

DIPLOMA IN

— — — — —
CYBER
SECURITY



CYBERYAAN
TRAINING & CONSULTANCY



Cyberyaan is a leading provider of cyber security services, offering a comprehensive range of solutions to help businesses protect themselves against cyber threats. With a team of experts in the field of cyber security, Cyberyaan provides businesses with the tools and knowledge they need to defend against cyber attacks.

we understand that each business has unique security needs, which is why we offer customized solutions tailored to each client's specific requirements. Our services include vulnerability assessments, penetration testing, incident response, security consulting, managed security services, and more.

Our team of experts is committed to staying up-to-date with the latest security technologies and best practices to ensure that we provide our clients with the most effective cyber security solutions.

Mr. Pankaj Yadav

CEO & Founder of Cyberyaan

Table of Content

▶ Networking Essentials	4
▶ Kali Linux	4
▶ Python Programming	4
▶ Ethical Hacking	5
▶ Network Penetration Testing	5
▶ Privilege Escalation Window Based	5
▶ Privilege Escalation Linux Based	6
▶ Active Directory	6
▶ Web Application Security	6
▶ Mobile Application Security	6
▶ SOC Fundamentals	7
▶ Splunk - Qradr - SIEM Tools Training	7
▶ ISO 27001 : 2022 Lead Auditor	7

|| Networking Essentials

- Introduction to Computer Network
- Network Topologies and Type
- IP Addressing
- Subnet Mask, Subnetting and CIDR
- VLSM, Wild Card, Summarization
- Networking Models
- OSI Model
- Networking Device, Cabling, Network Simulator Tools
- ARP and ICMP
- Packet Flow
- Routing - Static and Dynamic
- Static Routing - Next HOP IP & Exit Interface
- Dynamic Routing - RIP, EIGRP, & OSPF
- Remote Service Configuration
- DHCP Configuration
- ACLs
- Switching
- L2 Protocols - CDP, VLAN, STP, DTP, VTP
- Ether Channel
- Port Security

|| Kali Linux

- Introduction to Linux
- Setting up Lab
- Exploring Kali
- Sudo Overview
- Navigating the File System
- Basic Commands
- Creating, Viewing and Editing Text Files
- Managing Users and Group
- File Privileges / Permissions
- Linux Networking
- Process Management
- Services and Demons
- Log Analysis
- Archiving Files
- Debain Package Management
- Road Ahead - Towards Penetration Testing

|| Python Programming

- Introduction
- Set up
- Variables and Data Types
- Numbers
- String Formatting
- Booleans and Operators
- Tuples
- Lists
- Dictionaries
- Sets
- Conditionals
- Loops
- Reading and Writing Files
- User Input
- Exception and Error Handling
- Comprehensions
- Function and Code Reuse
- Lambdas
- The Python Package Manner
- Python Virtual Environment
- Introduction to Sys
- Introduction to Requests
- Introduction to Pwntools
- Projects

|| Ethical Hacking

- Networking Refresher
- Linux Refresher
- Introduction to Information Security
- Introduction to Ethical Hacking
- Foot printing / Information Gathering
- Scanning
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware and Threats
- Sniffing
- Social Engineering
- Denial of Service
- Session Hijacking
- IDS, IPS, and Firewalls
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Network
- Hacking Mobile Platforms
- Introduction to IOT
- Introduction to Cloud Computing
- Cryptography and Steganography

|| Network Penetration Testing

- Introduction to Kali Linux
- Command Line Fun
- Bash Scripting
- Passive Footprinting
- Active Footprinting
- Advanced Scanning
- Initial access CTFs
- Introduction to Linux Privilege Escalation
- Introduction to Windows Privilege Escalation
- Root Access CTFs
- Buffer overflow overview
- Antivirus Evasion
- Active Directory Overview
- Report Generation

|| Privilege Escalation (windows Based)

- Introduction to window privilege escalation
- Gaining Foothold
- Initial Enumeration
- Exploring Automated tools
- Kernel Exploits
- Password and Port Forwarding
- Windows subsystem for linux
- Impersonation and Potato attacks
- Getsystem
- Runas
- Registry
- Executables Files
- Startup Applications
- DLL Hijacking
- Service Permissions (paths)
- CVE 2019 – 1388
- Challenge

|| Privilege Escalation (Linux Based)

- Introduction to Linux Privilege Escalation
- Lab Overview
- Initial Enumeration
- Exploring Automated Tools
- Kernel Exploits
- Password and File Permissions
- Sudo
- SUID
- Capabilities
- Scheduled Tasks
- NFS Root Squashing
- Docker
- Challenge

|| Active Directory

- Introduction to Active Directory
- Active Directory Enumeration Principles
- External Reconnaissance
- Internal Enumerating and Footprinting
- Lateral Movement
- Enumerating and Exploiting Trusts
- Password Spraying
- LLMNR / NBT-NS Poisoning

|| Web Application Security

- Introduction to Web Application Security
- Setting up the Environment
- Reconnaissance and Scanning
- Exploitation Techniques
- Authentication and Session Management
- Advance Web Application Attacks
- Reporting and Remediation
- Legal and Ethical Consideration
- Practical Application
- Recape and Review

|| Mobile Application Security

- Introduction to Android Penetration Testing
- Setting Up Android Penetration Testing Environment
- Android Penetration Testing Methodologies
- Lab Setup Design
- Traditional Android Penetration Testing Report
- Traditional Android PT Approach & Guidelines
- Android Attack Surface – Client-Side Vulnerabilities
- Vulnerable Android Application Source Code Review
- Structure an Android Application Package (APK)
- Reversing an Android application using dex2jar
- Reversing an Android application using apktools
- Signing an Android Applications Manually
- Android Code Obfuscation & Code Protection

- Android Attack Surface - Server-Side Vulnerabilities
- Android Attack Surface Logical Security Threats
- Owasp Mobile Top 10
- Setup Android Debug Bridge Utility (adb)
- Adding Malicious Code to Android Apps
- Debugging Detection
- Root Detection
- VM Detection
- iOS Application Basic Standards

|| SOC Fundamentals

- Risk Management and Security
- Cyber Threats and Attack Patterns
- Incidents, Events and logging
- Security Incident and Recovery with SIEM
- Advanced Threat Detection and Analysis
- Security Event Response and Resolution

|| Splunk Fundamentals | Qradr SIEM | Tools

- Introduction to Splunk
- Installing and Configuring Splunk
- Searching and Reporting in Splunk
- Indexing and Data
- Splunk Search Language (SPL)
- Creating Dashboards and Visualization
- Alerts and Notification
- Splunk Administration and Security
- Splunk App Development
- Splunk Enterprise Security

|| ISO 27001 : 2022 Lead Auditor

- Fundamental concepts and principles of information security
- ISO/IEC 27001 certification process
- Information Security Management System (ISMS)
- The ISO/IEC 27000 family of standards
- Advantages of ISO/IEC 27001
- Fundamental of information and assets
- Fundamental principles of information security confidentiality, integrity, and availability

CYBERYAAN
TRAINING & CONSULTANCY

CYTC SECURITY PRIVATE LIMITED

1/4 single storey, 3rd floor
near vishal mega mart, tilak nagar
new delhi, 110018

 www.cyberyaan.in  info@cyberyaan.in

 +91 9560663331 | 7428748576

