COURSE CONTENT
Duration: **100+ hours**

Introduction:
- Includes Ethical Hacking Course
- Difference between VA & PT
- Domains Of VAPT
- Types of VAPT
- Red Team vs Blue Team

Linux Essentials:
- History
- Lab Setup
- OS Architecture
- Basic Commands of Linux
- Basic Commands of Windows
- OS Auditing

Web Scanners:
- Acunetix
- Vega
- ZAP
- Nikto

Burp Suite:
- Dashboard
- Target
- Proxy
- Intruder
- Repeater
- Sequencer
- Decoder
- Comparer
- Extender
- Project Options

Web Enumeration:
- Whois lookup
- Reverse lookup
- IP history
- Detecting Backend Technology
- Directory Fuzzing
- Subdomain Enumeration
- Eyewitness
- Google Dorking
- Shodan

CMS Testing:
- CMS
- WPScan
- JoomScan
- CMSmap

OWASP Top 10:
- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control
- Security Misconfiguration
- Cross Site Scripting
- Insecure Deserialization
- Using Components with known vulnerabilities
- Insufficient Logging & Monitoring

Web Extreme Bugs:
- Subdomain Takeover
- Misconfigured S3 Buckets
- HTTP Parameter Pollution
- SSRF
- CSRF
- Local File Inclusion
- Remote File Inclusion
- Clickjacking

CTF:
- Introduction
- Methods to solve
- Lab Setup
- Intial Foothold and exploitation

Metasploit:
- Introduction
- Information Gathering
- Payloads
- Meterpreter
- Auxiliary
- Reporting

Web VAPT Reporting:
- Ways to report
- Formatting & Guidelines of report
- Case Study

Web Patch Management:
- Securing Webapps
- Applying Input Validations
- IP Whitelisting
- Implementing access control
- Removing HTTP Headers
- Preventing CSRF With Token
- Setting Login Limits

Bug Bounty Hunting:
- Bug Hunting
- Common vulneabilities neglected by testers
- Making Valid POCs

CTF Creation:
- Introduction
- Static Analysis
- Initial Configurations
- Understanding Of services
- Researching
- Implementation
- Clearing Loopholes

Fundamentals of Reverse Engineering:
- Introduction
- Debugging Tools
- Understanding of Assembly

Network VAPT:

- Network Infrastructure
- Information Gathering
- Nmap Scanning
- Nessus
- Backdoors
- Compromising Dcs
- Role of AD
- Post Exploitation
- AV Evasion
- Empire
- Powershell

Metasploit:

- Introduction
- Information Gathering
- Payloads
- Auxiliary
- Meterpeter
- Armitage

SOC & Threat Intelligence:

- Monitoring & Detection
- Log Monitoring

For Course Details

Contact us at 8074557618 (whats app)

Instagram: @cyberblockz_official

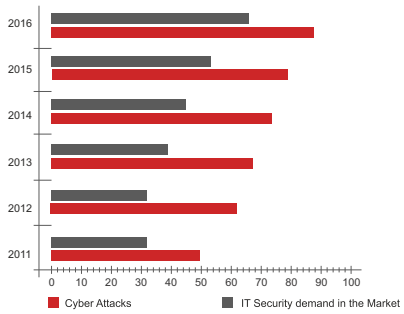
Check Youtube for Demo Class

JOB PROFILE

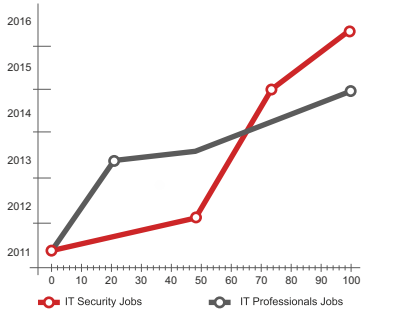
The penetration tester frequently works as a part of an information technology (IT) or cyber security team.

The kinds of jobs available are that of Network Security Engineer, System Security Manager, IT Security Auditor, IT Security Officers, Network Security Administrator, Web Security Administrator, Web Security Manager, Network Security Consultant, etc.

Cyber Attacks vs Demand for IT Security



IT Security Professionals vs IT Professionals Jobs



COURSE SPECIFICATIONS

Duration	100+ Hours
Batches	Regular / Weekends