Ethical Hacking

Robotech Labs Private Limited

Ethical Hacking Workshop

The Workshop has been designed for the engineering students regardless of the branch a student belongs to.

The workshop helps the students to know about Ethical Hacking and Information security thereby giving them knowledge about Reading the Hacker's mind and Understanding the hacking psychology and methodology, Bluetooth Hacking ,Google Hacking, Scanning , Sniffing Email hacking , System hacking, Trojans, network applications, web server as a target and wireless hacking and lots more with proper demonstrations and practical work .

The workshop would be conducted by faculty having International Level Expertise in the field of Information Security and Ethical Hacking.

The Course would be **Certified as Information Security and Ethical Hacking Expert .**

Workshop Curriculum

PART I – Ethics

- **Why is Security needed?**
- **What is ethical hacking?**
- **Ethical Hacker vs Malicious Hacker**
- **Types of Hackers**
- **Building an approach for ethical hacking**

PART II – Google Hacking

- **What is Google?**
- **How does Google work?**
- **Google Tricks**
- **Basic Hacks**
- **Google Tools**
- **How can Google hacking help an ethical hacker?**
- **Preventing Google Crawls**

PART III – Scanning

- **What is Scanning?**
- **Objectives of Scanning**

- **Scanning Tools to be used:**
    - **Nmap**
    - **Null Scan**
    - **Firewalk**
    - **XMAS Scan**
    - **NIKTO**
    - **GFI Languard**

PART IV – Email Hacking

- **How does Email work?**
- **Tracing an Email**
- **Spam**
    - **What is Spamming?**
    - **Methods of Prevention**
    - **Laws about Spamming**
- **Fake Emails**
    - **Detecting Fake Emails**
    - **Tracing Server variables**

Part V – Trojans

- **Definition**
- **Legend**
- **Difference b/w Trojan, virus and worms**
- **Working of Trojans**
- **Server, Client, Direct & Reverse connections**
- **Trojans on WAN**
- **Problems – Dynamic IP**
- **NAT**
- **Using netcat as a Trojan**
- **Antivirus Detection process**
- **Social Engineering – Deploying Trojans**
- **Manual Detection**

Part VI – Session Hijacking

- **Understanding Sessions**
- **Passive vs. Active session hijack**
- **TCP sessions and HTTP sessions**
- **TCP session hijacking – Telnet**
- **Stealing Cookies to Hijack Session ID – XSS**

Part VII – PHP Injection

- **Understanding Sever side scripting**
- **Using code-injection to escalate privileges**
- **Briefings on PHP, ASP etc.**
- **Coding PHP shell**
- **Using PHP shells**
- **Exploiting file upload vulnerability**
- **PHP vulnerable functions and safe mode**
- **Prevention of code injection**

Part VIII – SQL Injection

- **Defining SQL**
- **Understanding web application**
- **Using SQL to login via middleware language**
- **Checking SQL Injection vulnerability**
- **URL and forms**
- **SQL query SELECT, DROP etc.**
- **SQL cheat sheets**
- **Using source changes to bypass client side validation**
- **PHP magic quotes**
- **Using SQL injection tools**
- **Importance of Server side validation**

Part IX – Sniffing

- **Introduction**
- **Active, Passive**
- **DNS, ARP**
- **Tools**
- **Wireshark, Ettercap Cain n Abel**
- **Detecting Sniffing**
- **DNS Poisoning**
- **Router Hacking**
- **Emulating WAN sniffing**

Part X – Broadband Hacking

- **Introduction: Broadband**
- **Using Default Passwords**
- **Special Trick: Hack any MTNL/BSNL/Airtel Broadband!**
- **Using Support Administrator Login**
- **Exploiting the Router**
- **Poisoning the Router**
- **Controlling User's Internet Access**
- **Getting to the System from the Router**

Part XI - Cryptography

• **Introduction to Cryptography**
• **Classical Cryptographic Techniques - Encryption/Decryption**
• **Cryptographic Algorithms**
• **RSA (Rivest Shamir Adleman)**
• **Data Encryption Standard (DES)**
• **One-way Bash Functions - MD5**
• **SHA (Secure Hash Algorithm)**
• **SSL (Secure Sockets Layer)**
• **What is SSH?**
• **SSH (Secure Shell)**
• **Cryptography Attacks**
vBrute-Force Attack
• **Cracking S/MIME Encryption Using Idle CPU Time**

Part XII – Social Networking Sites & Hacking

• **Impersonating Facebook**
• **MW.Orc worm**
• **Impersonating on Facebook**
• **How to Steal Identity**
• **Comparison**
• **Original**
• **Identity Theft**
• **http://www.consumer.gov/idtheft/**

Charges:

Rs 1200 per person

Duration
2 Days (14-16 Hours)

Certification:

Certificate of Appreciation from Robotech Labs Private Limited and our associates.

Requirements:
Seminar Hall, Projector, Sound System and Internet Connection.