CYBER OPERATIONS PREP™ (COP™)

This is an intense, hands-on course designed to take students through a wide variety of topics relevant to operationally-focused cyber missions within the offensive and defensive arenas. Students will receive highly technical and mission relevant training needed to significantly minimize the burden of on-the-job training required to immediately impact operations. This 4 -week course focuses heavily on the TCP/IP stack, deep-packet analysis, network forensics, Windows and *NIX system operator fundamentals, malware triage and the post-compromise forensics of remote targets. Extensive analysis is conducted throughout each stage of the network attack methodology to include packet capturing and inspection, analyzing logs, deep dive examination of the compromised machine. During the last week students will learn how to build custom scripts to perform host surveys on a target system to help identify traces of compromise on the system. Skills learned during the week are evaluated each week on the final day with a hands-on culmination exercise, challenging the students to apply those skills and validate their knowledge.

CHIRON METHODOLOGY DOMAIN

CYBER OPERATIONS PREP™ (COP)™

DURATION

20 DAYS

RECOMMENDED PRE-REQUISITES

- Familiarity with VMware Player or Workstation
- Exposure to Windows Operating Systems
- Exposure to Linux or Unix-based Operating Systems
- Familiarity with network sniffing tools (Wireshark, TCPDUMP. WinDump)

PHONE: 410.672.1552 x 109 **FAX:** 410.672.3187 **ADDRESS** 7021 Columbia Gateway Dr. Suite 250 Columbia, MD 21046

CYBER OPERATIONS PREP™ (COP™)

COURSE OUTLINE

ASSESSMENT

- Students are administered a computer-based practical exercise on the first day of class.

  Assessment time: 3 hours

OUTLINE

- Topics covered:
- Networking and Protocol Analysis
- Windows Operating System Fundamentals
- Linux/Unix Operating System Fundamentals
- Scripting knowledge in both bash and Powershell

The assessment is designed to evaluate and assess each student's technical experience and capabilities. Instructors grade each Student's assessment, and then work to tailor the course schedule based upon the combined experience level of the students enrolled in an effort to maximize the training experience throughout the entire 5 weeks. This assessment is our most critical tool and has proven to provide significant results in the performance of each student as they progress throughout the training.

The assessment is Chiron controlled testing material; copies can be provided to select management personnel upon request.

NETWORKING

- Understand sources of open source research
- Knowledge of utilizing an attack platform
- Knowledge of networking basics and devices
- Understand and Identify Physical Topologies
- Perform IPv4 and IPv6 Subnetting
- Understand Ports, Protocols and Services
- Perform protocol analysis
- Reconstruct network traffic
- Identify files transferred in network traffic
- Understand common forms of protocol exploitation

OUTLINE

- Orientation
  - Introductions
  - Pre-assessment
- Active Operations (Tradecraft) Methodology
- Customizing an attack platform and tools
- TCP/IP Stack
  - Networking basics, devices, and topologies
  - 802.3
    - ARP and ARP cache poisoning
  - IPv4 and IPv6
  - Transport Layer Protocols
    - Session data
  - Application Protocols
    - Man in the middle (MITM)
- Protocol Analysis
  - Packet Carving
  - Recognizing File Signatures

CYBER OPERATIONS PREP™ (COP™)

COURSE OUTLINE

WINDOWS

- Understand the kernel versions of Windows operating systems
- Understand how processes, DLLs, handles, services, and drivers work with the operating systems
- Knowledge of user mode vs. kernel mode and what files Windows uses for each mode
- Understand the different SMB versions and how Windows communicates within a network
- Knowledge of how RPC functions
- Knowledge of the Windows boot process
- Demonstrate command line basics including getting help, situational awareness, and various ways of gathering information
- Understand how Windows authenticates a user during the logon process
- Knowledge of Windows Active Directory Domain Services
- Knowledge of the Windows registry
- Understand Windows security
- Introduction to Powershell
- Knowledge of Windows file times and what can affect file times

OUTLINE

- Kernel versions
  - Windows from 2000 server - 2016 server
- Windows internal devices and artifacts
  - Processes
  - DLLs
  - Handles
  - Services
  - Drivers
  - RPC
  - SMB
  - NetBIOS
- User mode vs. Kernel mode
- Windows boot process
  - Windows XP boot process
  - Windows 7 boot process
  - Windows 8.1 boot process
- Windows authentication
  - Winlogon.exe
  - Lsass.exe
  - Security tokens
- Active Directory Domain Services
  - Domain objects
  - Group Policy Objects
  - Security Policies
  - Kerberos
- Command line utilities
- Registry
  - Regedit
  - Reg.exe
- Windows Security
  - SIDs & RIDs
  - Access controls
  - User & group permissions
  - DEP & ASLR
  - Auditing
  - Resource protection
- Powershell basics

CYBER OPERATIONS PREP™ (COP™)

COURSE OUTLINE

LINUX/UNIX

- Understand the history of Unix / Linux, its applications for use, and key differences in versions and distributions
- Demonstrate command line basics including getting help, situational awareness, and various ways of gathering information
- Understand nix File Hierarchy Standard directory layout and navigation
- Knowledge of Bash shell including history, configuration files, and environment
- Understand Secure Shell (SSH)
- Knowledge of processes, process flow, and identification
- Demonstrate usage of different power tools
- Demonstrate compression, encryption & splitting of files
- Understand basics of different editors
- Understand network management and configuration utilities
- Knowledge of boot process, kernel and loadable modules, and service management
- Demonstrate the ability to identify authentication, administer users and groups, elevate and change permissions
- Understand security implementations, access control, firewalls, and logging

OUTLINE

- History
  - Unix / Linux history
  - Global usage
- Identifying Nix versions and distributions
- Login prompts and GUIs
- Nix help
- Situational awareness
  - VFS
  - BIOS
  - Information gathering tools
- File system basics, navigation, and hierarchy
  - Local, network, and user space file systems
  - Displaying and modifying permissions
  - Mounting a file system
  - Create, modify, and delete files
  - Timestamps
- Shells
  - Different shells
  - Determine current shell
  - Bash history, aliases, and variables
- SSH
  - SSH basics
  - SSH authentication
- SSHD
  - Configuration files
  - sshd authentication
- Processes, Jobs, Signals, and Identification
- Power Tools
- Compression
- Editor utilities
- Network Management
  - Status
  - Mapping
  - Resolution
- Boot processes
- Kernel
  - Rings, roles, trust
  - Loadable kernel modules
- Services
- Authentication
  - Local
  - Management
  - Change
- Logging and Auditing
  - Location and verification
  - Login
- Centralization
  - syslog, agents
- Firewalls and Access Control
  - DAC and MAC
- SSH Tunneling
  - Setting up multiple tunnels
  - Connecting to services using the established tunnels

COURSE OUTLINE

SCRIPTING

- Demonstrate ability to read scripts written in both bash and Powershell to determine goal of script and most likely output
- Demonstrate ability to design and develop basic scripts to perform simple administrative functionality
- Understanding of proper way to build host survey script

OUTLINE

- Overview of scripting
- Overview of editors
- Parts of a script
  - Variables
  - Loops
  - Output
  - Conditionals
  - Strings
- Overview of Bash scripting
- Identify key components of administrative scripts and malicious scripts
- Build simple scripts
  - Administrative scripts
  - Analysis scripts
- Overview of Powershell scripting
- Identify key components of administrative and malicious scripts
- Build simple scripts
  - Administrative
  - Analysis
- Review of persistent techniques used on Linux and Windows systems
- Reveiw of process interrogation on Linux and Windows Systems
- Build initial assessment script in Bash
  - Find key information about the system
  - Identify any misconfigurations
  - Identify key locations used by malware to persist reboots
  - Investigate cron jobs set to run on the system
  - Gather and assess startup services
- Build initial assessment script for Windows systems
  - Pull valuable system information
  - Identify open ports on the system
  - Gather information from the systems registry
  - Investigate running services on the target system