C|KLX

Certified Kali Linux Expert

Ducara Info Solutions (P) Ltd.

DUCARA

Why C|KLX?

Course Duration: 40 Hrs

This training session gives you an in depth understanding of how to use the Kali Linux with all features and functions.

This training reinforces the instruction by providing you with plenty of hands-on labs in which a wide range of network problems are closely examined.

Successfully achieving **Certified Kali Linux Expert** certification, a candidate will be able to discover the secrets of ethical hacking and network discovery, using Kali on this complete course.

It is used by all good ethical hackers, penetration testers, systems administrators, network analysts and anyone in fact who wants to discovery more about the security of a network and its hosts.

What is the Course Outcome?

The **C|KLX** certification training focuses to impart a deep and clear understanding of:

Assess

Assess network, server and system to drive towards sustainability and security.

Develop

Development of various policies reports and increased scrutiny of Audit practices.

Design

Design, develop, & build a leading and effective security framework, with appropriate policies, procedures, and resources in place.

Analyze

Analyze core elements of IT security components for providing best solutions for protecting information system against threats.

Implement

Check for strong password and learn to implement advanced architectural security techniques to secure wireless connections.

Who can get the Course benefits?

Auditors

Senior consultants, auditors and policy implementation professional at decision making level can get a quick reference to various techniques.

Pen-tester

Every Security Enthusiast/Learner with Essential knowledge of Cyber Security can go for C|KLX certification without doubt.

Security Analysts

This course is a perfect starting point for Information Security Professionals who want to learn penetration testing and ethical hacking.

What is the Course Outline?

Topics covered

1. Introduction to Kali Linux
2. Information Gathering
3. Network Scanning
4. Exploitation
5. Post Exploitation
6. Privilege Escalation
7. Wireless Exploitation
8. Exploitation of Web-based Applications
9. Exploiting Remote Access
10. Client-Side Attacks

Module 1: Introduction To Kali Linux

1. Kali Linux
2. Configuring Networks & Communications Security
3. How To Update Kali Linux
4. Configuring Kali Linux
5. Customizing Kali Linux
6. Third-party Applications
7. Penetration Testing Management

Module 2: Information Gathering

1. Active and Passive Reconnaissance
2. Principles of Reconnaissance
3. Open Source intelligence
4. WHOIS
5. DNS reconnaissance
6. Route-Distinguisher (RD) & Route-Target (RT)
7. gathering user information
8. Password Profiling

Module 3: Network Scanning

1. Stealth Port Scanning Methods
2. Network Infrastructure
3. Network Enumeration
4. Scanning Methodology
5. Using Nmap For Manual Vulnerability Assessment
6. Using Nmap With Metasploit
7. Vulnerability Scanning
8. Port Scanning
9. Ports In Networking
10. Service Discovery
11. OS Fingerprinting
12. Comprehensive Reconnaissance Tools

UCARA

Module 4: Exploitation

1. Threat Modeling Methodology
2. Exploit Using Metasploit Framework
3. Exploit A Vulnerable Target
4. Armitage Exploitation
5. Bypassing Detection Of Antivirus
6. Bypassing Detection Of Ids

Module 5: Post Exploitation

1. Engagement Rules Of Post Exploitation
2. Performing Infrastructure Analysis
3. Pillaging
4. Data Exfiltration
5. High Value Targets
6. Linux Post Exploitation Persistence
7. Cleaning Up Traces

Module 6: Privilege Escalation

1. What Is Privilege Escalation
2. Kernel Exploits
3. Applications & Services
4. Programs Running As Root
5. Exploiting SUID Executables
6. Exploiting Users With ‘.’ In Their PATH
7. Weak/Reused/Plaintext Passwords
8. File Systems
9. Exploiting SUDO Rights/User
10. Bad Path Configuration
11. CronJobs
12. Preparation & Finding Exploit Code

Module 7: Wireless Exploitation

1. Bypass WLAN Authentication
2. Cracking Wireless Encryptions
3. WLAN Infrastructure
4. Advanced Wireless Attacks Against Enterprise Networks
5. Wireless Client Attacks
6. Wi-Fi Worms, Backdoors And Botnets
7. Wi-Fi Attack Tools
8. Spectral Analysis
9. IoT Device

DUCARA

Module 8: Exploitation of Web-based Applications

1. Vulnerability Scanners
2. Client Application Security Testing
3. Server Vulnerability
4. Exploiting Server
5. Application Layer Attack
6. Maintaining Access With Web Backdoors

Module 9: Exploiting Remote Access

1. Exploiting Vulnerabilities In Communication Protocols
2. Exploiting Third-party Remote Access Software
3. SSL Attacks
4. IPSec VPN

Module 10: Client-Side Attacks

1. Hostile Scripts
2. XSS
3. BeeF
4. Integrating Metasploit With Browser Exploitation Framework
5. Tunneling With BeeF

Connect Us!

DUCARA

Ducara help harnessing latest security trends & enhancing skills to simplify IT security complexity efficiently.

info@ducarainfo.com ✉

www.ducarainfo.com 🌐