CYBERYAAN

TRAINING & CONSULTANCY

Network Vulnerability Testing Program

Website – www.cyberyaan.com

Email Id – Info@cyberyaan.com

CYBERYAAN

TRAINING & CONSULTANCY

Module 1 : Networking Essentials

1.1 : Introduction to Computer Network
1.2 : Network Topologies and Type
1.3 : IP Addressing
1.4 : Subnet Mask, Subnetting and CIDR
1.5 : VLSM, Wild Card, Summarization
1.6 : Networking Models
1.7 : OSI Model
1.8 : Networking Device, Cabling, Network Simulator Tools

CYBERYAAN
TRAINING & CONSULTANCY

Module 1 : Networking Essentials

1.9 : ARP and ICMP
1.10 : Packet Flow
1.11 : Routing – Static and Dynamic
1.12 : Static Routing – Next HOP IP and Exit Interface
1.13 : Dynamic Routing - RIP, EIGRP and OSPF
1.14 : Remote Service Confriguration
1.15 : DHCP Configuration
1.16 : ACLs

CYBERYAAN
TRAINING & CONSULTANCY

Module 1 : Networking Essentials

1.17 : Switching
1.18 : L2 Protocols - CDP, VLN, STP, DTP, VTP
1.19 : Ether Channel
1.20 : Port Security

CYBERYAAN
TRAINING & CONSULTANCY

Module 2 : Kali - Linux

2.1 : Introduction to linux
2.2 : Setting Up Lab
2.3 : Exploring Kali
2.4 : Sudo Overview
2.5 : Navigating the file system
2.6 : Basic Commands
2.7 : Creating, Viewing and Editing text Files
2.8 : Managing users and Group

CYBERYAAN

TRAINING & CONSULTANCY

Module 2 : Kali - Linux

2.9 : File Privileges and Permissions
2.10 : Linux Networking
2.11 : Process Management
2.12 : Services and Demos
2.13 : Log Analysis
2.14 : Archiving Files
2.15 : Debain Package Management
2.16 : Road Ahead – Towards Penetration Testing

CYBERYAAN

TRAINING & CONSULTANCY

Module 3 : Python Programming

3.1 : Introduction
3.2 : Set Up
3.3 : Variables and data types
3.4 : Numbers
3.5 : String formatting
3.6 : Booleans and Operators
3.7 : Tuples
3.8 : Lists

CYBERYAAN

TRAINING & CONSULTANCY

Module 3 : Python Programming

3.9 : Dictionaries
3.10 : Sets
3.11 : Conditionals
3.12 : Loops
3.13 : Reading and Writing
3.14 : User Input
3.15 : Exception and Error Handling
3.16 : Comprehensions

CYBERYAAN

TRAINING & CONSULTANCY

Module 3 : Python Programming

3.17 : Functions and Code Resuse
3.18 : Lambdas
3.19 : The Python Package Manner
3.20 : Python Virtual Enviornment
3.21 : Introduction to Sys
3.22 : Introduction to request
3.23 : Introduction to pwntools
3.24 : Projects

CYBERYAAN
TRAINING & CONSULTANCY

Module 4 : Ethical Hacking

4.1 : Networking Refresher
4.2 : Linux Refresher
4.3 : Introduction to Information Security
4.4 : Introduction to Ethical Hacking
4.5 : Foot Printing / Information Gathering
4.6 : Scanning
4.7 : Enumeration
4.8 : Vulnerabilities Analysis

CYBERYAAN

TRAINING & CONSULTANCY

Module 4 : Ethical Hacking

4.9 : System Hacking
4.10 : Malware and Threats
4.11 : Sniffing
4.12 : Social Engineering
4.13 : Denial of Service
4.14 : Session Hijacking
4.15 : IDS, IPS and Firewalls
4.16 : Hacking Web Servers

CYBERYAAN
TRAINING & CONSULTANCY

Module 4 : Ethical Hacking

4.17 : Hacking Web Applications
4.18 : SQL Injection
4.19 : Hacking Wireless Network
4.20 : Hacking Mobile Platforms
4.21 : Introduction to IOT
4.22 : Introduction to cloud computing
4.23 : Cryptography and Steganography

CYBERYAAN

TRAINING & CONSULTANCY

Module 5 : Network Penetration Testing

5.1 : Introduction to Kali Linux
5.2 : Command Line Fun
5.3 : Bash Scripting
5.4 : Passive Footprinting
5.5 : Active Footprinting
5.6 : Advanced Scanning
5.7 : Initial access CTFs
5.8 : Introduction to Linux Privilege Escalation

CYBERYAAN

TRAINING & CONSULTANCY

Module 5 : Network Penetration Testing

5.9 : Introduction to Windows Privilege Escalation
5.10 : Root Access CTFs
5.11 : Buffer overflow overview
5.12 : Antivirus Evasion
5.13 : Active Directory Overview
5.14 : Report Generation

CYBERYAAN

TRAINING & CONSULTANCY

Module 6 : Privilege Escalation (Linux Privilege Escalation)

6.1 : Introduction to Linux Privilege Escalation
6.2 : Lab Overview
6.3 : Initial Enumeration
6.4 : Exploring Automated Tools
6.5 : Kernel Exploits
6.6 : Password and File Permissions
6.7 : Sudo
6.8 : SUID

CYBERYAAN

TRAINING & CONSULTANCY

Module 6 : Privilege Escalationv (Linux Privilege Escalation)

6.9 : Capabilities
6.10 : Scheduled Tasks
6.11 : NFS Root Squashing
6.12 : Docker
6.13 : Challenge

CYBERYAAN

TRAINING & CONSULTANCY

Module 6 : Privilege Escalation (Windows Privilege Esclation)

6.1 : Introduction to window privilege escalation
6.2 : Gaining Foothold
6.3 : Initial Enumeration
6.4 : Exploring Automated tools
6.5 : Kernel Exploits
6.6 : Password and Port Forwarding
6.7 : Windows subsystem for linux
6.8 : Impersonation and Potato attacks

CYBERYAAN

TRAINING & CONSULTANCY

Module 6 : Privilege Escalation (Windows Privilege Esclation)

6.9 : Getsystem
6.10 : Runas
6.11 : Registry
6.12 : Executables Files
6.13 : Startup Applications
6.14 : DLL Hijacking
6.15 : Service Permissions (paths)
6.16 : CVE 2019 – 1388
6.17 : Challenge

CYBERYAAN

TRAINING & CONSULTANCY

Module 7 : Active Directory

7.1 : Introduction to Active Directory
7.2 : Active Directory Enumeration Principles
7.3 : External Reconnaissance
7.4 : Internal Enumerating and Footprinting
7.5 : Lateral Movement
7.6 : Enumerating and Exploiting Trusts
7.7 : Password Spraying
7.8 : LLMNR / NBT-NS Poisioning

CYBERYAAN

TRAINING & CONSULTANCY

Module 7 : Active Directory

7.9 : Gaining Privileged Access
7.10 : Using Native Tools to perform actions
7.11 : Kerberoasting
7.12 : Performing ACL Attacks
7.13 : Active Directory Hardening Principles

CYBERYAAN
TRAINING & CONSULTANCY

Training Duration : 280 to 320 Hrs
Training Mode : Online and Offline

Important Notes :
1. Laptop is Mandatory
2. Fees is 70000 + 18% Gst (CEH Practical Exam Voucher Included)
3. Instalment Date is before of 10th of Every Month.
4. Late Fees is applicable – 1000

Website – www.cyberyaan.com

Email Id – Info@cyberyaan.com

CYBERYAAN

TRAINING & CONSULTANCY

Contact Us

¼, Single Storey, 3rd Floor, Near Vishal Mega Mart, Tilak Nagar, New Delhi – 110018

Follows

Instagram : @_cyberyaan_

LinkedIn : Cyberyaan Training and Consultancy

Website – www.cyberyaan.com

Email Id – info@cyberyaan.com