04.05. - 08.05.2009
28.09. - 02.10.2009

Ort:

OpenSource Training
Ralf Spenneberg
Am Bahnhof 3-5
48565 Steinfurt

Hotelempfehlung:

Hotel-Restaurant
Schünemann
Altenberger Straße 109
48565 Steinfurt
02552 - 70248-0
www.hotel-schuenemann.de

Überblick:

Entgegen aller vollmundigen Versprechen in den Hochglanzbroschüren der entsprechenden Hersteller bietet keine Firewall und kein VPN einen 100% Schutz. Unbekannte Sicherheitslücken, versäumte Patches oder Konfigurationsfehler erlauben es den Einbrechern immer wieder in die Netzwerkwerke einzudringen. Hier kann nur ein Intrusion Detection System helfen. Inzwischen existieren mit Snort 2.x und Samhain mächtige Systeme für Linux, die auch heterogene Netzwerke schützen können und sich nicht vor kommerziellen Lösungen verstecken müssen.

Voraussetzungen:

Erfahrung in der Installation und Administration von Linux.
Umgang mit der Kommandozeile.
Grundlegende Kenntnisse der Netzwerkprotokolle.

Inhalte:

- * IDS Grundlagen
 - o Host IDS
 - o Netzwerk IDS
- * Samhain
 - o Installation und Konfiguration
 - o Verwaltung im Netzwerk mit Beltane
- * Snort
 - o Installation und Konfiguration
 - o Verwaltung im Netzwerk mit BASE Neu!
- * Prelude Neu!
 - o Ein Überblick
- * Incident Handling
 - o Erzeugung von Sicherheitsrichtlinien
 - o Forensische Analyse mit
 - + Ethereal
 - + Sleuthkit/Autopsy

OpenSource Training Ralf Spenneberg

Schulungen direkt vom Autor

<http://www.opensource-training.de>

<http://www-os-t.de>

info@os-t.de

Telefon: 02552/638755

Telefax: 02552/638757