MISSION PROTECTION COURSE

This two-week course is focused on the methodologies and processes used by professional "Blue" teams in corporate and government spaces. Instructors use open-source tools to teach students methodologies of securing a network and its hosts. Students will learn the necessary skills to successfully identify: the customer's network, tools required and allowed, mission scope & key terrain, then map the network, and its hosts. They will learn to protect: verifying base-lines, check configurations, evaluate A/V & IDS systems. Student will detect: perform host based assessments, finding vulnerabilities and anomalies, helping the customer with continuous integrity monitoring. They will respond: develop and implement an incident response plan, suggest better sensor placements, help with log correlation, coordinate response activities, develop and apply risk mitigation response. Finally students will recover: developing a recovery plan and making final recommendations to their customers. Their final recommendations will take into account system hardening techniques, priority lists, and risk mitigation. Each of the segments will cover network devices, Unix and Windows Operating Systems and policy.

CHIRON METHODOLOGY DOMAIN

CYBER PROTECTION PROFESSIONAL™ (CPP)™

DURATION

10 DAYS

RECOMMENDED PRE-REQUISITES

- Familiarity with VMware Player or Workstation
- Exposure to Linux or Unix-based Operating Systems
- Exposure to Windows workstations and servers
- Firm understanding of the TCP/IP protocols

COURSE SCHEDULE

DAY 1:

LEARNING OBJECTIVES

- Understanding the roles and processes of a cyber-protection team.
- Awareness of government standards such as the NIST cyber security framework and risk assessment guidelines (NIST 800 series).
- Technical assessment of Unix, Windows, Cisco IOS and packet analysis abilities.

OUTLINE: UNDERSTANDING A CYBER PROTECTION TEAM

- Orientation & overview
- What is a Cyber Protection Team?
    - Tasks: Identify, Protect, Detect, Respond, & Recover
    - Understand the different teams on a CPT
        - MPS (Blue), DCIS (Black), CTES (Red)
- Mission Protection process
    - Scheduling & overall steps
    - Work roles involved at each step & identifying the ultimate goal
    - Tools used to keep track of the mission
    - RFI process to customers
- Roles (Cyber Protection Team)
    - Network Defense Manager
    - Cyber Security Analyst
    - Systems Architect (securely provision)
    - Operators
    - Network Infrastructure Specialist (operate & maintain)
- Governing Documentation
    - NIST 800-53v1 (Cybersecurity framework)
        - Identify
        - Protect
        - Detect
        - Respond
        - Recover
    - NIST 800-30r1 (risk assessment)
        - Prepare for risk assessment
        - Conduct risk assessment
        - Communicate and share risk assessment results
        - Maintain risk assessment
- Risk vs. Security
    - CIA model & InfoSec triangle
    - OSI layer review w/ security risks
    - Roles and risks of Windows, Unix and other devices
        - Key aspects of the OSes and devices
- Command line review
    - Unix, Windows, Cisco IOS, PCAP exercises

COURSE SCHEDULE

DAY 2:

LEARNING OBJECTIVES

- Understanding of customer interaction, building a customer profile and maintaining proper communication channels and documentation.
- Demonstrate the ability to prepare for a risk assessment in accordance with NIST guidelines.
- Demonstrate proper inter-team communication and collaboration.

OUTLINE: IDENTIFY PHASE

- Overview of identify
  - Prepare for risk assessment
  - Conduct risk assessment
  - Communicate and share risk assessment results
  - Maintain risk assessment
- Customer interaction (800-30 tasks 1-1, 1-2, 1-3)
  - Build customer profile
  - Get all contact and other necessary information
  - POCs (IT, command & security)
  - Plan dates, accesses, travel stay & clearances
  - Determine Mission Scope, Rules of Engagement & Key Cyber Terrain
    - Possible threat vectors
  - Proceed under Proper Guidance with CNDSP (customer)
  - Proper guidance on handling of PII, proprietary data & classified information
- Building the risk assessment (800-30 tasks 1-4, 1-5)
  - Identify information sources
  - Determine customer's preferred reporting schedule (daily/weekly)
  - Identify risk model and analytic approach
- Review on collaboration and organization
  - Utilize standardized forms
    - RFIs, WARNOs/FRAGOs/OPORDs, IRRs
  - Fully document all actions taken
  - Organize all the data
    - Centralization of information storage
    - Standardized formatting of information
    - Collaboration tools and information officers

COURSE SCHEDULE

DAY 3: LEARNING OBJECTIVES

- Demonstrate ability to collect proper up to date information in order to conduct the risk assessment.
- Fundamental knowledge of open source investigation tactics.
- Understanding of the tools, techniques and procedures utilized in social engineering.
- Understanding of vulnerabilities inherent to physical security and layer 1 technologies.

OUTLINE: IDENTIFY PHASE (CONTINUED)

- Perform Survey to conduct Risk Assessment
  (800-30 tasks 2-1, 2-2)
  - Review previous & current info
    - Get list of devices, IPs, users, groups, software, configs
      - Is there a device inventory, network map, data flow?
    - Get gold-disks, hash-list, base-lining; or create it
    - Get policies, processes, procedures & guidelines, (ATTP?)
      - BYOD policy, 3rd party integrated (cloud, HVAC, etc.), software inventoried, CM, how does the org communicate, how does
        data flow?
      - Is there a list of resources prioritized on classification, criticality and business value?
      - Do mission critical systems have redundancy in place, validated on a frequent basis? COOP (people, buildings, systems)
      - Organizational IT usage policy, security policy, risk management policy in place, reviewed, updated?
      - List potential & known internal &
        external threats
      - Potential business impacts & likelihoods
      - Risk responses & risk tolerance identified &
        clearly expressed
      - Ensure response plans developed for all potential scenarios
        - Natural disaster, intrusions, data breach, physical attack, loss of key personnel, etc.
  - Open Source Intelligence: Find externally available information to determine Operational Security posture.
    - Resumes, job openings, social media, public web sites, satellite imagery, pictures, etc.
  - Social engineering
    - Collecting more information, determining bad practices
  - Physical walk through
    - Physical security problems
      - Keys, alarms, etc.
    - Layer 1 problems
    - Exposed wire runs, wifi, etc.

COURSE SCHEDULE

DAY 4:

LEARNING OBJECTIVES

- Demonstrate ability to enumerate a network using proper scanning tools and techniques.
- Demonstrate ability to analyze a host utilizing survey tools and service enumeration techniques to detect vulnerabilities and misconfigurations.
- Demonstrate ability to conduct vulnerability and risk assessments according to NIST guidelines including communicating and sharing pertinent information with the customer.

OUTLINE: IDENTIFY PHASE (CONTINUED)

- Identify & Deploy Survey Tools
  - Know which tools are needed & allowed
  - Utilizing survey scripts
- Host / device discovery
  - Passive & active scanning
    - OpenVAS/Nessus
    - Nmap
    - ARP scanning
    - DNS enumeration
  - Sniffers
    - Tcpdump/WinPCAP/Wireshark
  - Compare against inventory list: anything new or missing?
- Port scanning and service enumeration
  - Based on software list, any unauthorized service found?
    - Nmap
    - Nikto
    - SMB enumeration
- Vulnerability assessment (800-30 tasks 2-3, 2-4, 2-5, 2-6)
  - Automated research
    - OpenVAS/Nessus/Nikto
    - MBSA
    - Lynis
  - Manual research
    - Exploit-db/searchsploit, search-engines
    - nvd.nist.gov
    - Finding configuration vulnerabilities
    - Finding software vulnerabilities
    - Finding firmware vulnerabilities
  - Analyze vulnerability/threat risk
    - Likelihood of event occurring
    - Impact of potential event
    - Overall risk level
- Follow-up with Customer (800-30 tasks 3-1, 3-2, 4-1, 4-2)
  - Discuss results of risk assessment
  - Share information gathered regarding risk
  - Update risk assessment & assist customer in developing plan for continual monitoring of the network

COURSE SCHEDULE

DAY 5:

LEARNING OBJECTIVES

- Demonstrate ability to properly manage access controls to enhance both physical and network security.
- Understanding of protection methods for both data at rest and in transit.
- Demonstrate ability to properly evaluate security processes including logging, Windows active directory and group policy.

OUTLINE: PROTECT PHASE

- ➢ Overview of protect
- ➢ Manage Access Control
  - » Physical access to assets is managed and protected
  - » The following covers in as much as possible:
    - ◇ Facilities, Network, Devices, Unix, Windows
    - ◇ Identities & credentials are managed for authorized devices & users
- ➢ Active Directory, users & computers
- ➢ SELinux, /etc/sudoers
    - ◇ Remote access is managed
- ➢ Active Directory Terminal Services (RDP)
- ➢ SSH Keys
    - ◇ Access permissions are managed w/ least privilege & separation of duty
- ➢ local vs. domain accounts
    - ◇ Network integrity is protected incorporating segregation where appropriate
- ➢ Data Security
  - » Data at rest is protected
    - ◇ Full disk encryption, backups, erasure
    - ◇ Integrity checks are used to verify software, firmware & information integrity
  - » Data in transit is protected
    - ◇ Crypto primer
    - ◇ Tempest, hardware crypto, software crypto
    - ◇ Protections against data leaks are implemented
    - ◇ Development, testing & operational environments are separated
- ➢ Verify proper separation of networks based on classification/function
  - » Ensure no bleedover between networks
  - » Data in process is protected
    - ◇ ASLR
    - ◇ DEP
- ➢ Information Protection
  - » Baseline configs are created and maintained
  - » System development lifecycle managing systems is implemented
    - ◇ Baking security in from the ground up
    - ◇ Proper disposal, destruction of EOL systems
  - » Configuration change control processes are in place
  - » Backups are conducted, maintained and tested periodically
  - » Incident & disaster response & recovery plans are in place, freq. updated & tested
  - » Vulnerability management plan is developed and implemented
- ➢ Evaluate data security processes & protective technology
  - » Audit & system logs are implemented & reviewed
    - ◇ Log centralization, log storage & archival, log correlation
    - ◇ Windows Active directory: GPO audit policy, event logs
    - ◇ Linux auditd, (r)syslogd
    - ◇ Cisco logging

MISSION PROTECTION COURSE

COURSE SCHEDULE

DAY 6: LEARNING OBJECTIVES

- Understanding of proper maintenance methods and documentation, as well as possible vulnerabilities arising from improper procedures.
- Understanding of training and user awareness practices regarding cyber security.
- Demonstrate ability to properly deploy and configure protective technologies including antivirus suites, firewalls, intrusion detection & protection systems

OUTLINE: PROTECT PHASE (CONTINUED)

- Maintenance
  - Maintenance & repair is performed w/ approved tools and logged, ensuring prevention of unauthorized access.
- Awareness & Training
  - Organization provides cyber security awareness training
  - All users are informed & trained understanding their roles & responsibilities
    - Privileged users, executives & security personnel
- Protective Technology
  - Removable media is protected & restricted according to policy
  - Communications & control networks are protected
  - A/V (Malware Protection)
  - IDS / IPS
  - Firewalls
    - Windows local and domain firewalls
    - Linux iptables
    - Cisco extended ACLs

DAY 7: LEARNING OBJECTIVES

- Understanding proper methods to characterize normal network and host behavior.
- Demonstrate ability to detect abnormal network and host behavior as well as misconfigurations.
- Demonstrate ability to utilize baseline image comparisons in support of anomaly detection.

OUTLINE: DETECT PHASE

- Overview of detect
- Characterize Normal & Detect Abnormal
  - Anomalies are detected in a timely manner
    - Baseline of network operations, expected data flows (DCI)
    - Look for odd processes & network connections
      - netstat, ps/tasklist, router/firewall logs, etc.
    - Check for misconfigurations
      - Determining risks in improperly configured services and systems
- Characterize Normal & Detect Abnormal *(continued)*
    - Verify processes and drivers are signed/authentic
    - Compare deployed systems with baselines
      - Windows
        - What Changed, Regshot, diff, etc.
        - Registry changes in important keys
        - Looking for specific artifacts
      - Linux
  - diff, hash compare known baseline files
      - Cisco
        - nmap ndiff, config comparison .

DAY 8: LEARNING OBJECTIVES

- Understanding impacts of potential events on continuing operations.
- Demonstrate ability to determine the scope of an intrusion.
- Demonstrate ability to utilize and integrate all available tools and techniques to implement a continuous monitoring system to assist with intrusion detection.

OUTLINE: DETECT PHASE (CONTNUED)

- Analyze and maintain
  - Potential impact of events is understood
    - Impact on continuing operations, data loss, compromise of classified resources
    - Which systems are affected, what risk do they pose
    - Verify all user accounts are either authorized or disabled
  - Perform Integrity Check (continuous monitor)
    - Log monitoring, user authentication, running processes, sockets
    - New devices on the net, new hardware in the devices
    - Scheduled jobs to run checks during non-peak hours
    - Physical environment is monitored
- Monitor & correlate badging logs, security systems, system login log

COURSE SCHEDULE

DAY 9: LEARNING OBJECTIVES

- Understanding fundamentals of response planning.
- Understanding of proper response coordination activities, Red Team deconfliction, and procedures for involving law enforcement if necessary.
- Demonstrate proper reporting procedures including risk mitigation recommendations and alternatives
- Understanding of disaster recovery concepts and continuation of operation planning fundamentals.
- Demonstrate ability to develop and maintain proper disaster recovery and COOP plans.
- Understanding of media management and how it relates to public relations and company reputation.

OUTLINE: RESPOND PHASE

- Overview of respond
- Response Planning
  - Determine which response plan is most applicable to current incident
- Response plans are executed during or after event, updated and tested
  - Gather initial information
    - Determine nature of incident
- Security (DCI) vs. Legal/Criminal (CID)
    - Run deconfliction with CTES
    - Coordinate Response Activities
- Ensure everyone necessary is in the loop
  - Notification of the customer, DCI, and CRS
    - Deploy incident response tools/scripts
    - Establish timeline
    - Determine root cause/initial intrusion point of incident
- Check for potential persistence vectors utilized
- Resolve Sensor Gaps
  - Redesign sensors/monitors deployment scheme to ensure complete coverage
    - Confirm centralization of C&C/logging
- Impact analysis
  - Work with DCI for technical event details and then create risk analysis based on the mission criticality of the system and the impact the event had on the customer's mission.
- Reporting
  - Develop risk mitigation recommendations & alternatives
  - Present to customer
- Mitigation
  - Incidents are contained and mitigated (DCI)
  - New security measures are adopted & implemented
  - Response strategies and planning are updated or created as needed

DAY 10: LEARNING OBJECTIVES

- Understanding proper methods to characterize normal network and host behavior.
- Demonstrate ability to detect abnormal network and host behavior as well as misconfigurations.
- Demonstrate ability to utilize baseline image comparisons in support of anomaly detection.

OUTLINE: RECOVER PHASE

- Overview of detect
- Characterize Normal & Detect Abnormal
  - Anomalies are detected in a timely manner
    - Baseline of network operations, expected data flows (DCI)
    - Look for odd processes & network connections
- netstat, ps/tasklist, router/firewall logs, etc.
    - Check for misconfigurations
- Determining risks in improperly configured services and systems
    - Verify processes and drivers are signed/authentic
    - Compare deployed systems with baselines
- Windows
  - What Changed, Regshot, diff, etc.
  - Registry changes in important keys
  - Looking for specific artifacts
- Linux
  - diff, hash compare known baseline files
- Cisco
  - nmap ndiff, config comparison