FreiOSS.net
Freiburger Open Source Netzwerk

Memory Forensik (Windows/Linux)

Administratoren stehen oft vor der Aufgabe, Spuren in einem kompromittierten System zu finden. Mit Volatility steht dazu ein hervorragendes Werkzeug zur Verfügung. Ein Memory Dump für Windows Systeme ist schnell erstellt. Für Linux und Android Smartphones ist etwas mehr Aufwand notwendig. (MAC OS ist ebenfalls möglich, wird aber hier nicht behandelt)

Die Teilnehmer erhalten eine remastered Ubuntu 13.04 DVD (64 Bit) mit allen notwendigen Werkzeugen und Plugins bereits vorinstalliert:

Im Kurs werden folgende Themen behandelt:

- Volatility Framework 2.3 zur Auswertung von Memory Dumps für die Betriebssysteme Windows XP, Windows 7, Linux und Android.
- Lime zur Erstellung von Memory Dumps unter Linux
- Coldboot Attacke per USB Boot nach Reset (Syslink startet msramdump)
- Diverse Windows Tools zur Erstellung von Memory Dumps unter Windows (32bit, 64 bit)

Folgende Memory Dumps werden ausgewertet:

WINDOWS:

- Memory Vergleich Windows XP Clean und Windows XP infiziert mit Ghostnet Trojaner
- Memory Dump Windows infiziert mit Stuxnet
- Memory Dump Windows infiziert mit Zeus

LINUX / ANDROID:

- Beispiele aus dem DFRWS Projekt

Die Kursteilnehmer lernen, wie Memory Dumps auf den o.g. Betriebssystemen erstellt

werden. Anschließend werden Plugins besprochen, die u. a. folgende Informationen aus dem Arbeitsspeicher rekonstruieren:

- Betriebssystemversion und Service Pack / Patchlevel
- aktuelle Netzwerkverbindungen
- Prozessliste
- zu Prozess ID's gehörende DLL's / Libraries
- Registry Dump diverser Hives u.a. zur Rekonstruktion von Login Informationen
- Spurensuche in Beispielen mit Malware Dumps
- Rekonstruktion der Registry aus Windows Systemen
- Rekonstruktion des Dateisystems bei Linuxsystemen
- Rekonstruktion von SQLite Datenbanken bei Android Systemen (Adressen, SMS, Kalender etc.)

Termin: 11.12.13 – 12.12.13 (2 Tagesseminar)
Zeiten: Mittwoch 09:30 – 18:30 und
Donnerstag 08:00 – 16:00

Kursgebühr: 360 EUR
ermäßigt: 180 EUR für die ersten 5 Anmeldungen von freiOSS Mitgliedern

Die VHS March stellt uns freundlicherweise den EDV Raum zur Verfügung. Die Abrechnung erfolgt deshalb ebenfalls über die VHS.

Charity Workshop: Aus den Kurseinnahmen fließen 2000 EUR in das Projekt www.linux4afrika.de. Davon die Hälfte für unser Projekt in Kenia, die andere Hälfte für das Projekt in Südafrika.

Ort: EDV Raum im Bürgerhaus March
http://www.march.de/de/Gemeinde/B%C3%BCrgerhaus+Hallen/B%C3%BCrgerhaus

Trainer: H.P. Merkel

Sollten Sie eine Unterbringung benötigen, so empfehlen wir Ihnen das nahe gelegene Hotel Sportpark mit einem guten Preis/Leistungsverhältnis:
http://www.sportpark-fitness.de/sportpark/hugstetten

Die Zahl der Teilnehmer ist begrenzt. Eine rechtzeitige Anmeldung ist deshalb empfehlenswert.

Anmeldungen und Fragen richten Sie bitte an hpm@hpmerkel.de