FreiOSS.net
Freiburger Open Source Netzwerk

Freiburger Open Source
Software Netzwerk e. V.
c/o Hans-Peter Merkel
Johann-Schill-Str. 24
79232 March
hpm@hpmerkel.com

2-tägiger Charity-Workshop
22. 03. und 23.03.2012

Digitale Spurensuche nach einem Einbruch in einen Linux-Server

Ein Linux Server wurde gehackt. Was kann ein Administrator tun, um die Spuren des Angriffs zu rekonstruieren?

Dieser Workshop wurde schon mehrfach für Forensik Experten deutscher Strafverfolgungsbehörden, sowie einem, dem Bundesministerium des Innern unterstehenden Bundesamt durchgeführt und wird nun mit dieser Charity Veranstaltung auch Administratoren von Linux Server Netzwerken zugängig gemacht.

Im vorliegenden Fall liegt das kompromittierte System als VMware Image im Suspended Mode vor. Dabei werden folgende Schritte mit den Teilnehmern durchgeführt:

- Starten des kompromittierten Systems in den Suspend Modus
- Nutzung einer CD mit statischen Binaries
- Erstellung eines Memory Abbildes und Übertragung auf eine Auswertestation
- Sammeln der flüchtigen Daten und Übertragung auf eine Auswertestation
- Erstellung eines Images im EWF Format
- Erstellen einer Dateiliste mit Timestamp Informationen
- Erstellen einer Hashliste zum Vergleich mit dem Originalsystem
- Mit diff/xxdiff evtentuell infizierte Dateien Suchen
- Rekonstruktion gelöschter Dateien in einem Linux System
- Auswertung des Unallocated Spaces der Festplatte
- Rekonstruktion des Angriffs aus dem Unallocated Space (wget, tar etc.)
- Internet Spuren suchen und den kompromittierten Diensten zuordnen (email, IP's URL's)
- Auswertung der Netzwerk Verbindungen und deren Dienste
- Weak Password Detection mit John (offline) und Metasploit (online)
- Banner Grabbing

Der zweitägige Workshop findet in den Räumen der VHS March, 8 km westlich von Freiburg im Breisgau statt.

Die Uhrzeiten wurden so gewählt, dass eine Anreise am ersten Tag möglich ist.

Termin: **Donnerstag, 22.03.2012 von 10:30 bis 17:00 Uhr und**
Freitag, 23.03.2012 von 08:30 bis 15:00 Uhr

Kursgebühr: **180 EUR**

Die Einnahmen des 1.Workshops fließen zu 100% in das Linux4Afrika-Projekt.
Aus den Einnahmen des 2. Workshops wird der Transport einer Palette mit Computern für die Ausstattung eines zweiten Computerraums für die “St. Scholastica’s Academy” der Missions-Benediktinerinnen von Tutzing finanziert.

Jeder Kursteilnehmer erhält eine Live DVD mit Ubuntu 11.10, speziell ausgelegt als forensische Auswertestation. Sie kann auf einer Festplatte permanent installiert werden.

Bei der Anmeldung sollte angegeben werden, ob eine 32 oder 64 Bit Version gewünscht wird. Die Kursunterlagen mit den Images befinden sich auf einer weiteren DVD.

Die Teilnehmerzahl ist begrenzt (first come, first serve). Nach offizieller Anmeldung wird vor Beginn des Workshops ein Zugang zur eLearning Plattform eingerichtet.

Anmeldungen oder Anfragen per mail an:

info@freioss.net

oder über unser Anmeldeformular auf http://www.freioss.net

Hans-Peter Merkel
Dipl. Ing.
www.hpmerkel.de