FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Forensische Untersuchung von Windows 7 mit PowerShell

Daniel Neus

IT Forensik
FH Aachen

Gliederung

- Beschreibung
- Vorgehen
- Erste Ergebnisse

Beschreibung

- Live Analyse eines Windows 7 PCs
- Erstellen eines Powershell Scripts
- Ausführung und Speicherung der gesammelten Daten auf USB-Stick
- Aufbereitung der Ergebnisse als Website

Warum Powershell?

- Sehr mächtige Skriptsprache
- Harmoniert sehr gut mit Windows 7
- Auf allen Windows 7 Systemen installiert
- Powershell Skripte sind einfach erweiterbar (modularer Aufbau)

Welche Daten sind interessant?

- Flüchtige Daten in „Order of Volatility“

Speicherabbild	Auslagerungsdatei
Inhalt Zwischenablage	Netzwerkverbindungen
Routing Tabelle	NetBIOS Name Table Cache
DNS Cache	ARP Tabelle
Angemeldete User	Process-to-Port Mapping
Laufende Prozesse	Dienste
Offene Dateien	Status der Netzwerkverb.
Netzlaufwerke	Netzfreigaben
System Zeit	Uptime

Schwierigkeiten

- Adminrechte auf zu untersuchendem System nötig
- Wie sicherstellen das Powershell selbst nicht kompromittiert?
- Ohne Zusatztools kommt man nicht aus
- In wie weit wird das System durch Ausführung des Skripts verändert?

Erste Ergebnisse

- Am Beispiel des Prozess Moduls

Vielen Dank für Ihre Aufmerksamkeit

Noch Fragen?

Daniel.Neus@alumni.fh-aachen.de