Certified Penetration Testing Consultant

KEY DATA

Course Name: C)PTC V3

Duration: 4 days
Language: English

Class Format:
- Instructor-led
- Live Online Training

Prerequisites:
- C)PTE or equivalent knowledge
- A minimum of 24 months experience in Networking Technologies
- Sound knowledge of TCP/IP
- Computer hardware knowledge

Student Materials:
- Student Workbook
- Student Lab Guide
- Student Prep Guide

Certification Exams:
- Mile2 C)PTC

CPEs: 32 Hours

WHO SHOULD ATTEND?

- IS Security Officers
- Cyber Security Managers/Admins
- Penetration Testers
- Ethical Hackers
- Auditors

COURSEOVERVIEW

The vendor neutral**Certified Penetration Testing Consultant** course is designed for IT Security Professionals and IT Network Administrators who are interested in conducting Penetration tests against large network infrastructures similar to large corporate networks, Services Providers and Telecommunication Companies. Instead of focusing on operating system level penetration testing, this course covers techniques on how to attack and prevent underlying network infrastructure and protocols. The training starts from basic packet capturing and analyzing by using both commercial and open source tools. From there, the student continues with Layer2 attack vectors, Layer3 based attacks; including both IPv4 and IPv6 stacks, routing protocol attacks (OSPF, BGP, etc) and then hops over to service provider level attacks related with very common used MPLS, how to use relays and pivots, VPN attacks including IPSEC protocol suite, and SSL attacks. Finally, the class will cover NIDS/NIPS evasion and implementation techniques.

This course uses in-depth lab exercises after each module. Students may spend 16 hours+ performing labs that emulate a real world Pen Testing model. Students will make use of scores of traditional and cutting edge Pen Testing tools (GUI and command line, Windows and Linux) as they make their way through mile2's time-tested methodology.

Pen Testing Hacking Career

C)VA Certified Vulnerability Assessor

C)PEH CERTIFIED PROFESSIONAL ETHICAL HACKER

C)PTE CERTIFIED PENETRATION TESTING ENGINEER

C)PTC * CERTIFIED PENETRATION TESTING CONSULTANT

All Combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide)
- Exam Prep Questions
- Exam
- Cyber Range Lab

C)PTC™ CERTIFIED PENETRATION TESTING CONSULTANT

mile2® CYBER SECURITY CERTIFICATIONS

ACCREDITATIONS

COMMITTEE ON NATIONAL SECURITY SYSTEMS — CNSS — SYSTEMS SECURITY FOR THE 21st CENTURY

NICCS™ NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

DEPARTMENT OF JUSTICE — FEDERAL BUREAU OF INVESTIGATION — FIDELITY BRAVERY INTEGRITY

UPON COMPLETION

Upon completion, **Certified Penetration Testing Consultant** students will be able to both establish an industry acceptable pen testing processas well as be prepared to competently take the C)PTC exam.

EXAM INFORMATION

The **Certified Penetration Testing Consultant**exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $400 USD and must be purchased from Mile2.com.

macs Assessment & Certification System

COURSE DETAILS

Module 0: CPTC Intro
Module 1: Packet Capturing
Module 2: Layer2 Attacks
Module3: Layer3 Attacks on Cisco Based Infrastructures
Module 4: Pivoting and Relays
Module 5: IPv6 Attacks
Module 6: VPN Attacks
Module 7: Defeating SSL
Module 8: IDS/IPS Evasion

LABORATORY EXERCISES

Lab 1: Working with Captured Files
Lab 2: Layer 2 Attacks
Lab 3: Attacking Routing Protocols
Lab 4: Using Pivot Machines
Lab 5: IPv6 Attacks
Lab 6: VPN attack
Lab 7: Defeating SSL –Decrypting Traffic and Man-in-the-middle attacks
Lab 8: NIDS/NIPS

C)PTC™ CERTIFIED PENETRATION TESTING CONSULTANT

mile2® CYBER SECURITY CERTIFICATIONS

DETAILED MODULE DESCRIPTION

Module 1: Packet Capturing

Packet Capturing
Packet capturing using libpcap
Capturing using ncap
Packet Capturing Software
Windump / TCPDump
Usage
Usage
Windump & PS
Wireshark
General Settings
Preferences
Capture Settings
Interface Options
Column Settings
Name Resolution Settings
Panes
Capture Options
Menu Shortcuts
Follow TCP Stream
Expert Infos
Packet Reassembly
Capturing VOIP Calls
VOIP Call Filtering
Call Setup
Playing the call
Saving the call into a file
SMB Export
HTTP Export

Module 2: Layer2 Attacks

Why Layer2?
FBI/CSI Risk Assessment
Ethernet Frame Formats
Different Types of attacks
Switch Learning Process
Excessive Flooding
Macof
Cisco Switches' Bridging Table Capacities
Mac Flooding Alternative: Mac Spoofing Attacks
Spanning Tree Basics
Frame Formats
Dissectoring
Main BPDU Formats
yersinia
STP Attacks supported in yersinia
Becoming Root Bridge
VLANs
Basic Trunk Port Defined
Dynamic Trunking Protocol (Cisco)
VLAN Hopping Attack
Double Tagging
How DHCP operates?
DHCP Request/Reply Types
DHCP Fields
DHCP Starvation Attack
Rogue DHCP Server Attack
ARP Function Review
Risk Analysis of ARP
ARP Spoofing Attack Tools
ARP Cache Poisoning
How PoE works?
Risk Analysis for PoE

Module 3: Layer3 Attacks on Cisco Based Infrastructures

Layer 3 protocols
Protocols: BGP
BGP MD5 crack
Protocols: BGP
BGP Route Injection
MP-BGP Route Injection

Protocols: OSPF
Protocols: ISIS
Protocols: HSRP/VRRP
DDoS detection
DDoS prevention
Ingress/egress filtering
Worm detection and protection
DDoS/worm research/future
MPLS
Bi-directional MPLS-VPN traffic redirection
Some More MPLS Attacks
MPLS
Router integrity checking

Module 4: Pivoting and Relays

Pivoting
Netcat
Backdoors with nc
Netcat – Basic Usage
Persistent Listeners
Shovel a shell
Shovel a file
netcat port scanner
Relays
Simple Netcat Relay
Two-Way Netcat Relay – The Newbie Approach
Named Pipes
I/O Streams and Redirection
Relay Scenario 1
Two-Way NC Relay with Named Pipe
Relay Scenario 2
Relay Scenario 3

Module 5: IPv6 Attacks

IPv4
IPv6
IPv4 & IPv6 Headers
IPv6 Header Format
End-to-End Principle
Differences with End-to-End
End point filters
Merging IPSEC and Firewall functions
Scanning
ICMPv6
ICMPv6 Neighbor Discovery
IPv6 Attack Tools
DAD DoS Attack
DAD DoS Attack
Auto-Configuration Mechanisms
Autoconfiguration – SLAAC, DHCPv6
Auto-Configuration IPv4 & IPv6
ICMPv6 Types
Neighbor Discovery
ND spoofing
http://www.thc.org/thc-ipv6
Dos-new-ipv6 (THC)
Parasite6 (THC)
Redir6 (THC)
Fake_router6
IPv6 in Today's Network
Extension Headers
Routing Header
Different Types of Routing Header
RH0 (Deprecated by RFC 5095) Format
Routing Header 0 Attack
Layer 3-4 Spoofing
Transition Mechanism Threats
IPv6 Firewalls
Making existing tools work
Summary

Module 6: VPN Attacks

VPNs
VPN Comparison
IPSec
Detecting IPSec VPNs
AH *versus* ESP
Tunnel mode *versus* Transport mode
Main mode *versus* aggressive mode
IKE Main Mode
IKE Aggressive Mode
IPv4 Header
Authentication Header
AH Transport Mode

AH Tunnel Mode
Authentication Algorithms
AH and NAT
ESP with Authentication
ESP in Transport Mode
ESP in Tunnel Mode
IKE
IKE-Scan
IKE-SCAN
Aggressive Mode
Main Mode
Aggressive Mode ID
Aggressive Mode PSK Attacks
Aggressive PSK Cracking
Aggressive Mode ID Enumeration
Main Mode PSK Attacks
Main Mode PSK Cracking
Main Mode Policy Enumeration
IKECrack
IKEProbe
IKE-PROBE
Other VPN Flaws
Insecure Storage of Credentials on VPN Clients
Username Enumeration

Module 7: Defeating SSL

Outline
How SSL Works
Certificate Types
Certificate Chaining
Chain of trust
Verifying a Certificate Chain
Certificate Chain That Cannot be Verified
What if…
Basic Constraints
Then the story started
SSLSNIFF
Running SSLSNIFF
Setting up IPTABLES
Running Arpspoof
SSLSTRIP
How SSL connection is initiated:
SSLSTRIP
How does it look like?
With SSLSTRIP
Running SSLSTRIP
Combining this technique with homograph attack
Certificates
Certificate Enrollment Request PKCS#10
Certificate (Subjects)
CN Encoding
PKCS #10 SUBJECT
PKCS #10 Certificate Signing Request
Disadvantages
Universal Wildcard
More Weird Stuff
What do we have to worry about?
Certificate Revocation
Defeating OCSP
OCSP-Aware SSLSNIFF
Updates
Update-Aware SSLSNIFF
Snort
What is Snort?
Snort Architecture
Packet Sniffing
Preprocessors
Detection Engine
Alerting Components
Three major modes
Using Snort as Packet Sniffer
Packet Sniffing
Snort as Packet Logger
Snort as NIDS
Snort Rule Tree
Decoding Ethernet Packet
Preprocessor Layout
Parts of a Rule
Outputs

Module 8: IDS/IPS Evasion

Evasion
Networking Standards
Evasion Principles

Evasion Layers
Layer 2
Layer 3-4
Fragmentation
Fragmentation Attacks – Ping O' Death
More Malicious Fragments
Fragmentation-Based Techniques
Sending Overlapping Fragments
Different Reassembly Timeout
Sending Fragment with Different TTLs
Insertion Attacks
Protocol Violation
Layer 5-7
Layer 5-7
SMB Evasions
SMB based vulnerabilities
How can IDS control SMB sessions?
DCERPC Evasions
How DCERPC works:
DCERPC Bind Evasions
DCERPC Call Evasions
DCERPC Transport Evasions
Obfuscation
Client Side Attack Evasions
Unicode
UTF-8 Overlong Strings
Javascript Evasions
Base64 your HTML
Encryption
DoS Attacks
Failure Points
Alert Management
Hardware Limitations
Session Tracking
Pattern Matching
Signature Matching

DETAILED LAB DESCRIPTION

Module 1: Working with captured files

Lab 1: Sniffing with Wireshark

Lab 2: HTTP Protocol Analysis

Lab 3: SMB Protocol Analysis

Lab 4: SIP/RTR Protocol Analysis

Lab 5: DNS Protocol Analysis

Module 2: Layer 2 Attacks

Lab1: MAC SPoofing

Lab 2: ARP Wireshark Network Sniffing

Lab 3: Analyzing the capture of Macof

Lab 4: Manipulating STP algorithm

Module 3: Layer 3 Attacks

Lab 1: Exploring Layer 3 with Loki tool on Kali

Lab 2: Cracking the BGP authentication key with Loki dictionary attack

Lab 3: OSPF Authentication

Lab 4: VRRP - Attacking the default gateway redundancy protocol

Module 4: Pivoting and Relays

Lab 1: Pivoting with Metasploit

Lab 2: Pivoting with SSH

Module 5: IPv6 Attacks

Lab 1: Man-in-the-Middle attacks using THC-IPv6 Parasite6

Lab 2: Flooding the Network

Lab 3: IPv6 SLACC Attacks

Module 6: VPN Attacks

Lab 1: Cracking IKE PSK

Lab 2: Enumerate VPN IPsec with iker.py

Module 7: Defeating SSL

Lab 1: Decrypting SSL

Lab 2: Use SSLSTRIP for SSL MITM

Module 8: IDS/IPS Evasion

Lab 1: Use Snort as Packet Sniffer

Lab 2: Use Snort as Packet Logger

Lab3: Check Snort's IDS abilities with pre-captured attack pattern files