

Certified Ethical Hacking Introduction

Length: 1 Day

Course Content

INTRODUCTION TO ETHICAL HACKING

- Internet Crime Current Report: IC3
- Data Breach Investigations Report
- Types of Data Stolen From the Organizations
- Essential Terminologies & Elements of Information Security
- Authenticity and Non-Repudiation
- The Security, Functionality, and Usability Triangle
- Security Challenges
- Effects of Hacking & Effects of Hacking on Business
- Who is a Hacker?
- Hacker Classes & Hacktivism
- What Does a Hacker Do?
- Phase 1 - Reconnaissance & Reconnaissance Types
- Phase 2 - Scanning
- Phase 3 – Gaining Access
- Phase 4 – Maintaining Access
- Phase 5 – Covering Tracks
- Types of Attacks on a System: Operating System Attacks, Application-Level Attacks, Shrink Wrap Code Attacks, & Misconfiguration Attacks
- Why Ethical Hacking is Necessary? What Do Ethical Hackers Do?
- Defense in Depth
- Scope and Limitations of Ethical Hacking
- Skills of an Ethical Hacker
- Vulnerability Research & Vulnerability Research Websites
- What is Penetration Testing? Why Penetration Testing?
- Penetration Testing Methodology

FOOTPRINTING AND RECONNAISSANCE

- Footprinting Terminologies & Objectives of Footprinting
 - What is Footprinting?
 - Footprinting Threats
 - Finding a Company's URL
 - Locate Internal URLs
 - Public and Restricted Websites
 - Search for Company's Information & Tools to Extract Company's Data
 - Footprinting Through Search Engines
 - Collect Location Information & Satellite Picture of a Residence
 - People Search
 - Gather Information from Financial Services
 - Footprinting Through Job Sites
 - Monitoring Target Using Alerts
 - Competitive Intelligence Gathering
 - WHOIS Lookup: Result Analysis, SmartWhois, Tools, & Online Tools
 - Extracting DNS Information
 - DNS Interrogation Tools & Online Tools
 - Locate the Network Range
 - Traceroute & Traceroute Analysis
 - Traceroute Tools: 3D Traceroute, LortotPro, & Path Analyzer Pro
 - Mirroring Entire Website & Website Mirroring Tools
 - Extract Website Information from <http://www.archive.org>
 - Monitoring Web Updates Using Website Watcher
 - Tracking Email Communications & Email Tracking Tools
 - Footprint Using Google Hacking Techniques
 - What a Hacker Can Do With Google Hacking?
-

- Google Advance Search Operators & Finding Resources using Google Advance Operator
- Google Hacking Tools: Google Hacking Database (GHDB)
- Additional Footprinting Tools, Countermeasures, & Pen Testing

SCANNING NETWORKS

- Network Scanning & Other Types of Scanning
 - Checking for Live Systems - ICMP Scanning
 - Ping Sweep & Ping Sweep Tools
 - Three-Way Handshake
 - TCP Communication Flags & Create Custom Packet using TCP Flags
 - Hping2 / Hping3 & Hping Commands
 - Scanning Techniques & IDS Evasion Techniques
 - IP Fragmentation Tools
 - Scanning Tools: Nmap, NetScan Tools Pro
 - Do Not Scan These IP Addresses (Unless you want to get into trouble)
 - Scanning Countermeasures
 - War Dialing
 - Why War Dialing?
 - War Dialing Tools
 - War Dialing Countermeasures & SandTrap Tool
 - OS Fingerprinting, Active Banner Grabbing Using Telnet & Banner Grabbing Tool: ID Serve
 - GET REQUESTS
 - Banner Grabbing Tools: Netcraft
 - Banner Grabbing Countermeasures: Disabling or Changing Banner
 - Hiding File Extensions & Hiding File Extensions from Webpages
 - Vulnerability Scanning
 - Vulnerability Scanning Tools: Nessus, SAINT, & GFI LANGuard
 - Network Vulnerability Scanners
 - LANsurveyor
 - Network Mappers
 - Proxy Servers & Why Attackers Use Proxy Servers?
 - Use of Proxies for Attack
 - How Does MultiProxy Work?
 - Free Proxy Servers & Proxy Workbench
 - Proxifier Tool: Create Chain of Proxy Servers
 - SocksChain
 - TOR (The Onion Routing) & TOR Proxy Chaining Software
 - HTTP Tunneling Techniques & Why do I Need HTTP Tunneling?
 - Super Network Tunnel Tool
 - Httptunnel for Windows & Additional HTTP Tunneling Tools
 - SSH Tunneling
 - SSL Proxy Tool & How to Run SSL Proxy?
 - Proxy Tools
 - Anonymizers & Types of Anonymizers
 - Case: Bloggers Write Text Backwards to Bypass Web Filters in China
 - Text Conversion to Avoid Filters
 - Censorship Circumvention Tool: Psiphon
 - How Psiphon Works?
 - How to Check if Your Website is Blocked in China or Not?
 - G-Zapper
 - Anonymizer Tools
 - Spoofing IP Address
 - IP Spoofing Detection Techniques: Direct TTL Probes, IP Identification Number, TCP Flow Control Method
 - IP Spoofing Countermeasures
 - Scanning Pen Testing
-