Host Forensic Track Overview

The host forensic track is part of a multi-track training program created by the Sandia National Laboratories' Tracer FIRE staff to indoctrinate participants to the overall methods that a high performing CSIRT (Cyber Security Incident Response Team) uses in its daily mission of hunting for and tracking down of attackers operating on the corporate enterprise network. The primary mission of CSIRTs is to continually patrol their organizations enterprise networks and systems in order to detect malicious activity and remediate these attacks. This is a complex and demanding job so it's not for the faint of heart.

In this track, you will gain an insight into how some of our experienced analysts perform their jobs and the techniques that they have discovered to be effective at identifying potential cyber threats operating within the organizations enterprise. Host forensics focuses on the acquisition and analysis of artifacts and data that reside on the hosts or endpoints. A lot of the adversary's effort is focused on subverting Microsoft Windows based servers and workstations so the majority of this track examines Windows based systems. However, similar concepts apply across Linux and MacOSX based systems as well. However, the tools will typically be somewhat different as well as the actual techniques used to conduct forensic analysis of those kinds of systems.

The following list enumerates the topics that will be covered in this track:

Malware Analysis and Incident Response

Adversarial Tactics and Event Reconstruction

Setting up a Malware Analysis Lab

Introduction to Memory Forensics

- Refresher on Virtual Memory Management (MS-Windows specific)
- Overview of Volatilty 2.4
- Analysis of Vmware vmem files
- Code Injection Techniques (Reflective DLL injection, Process Hollowing)
- Investigating Malicious Processes and Services
- System Event Log Analysis
- Registry Analysis

Introduction to Disk Forensics

- Refresher on Filesystems (NTFS, FAT, etc)
- Overview of Encase Enterprise
- Network acquisition of disk and memory images

Malicious PDF Documents and Shellcode

Windows Authentication and Passwords

Detection of Credential Stealing and Token Kidnapping

Timestomping

Web Browsers and the IE 10 Extensible Storage Engine

Case Studies

RSA Incident Response: Emerging Threat Profile Shell_Crew, http://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf, visited on 4/7/2015.

G Data Red Paper 2014: Uroburos Highly Complex Espionage Software with Russian Roots, https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf, visited on 4/7/2015.

Recommended Texts:

Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux and Mac Memory, Michael Hale Ligh et al, Wiley and Sons, 2014.

Practical Reverse Engineering: X86, X64, ARM, Windows Kernel Reversing Tools and Obfuscation, Bruce Dang, Wiley and Sons, 2014.

Windows Internals 7th Edition, Mark Russinovich, David A. Solomon, and Alex Ionescu. Microsoft Press, 2012.