Certified Dark Web Analyst (CDWA-320)

This document includes instructor led class overview and objectives, identifies target student and prerequisites, course outline, and course specific software and hardware requirements.

Course Length

5 days

Overview

The Dark Web is a vast, well-traveled, and nearly ignored waypoint of exfiltrated corporate assets as well as discussions of network attacks and methodology. Information security regularly overlooks the significance of this largely untapped resource. This course covers tools, techniques, and tactics for leveraging the Dark Web as a means for defending organizational assets proactively and reactively. The Dark Web consists of networking environments and infrastructure that does not leverage traditional TCP/IP technology. Appreciating these networks and adopting a successful defensive posture includes knowing what attack vectors are currently in use. Parsing nuances and critical distinctions can establish the difference between an attempted attack and a successful attack from the Dark Web. This course will prepare the student to understand the Dark Web, adopt protective practices for accessing Dark Networks, and find the places where ongoing attack discussions are unfolding in real time. Beyond navigation, the student will learn to use relevant tools to discover and gain entry to otherwise closed sessions. In addition, students will learn how to establish private and anonymous technologies to enhance their own efforts to conduct research and investigation. Access to the Dark Web requires specialized programs, such as TOR (The Onion Router). In depth coverage of such technology, as well as their proper installation, configuration, and use, is paramount to the proper capture of important information. Students will learn to use these tools and draw important distinctions between privacy, anonymity, and the means by which they can establish both. Lastly, the course will explore the burgeoning area of Open Source Intelligence (OSInt) over Dark Networks and includes frameworks, techniques, and recommendations for proper analysis and synthesis of discovered information.

Course Objectives

In this course, you will discover navigational techniques over Dark Networks and develop defensive and analyst skillsets including:

- Learning the origin and motives beyond Dark Network creation and evolution
- Relating Dark Web marketplaces and exfiltrated corporate assets
- Relating Dark Web content to your organization’s effort to secure assets
- Learning to find content on the Dark Web given the lack of conventional search
- Leveraging anonymizing technologies to enhance investigative efforts
- Capitalizing on the distinctions between privacy and anonymity

- Exploring technologies that provide or enhance privacy and anonymity
- Creating an anonymous Dark Web persona
- Conducting investigations with anonymous messaging and network access
- Gaining entry to otherwise restricted forums and markets
- Learning how cryptocurrencies and exploring alternatives beyond Bitcoin
- Learning how cryptocurrencies can be traceable and which ones afford greater anonymity
- Establishing methods for collecting and storing data securely
- Learning how and why work with Law Enforcement can facilitate investigation
- Learning how to configure a private and anonymous workstation
- Learning about alternative messaging technologies such as Bitmessage
- Learning about alternative Dark Networks such as I2P (Invisible Internet Project)
- Learning how to find exfiltrated data on the Dark Web
- Analyzing data on the Dark Web and answering questions such as:
    - How did data get on the Dark Web?
    - How can we minimize the effects of that data exfiltration?
    - How can we enhance our abilities to detect/prevent future exfiltration?
- Making use of the Dark Web response as part of Incident Management
- Making Dark Web a source for research regarding competitors and subjects of interest

Target Student

Any information security professional, including the CISO, Red Team, and Business Analyst, Network Security Administrator, and Risk Management Professional, can substantially benefit from an enhanced appreciate for private and anonymous technologies. This course is primarily designed for information security professionals who are tasked with conducting investigations and defending organizational assets. This training will augment the expertise of Penetration Testers exploring new avenues of potential exploit. In addition, business analysts can benefit by exploring additional sources of information regarding threats to organizational assets. Risk management professionals can glean information about current threats to organizational assets. Network administrations will better be able to determine whether such technologies are being used on corporate networks without authorization. CISOs will be able to better establish policy regarding the safe habits of employees and interactions with customers. Further, privacy enthusiasts, concerned with their ability to establish and maintain safer online habits, will learn valuable techniques and concepts necessary to operate over private connections and Dark Networks.

This class is not designed for those looking to abuse the Dark Web in furtherance of any illegal or unethical activities. Students are required to learn about their ethical obligations and sign a statement that their use of any tools, techniques or processes taught in this course will be for lawful purposes exclusively.

Prerequisites

This course is entry level for Cyber Security professionals. As such, a general knowledge of the following is recommended:

- Basic networking skills
- Knowledge of remedial risk management technologies and concepts
- Basic navigation of Windows and program installation
- Fundamental usage of website browsing

Course Outline

DOMAIN 1: FUNDAMENTALS OF IT SECURITY
A walkthrough of fundamental IT concepts and foundations

- Understand and Apply Concepts of Confidentiality, Integrity, Availability, and Anonymity
- Security Governance Principles
- Principles of Security
- Identification, Authentication, Authorization, and Accounting
- Cryptography and Asset Protection Techniques
- Distinctions between Privacy, Anonymity, and related goals
- Establishing a Private Investigation Workstation
- Principles of Virtualization and the Merits and Flaws of Various Options
- Private Browsing and Tracker/Fingerprint Mitigation
- Out-of-Band Communication Techniques
- Verification of Authenticity Regarding the Acquisition and Installation of Tools

DOMAIN 2: GOVERNANCE, RISK, AND COMPLIANCE
An exploration of organizational concepts, risk management, and legal/regulatory concerns.

- Concepts of Governance
- Understand Legal and Regulatory Issues that Pertain to Information Security globally
- Working with Law Enforcement (developed in conjunction with the Secret Service)
- Understand and Apply Dark Web Threat Modeling
- Forensics Investigations and the Dark Web
- Understand Business Continuity / Disaster Recovery Plans in relation to Dark Web attacks
- Understand and Implement Dark Web Professional Ethics
- Establish and Manage Security Education, Training, and Awareness of CIAA Topics

DOMAIN 3 - HISTORY OF THE INTERNET, DEEP WEB AND DARK WEB
A historical account of modern networking and the origins and definitions of the Web

- Definitions and Terminology
- History of the Internet

- History of the Deep Web
- Understanding the Deep Web
- History of the Dark Web
- Applying the Dark Web in a modern context

DOMAIN 4 - NETWORKING AND ROUTING ON THE DARK WEB
A technical account of modern networking and the role of TOR and Dark Net infrastructure.

- Communication Models
- Routing the Internet Protocol (IP)
- Observing Traffic Across a Network
- About TOR—The Onion Router
- Other Dark Networks (e.g. I2P)
- Understanding Dark Networks
- Understanding End-To-End Encryption
- Understanding Virtual Private Networks
- Drawing Distinctions Between VPN Privacy and Dark Web Anonymity
- Principles of Cryptography, Dark Networks, and Establishing Anonymity

DOMAIN 5 - ANONYMITY, THE DARK WEB, AND YOU
A discussion and explanation of technical and organizational implications for anonymity.

- Establishing and Maintaining Anonymity
- Discovering and Understanding Dark Web Content
- Establishing and Maintaining a Presence on the Dark Web
- Moving Between Surface, Deep, and Dark Web Content
- Identifying Best Practices
- Understanding and Using Cryptocurrency
- Leveraging Cryptocurrency Soft and Hard Wallets
- Exploring Dark Web Link Lists
- Exploring Dark Web Search Options
- Understanding Dark Web Markets
- Buying and Selling on the Dark Web
- Detecting and Avoiding Fraud on the Dark Web
- Leveraging Anonymous Messaging on the Dark Web
- Securely Storing Information

DOMAIN 6 - CRAWLERS AND DATA DISCOVERY IN THE DARK WEB
A high-level framework of analysis including GRC implications and praxis.

- Understanding Principles of OSInt
- Leveraging a Custom Information Discovery Framework
- Establishing Incident Response and Controls Introduction
- Navigating, Building, and Using Crawlers
- Integrating Dark Web into defender activities

Technical Requirements for Lab Access

- Windows 10 64-bit Operating System with Anti-Malware (Defender is acceptable)
- 8+ GB of RAM preferred (4 GB minimum)
- Intel i5 processor (or equivalent)
- 50 GB of free space on an SSD preferred (HDD minimum) for virtual machine storage
- Virtualization enabled in BIOS
- VirtualBox (You can use VMware products, but it is not recommended)
- A reliable internet connection at 10+ Mbps down 1+ Mbps up (preferably wired).
- Access to your own internet connection and system given the potential sensitivity of Dark Web content. (If using a company network or system, we strongly encourage written permission before class begins)
- Due to the nature of the course, some lab steps are **NOT** written

Assets Provided for Lab Access

- Download link to current version of lab machine (updated quarterly)
- USB Stick for Tails deployment

Lab Activities shall include, but not be limited to

- Virtualization: Installing and Configuring VirtualBox
- OS Hardening Techniques
- Antimalware Installation and Configuring
- Using Hashing Tools
- Digital Signatures: Using PGP
- Sandbox Considerations
- Private Browsing: Mitigating Fingerprinting and Tracking
- Reviewing and Changing a MAC Address
- Establishing Public VPN
- Anonymous Browsing: Installing the TOR Browser
- Using the TOR Browser to Access the Dark Web
- Establishing a Dark Web Identity
- Establishing Dark Web Anonymous Messaging
- Cryptocurrency Wallets
- Using I2P to Access the Dark Web
- OSINT Techniques
- Securely Creating Storage for Research
- Residual Data
- Covert Channels: Leveraging Steganography
- Installing and Configuring Tails in a VM
- Installing and Configure Tails on a Stand-Alone USB Stick