MAGNET FORENSICS TRAINING

Magnet AXIOM Incident Response Examinations (AX310)

AX310 is an expert-level four-day training course, designed for participants who are familiar with the principles of digital forensics and who are seeking to expand their knowledge base on advanced forensics and incident response techniques and want to improve computer investigations.

AX310 will give participants the knowledge and skills they need to track incidents where unauthorized computer access and file usage has taken place on a computer system. This course utilizes Magnet AXIOM and third-party tools to explore the evidence in greater depth by learning about volatile data collection. An incident response toolkit will be created to capture volatile data in class that students can take with them for use in applications beyond the classroom.

In this course, a deeper understanding of investigating incidents involving malware and network intrusions into Windows computers will be provided. Students will conduct a static analysis of malware by building a virtual environment and use Kali Linux in that environment to sandbox malware.

MAGNET FORENSICS

After the static analysis of the malware, students will activate the malware in the virtual environment and conduct a dynamic analysis. They will also capture packets during the malware activation to capture information from the malware regarding its command and control server. An analysis of the captured information from the network communication will then be conducted to determine what the malware is designed to do, such as spread laterally on the network, escalate user privileges, create new users, search for PII or send collected data back to the command and control server.

By searching through artifacts like Windows Ptrefetch, SRUM, AMCACHE, Jumplists, LNK files, SHIMCACHE, MUICACHE, UserAssist, Windows Event logs, and the $Logfile, participants will determine the initial attack vector of the malware and the chain of events that took place thereafter.

AXIOM INCIDENT RESPONSE EXAMINATIONS (AX310) MODULES

Each module of instruction employs instructor-led and student practical exercises to reinforce the learning objectives and provide the participants with the knowledge and skills necessary to successfully utilize Magnet AXIOM in their investigative workflow.

Module 1: Introduction and Installation of Magnet AXIOM

Students will be introduced to each other, to the instructor(s) and to Magnet AXIOM.

Module 2: Course Overview

An overview of the course will be presented to students along with the learning objectives and expected outcomes for the four-day training event.

Module 3: Malware Overview

This module focuses on malware — specifically, the footprints left behind from it, its common behavior, and what Windows is doing to stop it.

Module 4: Packet Captures (PCAP)

Network traffic is sometimes key to understanding how malware arrived into the network and how the malware allows nefarious actors to travel through the network. This module focuses on capturing, filtering, and analyzing network traffic to track down network intrusions and perform network forensics.

Module 5: Incident Response Toolkit

During this module, students will learn the necessity of collecting volatile data from a suspect computer. They will use the output to determine a starting point for the examination while the forensic images are being processed by AXIOM.

Module 6: RAM

Participants will parse RAM from a computer involved in a malware incident and determine what programs were running and from what location. Students will also investigate the malware to determine what computer user was associated with it.

Module 7: Static Analysis of Malware

Participants will set up and learn how to utilize virtual machine technology and Kali Linux to leverage good forensic practices and intrusion detection methodologies to infect a computer and examine the results and behavior of the malware.

Module 8: Dynamic Analysis of Malware

In this module, students will setup a Windows computer similar to the OS from the suspect computer and activate the extracted malware in a controlled environment (sandbox) and monitor the activity of the malware.

Module 9: Wrapping up the Investigation

Students will put all of the pieces or this malware puzzle together in order to get ready to report on the findings of their investigation.

Module 10: Finalizing the Investigation

During the module, students will learn how to put all the pieces of the investigation together through the correlation of all the data they have collected during the preceding modules.

Module 11: Cumulative Review Exercise.

To further reinforce the instructional goals of the course, students are presented with a final scenario-based practical exercise which represents a cumulative review of the exercises conducted in each of the previous modules.

For more information on Magnet Forensics Training and Certification programs, visit magnetforensics.com/training.

Any completed instructor-led Magnet Forensics training course (in-person or virtual) can be counted for 32 CPE credits through NASBA.

MAGNET FORENSICS