Network Forensics Training

Kursen kommer att ges på svenska med engelsk dokumentation.

The Network Forensics class consists of a mix of theory and hands-on labs, where participants will learn to analyze Full Packet Capture (FPC) files. The scenarios in the labs are primarily focused at network forensics for incident response, but are also relevant for law enforcement/internal security etc. where the network traffic of a suspect or insider is being monitored.

Instructors

Erik Hjelmvik is the creator of NetworkMiner and an experienced incident handler who has specialized in the field of network forensics.

Jonas Lejon is a security consultant with focus on state sponsored attacks.

Agenda - Theory and Practice using Open Source Tools

- Theory: Ethernet signaling
- Hardware: Network TAPs and Monitor ports / SPAN ports
- Sniffers: Recommendations for high-performance packet interception
- PCAP analysis: Extracting evidence and indicators of compromise using open source tools
- Defeating Big Data: Techniques for working with large data sets
- Whitelists: Learn how to detect 0-day exploit attacks without using IDS signatures
- Challenge: Find the needle in our haystack and win an honorable prize!

The Scenario

The scenario used in the class involves a new progressive Bank, which provides exchange services for Bitcoin and Litecoin. We've set up clients and a server for this bank using REAL physical machines and a REAL internet connection. All traffic on the network is captured to PCAP files by a SecurityOnion sensor. In the scenario this bank gets into lots of trouble with hackers and malware, such as:

- Defacement of the Bank's web server (see zone-h mirror)
- Man-on-the-Side (MOTS) attack (much like NSA/GCHQ's QUANTUM INSERT)
- Backdoor infection through trojanized software
- Spear phishing
- Use of a popular RAT (njRAT) to access the victims machine and exfiltrate the wallet.dat files for Bitcoin and Litecoin
- Infection with real malware (Nemucod, Miuref / Boaxxe and more)

Class attendees will learn to analyze captured network traffic from these events in order to:

- Investigate web server compromises and defacements
- Detect Man-on-the-Side attacks
- Identify covert backdoors
- Reassemble incoming emails and attachments

- Detect and decode RAT/backdoor traffic
- Detect malicious traffic without having to rely on blacklists, AV or third-party detection services

Target Audience

Q: Who should attend?
A: Anyone who want to improve their skills at finding evil stuff in full content packet captures.

Q: Who should NOT attend?
A: Those who are afraid of using Linux command line tools.

Training Preparations

Attendees will need to bring a laptop that fits the following specs:

- A PC running any 64 bit OS (Windows, Linux or Mac)
- At least 4GB RAM
- At least 40 GB free disk space
- VirtualBox, https://www.virtualbox.org/, (64 bit) installed (VMware will not be supported in the training)

Approximately one week before the course a link to a VirtualBox VM will be emailed to you.
Please download the VM to your computer before the course!

Please note that having a 64-bit CPU and a 64-bit OS is not always enough to support 64-bit virtualization. You might need to enable features such as ”AMD-V”, ”VT-x” or ”Hyper-V” in BIOS in order to run virtual machines in 64-bit mode. You might also need to turn off "Intel Trusted Execution" in BIOS. One way to verify that your laptop supports 64-bit virtualization is to download the SecurityOnion ISO, https://download.securityonion.net/file/Security-Onion-16/securityonion-16.04.6.3.iso, and see if it boots up in VirtualBox.