Digitale Spurensuche nach einem Einbruch

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

Dieses Thema wurde schon mehrfach für Forensik Experten verschiedener Dienststellen in Workshops behandelt und wird nun 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 Räumlichkeiten der VHS March statt. Die Uhrzeiten wurden so gewählt, dass ein Anreisen am gleichen Tag möglich ist.

Termin: Dienstag, 28.02.2012 von 10:30 bis 17:00 Uhr und
Mittwoch von 08:30 bis 15:00 Uhr

Kursgebühr: 180 EUR

Bei der Veranstaltung handelt es sich um eine Veranstaltung von FreiOSS. Die Einnahmen fließen zu 100% in das Projekt Linux4Afrika.

Für FreiOSS Mitglieder, die aktiv im Linux4Afrika Projekt mitarbeiten, sind besonders günstige Konditionen verfügbar. Details werden am Samstag in der Mitgliederversammlung bekannt gegeben.

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

Weitere Workshops ausschließlich für unsere Mitglieder werden in Kürze auf der Webseite von FreiOSS abrufbar sein (Proxmox VE, pfSense und GnuCash).

HP