Tel. +39 02 365738
info@overneteducation.it
www.overneteducation.it

CBROPS

Understanding Cisco Cybersecurity Operations Fundamentals

Durata: 5 gg

Descrizione

Questo corso è progettato per preparare il partecipante alla certificazione Cisco Certified CyberOps Associate ottenibile attraverso il superamento dell'esame CBROPS 210-201. Le organizzazioni moderne, che vogliano competere nel mercato attuale, hanno bisogno di essere dotate o servirsi di un centro definito SOC (Security Operations Center). Questa entità, composta da un Team di professionisti, si occupa di fornire i seguenti principali servizi:

- Servizi di Gestione: tutte le attività di gestione delle funzionalità di sicurezza legate all'infrastruttura IT (rete, sistemi ed applicazioni).
- Servizi di Monitoraggio: l'infrastruttura IT e di Sicurezza vengono monitorate in tempo reale al fine di individuare tempestivamente tentativi di intrusione, di attacco o di compromissione dei sistemi.
- Servizi Proattivi: sono servizi finalizzati a migliorare il livello di protezione dell'organizzazione (Security assessments, vulnerability assessments, early warning, security awareness).

Per supportare adeguatamente questi servizi, i SOC, devono servirsi di personale qualificato a vari livelli. Risorse professionalmente adeguate nell'ambito della Cybersecurity sono oggi di difficile reperimento. In tale contesto nasce questo percorso formativo qualificante. Esso è specificatamente strutturato per ottenere una figura professionale che possa inserirsi rapidamente in un Security Operations Center. Il corso è caratterizzato da una parte teorica e una pratica realizzata su Laboratori forniti direttamente da Cisco. Questa è una prerogativa concessa solo ed esclusivamente ai Cisco Learning Partner.

Prerequisiti

I partecipanti dovranno avere una conoscenza basilare scolastica della lingua Inglese.

Contenuti

Understanding the TCP/IP Protocol Suite

- •OSI Model
- •TCP/IP Model
- •IP Addressing
- •IP Address Classes
- •Reserved IP Addresses
- •Public and Private IP Addresses
- •IPv6 Addresses
- • TCP Three-Way Handshake
- •TCP and UDP Ports
- •Address Resolution Protocol
- •Host-to-Host Packet Delivery Using TCP
- •Dynamic Host Configuration Protocol
- •Domain Name System
- •Internet Control Message Protocol
- •Packet Capture Using tcpdump

- •Wireshark
- •Explore the TCP/IP Protocol Suite

Understanding the Network Infrastructure

- •Analyzing DHCP Operations
- •IP Subnetting
- •Hubs, Bridges, and Layer 2 Switches
- •VLANs and Trunks
- •Spanning Tree Protocols
- •Standalone (Autonomous) and Lightweight Access Points
- •Routers
- •Routing Protocols
- •Multilayer Switches
- •NAT Fundamentals
- •Packet Filtering with ACLs
- •ACLs with the Established Option
- •Explore the Network Infrastructure

Understanding Common TCP/IP Attacks

- •Legacy TCP/IP Vulnerabilities
- •IP Vulnerabilities
- •ICMP Vulnerabilities
- •TCP Vulnerabilities
- •UDP Vulnerabilities
- •Attack Surface and Attack Vectors
- •Reconnaissance Attacks
- •Access Attacks
- •Man-in-the-Middle Attacks
- •Denial of Service and Distributed Denial of Service
- •Reflection and Amplification Attacks
- •Spoofing Attacks
- •DHCP Attacks
- •Explore TCP/IP Attacks

Understanding Basic Cryptography Concepts

- •Impact of Cryptography on Security Investigations
- •Cryptography Overview
- •Hash Algorithms
- •Encryption Overview
- •Cryptanalysis
- •Symmetric Encryption Algorithms
- •Asymmetric Encryption Algorithms
- •Diffie-Hellman Key Agreement
- •Use Case: SSH
- •Digital Signatures
- •PKI Overview
- •PKI Operations
- •Use Case: SSL/TLS

- •Cipher Suite
- •Key Management
- •NSA Suite B
- •Explore Cryptographic Technologies

Describing Information Security Concepts

- •Information Security Confidentiality, Integrity, and Availability
- •Personally Identifiable Information
- •Risk
- •Vulnerability Assessment
- •CVSS v3.0
- •Access Control Models
- •Regulatory Compliance
- •Information Security Management
- •Security Operations Center

Understanding Network Applications

- •DNS Operations
- •Recursive DNS Query
- •Dynamic DNS
- •HTTP Operations
- •HTTPS Operations
- •Web Scripting
- •SQL Operations
- •SMTP Operations
- •Explore Network Applications

Understanding Common Network Application Attacks

- •Password Attacks
- •Pass-the-Hash Attacks
- •DNS-Based Attacks
- •DNS Tunneling
- •Web-Based Attacks
- •Malicious iFrames
- •HTTP 302 Cushioning
- •Domain Shadowing
- •Command Injections
- •SQL Injections
- •Cross-Site Scripting and Request Forgery
- •Email-Based Attacks
- •Explore Network Application Attacks

Understanding Windows Operating System Basics

- •Windows Operating System History
- •Windows Operating System Architecture
- •Windows Processes, Threads, and Handles
- •Windows Virtual Memory Address Space
- •Windows Services
- •Windows File System Overview

- •Windows File System Structure
- •Windows Domains and Local User Accounts
- •Windows Graphical User Interface
- •Run as Administrator
- •Windows Command Line Interface
- •Windows PowerShell
- •Windows net Command
- •Controlling Startup Services and Executing System Shutdown
- •Controlling Services and Processes
- •Monitoring System Resources
- •Windows Boot Process
- •Windows Networking
- •Windows netstat Command
- •Accessing Network Resources with Windows
- •Windows Registry
- •Windows Event Logs
- •Windows Management Instrumentation
- •Common Windows Server Functions
- •Common Third-Party Tools
- •Explore the Windows Operating System

Understanding Linux Operating System Basics

- •History and Benefits of Linux
- •Linux Architecture
- •Linux File System Overview
- •Basic File System Navigation and Management Commands
- •File Properties and Permissions
- •Editing File Properties
- •Root and Sudo
- •Disks and File Systems
- •System Initialization
- •Emergency/Alternate Startup Options
- •Shutting Down the System
- •System Processes
- •Interacting with Linux
- •Linux Command Shell Concepts
- •Piping Command Output
- •Other Useful Command Line Tools
- •Overview of Secure Shell Protocol
- •Networking
- •Managing Services in SysV Environments
- •Viewing Running Network Services
- •Name Resolution: DNS
- •Testing Name Resolution
- •Viewing Network Traffic
- •System Logs

- •Configuring Remote syslog
- •Running Software on Linux
- •Executables vs. Interpreters
- •Using Package Managers to Install Software in Linux
- •System Applications
- •Lightweight Directory Access Protocol
- •Explore the Linux Operating System

Understanding Common Endpoint Attacks

- •Classify Attacks, Exploits, and Vulnerabilities
- •Buffer Overflow
- •Malware
- •Reconnaissance
- •Gaining Access and Control
- •Gaining Access Via Social Engineering
- •Social Engineering Example: Phishing
- •Gaining Access Via Web-Based Attacks
- •Exploit Kits
- •Rootkits
- •Privilege Escalation
- •Pivoting
- •Post-Exploitation Tools Example
- •Exploit Kit Example: Angler
- •Explore Endpoint Attacks

Understanding Network Security Technologies

- •Defense-in-Depth Strategy
- •Defend Across the Attack Continuum
- •Authentication, Authorization, and Accounting
- •Identity and Access Management
- •Stateful Firewall
- •Network Taps
- •Switched Port Analyzer
- •emote Switched Port Analyzer
- •Intrusion Prevention System
- •IPS Evasion Techniques
- •Snort Rules
- •VPNs
- •Email Content Security
- •Web Content Security
- •DNS Security
- •Network-Based Malware Protection
- •Next Generation Firewall
- •Security Intelligence
- •Threat Analytic Systems
- •Network Security Device Form Factors
- •Security Onion Overview

- •Security Tools Reference
- •Explore Network Security Technologies

Understanding Endpoint Security Technologies

- •Host-Based Personal Firewall
- •Host-Based Anti-Virus
- •Host-Based Intrusion Prevention System
- •Application Whitelists and Blacklists
- •Host-Based Malware Protection
- •Sandboxing
- •File Integrity Checking
- •Explore Endpoint Security

Describing Security Data Collection

- •Network Security Monitoring Placement
- •Network Security Monitoring Data Types
- •Intrusion Prevention System Alerts
- •True/False, Positive/Negative IPS Alerts
- •IPS Alerts Analysis Process
- •Firewall Log
- •DNS Log
- •Web Proxy Log
- • Email Proxy Log
- •AAA Server Log
- •Next Generation Firewall Log
- •Applications Log
- •Packet Captures
- •NetFlow
- •Network Behavior Anomaly Detection
- •Data Loss Detection Using Netflow Example
- •Security Information and Event Management Systems
- •Explore Security Data for Analysis

Describing Security Event Analysis

- •Cyber Kill Chain
- •Advanced Persistent Threats
- •Diamond Model for Intrusion Analysis
- •Cybersecurity Threat Models Summary
- •SOC Runbook Automation
- •Malware Reverse Engineering
- •Chain of Custody

Defining the Security Operations Center

- •Types of Security Operations Centers
- •SOC Analyst Tools
- •Data Analytics
- •Hybrid Installations: Automated Reports, Anomaly Alerts
- •Sufficient Staffing Necessary for an Effective Incident Response Team
- •Roles in a Security Operations Center

- •Develop Key Relationships with External Resources

Understanding NSM Tools and Data

- •NSM Tools
- •NSM Data
- •Security Onion
- •Full Packet Capture
- •Session Data
- •Transaction Data
- •Alert Data
- •Other Data Types
- •Correlating NSM Data
- •Explore Network Security Monitoring Tools

Understanding Incident Analysis in a Threat-Centric SOC

- •Classic Kill Chain Model Overview
- •Kill Chain Phase 1: Reconnaissance
- •Kill Chain Phase 2: Weaponization
- •Kill Chain Phase 3: Delivery
- •Kill Chain Phase 4: Exploitation
- •Kill Chain Phase 5: Installation
- •Kill Chain Phase 6: Command-and-Control
- •Kill Chain Phase 7: Actions on Objectives
- •Applying the Kill Chain Model
- •Diamond Model Overview
- •Applying the Diamond Model
- •Exploit Kits
- •Investigate Hacker Methodology

Identifying Resources for Hunting Cyber Threats

- •Cyber-Threat Hunting Concepts
- •Hunting Maturity Model
- •Cyber-Threat Hunting Cycle
- •Common Vulnerability Scoring System
- •CVSS v3.0 Scoring
- •CVSS v3.0 Example
- •Hot Threat Dashboard
- •Publicly Available Threat Awareness Resources
- •Other External Threat Intelligence Sources and Feeds Reference
- •Hunt Malicious Traffic

Understanding Event Correlation and Normalization

- •Event Sources
- •Evidence
- •Security Data Normalization
- •Event Correlation
- •Other Security Data Manipulation
- •Correlate Event Logs, PCAPs, and Alerts of an Attack

Identifying Common Attack Vectors

- •Obfuscated JavaScript
- •Shellcode and Exploits
- •Common Metasploit Payloads
- •Directory Traversal
- •SQL Injection
- •Cross-Site Scripting
- •Punycode
- •DNS Tunneling
- •Pivoting
- •Investigate Browser-Based Attacks

Identifying Malicious Activity

- •Understanding the Network Design
- •Identifying Possible Threat Actors
- •Log Data Search
- •NetFlow as a Security Tool
- •DNS Risk and Mitigation Tool
- •Analyze Suspicious DNS Activity
- •tifying Patterns of Suspicious Behavior
- •Network Baselining
- •Identify Anomalies and Suspicious Behaviors
- •PCAP Analysis
- •Delivery
- •Investigate Suspicious Activity Using Security Onion

Conducting Security Incident Investigations

- •Security Incident Investigation Procedures
- •Threat Investigation Example: China Chopper Remote Access Trojan
- •Investigate Advanced Persistent Threats

Describing the SOC Playbook

- •Security Analytics
- •Playbook Definition
- •What Is in a Play?
- •Playbook Management System
- •Explore SOC Playbooks

Understanding the SOC Metrics

- •Security Data Aggregation
- •Time to Detection
- •Security Controls Detection Effectiveness
- •SOC Metrics

Understanding the SOC WMS and Automation

- •SOC WMS Concepts
- •Incident Response Workflow
- •SOC WMS Integration
- •SOC Workflow Automation Example

Describing the Incident Response Plan

- •Incident Response Planning

- •Incident Response Life Cycle
- •Incident Response Policy Elements
- •Incident Attack Categories
- •Reference: US-CERT Incident Categories
- •Regulatory Compliance Incident Response Requirements

Describing the Computer Security Incident Response Team

- •CSIRT Categories
- •CSIRT Framework
- •CSIRT Incident Handling Services

Understanding the use of VERIS

- •VERIS Overview
- •VERIS Incidents Structure
- •VERIS 4 A’s
- •VERIS Records
- •VERIS Community Database
- •Verizon Data Breach Investigations Report and Cisco Annual Security Report

Certificazioni

Corso di preparazione al conseguimento della
Certificazione Cisco Certified CyberOps Associate
Understanding Cisco Cybersecurity Operations Fundamentals