Cyber Threat Intelligence & OSINT

Course 71584 – 40 Hours

Overview

Open-source intelligence (OSINT) covers the techniques and procedures practiced retrieving targeted information from open-source networks containing immense amounts of data. This course teaches participants how to collect and analyze information using various tools and unique methods and apply targeted cyber intelligence to defensive operations to proactively act on threats. Students will be further exposed to collecting information from the Darknet, social networks, classifying diverse sources, and creating automated tools for a more advanced data gathering process.

The course helps prepare for the certification exams GOSI (SANS) and C|OSINT (Mcafee).

On completion, Delegates will be able to

- Provide students with all-source methodology of employing open-source intelligence gathering.
- Discover the tools, techniques and technologies needed to generate highly relevant intelligence.
- Create tools in Python for precise and customized data gathering.
- Understand how to collect information from various social networks.
- Explore the Darknet for its “undercover” information bases.

Who should attend

The course targets participants with a foundation understanding of the internet who wish to gain advanced open-source intelligence capabilities. Primarily:

- Threat intelligence analysts
- Cybersecurity professionals
- Law enforcement personnel
- Private investigators

Prerequisites

- Linux basics

Course Contents:

Module Title	Description
Module 1: Introduction to OSINT The first module will introduce participants to fundamental concepts of open-source intelligence and cover the basic data collection techniques. Students will set-up the virtual lab that will serve them throughout the course for data collection, anonymous browsing and more. During this module, some ethical and legal aspects of OSINT will also be mentioned.	▪ **Introduction to OSINT** ○ Open-source intelligence terminology and definitions ○ Becoming anonymous ○ Reconnaissance of an Organization ○ Gray areas and ethics in OSINT ○ Building OSINT plan
Module 2: OSINT Tools and Search Engines Throughout this module, students will get to know some practical tools and search engines they will handle during the course for collecting data. They will deepen their understanding between various information sources, and will focus on gathering data from social networks. One of the key capabilities' participants will gain during this part, is setting-up search engines and OSINT tools to work more effectively using automation.	▪ **Searching for OSINT information** ○ Dive into metadata ○ Types of OSINT sources ○ Reverse image search ▪ **OSINT Tools** ○ Online tools and frameworks ○ Introduction to basic bash scripting and automation ○ Extracting information from major social networks ○ Geolocation
Module 3: Advanced OSINT Tools and Search Engines In this module, students will become familiar with a wider and more advanced array of OSINT tools and search engines. They will understand how to use metadata, and maximize the use of different filtering and customization options for searching. This will give them capabilities of identifying further information that may not be disclosed in a standard Google search. During this stage, participants will practice each tool and test its capabilities. By the end of this session, they will acquire advanced capabilities of locating and extracting information, and getting as quickly as possible to as much of the desired information.	▪ **Mastering google search engine** ○ Google search engine advanced search ○ Geographic information gathering ○ Searching in different languages ○ Building a google custom search engine ○ Reverse image search ○ Legal concerns and privacy issues ▪ **OSINT tools in-depth** ○ Crawlers ○ Mapping ○ Passive Target Scanners
Module 4: The Darknet The Darknet is considered the most prominent source of huge amounts of relevant information that is not accessible through the usual network. During this module, participants will learn to use the Darknet,	▪ **Darknet overview** ○ Understanding global internet layers ○ Surface web and deep web ○ Installing and configuration of the Tor browser ○ Darknet search engines

how to pinpoint to the information they are looking for, collect it, use avatars, purchase databases with sensitive information, and activate different automated tools for browsing and extracting information from the Darknet.	○ Installation and security concerns ○ The Tor UI ○ Onion system ○ Find hidden services ○ How crawlers operate ○ Understanding Crypto currency marketing ○ Using leaked password databases