Penetration Testing

Index: **BT212**
Duration: **40 Hours**

Description
Penetration testers face with a combination of intrusion detection systems, host-based protection, hardened systems, and analysts that pour over data collected by their security information management systems.

Penetration tests help find flaws in the system to take appropriate security measures to protect the data and maintain functionality. This training will provide the student with a steppingstone on how to use it in practice and take on the complex and task of effectively measuring the entire attack surface of a traditionally secured environment.

Target Audience
- Security Analysts
- Risk Managers
- Security Officers
- System Managers
- Architects
- Penetration Testers

Pre-requisites
- ThinkCyber Level-1 courses

Objectives
- Becoming familiar with Penetration
- Testing existing security weaknesses
- Gathering information
- Bypass security and attack the network

Module 1: Planning and Collecting Information

Before the penetration testing team could start to analyze and conduct a series of tests and attacks, the team needs to gather data to construct a better plan of action. In this module, the student will go through the basics of information gathering and reconnaissance.

- **Passive Information Gathering**
  - The OSINT Framework
  - Monitoring Personal and Corporate Blogs
    - Collecting Employee Personal Information
    - Harvesting Organization Emails
  - Google-Dorks
- **Finding Web directories and files**
  - Using Brute-Forcing Techniques
  - Brute-Forcing Tools
    - Dirbuster
    - Dirb
  - Identifying Admin Pages
  - XSS and SQL Injections
  - Dictionary Attacks
  - Hybrid Attacks

Module 2: Identifying Vulnerabilities and Security analysis

After gaining the basic information about the network and employees, they can move on to scanning and gathering further intelligence on their target machines and systems. In this module, the students will learn the process of identifying possible exploits and making up an assessment of potential risks.

- **Active Information Gathering**
  - NMAP Ports Scanning
    - Port Identification
    - Scanning for OS Version
    - Uncovering Services Versions
    - Aggressive Scanning
  - DNS Enumeration
    - Dig and Host for Basic Queries
    - DNSrecon
    - DNS Zone Transfer
- **Identifying vulnerability and exploits**
  - NSE Scripting
  - Banner-Grabbing Methods
  - Vulnerabilities Detection Methods
  - Shodan Search Engine
  - Finding Exploits
    - Common Vulnerabilities and Exposures (CVE)
    - MITRE Database
    - Searchsploit
    - Exploit-Suggested
  - Github Tools
  - Automating the Scanning

Module 3: Gaining Access and Post-Exploitation

In this module, the students will learn to use the knowledge they gained in the first two phases to gain access, either using an existing exploit or by brute-forcing the way into the network. After gaining control of the target, the students will learn to abuse existing services to elevate their permissions.

- **Finding a way in**
  - Introduction to Metasploit Framework
    - Auxiliaries and Scanners
    - Exploit and Post-Exploitation
    - Privesc and Shell-Escapes
  - Social Engineering
    - Social Fish
    - SET Toolkit
  - Brute-forcing services
    - CUP and Crunch
    - Hydra Attacks
    - Crowbar
- **Gaining access through Wi-Fi**
  - Wi-Fi Basics
    - Four-Way Handshakes
    - Initializing Devices
  - Management and Monitor Modes
  - Gaining Access to the Network
    - Deauthing Targets
    - Capturing the Handshake
    - Handshake Brute-Force Techniques
  - Karma Attack (Evil-Twin)
- **Post Exploitation and Evidence gathering**
  - Basic Privilege Escalation
  - Using the Meterpreter Modules
    - Extracting User Credentials
    - Enumerating the Machine
  - Windows and Linux Privesc Basics
    - Enumeration of Services and Process
    - Understanding Permissions
    - Common Techniques
  - Network Pivoting

Module 4: Maintaining-Access and Covering Tracks

While gaining access to a system could be quite easy, maintaining control on the target without being noticed by the System Administrators would be hard. In this module, the students will learn how to use existing components on the network to maintain their control of the network. Also, the students will learn the basics of removing all semblance of detection.

- **Maintaining-Access**
  - Backdooring
    - Bind-Shell vs. Reverse-Shell
    - Backdoor-Factory
    - Metasploit Built-in Persistence and Metsvc
  - Advanced Netcat Usage
    - File Transferring
    - Spawning a Shell
  - Abusing Crontab and Bashrc
- **Covering Tracks**
  - Camouflaging the Backdoors
  - Detecting Log Collectors
    - Log Tampering
    - AuditPol
    - Elsave
    - Tracks Eraser Pro
  - Restoring the System to Order
- **Researching Security Solutions**
  - Creating Research Labs
    - Constructing the Environment
    - Crafting Trojans
    - Understanding AV Mechanism
    - AV Evasion Technics
    - Bypassing Security

Module 5: Penetration Testing Reporting

At last, the students will learn to conduct their reports based on their team findings; the students will present the evidence they have gathered through the previous stages; furthermore, this module will also teach possible fixes to some of the security flaws.

- **Writing Penetration Reports**
  - Describing the Information Gathering Process
  - Being Technical and Contextualized
  - Potential Impacts of Existing Vulnerabilities
  - Breaking Down the Risk
  - An Assessment of Potential Data Loss
  - Possible Remediation Options