CPEH - Certified Professional Ethical Hacker

Course Overview

This course will teach students about ethical hacking. Topics covered include cryptography, password cracking, malware, social engineering, network attacks, hacking wireless networks, and more.

Course Introduction **6**m
Course Introduction

Module 1 - Introduction to Ethical Hacking 44m
Introduction to Ethical Hacking
Where are We?
Overview
Section 1: What and Why
What is Ethical Hacking?
What is Ethical Hacking?
Why Ethical Hacking?
Downfalls
Section 2: Differences
Items we Cover
What is a Penetration Test?
White Hat/Red Team
Red Team/Security Researcher
Differences
Task Differences
Hacker vs. Ethical Hacker
Section 3: Security Definitions
Types of Hackers
CIA Triad in Detail
Security Definitions
Exploit and Vulnerability Lifecycle
Zero Day Anyone?
Risk Assessment
Mile2 Glossary of Terms
Section 4: Risk Management
Risk Management Flow
What is the Value of an Asset?
Risk Based Definitions
What is a Threat Source/Agent?
What is a Threat?
What is a Vulnerability?
Examples of Some Vulnerabilities that Are Not Always Obvious

What is a Control?
What is the Likelihood?
What is the Impact?
Control Effectiveness
Risk Management
Reference Documents
NIST SP 800-39 Risk Context
Purpose of Risk Management
Section 5: Methodologies
Options
Ethical Hacking Methodologies
Penetration Testing Methodologies
OSSTMM
OSSTMM - The Trifecta
OSSTMM Combining Trifecta and 4PP
NIST SP-800-115
NIST SP-800-115
ISSAF Four Phases
ISSAF Diagram
PTES
Methodology for Penetration Testing
So Which One?
Not Just Tools
Review

Module 2 - Linux Fundamentals 36m

Linux Fundamentals
Where are We?
Overview
Section 1: Core Concepts
What is Linux?
Linus + Minix = Linux
GNU
Linux GUI Desktops
Top 10 Latest GUI Releases
Distributions
Resources
Section 2: The Shell and other items you need to know
Shell
Linux Shell
Linux Bash Shell
File System Structure
File System Structure
File System Structure
Mounting Drives with Linux
Tarballs and Zips
Compiling Programs in Linux

Iptables
Iptables
IP Forwarding
Section 3: Managing Users
Accounts and Groups
Password & Shadow File Formats
Password & Shadow File Formats
Accounts and Groups
User Account Management
Changing a User Account Password
Root Account
Linux and Unix Permissions
Linux and Unix Permissions
Linux and Unix Permissions
Linux and Unix Permissions
Section 4: Basic Commands
Network Config
Where is my C:\ Drive?
Mounting CD
Manage Directories and Files
Review

Module 3 - Protocols 55m

Protocols
Where are We?
Overview
Section 1: Network Models
Network Models
OSI Model
Layer 7: Application
Layer 6: Presentation
Layer 5: Session
Layer 4: Transport
Layer 3: Network
Layer 2: Data Link
Layer 1: Physical
TCP/IP
Layer 4: Application Layer
Layer 3: Transport Layer
Layer 2: Internet Layer
Layer 1: Network Interface Layer
OSI/TCP IP
Section 2: Protocols & Services
Protocols at Each OSI Model Layer
Ports and Protocols
TCP vs UDP
TCP Packet Content

UDP Packet Content
Three Way Handshake
TCP Flags
ARP
ARP Process
ICMP
ICMP Messages
DNS
DNS Insecurities
SNMP
SNMP Insecurities
SMTP
SMTP Insecurities
LDAP
LDAP Insecurities
Services to Consider
Review

Module 4 - Cryptography 1h 12m

Cryptography
Where are We?
Overview
Section 1: Understanding Cryptography
Cryptographic Definitions
Cryptographic Definitions
A Few More Definitions
Cryptography Usage
Types of Cryptographic Algorithms
Encryption/Decryption Methods
Section 2: Symmetric Encryption
Symmetric Cryptography - Use of Secret Keys
Symmetric Encryption
Symmetric Keys
Stream Cipher & Block Cipher
Symmetric Cipher - Stream Cipher
XOR Encryption Process
Stream Cipher Modes
Strength of a Stream Cipher
Symmetric Cipher - Block Cipher
S-Boxes Used in Block Ciphers
Block Cipher Modes
Block Ciphers - ECB
Block Cipher - CBC
CBC Mode
Block Cipher Modes - CFB and OFB
CTR Mode
Symmetric Algorithms - DES

Evolution of 3DES
Symmetric Cipher - AES
Other Symmetric Algorithms
Section 3: Asymmetric Encryption
Asymmetric Cryptography
Asymmetric Encryption
When to Use Which Key?
Asymmetric
Key Exchange
Diffie-Hellman
Asymmetric Algorithm - RSA
Asymmetric Algorithms - El Gamal and ECC
Public Key Cryptography Advantages
Asymmetric Algorithm Disadvantages
Symmetric versus Asymmetric
Example of Hybrid Cryptography
Digital Signatures
Digital Signature
Section 4: Hashing
Hashing Algorithms
Protecting the Integrity of Data
Data Integrity Mechanisms
Security Issues in Hashing
Simple MAC
Weakness in Using Only Hash Algorithms
HMAC - Sender
HMAC - Receiver
QKD
QKD
Section 5: Cryptography in Use
Link versus End-to-End Encryption
End-to-End Encryption
Network Layer Protection
IPSec Key Management
IPSec Handshaking Process
SAs in Use
IPSec is a Suite of Protocols
IPSec Datagrams
SSL/TLS Hybrid Encryption
SSH Security Protocol
E-mail Standards
Encrypted Message
Secure E-mail Standard
Section 6: Crypto Attacks
Theoretical Cryptanalysis
Theoretical Cryptanalysis
Theoretical Cryptanalysis
Birthday Attack

Example of a Birthday Attack
Applied Cryptanalysis
Applied Cryptanalysis
Applied Cryptanalysis
Applied Cryptanalysis
Review

Module 5 - Password Cracking 45m

Password Cracking
Where are We?
Overview
Section 1: What and Why
Why it is kind of a no brainer!
Password Cracking Strategy
Password Cracking Strategy
Password Cracking Strategy
Cracking Techniques
Section 2: Attacks and Tools of the Trade
Password Guessing
Password Cracking LM/NTLM Hashes
Syskey Encryption
Rainbow Tables
GPU and/or CPU for Password Cracking
Cain and Abel's Cracking Methods
Rainbow Tables Limitations
Password Salting
Password Salting
NTPASSWD: Hash Insertion Attack
Password Sniffing
Mimikatz
A Few other Common Tools
Section 3: Countermeasures
Implement General Password Policies that Work!
Consider Something Better
Understand the Windows Authentication Protocols
Security Items to Consider
Security Items to Consider
Review

Module 6 - Malware 1h 19m

Malware
Where are We?
Overview
Section 1: DOS & DDOS
Denial of Service
Distributed Denial of Service
Distributed Denial of Service

Denial of Service Impact
DoS Attack Symptoms
Digital Attack Map: A Global Threat Visualization
DoS Attack Methods
BOTNET
Botnet Ecosystem
BOTNET Propagation
BOTNET Tools
DoS/DDoS Attack Tools
High Orbit Ion Canon (HOIC)
DoS Attack Detection
DoS Detection - Activity Profiling
DoS Detection Sequential Change Point Detection
DoS Detection - Wavelet Analysis
DoS/DDoS Countermeasures
Botnet Countermeasures
Advanced DoS/DDoS Protection Tools
Advanced DDoS Protection Methods
Section 2: Viruses and Worms
What is a Virus?
How it works
What they do
Types of Viruses
Types of Viruses
Types of Viruses
Types of Viruses
Types of Viruses
Stealth Strategies
How do you get Infected?
DNS Changer Virus
Melissa Virus
Worms
How bad is it?
Storm Worm
Stuxnet
conficker
Section 3: Trojans & Backdoors
Trojans and Backdoors
Distributing Malware
Malware Capabilities
Trojan Types
Netcat
Netcat Switches
Remote Access Trojan (RAT) Components
Meet Zberb
Executable Wrappers
Avoiding Detection
REFUD

Today's Wrappers
Malware Countermeasures
Malware Reference: www.BleepingComputer.com
Monitoring Autostart Methods
Port Monitoring Software
File Protection Software
SigCheck
Hardware-based Malware Detectors
User Education
Section 4: Ransomware
Ransomware
Famous Ransomware
Famous Ransomware
Ransomware and Cryptocurrency
Review

Module 7 - Security Devices 40m
Security Devices
Where are We?
Overview
Section 1: Basic Security Elements
Introduction
Switching and Routing
Switch Security
Router Security
Router Security
VLAN
VLAN
Proxy, NAT, PAT
Section 2: Security Appliances
Firewall
Next Generation Firewall
DMZ
IDS
IDS
IPS
IPS
SIEM
SIEM Capabilities
Review

Module 8 - Information Gathering - Reconnaissance-Passive (External Only) 1h
Information Gathering - Reconnaissance-Passive (External Only)
Where are We?
Overview
Section 1: What are we looking for?
What is it?

Open-Source Intelligence (OSINT)
Why do we do it?
What do we want?
What do we want?
What do we want?
What do we want?
Section 2: Where/How do we find this information?
Where?
Where Do We Find This Information?
Domain Name Registration
WHOIS
DNS Databases
Using Nslookup
Username Searches
eMail Address Searches
People Search Engines
Business Search Engines
Web Server Info Tool: Netcraft
Internet Archive: The WayBack Machine
Job Postings
Blogs & Forums
Shodan
Google Hacking
GHDB
Section 3: Are there tools to help?
Maltego - Clear Leader
Maltego - Clear Leader
Recon-ng
Recon-ng
theharvester
Firecat/Kromcat
Review

Module 9 - Social Engineering 41m

Social Engineering
Where are We?
Overview
Section 1: Social Engineering Types
Vulnerable Human Behavior
Organization Vulnerabilities
Human Based Social Engineering
Human Based Social Engineering
Social Engineering Techniques
Social Engineering Gaps
Computer Based Social Engineering
Social Network Lookup http://namechk.com/
Impact of Social Engineering

Social Media Protection
Identity Theft and PII
Identity Theft and PII Protection
Identity Theft and PII Protection
Section 2: Phishing Scams
Phishing
Spear Phishing
Whaling Attacks
Recent Successful Whaling Attacks
Whaling Mitigation
Phishing Protection
Review

Module 10 - Reconnaissance-Active Scanning-Enumeration 54m
Reconnaissance-Active Scanning-Enumeration
Where are We?
Overview
Section 1: What are we looking for?
Where are we in the Process?
What is it?
What are we looking for?
Methods of Obtaining Information
Physical Access
Social Access Covered in Module 9
Section 2: Port Scanning
Introduction to Port Scanning
Which Services use which Ports?
Legalities
Port Scan Tips
Port Scans Should Reveal…
Comparison of Models
Types of Scans
TCP/IP Suite
TCP Flags
TCP 3-Way Handshake
TCP Connect Port Scan
Half-open Scan (SynScan)
Firewalled Ports
UDP versus TCP
UDP Port Scan
Section 3: Are there tools to help?
Popular Port Scanning Tools
Stealth Online Ping
Online Tools
Fing & Fing Mobile
Solarwinds Port Scanner
Hping3

Hping3
P0f
NMAP: Is the Host online?
ICMP Disabled?
NMAP TCP Connect Scan
NMAP
Tool Practice: TCP Half-open & Ping Scan
NMAP Service Version Detection
Additional NMAP Scans
Saving NMAP Results
NMAP UDP Scans
Section 4: Banner Grabbing
Introduction
Why Banner Grabbing?
Banner Grabbing Tools
Banner Grabbing Tools - ID Serve
Banner Grabbing Tools - Netcraft
Banner Grabbing Tools - Netcat
Banner Grabbing Tools - Telnet
Practice: Banner Grabbing with Telnet
Banner Grabbing Tools - NMAP
Section 5: Enumeration
Enumeration
Services to Enumerate:
SNMP
LDAP
NTP
SMTP
DNS
Review

Module 11 - Vulnerability Assessment 30m

Vulnerability Assessment
Where are We?
Overview
Section 1: What is a Vulnerability Assessment?
Review from CSP+
What is a Vulnerability Assessment (VA)?
Benefits of a Vulnerability Assessment
Types of Vulnerability Assessments
How do we know about Vulnerabilities?
Typical Vulnerability Assessment Process
Section 2: Tools of the Trade
Choosing the Right Tool
Different Types of Tools
The List
Network Based Tools Comparison

Application Based Tools Comparison
Section 3: Testing Internal/External Systems
It starts here!
Enumeration
Detection
Additional Details
Easily Exploitable Vulnerabilities
Review

Module 12 - Network Attacks 1h 4m
Network Attacks
Where are We?
Overview
Section 1: Sniffing Techniques
Packet Sniffers
Example Packet Sniffers
Tool: Pcap & WinPcap
Tool: Wireshark
TCP Stream Re-assembling
tcpdump & windump
TCP Dump Examples
Sniffer Detection using Cain & Abel
Passive Sniffing
Active Sniffing
Active Sniffing Methods
Switch Table Flooding
ARP Cache Poisoning
ARP Normal Operation
ARP Cache Poisoning
Technique: ARP Cache Poisoning (Linux)
MAC Spoofing
DNS Poisoning
Source Routing
Advertise Bogus Routes
Rogue DHCP
Tool: Cain and Abel
Ettercap
Linux Tool Set: Dsniff Suite
What is DNS Spoofing?
Tools: DNS Spoofing
Breaking SSL Traffic
Breaking SSL Traffic
URL Obfuscation
Intercepting VoIP
Countermeasures
Countermeasures
Countermeasures for Sniffing

Section 2: Hijacking
Session Hijacking
Session Hijacking
Contributors to Session Hijacking
Impact of Session Hijacking
Session Hijacking Techniques
Brute Force Attack
Stealing and Calculating Session IDs
Session Hijacking Process
Types of Session Hijacking
Application-level Session Hijacking
Predicting Session Token
Man-in-the-Middle Attacks
Client-side Attacks
Man-in-the-Browser Attacks
Session Sniffing
Cross-site Script Attacks
Network-level Session Hijacking
TCP/IP Hijacking
Session Hijacking Tools
Burp Suite
Session Hijacking Tools
Protecting against Session Hijacking
Protecting against Session Hijacking
Protecting against Session Hijacking
Protecting against Session Hijacking - Web Users
Review

Module 13 - Hacking Servers 49m
Hacking Servers
Where are We?
Overview
Section 1: Servers, what are they good for?
Servers, what are they good for?
Know the OS
Know How it is Used
Find the Exploit
Section 2: What is an Exploit?
What is an Exploit?
Exploit Development
Exploit Development
Section 3: Tools of the Trade
Exploit-db
Search Exploit-db
Metasploit
Metasploit
Understanding Metasploit

Hands on Metasploit
Core Impact
SaintExploit at a Glance
Section 4: Testing Internal/External Systems
It starts here!
External Systems
Outside of Possible Evasion Techniques
Internal Systems
Inside out Possible Evasion Techniques
Client-Side Attacks
Physical Access Attacks
Review

Module 14 - Assessing and Hacking Web Technologies 48m
Assessing and Hacking Web Technologies
Where are We?
Overview
Section 1: OWASP Top 10
OWASP Top 10
A1 - Injection
A2 - Broken Authentication
A3 - Sensitive Data Exposure
A4 - XML External Entities (XXE)
A5 - Broken Access Control
A6 - Security Misconfiguration
A7 - Cross-Site Scripting
A8 - Insecure Deserialization
A9 - Using Components with Known Vulnerabilities
A10 - Insufficient Logging and Monitoring
Section 2: SQL Injection
Introduction
SQL Injection Attack Characters
SQL Injection Methodology
SQL Injection Attacks
Types of SQL Injection
Blind SQL Injection
Simple SQL Injection Attack
Union & Error Based SQL Injection
SQL Injection Tools
SQL Injection Tools
SQL Injection Tools
SQL Injection Detection Tool
SQL Injection Detection Tool
SQL Injection Detection Tool
SQL Injection Detection Tool
Section 3: XSS
Cross-Site Scripting (XSS/CSS)

Introduction to Cross-Site Scripting
Type of XSS
Stored XSS or Persistent/Type I
Reflected XSS (Non-Persistent or Type II)
DOM Based XSS (Type-0)
Server XSS
Client XSS
XSS Types in the Matrix
Test for XSS Vulnerability
Code Review
Web Application Security Scanners
Testing
Review

Module 15 - Hacking Wireless Networks 1h 39m

Hacking Wireless Networks
Where are We?
Overview
Section 1: Wireless Technologies
802.11 Wireless Background Information
Wireless LAN (WLAN)
Standards Comparison
Basic Items SSID (Service Set Identity)
Basic Items MAC Filtering
Encryption Protocols
Wireless Security Wired Equivalent Privacy
WEP
WEP Weak IV Packets
WEP Weaknesses
Wireless Security Wi-Fi Protected Access
How WPA Improves on WEP
Temporal Key Integrity Protocol (TKIP)
WPA (TKIP Flow Chart)
The WPA MIC Vulnerability
WPA-PSK Encryption
Wireless Security 802.11i - WPA2
Wireless Security 802.11i - WPA2
WPA and WPA2 Mode Types
WPA2 (AES Encryption)
4-Way Handshake AES-CCMP - WPA2
WPA2 Weaknesses
Wireless Security WPA3
WPA3 Improvements
WPA3 Improvements
WPA3 Improvements
Wi-Fi Protected Setup
Authentication

Open Authentication
Shared Key Authentication
EAP Authentication
MAC Address Authentication
Bluetooth
Bluetooth
Bluetooth Protocol Stack
The Pairing Process
Basics of Bluetooth Security
Basics of Bluetooth Security
Bluetooth Security
Section 2: Mobile and IoT Technologies
Overview of Smartphones Communication
Risks and Threats Mobile Devices
Risks and Threats Mobile Devices
IoT Risks and Threats
Section 3: Various Tools Used
Wireless Hardware Needed
Aircrack-ng Suite Used for both WEP and WPA
Airodump-ng Used for both WEP and WPA
Aireplay Used for both WEP and WPA
Aircrack-ng Used for both WEP and WPA
Wesside-ng Used for both WEP and WPA
Kismet
Wireshark
coWPAtty
NetStumbler: This Product has not been updated in some time
Other Notable Tools
Bluetooth Equipment
Bluetooth Tools
Bluetooth Tools
Section 4: Hacking Techniques
DOS: Deauth/Disassociation Attack
Attacking WEP
Attacking WPA
Attacking WPA2
Attacking WPA2 via Linux/Android
Attacking WPA2 via Linux/Android
Recon: Bluetooth
Attacking Bluetooth
Bypassing Smartphone Security
Section 5: Countermeasures
Umm, Patching?
Require Network Authentication 802.1X: EAP Types
Comparing 802.1X Authentication Methods
EAP/TLS Deployment
Wireless Intrusion Detection
Mobile/IoT Areas to Consider

Mobile/IoT Device Security
Mobile/IoT Device Security
Mobile/IoT Application Security
Mobile/IoT Application Security
Mobile Device Connections to Secure
Hardening the Devices
Is IoT Any Different?
Security Areas that Apply to IoT
General Hardening Recommendations for IoT
Implement IoT Standards
Mobile Deployment Models
BYOD Issues/Concerns
Mobile/IoT Initial Recommendations
Develop Internal Policies
Review

Module 16 - Maintaining Access and Covering Tracks 36m
Maintaining Access and Covering Tracks
Where are We?
Overview
Section 1: Maintaining Access
Back Doors
Covert Channel
Encrypted Tunnel Notes
Backdoor via Rootkits
Rootkits - Not as many today
Netcat - Still Here and Still Works
Netcat Switches
Netcat as a Listener
Meterpreter - Very Widely Used Today
Meterpreter in Use
Leverage PowerShell for Backdoors!
Section 2: Covering Tracks
What and Why
Clearing Event Logs
Clearing Event Logs
Hiding Files with NTFS Alternate Data Streams
What is Steganography?
Steganography Tools - There are many!
Shedding Files Left Behind
More Anonymous Software
Anonymous Internet Access
Anonymous Browsing
Leaving No Local Trace
Review

Total Duration: 14h 18m