CPTC - Certified Penetration Testing Consultant

Course Overview

This course will teach students about becoming a Certified Penetration Testing Consultant. Topics covered include team formation, the exploitation process, buffer overflow exploits, web application security, penetration testing report writing, and more.

Module 1 - Pentesting Team Formation 31m

Pentesting Team Formation
What are we covering?
Section 1: Project Management
PMBOK
PMBOK
Initiating Process Activities
Planning Process Activities
Planning Process (cont.)
Planning Process (cont.)
Executing Process Activities
Executing Process (cont.)
Closing Process Activities
Section 2: Pentesting Metrics
Types of Analysis
Quantitative Analysis
Qualitative Analysis
Mixed-Method Analysis
Section 3: Team Roles, Responsibilities, and Benefits
Pentesting Team Structure
Roles/Responsibilities
Benefits
Module 1 Review

Module 2 - NMAP Automation 30m

NMAP Automation
Introduction
What are we covering?
Section 1: NMAP Basics
NMAP Basics
NMAP Basics
NMAP Basics - Options Summary
NMAP Basics - Target Specification
NMAP Basics - Host Discovery
NMAP Basics - Host Discovery (cont.)
NMAP Basics - Port Scanning Basics

NMAP Basics - Port Scanning Techniques
NMAP Basics - Port Specification and Scan Order
NMAP Basics - Service and Version Detection
NMAP Basics - OS Detection
NMAP Basics - NMAP Scripting Engine
NMAP Basics - NMAP Scripting Engine
NMAP Basics - Timing and Performance
NMAP Basics - Output
NMAP Basics - Miscellaneous Options
NMAP Basics - Runtime Interaction
NMAP Basics - Examples
Section 2: NMAP Automation
NMAP Automation
NMAP Automation
Section 3: NMAP Report Documentation
NMAP Report Documentation
NMAP Report Documentation
Module 2 Review

Module 3 - Exploitation Process 21m
Exploitation Process
Review
What are we covering?
Section 1: Purpose
Purpose
Section 2: Countermeasures
Countermeasures
Countermeasures
Countermeasures
Countermeasures
Countermeasures
Section 3: Evasion
Evasion
Section 4: Precision Strike
Precision Strike
Section 5: Customized Exploitation
Customized Exploitation
Section 6: Tailored Exploits
Tailored Exploits
Section 7: Zero-Day Angle
Zero-Day Angle
Section 8: Example Avenues of Attack
Example Avenues of Attack
Section 9: Overall Objective of Exploitation
Overall Objective
Module 3 Review

Module 4 - Fuzzing with Spike 22m

Fuzzing with Spike
What are we covering?
Introduction to Spike
Introduction to Spike
Section 1: Vulnserver
What is Vulnserver?
What is Vulnserver? (cont.)
Vulnserver Source Code
Source Code (cont.)
Source Code (cont.)
Booting Vulnserver
Vulnserver
Section 2: Spike Fuzzing Setup
Built-in 'Spike'
Spikes
Section 3: Fuzzing a TCP Application
Generic_send_tcp
Generic_send_tcp (cont.)
Generic_send_tcp (cont.)
Generic_send_tcp (cont.)
Section 4: Custom Fuzzing Script
TRUN primitive
TRUN primitive
Spiketrunaudit.spk
Fuzzing in progress…
Fuzzing Complete!
Final Thoughts
Module 4 Review

Module 5 - Writing Simple Buffer Overflow Exploits 22m

Writing Simple Buffer Overflow Exploits
Introduction
What are we covering?
Setup
Section 1: Exploit-DB
Exploit-DB
Exploit-DB
Searchsploit
Searchsploit
Section 2: Immunity Debugger
Immunity Debugger
Immunity Debugger
Immunity Layout
Immunity Layout
Immunity Layout
Immunity Layout

32-bit Registers
32-bit Registers
What is a Buffer Overflow?
Running DPE
Section 3: Python
Searching Exploit-DB
Pythons you say?
Continued?
Section 4: Shellcode
MSFVenom
MSFVenom
Sending our Exploit
Connect and Win
Module 5 Review

Module 6 - Stack Based Windows Buffer Overflow 1h

Stack Based Windows Buffer Overflow
Introduction
What are we covering?
Section 1: Debugger
Debugger
Immunity!
Immunity!
Immunity!
Debugger
Immunity!
Section 2: Vulnerability Research
Vulnerability Research
Exploit-DB
MiniShare Exploit Explained
Proof of Concept Code
Running the Script
Running the Script
Section 3: Control EIP, Control the Crash
Control EIP, Control the Crash
Control EIP, Control the Crash
Section 4: JMP ESP Instruction
JMP ESP Instruction
Finding Loaded Modules
Exploit Note
Finding JMP ESP
Search DLL for \xff\xe4
Section 5: Finding the Offset
Finding the Offset
Pattern_create.rb
Proof of Concept Code (Update: pattern_create.rb)
Running the Script

Finding the Offset
Proof of Concept Code (Update: Control EIP Overwrite)
Running the Script
Section 6: Code Execution and Shellcode
Code Execution and Shellcode
Proof of Concept Code (Update: JMP ESP Addition)
Code Execution and Shellcode
Running the Script
Code Execution and Shellcode
Proof of Concept Code (Update: Adding Shellcode)
Section 7: Does the Exploit Work?
Does the Exploit Work?
Does the Exploit Work?
Module 6 Review

Module 7 - Web Application Security and Exploitation 21m

Web Application Security and Exploitation
Introduction
What are we covering?
Section 1: Web Applications
Why Though?
Where Though?
Compromise
Section 2: OWASP Top 10 - 2017
Top 10
A1 Injection
A1 Injection (cont.)
A2 Broken Authentication
A3 Sensitive Data Exposure
A4 XML External Entities
A5 Broken Access Control
A6 Security Misconfiguration
A7 Cross-Site Scripting
A8 Insecure Deserialization
A9 Using Components with Known Vulnerabilities
A9 Using Components with Known Vulnerabilities (cont.)
A10 Insufficient Logging & Monitoring
Tying it all together
Section 3: Zap
Everything you need for Free
Proxy Connection
Zed Attack Proxy
Do What Now?
Intercept All the Things!!
Intercept All the Things!!
Intercept All the Things!!
Intercept All the Things!!

Intercept All the Things!!
Do What Now?
So Then
Section 4: Scapy
The way of the packet
The way of the packet
Finding the Way
Picturing the Way
Module 7 Review

Module 8 - Linux Stack Smashing 19m
Linux Stack Smashing
Introduction
What are we covering?
Section 1: Exploiting the Stack on Linux
Demo: Exploiting the Stack on Linux
Mile2_smash Program
Buffer Overflow Found
Creating the Exploit
Looking to Overwrite RIP
gdb ./mile2_smash
gdb ./mile2_smash (part 2)
Program Crashed
Pattern_create
gdb ./mile2_smash (pattern_create)
gdb ./mile2_smash (pattern_create) (part 2)
Finding the Offset
Updating the Exploit
gdb ./mile2_smash (updated exploit)
gdb ./mile2_smash (updated exploit) (part 2)
gdb ./mile2_smash (updated exploit) (part 3)
Gained Control RIP
Environment Variable Location
Final Updates to the Exploit
Throwing our Exploit
Module 8 Review

Module 9 - Linux Address Space Layout Randomization 25m
Linux Address Space Layout Randomization
Introduction
What are we covering?
Section 1: Stack Smashing to the Extreme
Demo: Stack Smashing to the Extreme
Mile2_leak Program
ASLR Explained
Additional ASLR Information
Additional ASLR Information

Mile2_leak Program (cont.)
Mile2_leak Program (cont.)
Mile2_leak Program (cont.)
Mile2_leak Program (cont.)
Mile2_leak Program (cont.)
Mile2_leak Program (cont.)
Mile2_leak Program (cont.)
Mile2_leak Program (cont.)
Global Offset Table (memset())
poc.py Program (part 1)
poc.py Program (part 2)
Confirming memset()'s Address
Calculate libc's Base Address
Calculate libc's Base Address
memset()'s offset
system()'s offset
Find the address of any library function
poc.py updated (part 1)
poc.py updated (part 2)
Seeing our PoC in action
ret2libc to complete the exploit
poc.py final (part 1)
poc.py final (part 2)
poc.py final (part 3)
Final PoC in action
Module 9 Review

Module 10 - Windows Exploit Protection 27m
Windows Exploit Protection
What are we covering?
Section 1: Introduction to Windows Exploit Protection
Software Exploits
Common Targets
Common Targets - YOU!
Section 2: Structured Exception Handling (SEH)
Structured Exception Handling
Types of SEH
How to Use SEH
How to Use SEH (cont.)
How to Use SEH (cont.)
Section 3: Data Execution Prevention (DEP)
Data Execution Prevention
DEP Types
DEP Benefits
Configuring DEP
Configuring DEP (cont.)
Configuring DEP (cont.)

Configuring DEP (cont.)
Configuring DEP (cont.)
Configuring DEP (cont.)
Section 4: SafeSEH/SEHOP
SEH Exploit Buffer
SEH Exploit Buffer, Explained
SafeSEH
SEHOP
Module 10 Review

Module 11 - Getting Around SEH and ASLR (Windows) 35m
Getting Around SEH and ASLR (Windows)
Introduction
What are we covering?
Section 1: Vulnerable Server Setup
Vulnerable Server Setup
VulnServer in Action
Section 2: Time to Test it out
Time to Test it out
Section 3: "VulnServer" meet Immunity
Immunity!
Immunity!
Section 4: VulnServer Demo
Demo: Getting Around SEH and ASLR
Proof of Concept Code
Running the Script
Immunity Crash Review
Immunity Crash Review (cont.)
Immunity Crash Review (cont.)
Immunity Debugger
Proof of Concept Code (updated)
Crash Again
Crash Again (cont.)
Immunity Debugger
Proof of Concept Code (updated)
Crash Again
Immunity Debugger
Proof of Concept Code (updated)
Crash Again
Crash Again (cont.)
Finding loaded modules
Redirecting Mona logs
Finding ROP Gadgets with Mona
Immunity Debugger
Proof of Concept Code (updated)
Crash Again
Crash Again (cont.)

nasm_shell
Proof of Concept Code (updated)
Crash Again
Crash Again (cont.)
Crash Again (cont.)
Immunity Debugger
Proof of Concept Code (updated)
Crash Again
Immunity Debugger
Proof of Concept Code (updated)
Crash Again
Crash Again (cont.)
Crash Again (cont.)
Crash Again (cont.)
Crash Again (cont.)
Crash Again (cont.)
Crash Again (cont.)
Crash Again (cont.)
Crash Again (cont.)
Vulnerable Server
Proof of Concept Code (updated)
Proof of Concept Code (updated)
Throwing our Exploit
Module 11 Review

Module 12 - Penetration Testing Report Writing 32m
Penetration Testing Report Writing
What are we covering?
Introduction
Findings Document
Section 1: Reporting
Pentest Report Format Sections
Cover Page
Confidentiality Statement
Confidentiality Statement
Confidentiality Statement
Document Control
Timeline
Executive Summary
Executive Summary Sections
Executive Summary Sections
Executive Summary Sections
Security Risk Origin/Category
Executive Summary Sections
Executive Summary Sections
Executive Summary Sections
Technical Report

Technical Report Sections
Technical Report Sections
Technical Report Sections
Technical Report Sections
Technical Report Sections
Technical Report Sections
Technical Report Sections
Technical Report Sections
Technical Report Sections
Technical Report Sections
Technical Report Sections
Module 12 Review

Total Duration: 5h 46m