EC-Council Certified Network Defense Architect (CNDA)

Register Online

Schedule

Class Length: 5 Days

G2R = “Guaranteed to Run” | OLL = “Online LIVE”
ILT = “Instructor-Led-Training”

This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.

Overview

In this course, students will be shown how to scan, test, hack and secure their own systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed.

Target Audience

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Course Outline

Introduction to Ethical Hacking

Why Security?
The Security, functionality and ease of use Triangle
Can Hacking be Ethical?
Essential Terminology.
Elements of Security.
What does a Malicious Hacker do?
Difference between Penetration Testing and Ethical Hacking.
Hacker Classes.
What do Ethical Hackers do?
Skill Profile of an Ethical Hacker.
Modes of Ethical Hacking.
Security Testing.
Deliverables.
Computer Crimes and Implications.
Legal Perspective (US Federal Laws).

Footprinting

Defining Footprinting.
Information Gathering Methodology.
Locate the Network Range.
Hacking Tools

Scanning

Definition of Scanning.
Types of scanning
Objectives of Scanning
Scanning Methodology
Classification of Scanning
Hacking Tools
IPsec Scan
NetScan Tools pro 2003
OS Fingerprinting
Active Stack fingerprinting
Passive Fingerprinting
Proxy Servers
Countermeasures

Enumeration

What is Enumeration?
NetBios Null Sessions
Null Session Countermeasures
NetBIOS Enumeration
Simple Network Management Protocol (SNMP) Enumeration
SNMP Enumeration Countermeasures
Management Information Base (MIB)
Windows 2000 DNS Zone Transfer
Blocking Win 2k DNS Zone Transfer
Enumerating User Accounts
DumpReg
Active Directory Enumeration and Countermeasures

System Hacking

Administrator Password Guessing
Manual Password Cracking Algorithm
Automated Password Cracking
Password Types
Types of Password Attacks
Performing Automated Password Guessing
Password Sniffing
Password Cracking Countermeasures
Syskey Utility
Cracking NT/2000 Passwords
SMBRelay Man-in-the-Middle Scenario
SMBRelay Weaknesses and Countermeasures
Keystroke Loggers
Hiding Files
Creating Alternate Data Streams
ADS creation and detection
LADS (List Alternate Data Streams)
NTFS Streams Countermeasures
Stealing Files Using Word Documents
Field Code Countermeasures
Steganography
Steganography Detection
Covering Tracks
Disabling Auditing and clearing Event Logs
Dump Event Log
RootKit
Planting the NT/2000 RootKit
Rootkit Countermeasures

Trojans and Backdoors

Effect on Business
What is a Trojan?
Overt and Covert Channels
Working of Trojans
Different Types of Trojans
What Trojan Creators look for?
Different ways a Trojan can get into a system
Indications of a Trojan Attack
Some famous Trojans and ports used by them
How to determine which ports are “Listening”?
Different Trojans found in the Wild
Wrappers
Packaging Tool : Wordpad
ICMP Tunneling
Loki Countermeasures
Reverse WWW Shell – Covert Channels using HTTP
Process Viewer
System File Verification
Anti-Trojan
Reverse Engineering Trojans
Backdoor Countermeasures

Sniffers

Definition of sniffing
How a Sniffer works?
Passive Sniffing
Active Sniffing
Man-in-the-Midle Attacks
Spoofing and Sniffing Attacks
ARP Poisoning and countermeasures
Network Probe
Sniffing Countermeasures

Denial of Service

What is Denial of Service?
Goal of DoS(Denial of Service)
Impact and Modes of Attack
DoS Attack Classification
Buffer Overflow Attacks
Distributed DOS Attacks and Characteristics
Agent Handler Model
IRC-Based DDoS Attack Model
DDoS Attack taxonomy
DDoS Tools
Reflected DOS Attacks
Reflection of the Exploit
Countermeasures for Reflected DoS
DDoS Countermeasures
Defensive Tool: Zombie Zapper
Worms: Slammer and MyDoom.B

Social Engineering

What is Social Engineering?
Art of Manipulation
Human Weakness
Common Types of Social Engineering
Human Based Impersonation
Example of social engineering
Computer Based Social Engineering
Reverse Social Engineering
Policies and procedures
Security Policies-checklist

Session Hijacking

Understanding Session Hijacking
Spoofing vs Hijacking
Steps in Session Hijacking
Types of Session Hijacking
TCP Concepts 3 Way Handshake
Sequence numbers
Remote TCP Session Reset Utility
Dangers Posed by Session Hijacking
Protection against Session Hijacking
Countermeasures: IP Security

Hacking Web Servers

How Web Servers Work?
How are Web Servers Compromised?
Popular Web Servers and Common Security Threats
Apache Vulnerability
Attack against IIS
IIS Components
Sample Buffer Overflow Vulnerabilities
ISAPI.DLL Exploit
Code Red and ISAPI.DLL Exploit
Unicode
Unicode Directory Traversal Vulnerability
Msw 3prt IPP Vulnerability
IPP Buffer Overflow Countermeasures
Unspecified Executed Path Vulnerability
File System Traversal Countermeasures
WebDAV/ ntdll.dll Vulnerability
RPCDCOM Vulnerability
ASN Exploits
IIS Logs
Network Tool: Log Analyzer
Hacking Tool: Clean IISLog
Escalating Privileges on IIS
Microsoft IIS 5.0 - 5.1 remote denial of service Exploit Tool
Microsoft Frontpage Server Extensions fp30reg.dll Exploit Tool
GDI+ JPEG Remote Exploit Tool
Windows Task Scheduler Exploit Tool
Microsoft Windows POSIX Subsystem Local Privilege Escalation Exploit Tool
Hot Fixes and Patches
Vulnerability Scanners
Network Tools
Countermeasures
Increasing Web Server Security

DNNStuff - InjectAnything

Web Application Vulnerabilities

Web Application Set-up
Web Application Hacking
Anatomy of an Attack
Web Application Threats
Cross Site Scripting/XSS Flaws
Countermeasures
SQL Injection
Command Injection Flaws
Countermeasures
Cookie/Session Poisoning
Countermeasures
Parameter/Form Tampering
Buffer Overflow
Countermeasures
Directory Traversal/Forceful Browsing
Countermeasures
Cryptographic Interception
Authentication Hijacking
Countermeasures
Log Tampering
Error Message Interception
Attack Obfuscation
Platform Exploits
Internet Explorer Exploits
DMZ Protocol Attacks
DMZ
Countermeasures
Security Management Exploits
Web Services Attacks
Zero Day Attacks
Network Access Attacks
TCP Fragmentation
Hacking Tools:
Burp: Positioning Payloads
Burp: Configuring Payloads and Content Enumeration
Burp
Burp Proxy: Intercepting HTTP/S Traffic
Burp Proxy: Hex-editing of Intercepted Traffic
Burp Proxy: Browser Access to Request History
Carnivore
Google Hacking

Web Based Password Cracking Techniquesq

Authentication- Definition
Authentication Mechanisms
HTTP Authentication
Basic Authentication
Digest Authentication
Integrated Windows (NTLM) Authentication
Negotiate Authentication
Certificate-based Authentication
Forms-based Authentication
Microsoft Passport Authentication
What is a Password Cracker?
Modus Operandi of an Attacker using Password Cracker
How does a Password Cracker work?
Attacks- Classification
Password Guessing
Query String
Cookies
Dictionary Maker

SQL Injection

Attacking SQL Servers
SQL Server Resolution Service (SSRS)
Osql-L Probing
Port Scanning
Sniffing, Brute Forcing and finding Application Configuration Files
Database Scanner
Input Validation Attack
Login Guessing & Insertion
Shutting Down SQL Server
Extended Stored Procedures
SQL Server Talks
Preventive Measures

Hacking Wireless Networks

Introduction to Wireless Networking
Business and Wireless Attacks
Wireless Basics
Components of Wireless Network
Types of Wireless Network
Setting up WLAN
Detecting a Wireless Network
How to access a WLAN
Advantages and Disadvantages of Wireless Network
Antennas
SSIDs
Access Point Positioning
Rogue Access Points
What is Wireless Equivalent Privacy (WEP)?
WEP Tool:
Related Technology and Carrier Networks
MAC Sniffing and AP Spoofing
Terminology
Denial of Service Attacks
Man-in-the-Middle Attack (MITM)
Multi Use Tool: THC-RUT
Tool: WinPcap
Auditing Tool: bsd-airtools
WIDZ- Wireless Detection Intrusion System
Securing Wireless Networks
Out of the box Security
Radius: Used as Additional layer in security
Maximum Security: Add VPN to Wireless LAN

Virus and Worms

Virus Characteristics
Symptoms of ‘virus-like’ attack
What is a Virus Hoax?
Terminologies
How is a worm different from virus?
Indications of a Virus Attack
Virus History
Virus damage
Effect of Virus on Business
Access Methods of a Virus
Mode of Virus Infection
Life Cycle of a virus
What Virus Infect?
How virus infect?
Writing a simple virus program.
Writing DDOS Zombie Virus
Virus Construction Kits
Virus Creation Scripts
Virus Detection Methods
Virus Incident Response
What is Sheep Dip?
Prevention is better than Cure
Anti-Virus Software
Popular Anti-Virus packages
Virus Analyzers

Physical Security

Security statistics
Physical Security breach incidents
Understanding Physical Security
What is the need of Physical Security?
Who is Accountable for Physical Security?
Factors affecting Physical Security
Physical Security checklist
Company surroundings
Premises
Reception
Server
Workstation Area
Wireless Access Points
Other Equipments such as fax, removable media etc
Access Control
Computer Equipment Maintenance
Wiretapping
Remote access
Lock Picking Techniques
Spying Technologies

Linux Hacking

Why Linux?
Linux basics
Chrooting
Why is Linux Hacked?
Linux Vulnerabilities in 2003
How to apply patches to vulnerable programs
Scanning Networks
Password cracking in Linux.
ipchains vs. ipfwadm
How to Organize Firewall Rules
Security Auditor's Research Assistant (SARA)
TCP Wrappers
Linux Loadable Kernel Modules
Rootkit countermeasures:
Advanced Intrusion Detection System (AIDE)
Linux Security testing tools
NMap
LSOF
Netcat
Nemesis
Linux tools: Log and traffic monitors:
Linux Security Auditing Tool (LSAT)
Linux Security countermeasures

Evading Firewalls, IDS and Honeypots

Intrusion Detection Systems
Ways to Detect Intrusion
Types of Intrusion Detection System
Intrusion Detection Tools
Steps to perform after an IDS detects an intrusion
Evading IDS systems
Tools to Evade IDS
Introduction to Firewalls
Firewall Identification
Firewalking
Banner Grabbing
Breaching Firewalls
Placing Backdoors through Firewalls
Hiding Behind Covert Channel: Loki
ACK tunneling
Tools for testing IDS and Firewalls
Introduction to Honeypots
Honeypot Project
Types of Honeypots
Honeypot: Specter
Honeypot: Honeyd
Honeypot: KFSensor
Hacking Tool: Sebek
Tools to Detect Honeypot
Send-Safe Honeypot Hunter
Nessus Security Scanner

Buffer Overflows

Significance of Buffer Overflow Vulnerability
Why are Programs/Applications Vulnerable?
Buffer Overflows
Reasons for Buffer Overflow Attacks
Knowledge required writing Buffer Overflow Exploits
How a Buffer Overflow occurs?
Understanding Stacks
Stack Implementation
Stack based buffer overflow
Shellcode
Heap Based buffer overflow
How to detect Buffer Overflows in a Program?
Attacking a real program
NOPS
How to mutate a Buffer Overflow Exploit? featuring ADMutate
Countermeasures
Return Address Defender (RAD)
StackGuard
Immunix System
Vulnerability Search - ICAT

Cryptography

Public-key Cryptography
Working of Encryption
Digital Signature
Digital Certificate
RSA (Rivest Shamir Adleman)
RSA Attacks
Brute forcing RSA factoring
Esoteric attack
Chosen cipher text attack
Low encryption exponent attack
Error analysis
Other attacks
MD5
SHA (Secure Hash Algorithm)
SSL (Secure Socket Layer)
RC5
What is SSH?
Government Access to Keys (GAK)
RSA Challenge
distributed.net
PGP (Pretty Good Privacy)
Code Breaking Methodologies
Using Brute Force
Frequency Analysis
Trickery and Deceit
One-Time Pad
Cryptography Attacks
Disk Encryption
Cracking S/MIME Encryption using idle CPU Time
Command Line Scriptor

Penetration Testing - Part 1

Need for a Methodology
Penetration Test vs. Vulnerability Test
Reliance on Checklists and Templates
Phases of Penetration Testing
Passive Reconnaissance
Best Practices
Results that can be expected
Indicative passive reconnaissance steps include (but are not limited to)
Introduction to Penetration Testing
Type of Penetration Testing Methodologies
Open Source Vs Proprietary Methodologies
Security Assessment Vs Security Auditing
Risk Analysis
Types of Penetration Testing
Types Ethical Hacking
Vulnerability Assessment Vs Penetration Testing
Do-it Yourself Testing
Firms Offering Penetration Testing Services
Penetration Testing Insurance
Explication of Terms of Engagement
Pen-Test Service Level Agreements
Offer of Compensation
Starting Point and Ending Points of Testing
Penetration Testing Locations
Black Box Testing
White Box Testing
Grey Box Testing
Manual Penetration Testing
Automated Penetration Testing
Selecting the Right Tools
Pen Test Using Appscan
Evaluating Different Types of Pen-Test Tools
Platform on Which Tools Will be Used
Asset Audit
Fault Tree and Attack Trees
GAP Analysis
Device Inventory
Perimeter Firewall Inventory
Web Server Inventory
Load Balancer Inventory
Local Area Network Inventory
Demilitarized Zone Firewall
Internal Switch Network Sniffer
Application Server Inventory
Database Server Inventory
Name Controller and Domain Name Server
Physical Security
ISP Routers
Legitimate Network Traffic Threat
Unauthorized Network Traffic Threat
Unauthorized Running Process Threat
Loss of Confidential Information
Business Impact of Threat
Pre-testing Dependencies
Post-testing Dependencies

Failure Management
Test Documentation Processes
Penetration Testing Tools
Defect Tracking Tools
Configuration Management Tools
Disk Replication Tools
Pen-Test Project Scheduling Tools
Network Auditing Tools
DNS Zone Transfer Testing Tools
Trace Route Tools and Services
Network Sniffing Tools
Denial of Service Emulation Tools
Traditional Load Testing Tools
System Software Assessment Tools
Operating System Protection Tools
Fingerprinting Tools
Port Scanning Tools
Directory and File Access Control Tools
File Share Scanning Tools
Password Directories
Password Guessing Tools
Link Checking Tools
Web site Crawlers
Web-Testing based Scripting Tools
Buffer Overflow Protection Tools

Penetration Testing - Part 2

File encryption Tools
Database Assessment Tools
Keyboard Logging and Screen Reordering Tools
System Event Logging and Reviewing Tools
Tripwire and Checksum Tools
Mobile-Code Scanning Tools
Centralized Security Monitoring Tools
Web Log Analysis Tools
Forensic Data and Collection Tools
Security Assessment Tools
Multiple OS Management Tools
Penetration Testing Deliverable Templates

Related Courses, Certifications, Exams

- EC Council Certified Network Defense Architect
- 312-99 - Certified Network Defense Architect

New Horizons Dubai
+971 4 3962222
New Horizons Dubai, 201 - Business Center, Standard Chartered Building
PO Box 37022, Dubai

Contact Us
courses.dubai@newhorizons.com
www.newhorizons.ae