SecuLabs

Backtrack Hacking

- Introduction to Backtrack Operating System
- Introduction to Metasploit Framework
- Foot printing and Enumeration
- Data and Information Gathering
- Network Scanning on Backtrack OS
- Exploiting Servers with Backtrack OS
- Hacking Windows 2000 With Backtrack OS
- Hacking Windows XP with Backtrack OS
- Hacking Windows Vista with Backtrack OS
- Hacking Windows Seven With Backtrack OS
- Hacking Windows 8 with Backtrack OS
- Introduction To Penetration Testing
- Overview of Penetrating Testing Tools
- Security and Network Scanning
- Cracking Wi-Fi (WEP, WPA, WPA2-PSK)
- Post Exploitation Hacking
- Cracking Word Dictionaries
- Buffer Overflow Attack
- DNS Hacking & DNS Enumeration
- DHCP Exploitation
- Sniffing and Session Hijacking
- Packet Capturing on Wireless Networks
- HTTP and HTTPS Sniffing on Wireless Networks
- Securing a LAN/MAN/WAN Network
- Network Card Exploitation
- Shell Scripting in Backtrack OS
- Meterpreter Hacking
- Java Applet Exploitation
- SMTP Scanning and Tracing
- WIFI Hacking With and Without Dictionary
- Ettercap Sniffing with Wireshark
- Network Analyzing
- Server and Client Side Attacks
- Make Own Payloads and Exploits
- Hacking Through IP Address

SecuLabs

Worm, Viruses & Trojans - Backdoors

- Introduction to Trojans, Worms & Viruses – **Construction Kit**
- Building & Writing the Trojans – **Including Registry & Java Based**
- Trojan Binding & Crypting – **Fully Undetectable**
- Making Fully Undetectable Trojans/Viruses/Worms – **Manually and Tool Based**
- Controlling the remote system from your system – **FTP & RDP Exploitation**
- Detection and removing of Trojan – **Including Identification of Viruses**
- Remote Administration Tools – **Windows and Linux Based – Including Macintosh RATs**
- Cryptography – **Encryption & Decryption Algorithms**
- Digital Certificates – **SHA, MD5, RSA, RC5, SSH, SSL Mechanisms**
- Firewalls & Honey pots – **Installation, Configuration & Managing IDS Based Systems**
- Physical Security & Financial Frauds – **Security & Protection from Phishing**

Attacks on Network

- LAN based attacks – **ARP Poisoning & Deploy Whole Network**
- Metasploit Framework – **In Backtrack Operating System – Command Line**
- Enumerating the network details – **Internet Host and Network Enumeration**
- Inside & Outside of the SET - **Social Engineering Toolkit – LINUX Based**
- Ettercap Sniffing – **Man in the Middle Attack**
- Sniffing the network data – **With or Without Client-Server Restrictions**
- Poisoning the network details and side jacking their credentials – **Network Dumping**
- Perform the DNS spoofing attack – **Including Web Debugging Proxy & ARP Spoofing**
- Trace the attacker on the LAN and shutting down the network attacks – **With Protection**
- Protection and security – **Including LAN & Wireless Networks**
- SYN Flooding & Ping of Death – **Denial of Service**
- Server Masking & IIS Vulnerabilities – **FTP Brute forcing Included**
- LAN Exploitation - Take Server Down/Disconnect

Website Exploitation & Security

- Breaking into Databases – **Input Validation Attacks**
- SQL Injection – **Error Based, String Based, Boolean Based, Blind Injection**
- Website Security - **Protection & Security**

- Cross Site Scripting– **XSS - Persistent & Non-Persistent**

- Remote & Local File Inclusion – **RFI and LFI Exploitation**
- Cross Site Request Forgery – **CSRF Detection and Prevention**
- Server Side Injection – **SSI Injection and Prevention**
- Placing backdoors in Websites – **Through Vulnerabilities**
- Exploiting ASP Based Servers – **DNN Dot Net Nuke**
- Advanced Phishing and its countermeasures – **Reporting, Protection & Security**
- Creating Backdoors & Shells – **Perl and Python Based**
- Google Dorks & Make your own Google Dorks - **GHDB**
- Review on Exploits& How to make an Exploit – **Exploit Writing**
- Live Camera Exploitation – **IP and DVR based**
- Denial of Service – **DOS Protection & Network Intrusion Prevention**
- Distributed Denial of Service – **DDOS Client & Server Side Protection**
- JDB Exploitation – **Java Drive Exploitation**
- Desktop Exploitation – **VNC Hijacking**
- Shell Uploading – **Through Vulnerabilities & Exploits**
- Apache and IIS Privileges – **Buffer Overflow Exploitation**
- Hacking Web Servers & Target Hacking – **Root Exploitation**
- Server Rooting & Mass Defacement – **NETCAT And Binding Ports**
- Wordpress & Joomla Exploitation – **Symlinking the Servers**
- Safe Mode Exploitation – **Config Web Killers**

Wireless Exploitation & Wireless Security

- Wi-Fi Packet Capturing & Session Hijacking – **Wireless Man in the Middle Attack**
- Fake Wireless Access Points - **In Backtrack Operating System**
- Wi-Fi Cracking – WEP / WPA-PSK / WPA2-PSK – **With or Without Clients**
- Introduction to Penetration Testing & Vulnerability Assessment – **Methodologies**
- Wireless DOS Attacks – **Client Deauthentication**
- WLAN Sniffers and Scanners – **Including MAC Sniffing**
- Securing Wireless Networks – **MAC Filtering & ESSID/BSSID Protection**
- Sniffing the Whole Traffic in a Wireless Network – **Wireshark**
- MAC Filtering & Netstumbler – **Mac Address Spoofing Linux Based**
- FTP/NFS/DNS/DHCP/SQUID/MAIL/SAMBA Servers – **Installation & Configuration**

Cyber Forensics & Mobile Exploitation

- SMS Spoofing & Bombing
- Call Spoofing & Tracing – **VOIP & SIP LINES**
- Bluetooth Hacking & Mobile Phone Exploitation
- Cyber Crime & Laws - **Overview**
- Cyber Forensics - **Overview**

Programming & Work Related

- **Make your own** Key loggers, Crypters, Trojans, Botnets, IP Loggers, Exploits
- Make your own Hacking Tools **(Basic + Advanced)**
- Make your own Servers **(VPN + VPS + Local + Proxy)**
- Maintain a Network Lab with 50 + Systems – **Server Administration**
- Reverse Engineering & Assembly Language **- Overview**
- Make your own Admin Panel Finding Scripts – **Perl & Python**
- Make your own Hacking Scripts – **Shell Backdooring & PHP Encryption/Decryption**
- Credit Card Frauds
- Securing Routers – **LAN & Wi-Fi Security**
- Burp Suite **– Walk through**
- Google Adsense via White Hat & Black Hat **– Search Engine Optimization**
- Review on **Cyber Forensics Tools**
- Computer Forensics – **SNORT Logs Analysis**
- Black Hat Hacking – **Sell/Buy Illegal Stuff**