DISCOVERY & COUNTER INFILTRATION COURSE

This course is focused on the methodologies and processes used by professional "Hunt" teams in corporate and government spaces. Instructors, with multiple years of Hunt experience, use open-source tools to teach students the necessary skills to successfully identify malicious behavior not caught by traditional security products. Students will set up security products and use analytic tools on a mock network to ensure they understand the capabilities of traditional security measures, as well as the gaps. Students will learn how to implement signatures and analyze heuristics to identify anomalous behavior. They will provide written reports for each behavior they identify and build actor profiles based off their findings. They will use timeline analysis and log analysis to map out the incident. Using incident response techniques, they will take the data collected and implement real-time solutions to the customer while providing risk management analysis to help protect networks in the future.

CHIRON METHODOLOGY DOMAIN

DISCOVERY AND COUNTER-INFILTRATION PROFESSIONAL™ (DCIP)™

DURATION

5 DAYS

RECOMMENDED PRE-REQUISITES

- Familiarity with VMware Player or Workstation
- Exposure to Linux or Unix-based Operating Systems
- Exposure to Windows Operating Systems
- Understanding of the TCP/IP protocols

© 2016 CHIRON TECHNOLOGY SERVICES, INC.

DISCOVERY & COUNTER INFILTRATION COURSE

COURSE SCHEDULE

DAY 1: LEARNING OBJECTIVES

- Student knowledge assessment of technical fundamentals
- Introduction to work roles in a Cyber Protection Team (CPT)
- Introduction to mission expectations and processes

OUTLINE

- Pre-Assessment
  - Test knowledge on Network analysis, Windows and Unix Triage/Survey
- Introductions
- CPT Overview
  - CPT Tasks: Identify, Protect, Detect, Respond, and Recover
  - Teams and Team roles
- CPT Process
  - Initial communication with the customer
  - Communicating with management
  - Legalities
- Expectation of privacy
- Full scope of AOR and restraints
- DCI Process
  - Scheduling and steps
  - Work roles
- Mission Goals and Objectives Identified
- Hacking Concepts Review (Kill Chain overview)
- Mission Process
  - Request for Information Process
  - Customer Interaction
  - CPT Management
- Mission Preparation
  - Necessary initial information
  - Delegation of assigned tasks
- Mission Tools
  - Intrusion Detection Systems
  - Host agents
  - Log correlation
  - Security products
- Mission Tracking Tools
  - Planning
  - Operator Notes
  - Ticket tracking system (Redmine)

DAY 2: LEARNING OBJECTIVES

- Understand the analytic process to successfully analyze and determine compromise on a Windows host
- Take proper procedures and note-taking to ensure little compromise to an infected host
- Use native CMD and PowerShell tools to assist in the process

OUTLINE

- Gather and aggregate logs on servers and high-value target systems (admins, commanders, etc.)
  - Successful/non-successful logins
  - Remote administration
- Analyze incident alerts from host agents and anti-virus software
  - Understand the tools involved
  - Create a "next-steps" process for high-level threats found
- Baseline and characterize individual systems using whitelisting applications
- Identify and analyze non-authorized software
- Evaluate host event logs and third party software logs
- Analyze Mission Protection data across other systems and identify key differences in dlls/exes on host
- Understand key differences in machines with the same baseline
- Windows Security & Active Directory
- Windows Powershell and CMD usage
- Native windows tools
- SysInternal tools
- CMD line third party tools

© 2016 CHIRON TECHNOLOGY SERVICES, INC.

DISCOVERY & COUNTER INFILTRATION COURSE

COURSE SCHEDULE

DAY 3:

LEARNING OBJECTIVES

- Understand the analytic process to successfully analyze and determine compromise on a Linux host
- Use proper procedures and documentation to determine level of host compromise
- Use native tools to assist in the process

OUTLINE

- Log analysis on servers
  - Log configuration files
  - Local and remote logs (make sure they match up)
  - Default log locations and file types
  - Identify suspicious logs
  - Determine log manipulation using timestamp analysis
- Baseline host network configurations and connections Application update traffic
  - Mail protocol traffic
  - Encrypted channel endpoints
  - Check for changes in configuration files
- File-hash techniques for file modification comparisons
- Legitimate timestamps versus configuration updates

DAY 4:

LEARNING OBJECTIVES

- Analyze different systems
- Understand defensive hardening techniques
- Deploy systems that will assist in the "hunt" mission

OUTLINE

- Why hardening is crucial to the DCI mission
- Identify whitelisted applications and exceptions
- Identify unauthorized/rogue users and groups with access and permission levels
- Identify patch systems and latest authorized patch level
- Identify current security products and last update
- Harden Linux systems
- Harden Windows systems
- Deploy systems
  - Get authorization for deployment and implement OPPLANS
  - Test security features and policies pre-rollout
  - Implement policies that do not disrupt unit mission

© 2016 CHIRON TECHNOLOGY SERVICES, INC.

DISCOVERY & COUNTER INFILTRATION COURSE

COURSE SCHEDULE

DAY 5: LEARNING OBJECTIVES

- Determine abnormal programs or processes on compromised hosts
- Understand and catalogue indicators of compromise
- Identify and assess intrusion damage
- Identify exploited vulnerability and future prevention
- Triage activity

OUTLINE

- Use sandbox techniques to identify suspected malware
  - Identify questionable processes/files to test
  - Set up a sandbox environment
  - Analyze before and after snapshots
- Perform system forensics and analysis
  - Compare "known good" file hashes to compromised system files
  - Memory analysis
  - Timeline analysis
- Reverse Engineering
  - Provide step-by-step analysis
  - Use debuggers/disassemblers to characterize malware
  - Understand proper storage of malware
  - Translate technical data into reportable intelligence

DAY 6: LEARNING OBJECTIVES

- Create network visualizations and perform a network survey
- Understand and track potential vulnerabilities
- Understand risk assessment contents

OUTLINE

- Set up an IDS: Security Onion (standalone and sensor/server setup)
- Understand proper/common net flow
- Understand Syslog servers and log data
- Initial review of key servers, systems, event logs
  - Understand ACLs for routers and firewalls
  - Analyze network diagrams and identify gaps
- Site Survey
  - Deploy initial systems
  - Create accounts and add them to the domain
  - Detect hosts on the network
  - Identify key hosts and traffic flow
  - Compare given data to initial network survey

DAY 7-8: LEARNING OBJECTIVES

- Develop strong understanding of network protocols and associated logs
- Use key networking tools to assist in network forensic analysis
- Understand the process from initial indicators through the end-report

OUTLINE

- Network traffic analysis
- Characterize protocols through sensor logs
- Identify "known goods" and record them in the customer profile or a database
- Identify initial "unknown" traffic and understand next steps
- Learning the tools:
  - Security Onion
  - Bro 2.0/ELSA
  - Snort/Snorby/Squert/Squil
  - Network Miner
  - Wireshark
- Network Tasks
  - Analyze network flow statistics and using a SIEM to identify unusual behavior.
  - Identify protocols & hosts allowed to communicate out of the network.
  - Looking at anomalies within common protocols
- HTTP
- ICMP
- DNS
- Correlating logs using Bro 2.0 & ELSA
  - Command line
  - Scripting

© 2016 CHIRON TECHNOLOGY SERVICES, INC.

COURSE SCHEDULE

DAY 9:

LEARNING OBJECTIVES

- Perform a live exercise utilizing a Windows host, a Linux host and network logs/pcap to determine the compromise
- Utilize all the necessary tools and techniques to create detailed notes and reports
- Present analytic findings and "next step" procedures to an audience.

OUTLINE

- Reporting
- Know the customer technical level
  - What does the customer need to know?
  - Recommend training
  - Schedule follow on evaluations
  - Identify permanent equipment
  - Understand key information to provide to customer and local leadership
- Document valuable information identified during mission

DAY 10:

LEARNING OBJECTIVES

- Demonstrate core course competencies in key areas
- Documentation: Operator Plans & Operator Notes
- Host Analysis: Linux and Windows Systems
- Network Analysis and Log Correlation
- Memory Dump of compromised hosts

OUTLINE

- Prepare and present customer and team deliverables
  - Mission Summary and objectives
  - Network Visualization
  - Event Timeline
  - Summary of Findings

© 2016 CHIRON TECHNOLOGY SERVICES, INC.