LINUX LEARNING CENTRE LTD,
HURLINGHAM GROVE MAISONNETTES,
OFF ARGWINGS KODHEK ROAD,
P.O BOX 16939, 00100 NAIROBI, KENYA
PHONE : 0718722711 0734663771
EMAIL : info@linuxlearningcentre.co.ke
WEBSITE : www.linuxlearningcentre.co.ke

LLC 502 CYBERSECURITY AND ETHICAL HACKING II

COURSE OUTLINE

1. Malware Threats and Countermeasures

- Definition of Malware
- Trojan Concepts
- Virus and Worms Concepts
- Virus Analysis and Detection Methods
- Malware Reverse Engineering
- Sheep Dipping
- Malware Analysis
- Lab HTTP RAT Trojan
- Lab Monitoring TCP/IP connection using CurrPort tool

2. Sniffing and Countermeasures

- Introduction to Sniffing
- Working of Sniffers
- Types of Sniffing
- Hardware Protocol Analyzer
- SPAN Port and Wiretapping
- MAC Attacks and Defense
- DHCP Attacks and Defense
- ARP Poisoning and Defense
- DNS Poisoning Techniques and Defense
- Lab - Sniffing using Wireshark and Countermeasures
- Lab – Sniffing Detection Techniques

3. Phishing and Social Engineering Techniques

- Phishing versus Social Engineering
- Introduction to Social Engineering

- Phases of Social Engineering Attack
- Social Engineering Techniques
- Insider Attack, Impersonation and Identity Theft
- Lab – Social Engineering using KALI Linux
- Lab – Social Engineering Countermeasures

4. DoS and DDoS Attack Techniques and Countermeasures

- Denial of Service (DoS)
- Distributed Denial of Service (DdoS)
- DoS and DDoS Attack Techniques
- Botnet Setup
- Propagation of Malicious Codes
- Botnet Trojan
- DoS and DDoS Attack Tools
- Lab 1 – SYN Flooding Attack using Metasploit
- Lab 2 – SYN Flooding Attack using Hping3
- DoS and DdoS Attack Countermeasures

5. Web Server Attacks and Countermeasures

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Lab 1 – Web Server Footprinting
- Web Server Countermeasures
- Web Server Patch Management
- Lab 2 – Microsoft Baseline Security Analyzer (MBSA)
- Lab 3 – Web Server Security Tool

6. Web Application Attacks and Countermeasures

- Web Application Concepts
- Web Application Assessment Methodology
- Web Application Enumeration
- Web Application Assessment Tools using DIRB, Burp Suite and Nikto
- Exploiting Web-Based Vulnerabilities

- Web Application Attack Countermeasures

7. SQL Injection and Countermeasures

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- Evasion Techniques
- Lab 1 – Using IBM Security AppScan Standard

8. Session Hijacking and Countermeasures

- Session Hijacking
- Session Hijacking Techniques
- Session Hijacking Process
- Types of Session Hijacking
- Spoofing versus Hijacking
- Application Level Session Hijacking
- Networking-Level Session Hijacking
- Session Hijacking Countermeasures

9. Email Attacks and Countermeasures

- Email Header Analysis
- Email Attacks
- Email Hacking Tools
- Email Hacking Methodology
- Email Forensic Tools
- Lab 1 - Securing Emails with Encryption, Digital Signature and Pretty Good Privacy (PGP)
- Lab 2 - SSL and TLS for Secure Communication

10. Wireless Attacks and Countermeasures

- Wireless Networks
- Wi-Fi Technology
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Security Tools

- Lab 1 – Hacking Wi-Fi Protected Access Network using Aircrack-ng
- Lab 2 – Wireless Attacks Countermeasures

TARGET AUDIENCE

- Information Security Officers
- ICT Directors & Managers
- Finance Officers and Auditors
- Network Administrators
- System Administrators
- Database Administrators
- Software, Mobile and Application Developers

PREREQUISITE

- LLC 502 Cybersecurity and Ethical Hacking I
- LPIC 1 Linux System Administration Certification

CERTIFICATION EXAM CHALLENGE

- LLC 502 Cybersecurity and Ethical Hacking II Practical Exam