Real Time College

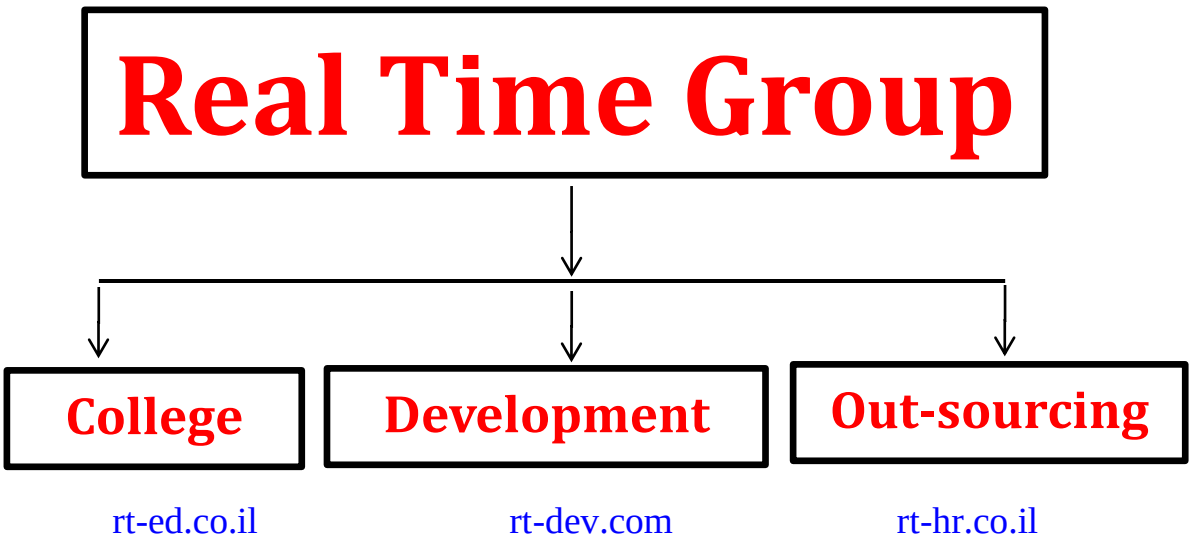
Course: Penetrating Testing

Duration: 50 Hours
Hands-On-Training: 50%

Real Time Group is a multi-disciplinary dynamic and innovative Real-Time O.S. and Software Solutions Center, established in 2007.

Providing Software, Security and Embedded Linux solutions, professional services and consulting, end-to-end flexible system infrastructure, outsourcing, integration and training services for Hardware, Software and RT-OS \ Embedded Systems.

The company is divided into the following three Divisions:



Training Division:

Professional Training Services for Software, Cyber Security, IT, RT-OS and Embedded systems industries.

We provide the knowledge and experience needed to enable professional engineers to Develop, Integrate and Automate Hardware, Software and Networking Projects.

To ensure experience, all courses are practical – Hands-On-Training.
The latest Development, Cyber Security, IT and Automation equipment which are adopted by the industry are used.

All students are supplied with necessary equipment (i.e. software license, AWS Account, etc) for Class -work \ Home-work and course projects.

Course Overview:

This **Penetrating Testing Course** is part of RT-Group's Cyber-Security Complete Track hand-on-training course, which provides the most complete and comprehensive Cyber Security Course.

This comprehensive Penetration Testing course explores web applications hacking & Bug Bounty hunting,
By the end of this course you'll know how to hack into websites and how to secure them. We'll discover, exploit and mitigate a number of dangerous web vulnerabilities, learn to Adopt SQL queries to discover and exploit SQL injections in secure pages, use SQL queries to find databases, tables and sensitive data such as usernames and passwords - Gain full control over target server.

We'll use Linux – as a penetration testing operating system, Learn Linux commands to unpublished directories & files associated with a target website. access server's file system (read/write files).

Who should attend:

- Student with no experience who wish to learn Cyber Security – **must first pass the Cyber Fundamentals Exam\Course**.
- Anyone interested in learning Ethical Hacking or Penetration Testing
- System\Linux Administrators wishing to upgrade their knowledge in Cyber Security.
- Architects \ Team Leaders \ Engineers \ Programmers who wish to participate in Cyber Security projects.

Prerequisite:

- Knowledge or experience in Networking is needed
- A medium level of computer literacy is expected, using a PC running Windows.
- Experience implementing scripts - Advantage.
- Experience in Linux or UNIX is necessary.

Cyber Penetration Testing

1. **Introduction to Penetration Testing**
   a. The Stages of the Penetration Test
   b. Pre-engagement
   c. Information Gathering
   d. Threat Modeling
   e. Vulnerability Analysis
   f. Exploitation
   g. Post Exploitation.

2. **Information Gathering**
   h. Open Source Intelligence Gathering
   i. Netcraft
   j. Who is Lookups
   k. DNS Reconnaissance.
   l. Searching for Email Addresses
   m. Manual Port Scanning
   n. Port Scanning with Nmap
   o. investigating TCP/IP Connections
   p. Check to See If a Port Is Listening

3. **Finding Vulnerabilities**
   a. Nessus Policies
   b. Scanning with Nessus
   c. Why Use Vulnerability Scanners
   d. Exporting Nessus Results
   e. Researching Vulnerabilities
   f. Running a Single NSE Script
   g. Metasploit Exploit Check Functions
   h. Web Application Scanning
   i. Nikto
   j. Default Credentials
   k. Manual Analysis
   l. Finding Valid Usernames

4. **Capturing Traffic**
    a. Networking for Capturing Traffic
    b. Using Wireshark
    c. Filtering Traffic
    d. Following a TCP Stream
    e. ARP Cache Poisoning
    f. IP Forwarding
    g. ARP Cache Poisoning with Arpspoof
    h. Using ARP Cache Poisoning to Impersonate the Default Gateway . . . . . .
    i. DNS Cache Poisoning
    j. Using Dns-spoof
    k. SSL Attacks
    l. Using Ettercap for SSL Man-in-the-Middle Attacks
    m. SSL Stripping

5. **Exploitation**
    a. Revisiting MS08-067
    b. Exploiting WebDAV Default Credentials
    c. Uploading a Msfvenom Payload
    d. Exploiting Open phpMyAdmin
    e. Downloading a File with TFTP
    f. Downloading the Windows SAM
    g. Exploiting a Buffer Overflow in Third-Party Software
    h. Exploiting Third-Party Web Applications
    i. Exploiting a Compromised Service
    j. Exploiting Open NFS Shares

6. **Password Attacks (Based on Timing Constraints)**
    a. Password Management
    b. Online Password Attacks
    c. Guessing Usernames and Passwords with Hydra
    d. Offline Password Attacks
    e. Recovering Password Hashes from a Windows SAM File
    f. Dumping Password Hashes with Physical Access
    g. LM vs. NTLM Hashing Algorithms
    h. The Trouble with LM Password Hashes
    i. Cracking Linux Passwords

7. **Social Engineering (Based on Timing Constraints)**
   a. The Social-Engineer Toolkit .
   b. Spear-Phishing Attacks .
   c. Exploiting a Payload .
   d. Setting the Target
   e. Setting Up a Listener
   f. Web Attacks
   g. Mass Email Attacks
   h. Multipronged Attacks

8. **Web Application Testing (Based on Timing Constraints)**
   i. Using Burp Proxy
   j. SQL Injection
   k. Testing for SQL Injection Vulnerabilities
   l. Exploiting SQL Injection Vulnerabilities
   m. Using SQL Map
   n. XPath Injection
   o. Local File Inclusion
   p. Remote File Inclusion
   q. Checking for a Reflected XSS Vulnerability
   r. Web Application Scanning with w3af