



Kursbeschreibung

„Forensik Workshop:
Speicheranalyse mit Andreas
Schuster“

Wien, 22.-23.04.2010



Kursbeschreibung

Dieser 2-tägige Forensik Spezialworkshop zum Thema Speicheranalyse beschäftigt sich mit folgenden Themen:

- Intel x86 Hardware Platform
- Random Access Memory (RAM)
- Adressierungsarten
- Forensische Sicherung des Arbeitsspeichers, Methoden und Werkzeuge
- Architektur des Microsoft Windows Betriebssystemkerns
- Windows Speicherverwaltung
- Objekte des Betriebssystemkerns
- Analysetechniken
- Einsatz des Microsoft Debuggers und des Volatility Frameworks
- Übungen an Speicherabbildern

Der Kurs wendet sich an Spezialisten im Forensik Bereich mit entsprechendem forensischen Know How.

Über den Vortragenden

Andreas Schuster ist seit 2003 als IT-Forensiker bei einem international operierenden Großunternehmen der IT- und Telekommunikationsbranche beschäftigt. Vorher leitete er ein kommerzielles Computer Incident Response Team und arbeitete als Systemadministrator bei unterschiedlichen Internet Service Providern. Insgesamt blickt Herr Schuster auf über 25 Jahre Erfahrung in der Computertechnik zurück.

Neben der täglichen Laborroutine untersucht Herr Schuster Dateiformate und Arbeitsspeicherinhalte unter dem Betriebssystem Microsoft Windows. Er ist Autor einschlägiger Analysewerkzeuge und Fachartikel sowie ein gefragter Referent für Vorträge und Trainings. Für seine Arbeiten auf dem Gebiet der Speicheranalyse wurde er 2006 mit dem Best Paper Award des Digital Forensic Research Workshops und im Jahre 2008 mit dem Deutschen IT-Sicherheitspreis ausgezeichnet.



Andreas Schuster ist Mitglied der ACM, der Deutschen Gesellschaft für Informatik und ihrer Fachgruppe SIDAR. Er ist weiterhin Mitglied des Digital Forensics Research Workshops und Gutachter für das bei Elsevier erscheinende Journal "Digital Investigation".

Benötigte Ausstattung

Im Rahmen des Workshops werden viele Beispiele gemeinsam und interaktiv gestaltet. Hierzu benötigen alle Teilnehmer einen eigenen Laptop mit zumindest folgender Konfiguration:

- Betriebssystem: Microsoft Windows XP empfohlen, Linux und Mac OS X erfordern eine vom Teilnehmer zu erstellende virtuelle Maschine mit Microsoft Windows
- mindestens 8 GB Festplatte frei
- mindestens 1 GB RAM frei
- DVD Laufwerk
- VMware player oder VMware workstation (Linux/Windows) Version 6.5.2 bzw. VMware Fusion (Mac OS X)
- Microsoft Debugging tools for Windows, <http://www.microsoft.com/whdc/DevTools/Debugging/>
- MANDIANT Highlighter <http://www.mandiant.com/software/highlighter.htm> (bitte auch dessen Systemvoraussetzungen beachten!)

Ort

Security Research
Sommerpalais Harrach
Favoritenstrasse 16, 1040 Wien

Anmeldung

Die Anmeldung erfolgt schriftlich über ein Mail an anfragen@securityresearch.at unter Angabe von Namen, Firma, Funktion und den benötigten Rechnungsdaten. Die Anmeldung ist erst nach Rückbestätigung seitens Security Research gültig.



Kosten

1200 EUR netto, Verpflegung und Unterlagen inklusive

Der Kursbetrag muss bis 14 Tage vor Beginn gezahlt werden und ist nicht rückerstattbar. Bei Ausfall des Trainers wird ein Ersatztermin angeboten. Der Kurs findet ab einer Mindestteilnehmeranzahl von 3 Teilnehmern statt. Eine etwaige Absage wird spätestens eine Woche vor Beginn bekannt gegeben.

Referenzen

Publikationen

Eckstein, K. und **Schuster, A.**: Die Geschwätzigkeit des verlorenen Laptops, in: digma Zeitschrift für Datenrecht und Informationssicherheit, 8 (2008) 4, S. 154-159.

Schuster, A.: The impact of Microsoft Windows pool allocation strategies on memory forensics, in: Digital Investigation, 5 (2008) S, pp. S58-S64. (↗
<http://www.dfrws.org/2008/proceedings/p58-schuster.pdf>)

Schuster, A.: File Carving - Grundlagen und neue Techniken, in: Paulsen, C. (Hrsg.): Tagungsband des 15. DFN-CERT Workshops „Sicherheit in vernetzten Systemen“, Norderstedt 2008, S. A1-A14.

Schuster, A.: Introducing the Microsoft Vista event log file format in: Digital Investigation, 4 (2007) S, pp. S65-S72. (↗
<http://www.dfrws.org/2007/proceedings/p65-schuster.pdf>)

Schuster, A.: Pool Allocations as an Information Source in Windows Memory Forensics, in: O. Göbel, D. Schadt, S. Frings, H. Hase, D. Günther & J. Nedon (Eds.): IT-Incident Management & IT-Forensics – IMF 2006 (pp. 104-115). Bonn 2006, pp. 104-115.

Schuster, A.: Searching for Processes and Threads in Microsoft Windows Memory Dumps, in: Digital Investigation, 3 (2006) S, pp. S10-S16. (↗
<http://www.dfrws.org/2006/proceedings/2-Schuster.pdf>)



Schuster, A.: Forensische Analyse des Arbeitsspeichers am Beispiel von Microsoft Windows 2000, in: Paulsen, C. (Hrsg.): Tagungsband des 13. DFN-CERT Workshops „Sicherheit in vernetzten Systemen“, Norderstedt 2006, S. 11-120.

Schuster, A.: Windows Eventlogs in der forensischen Analyse, in: Thorbrügge, M. (Hrsg.): Tagungsband des 12. DFN-CERT Workshops „Sicherheit in vernetzten Systemen“, Norderstedt 2005, S. D1-D16.

Mehr als 50 weitere Beiträge zu Themen der Computertechnik in verschiedenen Publikumszeitschriften.

Vorträge

(Auswahl)

Schuster, A.: Windows Memory Analysis with Volatility. 21st FIRST Conference, Kyoto 2009.

Schuster, A. and Walters, A.: Two-day Course on Advanced Memory Forensics and Malware Analysis. Hoffmann BV, Almere (NL) 2009.

Schuster, A.: Betrachtung volatiler Daten in IT-Forensik und Incident Response. econique, 9. CxO Dialog Information Risk Management, Berlin 2009.

Schuster, A.: Microsoft Vista Event Log. High Tech Crime Expert Meeting, Europol, Den Haag 2008.

Schuster, A.: Workshop on Memory Analysis on the Microsoft Windows Platform. IMF, Stuttgart 2007.

Österberg, P. and **Schuster A.:** Workshop on Microsoft Windows Incident Response and Memory Analysis. 19th FIRST Conference. Sevilla, Spain, 2007.

Schuster, A.: Digitale Forensik unter Microsoft Windows. Universität Mannheim, Lehrstuhl für Praktische Informatik I, 2007.

Schuster, A.: Forensische Analyse des Arbeitsspeichers bei Microsoft Windows. n.runs High-Level Security Board, 2006.



Schuster, A. Einführung in die forensische Analyse des Arbeitsspeichers unter Microsoft Windows – Abbilderstellung und Auswertung. Landeskriminalamt Baden-Württemberg, 2006.

Schuster, A. Das neue Ereignisprotokoll von Windows Vista – Format und Auswirkungen auf die forensische Praxis. Bundeskriminalamt Meckenheim, 2005.

Schuster, A. Analyse von Rootkits und Trojanischen Pferden mit IDA Pro. Bundeskriminalamt Meckenheim, 2005.