Der Workshop

Ziel des Workshops ist es grob nachzuvollziehen, was in ein Ermittler vor Ort an einem PC machen könnte. Im Rahmen dieser Veranstaltung ist es aber leider nicht möglich, auf alle Themen im Detail einzugehen. Daher beschränken wir uns auf wichtige und interessante Bereiche die jeder auch ohne genaues Fachwissen nachvollziehen kann. Z.B. ist die Analyse von Arbeitsspeicherabbildern nicht nur kompliziert sondern auch sehr Zeitintensiv. Außerdem werden wir nicht so viel Wert darauf legen, keine Spuren zu hinterlassen: Wir speichern Daten auf der Systemplatte, was „im echten Leben“ so nicht passieren sollte.

Die Umgebung sichten

Die vorbereitete Virtuelle Maschine stellt einen laufenden Rechner da, von dem der Ermittler nun Daten sichern möchte. Da niemand den Stecker ziehen kann, keine Mitarbeiter anzuweisen sind und die VM mit allen nötigen Tools vorbereitet ist, gibt es keine weiteren Vorbereitungen zu treffen. Am Bildschirm hing ein Post-It mit der Aufschrift „pw: butterblume“.

Vorgehen

Um bei nachfolgenden Untersuchungen den Anfang der Untersuchung zu kennzeichnen ist es wichtig, die aktuelle Uhrzeit zu erfahren. Im CD-Laufwerk befindet sich „Helix“, eine Sammlung mehrerer Forensik-Tools. Gerne können Sie zwischendurch auch weitere Funktionen der CD testen, die hier nicht besprochen werden. Nutzen Sie den Autostart der CD und wählen sie explizit nochmal Englisch als Sprache aus (auch, wenn das schon voreingestellt ist). Die deutsche Übersetzung enthält leider einige Fehle. Ist Helix gestartet, befindet sich im Menü „Schnellstart“ eine Kommandozeile „command shell“. Es ist nicht möglich, die eigene „cmd“ der virtuelle Maschine zu benutzen: Man muss davon ausgehen, dass jede installierte Software so verändert wurde, dass sie nicht die erwarteten Daten ausgibt. Daher verwenden Sie eine vertrauenswürdige Shell von der Helix-CD. Der Befehl „time“ gibt die Uhrzeit aus. Notieren Sie diese.

Nun wird der Arbeitsspeicher gesichert: Ein Klick auf die Kamera links im Helix-Menü öffnet das richtige Fenster. Wählen Sie einen Speicherort (z.B. der Ordner „Forensik“ auf dem Desktop) für das Image und lassen Sie es erstellen um später im Büro des Ermittlers weitere Analysen starten zu können. Auf dieselbe Art kann man übrigens auch ein Image der Datenträger erzeugen.

Im nächsten Punkt werden Sie sich einen Überblick über den Rechner verschaffen. Dazu klicken Sie links auf die Lupe über dem Chip und danach auf den Pfeil nach rechts direkt daneben. Starten Sie das Tool „WinAudit“ und starten Sie die Untersuchung. Stöbern Sie ein wenig durch den Bericht und sammeln Daten:

- installierte Programme, die im Zusammenhang mit einer Ermittlung interessant sein könnten
- offene Netzwerkverbindungen (interessante Ports/Programme?)
- Gibt es noch andere Benutzer am System?
- Wurde der Computer oft genutzt, seit dem er installiert wurde?
- Existieren Netzwerk-Shares?

- Wie lautet die aktuelle IP?
- Welche Kapazität haben die physikalischen Laufwerke?
- Passt der Wert zur Größe der Partitionen?
- Stehen interessante Programme im Autostart?
- Läuft derzeit möglicherweise offensichtlich Schadsoftware?

Speichern sie den Bericht.

Zurück in Helix können Sie sich einen Überblick verschaffen, wann der PC in der letzten Zeit an war: „PC On/Off Time“ liefert eine Tabelle: Zu blau markierten Zeiten war der PC an (bzw. die Virtuelle Maschine lief).

Als Nächstes werden Sie versuchen ein paar Anwendungsdaten zu gewinnen und Analysieren. Dazu wechseln sie auf die 3. Seite der aktuellen Helix-Ansicht (nochmal auf den Pfeil nach rechts klicken). Auf dieser Seite finden sich einige Tools. Starten sie die folgenden Tools, überlegen Sie welche Informationen sie jeweils erhalten und notieren Informationen, die Sie für wichtig halten:

- PST Password Viewer / Mail Password Viewer
- Messenger Password
- Protected Storage Viewer
- IE History Viewer
- IE Cookie Viewer
- IE Password Viewer
- USB Deview

Hier haben Sie gerade wichtige Informationen gesammelt: Sie kennen nun Accountdaten für Email und Instant-Messaging des Täters. Auch die Internet Explorer-History gibt einiges her: Auf welchen Seiten war der Nutzer? Hat er Suchmaschinen genutzt? Sind im Internet Explorer Passwörter gespeichet?

Helix hat nun genug Daten gesammelt. Beenden Sie Helix. Speichern Sie den Bericht, den Helix angefertigt hat und schauen ihn sich an. Es wurde genau protokolliert, wann welche Tools gestartet wurden. Im Ordner „Forensik“ auf dem Desktop befindet sich ein weiteres Tool zum sammeln von Daten: Das „Windows Forensic Toolchest“. Starten Sie die „wft.exe“. Ein etwas längerer Dialog bestimmt, welche Daten gesammelt werden sollen. Wenn Sie möchten, kann man den Vorgang beschleunigen: 10x mit Enter die Standarteinstellung wählen, die Frage nach den „slow-tools“ verneinen, bis zum Ende mit Enter bestätigen. Eine vollständige Analyse wäre zwar schön, dauert hier aber viel zu lange. Nun werden automatisiert Daten gesammelt. Fehler können Sie ignorieren. wft erstellt einen Ordner mit einem Bericht über die gesammelten Daten. Öffnen Sie ihn und stöbern Sie ein wenig durch die Daten. Hierbei ist interessant, dass für jede Ausgabe eines Tools auch gleich ein Hash der Ausgabe erstellt wurde. Das ist wichtig für die Beweiskette: Im Nachhinein kann nachgewiesen werden, dass die Daten nicht verändert wurden, da sonst der Hash nicht mehr übereinstimmen würde. Im Folgenden ein kleiner Überblick mit den wichtigen Analysen:

- PCCLIP: Inhalt der Zwischenablage
- MEM_P: An welchen Stellen im RAM liegt gerade was?

- LAST_ACCESED: Zuletzt genutzte Dateien. Diese Analyse dauert etwas länger, daher haben wir hier darauf verzichtet
- PSINFO: Allgemeine Informationen über das System
- ENVIRONMENT: Umgebungsvariablen
- PSLIST: Laufende Prozesse
- PSTAT: Analysiert Threads
- PROCESS_HANDLES: Eine Liste aller offenen Handles
- IPCONFIG: Netzwerkkonfiguration
- ARP: Anzeige des Address-Resolution-Protocol-Cache
- NETSTAT_-AN: Offene Netzwerkverbindungen
- FPORT_APPS: Offene Ports mit den entsprechenden Programmen
- SYSTEM_LOG: Darstellung des System-Logbuchs
- RECENT: Zuletzt benutzte Dateien
- LAST_FILES_SAVED: Daten, die der Internet Explorer gespeichert hat
- IE_HISTORY: Internet Explorer-History
- TYPED_URLS: In die Adresszeile getippte URLs
- PSTOREVIEW: Zeigt Daten aus dem gesicherten IE/Outlook-Speicher an

Nun sind einige flüchtige Daten gesichert. Es sind aber noch ein paar weitere Datenspuren versteckt. Interessierte können versuchen Sie alleine an einige Informationen zu gelangen:

- Inhalt von Mails
- Verschlüsselungssoftware
- Zuletzt geöffnete Daten z.B. in Adobe Reader
- Informationen in Google-Earth
- Chat-Protokolle
- Entwicklungsumgebungen

Notieren sie sich nun in Stichworten, welche Indizien Sie gesammelt haben. Was lässt sich daraus schließen?

Falls weiter Interesse an Helix besteht (enthält auch das wft) haben die Tutoren das CD-Image vorbereitet, dass Sie sich gerne kopieren können. Außer Helix sind auch noch weitere Forenisk-Tools verfügbar.