



Certified Penetration Testing Consultant

Duration: 4 Days

Language: English

Course Delivery: Classroom

COURSE BENEFITS

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.

Examination

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.

Course Outline

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
Dissecting
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

RHO (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