4B. IT SECURITY

Certified Network Penetration Tester

1	Cyber Ethics
1.1	What is Hacking?
1.2	Who is a Hacker?
1.3	Who is an Ethical Hacker?
1.4	What is Cracking?
1.5	Who is a Cracker?
1.6	Types of Hackers
2	**Establishing the Base**
2.1	What is Information Security?
2.2	Information Security Goals
2.3	Five Principles to Remember
2.4	TCP/IP Stack Review
2.5	Network Security Basics
2.5.1	IP Address
2.5.2	MAC Address
2.5.3	Client & Server
2.5.4	Web Server
2.5.5	DNS Server
2.5.6	Network Devices
3	**Footprinting**
3.1	What is Footprinting?
3.2	Why is Footprinting Necessary?
3.3	WHOIS lookup
3.4	DNS Enumeration
3.5	DNS Interrogation
3.6	Network Reconnaissance
3.7	Footprinting Tools
3.7.1	Whois lookup, Wikto
3.7.2	Online Tools – Samspade, What is MyIP
3.7.3	DNS Enumerator – nslookup
3.7.4	Traceroute – Neo Trace, VisualRoute
3.7.5	Tracing Emails – VisualRoute Mail Tracer, eMailTracker Pro

4 Scanning

4.1 Determining if the System is Alive
4.2 Determining which Services are Running or Listening
4.3 Scan Types
4.4 Identifying TCP and UDP Services Running
4.5 Windows-Based Port Scanners
4.6 Port Scanning Breakdown
4.7 Daemon Banner Grabbing
4.8 Firewall Detection
4.9 Detecting the Operating System
4.10 Active Stack Fingerprinting
4.11 Passive Stack Fingerprinting

5 Maintaining Anonymity

5.1 Proxy Servers
5.2 Anonymizers
5.3 Proxy Chaining- The Onion Routing (TOR)

6 Enumeration

6.1 Enumerating Remote Maintenance Services
6.2 Enumerating Remote Information Service
6.3 Enumerating Web Servers
6.4 Enumerating Database Services
6.5 Enumerating Mail Services
6.6 Enumerating Windows Networking Services
6.7 Tools- Nbtstat, Httprint, Wikto, Brutus, RpcScan

7 Google Hacking

7.1 Using google as a hacking tool
7.2 Google Searching with Advanced Operators
7.3 Directory Listings
7.4 Directory Traversal
7.5 Extension Walking
7.6 Network Mapping
7.7 Locating Vulnerable Targets
7.8 Searching for Usernames, Password & Secrets
7.9 Google Hacking Database (GHDB)
7.10 Tools- Site Digger, Google Hacks

8 Vulnerability Assessment

8.1 What are Vulnerabilities?
8.2 Categories of Vulnerabilities
8.2.1 Local
8.2.2 Remote
8.3 Types of System Vulnerabilities
8.3.1 Memory safety violation
8.3.1.1 Buffer Overflow
8.3.1.2 Heap overflow
8.3.2 Input validation errors
8.3.2.1 Format String
8.3.2.2 SQL injection
8.3.2.3 Code injection
8.3.2.4 E-mail injection
8.3.2.5 Directory traversal
8.3.2.6 Cross-site scripting in web applications
8.3.2.7 HTTP header injection
8.3.2.8 HTTP response splitting
8.3.3 Privilege-confusion
8.4 Scanning Tools- Superscan, Xprobe, Netcat, TOR, Nmap, GFI Languard, Nessus

9 Exploitation
9.1 Sniffing and ARP poisoning
9.2 Extracting and Cracking Passwords
9.3 Man-In-The-Middle Attack
9.4 Exploiting Network Services with Metasploit Framework
9.5 Privilege Escalation
9.6 Gaining Access to Remote Control
9.7 Maintaining Access to the Compromised Machine
9.8 Executing Applications
9.8.1 Key Loggers
9.8.2 Spywares
9.8.3 Trojans and Backdoors
9.9 Hiding and Covering the Tracks
9.10 Tools- Wireshark, Cain and Abel, Hydra, John the Ripper, Metasploit, VNC, Fpipe

10 Wireless Attacks
10.1 Introduction to Wireless Technology
10.2 Wired Network vs. Wireless Network
10.3 Types of Wireless Network
10.4 Types of Wireless Standards

11.3.2 OWASP Top 10 Vulnerabilities and Countermeasures
11.4 Attacking Authentication
11.4.1 Weak Authentication
11.4.2 Brute-Force Attacks
11.4.3 Exploiting Authentication – Live demonstration against a sample application
11.4.4 Countermeasures To Stop Authentication Attacks
11.5 Attacking Authorization
11.5.1 Broken Authorization
11.5.2 Attacking Broken Authorization – Live demonstration against a sample application
11.5.3 Preventing Authorization Attacks
11.6 Attacking Session Management
11.6.1 Session Fixation Attacks
11.6.2 Cookie Poisoning/Manipulation
11.6.3 Attacking Poor Session Management – Live demonstration against a sample application
11.6.4 Preventing Session Management Attacks
11.7 Injecting Code
11.7.1 Buffer Overflow - Live demonstration against a sample application
11.7.2 HTML Injection – Live demonstration against a sample application
11.7.3 Cross -Site Scripting (XSS) Attack – Live demonstration against a sample application
11.7.4 SQL Injection – Live demonstration against a sample application
11.7.5 OS Command Injection – Live demonstration against a sample application
11.7.6 Countermeasures
11.8 Error Handling/ Information Leakage
11.8.1 Exploiting Poor Error Handling – Live demonstration against a sample application
11.8.2 Preventing Information Leakage
11.9 Logging
11.9.1 Insecure Logging – Live demonstration against a sample application
11.9.2 Logging Best Practices

12 Social Engineering Attacks
12.1 Email Attacks
12.2 Browser Based Attacks
12.3 Software Targeted Attacks

Benefits

The Course educates participants on:

- ✓ The Methodology used to perform penetration testing
- ✓ How to compromise systems security
- ✓ How to utilize tools to exploit vulnerable systems

- ✓ How to apply countermeasures to protect an organization from exploitation

Target Audience

Windows administrators, UNIX/Linux administrators, Desktop Engineers, Network Engineers, IT Managers, other professionals who want to exploit & defend their network.

Mandatory Pre-requisites

The prospective participant should:

- ✓ Be familiar with both Windows and Linux operating systems
- ✓ Have an understanding of TCP/IP

Helpful Pre-requisites

Knowledge of Networking Protocols

Duration

12 Days