Cyber Defender 1: Network Traffic and Log Analysis

An Information Security Course for Experienced IT Personnel

Cyber Defender 1 is a mentored, learn-by-doing course that is delivered online. Students will gain the basic skills of analyzing network traffic at the packet level, as well as analyzing system and network logs for indicators of malicious activity. They will then learn more complex techniques of log analysis and extraction, and static and dynamic analysis of potentially malicious files.

Tasks:

- Analyze malicious network traffic

  Students analyze network traffic moving in and out of a military aide's personal laptop. Using packet capture (PCAP) files, students determine if it was infected by malware and if so what malware and how the infection occurred. Students then perform an attribution analysis on the actors involved in the attack. (They analyze evidence they find and use open source intelligence about a particular exploit kit to make hypotheses about the attackers' identities.)

  OBJECTIVE: Analyze suspicious network traffic in a PCAP using Snort and Wireshark.
  OBJECTIVE: Recognize a cushion redirect in network traffic.
  OBJECTIVE: Recognize the identifying features of a specific exploit kit.
  OBJECTIVE: Recognize a malware payload being transferred to a targeted host.

- Analyze a remote intrusion attempt

  A security operations center analyst has seen evidence of a password cracking attempt within a key network. Students analyze a PCAP and event logs within a security information and event management system (the Splunk SIEM) to determine whether or not any passwords were compromised, and if the network was breached as a result. The student must also identify which tools were used by the attacker, and which steps should be taken to safeguard specific hosts in the network from similar cracking attempts in the future.

  OBJECTIVE: Analyze suspicious network traffic in a PCAP using Wireshark.
  OBJECTIVE: Analyze network and system logs using Splunk

OBJECTIVE: Cross-correlate events seen in a PCAP with events seen in logs
OBJECTIVE: Recognize a Hydra brute-forcing attack
OBJECTIVE: Determine if a brute-forcing attack has been successful

- Investigate an incident using a Security Information and Event Management System (SIEM)

  Students analyze a possible "watering hole" attack in which clicking on a malicious link embedded in an otherwise legitimate website launches an exploit kit that infects a user's machine with a "banking trojan." To accomplish this, they must analyze multiple logs within the Splunk SIEM.

  OBECTIVE: Analyze network and system logs using Splunk
  OBJECTIVE: Pivot among multiple logs using Splunk's search facilities
  OBJECTIVE: Identify possible indicators of compromise
  OBJECTIVE: Determine if devices are likely to have been infected using indicators of compromise
  OBJECTIVE: Tentatively identify the malware used and the intent of the attack

- Analyze and understand malware using a sandbox coupled with open source intelligence gathering

  Students use a "hash" of the possible malware-containing file to conduct research using VirusTotal, online sandboxes, and open source intelligence sources to determine specific indicators of compromise to guide forensic analysis of memory and file system images of infected devices.

  OBJECTIVE: Use VirusTotal to identify a malware sample
  OBJECTIVE: Use advanced features of VirusTotal to learn detailed information about a malware sample
  OBJECTIVE: Use the HybridAnalysis sandbox to perform static and dynamic analysis of a malware sample
  OBJECTIVE: Use open source threat intelligence to learn more about specific malware

Duration: 6 weeks at 25 hours/week
Prerequisites: Applied knowledge of computer networks and protocols, knowledge of the Windows and Linux operating systems, and experience using command line interfaces.