3D EDUCATORS
Trainers & Consultants

CYBRON– OFFENSIVE PENETRATION TESTING CERTIFIED PROFESSIONAL

Training Program

Who can do?

- Security Professionals who are transition to pen testing.
- Pen testers
- Lead Security Professional
- Network Administrators
- Other technology Professionals
- And those who would like to develop their career in the field of pen testing

100,000+ Students have been Trained since 1997

Invest in People the only Asset that Appreciates

Program is offered by

3D EDUCATORS - INT

22 Years of Excellence in Training & Development

www.3dedudcators.com
info@3deducators.com

CYBRON– OFFENSIVE PENETRATION TESTING CERTIFIED PROFESSIONAL

Course Objective:

The Cybron - -Offensive Penetration Testing Certified Professional with Kali Linux just got even better with the addition of five recently retired penetration testing techniques. Avail more value able out of your lab time, and enjoy extra preparation with Kali Linux.

This course is comprises lots of labs related to the ethical hacking and complete course is live online with certified instructors. It introduces penetration testing tools and techniques via hands-on experience. Its increase your capability and mindset required to be successful penetration tester.

Learn and earn the Cybron Offensive Penetration Testing Certified Professional with hands-on experience and skills.

CYBRON– OFFENSIVE
PENETRATION TESTING
CERTIFIED PROFESSIONAL

Table of Content

CYBRON– OFFENSIVE
PENETRATION TESTING
CERTIFIED PROFESSIONAL

Program Details

Inauguration

The Training Program will be inaugurated by a senior member of 3DEducators

Program Structure

No of classes per week	**02 - Class**
Duration of each class	**03 - Hour**
Total Duration	**60-Hours**

Other Learning Activities

Classroom Assignments	**16**
Presentations by Trainees	**01**

About the Program Instructor

The "Cybron – Offensive Penetration Testing Certified Professional" Program conducted by Certified Consultant & Professionals, who having the vast experience of training and information security consulting services. They have worked with various large Government, National, and multinational organizations locally and abroad.

The Trainers who are conducting this program have are on the position of the following:

- ✓ CIO
- ✓ CISO
- ✓ Lead Security Managers

They trainers are foreign qualified and having the International certification of information Security.

As Consultant & Senior Trainers the team of trainers from Engineering side we 3D Educators – Trainers & Consultants would not compromise on the faculty.

In Affiliation with

CYBRON– OFFENSIVE PENETRATION TESTING CERTIFIED PROFESSIONAL

COURSE OUTLINE:

1 Penetration Testing with Kali Linux: General Course Information
- 1.1 About the PWK Course
- 1.1.1 PWK Course Materials
- 1.1.2 Access to the Internal VPN Lab Network
- 1.1.3 The Offensive Security Student Forum
- 1.1.4 Live Support
- 1.1.5 OSCP Exam Attempt

1.2 Overall Strategies for Approaching the Course
- 1.2.1 Welcome and Course Information Emails
- 1.2.2 Course Materials
- 1.2.3 Course Exercises
- 1.2.4 PWK Labs

1.3 Obtaining Support

1.4 About Penetration Testing

1.5 Legal

1.6 The MegaCorpone.com and Sandbox.local Domains

1.7 About the PWK VPN Labs
- 1.7.1 Lab Warning
- 1.7.2 Control Panel
- 1.7.3 Reverts
- 1.7.4 Client Machines
- 1.7.5 Kali Virtual Machine
- 1.7.6 Lab Behavior and Lab Restrictions

1.8 Reporting

- 1.8.1 Consider the Objective
- 1.8.2 Consider the Audience
- 1.8.3 Consider What to Include
- 1.8.4 Consider the Presentation
- 1.8.5 The PWK Report
- 1.8.6 Note Taking

1.9 About the OSCP Exam

- 1.9.1 Metasploit Usage - Lab vs Exam

1.10 Wrapping Up

2 Getting Comfortable with Kali Linux

- 2.1 Booting Up Kali Linux
- 2.2 The Kali Menu
- 2.3 Kali Documentation
  - 2.3.1 The Kali Linux Official Documentation
  - 2.3.2 The Kali Linux Support Forum
  - 2.3.3 The Kali Linux Tools Site
  - 2.3.4 The Kali Linux Bug Tracker
  - 2.3.5 The Kali Training Site
  - 2.3.6 Exercises

- 2.4 Finding Your Way Around Kali
  - 2.4.1 The Linux Filesystem
  - 2.4.2 Basic Linux Commands
  - 2.4.3 Finding Files in Kali Linux

2.5 Managing Kali Linux Services

2.5.1 SSH Service

2.5.2 HTTP Service

2.5.3 Exercises

2.6 Searching, Installing, and Removing Tools

2.6.1 apt update

2.6.2 apt upgrade

2.6.3 apt-cache search and apt show

2.6.4 apt install

2.6.5 apt remove –purge

2.6.6 dpkg

2.7 Wrapping Up

3 Command Line Fun

3.1 The Bash Environment

3.1.1 Environment Variables

3.1.2 Tab Completion

3.1.3 Bash History Tricks

3.2 Piping and Redirection

3.2.1 Redirecting to a New File

3.2.2 Redirecting to an Existing File

3.2.3 Redirecting from a File

3.2.4 Redirecting STDERR

3.2.5 Piping

3.3 Text Searching and Manipulation
- 3.3.1 grep
- 3.3.2 sed
- 3.3.3 cut
- 3.3.4 awk
- 3.3.5 Practical Example

3.4 Editing Files from the Command Line
- 3.4.1 nano
- 3.4.2 vi

3.5 Comparing Files
- 3.5.1 comm
- 3.5.2 diff
- 3.5.3 vimdiff

3.6 Managing Processes

- 3.6.1 Backgrounding Processes (bg)
- 3.6.2 Jobs Control: jobs and fg
- 3.6.3 Process Control: ps and kill

3.7 File and Command Monitoring

- 3.7.1 tail
- 3.7.2 watch

3.8 Downloading Files
- 3.8.1 wget
- 3.8.2 curl
- 3.8.3 axel

3.9 Customizing the Bash Environment
- 3.9.1 Bash History Customization
- 3.9.2 Alias

3.9.3 Persistent Bash Customization

3.10 Wrapping Up

4 Practical Tools

4.1 Netcat
- 4.1.1 Connecting to a TCP/UDP Port
- 4.1.2 Listening on a TCP/UDP Port
- 4.1.3 Transferring Files with Netcat
- 4.1.4 Remote Administration with Netcat

4.2 Socat
- 4.2.1 Netcat vs Socat
- 4.2.2 Socat File Transfers
- 4.2.3 Socat Reverse Shells
- 4.2.4 Socat Encrypted Bind Shells

4.3 PowerShell and Powercat
- 4.3.1 PowerShell File Transfers
- 4.3.2 PowerShell Reverse Shells
- 4.3.3 PowerShell Bind Shells
- 4.3.4 Powercat
- 4.3.5 Powercat File Transfers
- 4.3.6 Powercat Reverse Shells
- 4.3.7 Powercat Bind Shells
- 4.3.8 Powercat Stand-Alone Payloads

4.4 Wireshark
- 4.4.1 Wireshark Basics
- 4.4.2 Launching Wireshark
- 4.4.3 Capture Filters
- 4.4.4 Display Filters
- 4.4.5 Following TCP Streams

4.5 Tcpdump
- 4.5.2 Filtering Traffic
- 4.5.3 Advanced Header Filtering

4.6 Wrapping Up

5 Bash Scripting
- 5.1 Intro to Bash Scripting
- 5.2 Variables
- 5.2.1 Arguments
- 5.2.2 Reading User Input

5.3 If, Else, Elif Statements

5.4 Boolean Logical Operations

5.5 Loops
- 5.5.1 For Loops
- 5.5.2 While Loops

5.6 Functions
- 5.7 Practical Examples
- 5.7.1 Practical Bash Usage – Example 1
- 5.7.2 Practical Bash Usage – Example 2
- 5.7.3 Practical Bash Usage – Example 3

5.8 Wrapping Up

6 Passive Information Gathering
- 6.1 Taking Notes
- 6.2 Website Recon

- 6.3 Whois Enumeration
    - 6.4 Google Hacking
    - 6.5 Netcraft
    - 6.6 Recon-ng
    - 6.7 Open-Source Code
- 6.8 Shodan
- 6.9 Security Headers Scanner
- 6.10 SSL Server Test
- 6.11 Pastebin
- 6.12 User Information Gathering
    - 6.12.1 Email Harvesting
    - 6.12.2 Password Dumps
- 6.13 Social Media Tools
    - 6.13.2 Site-Specific Tools
- 6.14 Stack Overflow
- 6.15 Information Gathering Frameworks
    - 6.15.1 OSINT Framework
    - 6.15.2 Maltego
- 6.16 Wrapping Up
- 7 Active Information Gathering
    - 7.1 DNS Enumeration
    - 7.1.1 Interacting with a DNS Server
    - 7.1.2 Automating Lookups
    - 7.1.3 Forward Lookup Brute Force
    - 7.1.4 Reverse Lookup Brute Force

- 7.1.5 DNS Zone Transfers
- 7.1.6 Relevant Tools in Kali Linux

7.2 Port Scanning

- 7.2.1 TCP / UDP Scanning

7.2.2 Port Scanning with Nmap

7.2.3 Masscan

7.3 SMB Enumeration

- 7.3.1 Scanning for the NetBIOS Service

7.2 Port Scanning

- 7.2.1 TCP / UDP Scanning

7.2.2 Port Scanning with Nmap

7.2.3 Masscan

7.3 SMB Enumeration

- 7.3.1 Scanning for the NetBIOS Service

- 7.3.2 Nmap SMB NSE Scripts

7.4 NFS Enumeration

- 7.4.1 Scanning for NFS Shares
- 7.4.2 Nmap NFS NSE Scripts

7.5 SMTP Enumeration

7.6 SNMP Enumeration

- 7.6.1 The SNMP MIB Tree
- 7.6.2 Scanning for SNMP
- 7.6.3 Windows SNMP Enumeration Example

7.7 Wrapping Up

8 Vulnerability Scanning

8.1 Vulnerability Scanning Overview and Considerations
- 8.1.1 How Vulnerability Scanners Work
- 8.1.2 Manual vs. Automated Scanning
- 8.1.3 Internet Scanning vs Internal Scanning
- 8.1.4 Authenticated vs Unauthenticated Scanning

8.2 Vulnerability Scanning with Nessus
- 8.2.1 Installing Nessus
- 8.2.2 Defining Targets
- 8.2.3 Configuring Scan Definitions

- 8.2.4 Unauthenticated Scanning With Nessus
- 8.2.5 Authenticated Scanning With Nessus
- 8.2.6 Scanning with Individual Nessus Plugins

8.3 Vulnerability Scanning with Nmap
8.4 Wrapping Up

9 Web Application Attacks
- 9.1 Web Application Assessment Methodology
- 9.2 Web Application Enumeration
- 9.2.1 Inspecting URLs
- 9.2.2 Inspecting Page Content
- 9.2.3 Viewing Response Headers
- 9.2.4 Inspecting Sitemaps
- 9.2.5 Locating Administration Consoles

- 9.3 Web Application Assessment Tools
  - 9.3.2 DIRB
  - 9.3.3 Burp Suite
  - 9.3.4 Nikto
- 9.4 Exploiting Web-based Vulnerabilities
  - 9.4.1 Exploiting Admin Consoles
  - 9.4.2 Cross-Site Scripting (XSS)
  - 9.4.3 Directory Traversal Vulnerabilities
  - 9.4.4 File Inclusion Vulnerabilities
  - 9.4.5 SQL Injection
- 9.5 Extra Miles
  - 9.5.1 Exercises
- 9.6 Wrapping Up

- 10 Introduction to Buffer Overflows
  - 10.1 Introduction to the x Architecture
  - 10.1.1 Program Memory
  - 10.1.2 CPU Registers
  - 10.2 Buffer Overflow Walkthrough
  - 10.2.1 Sample Vulnerable Code
  - 10.2.2 Introducing the Immunity Debugger
  - 10.2.3 Navigating Code
  - 10.2.4 Overflowing the Buffer
  - 10.2.5 Exercises
  - 10.3 Wrapping Up

11 Windows Buffer Overflows
- 11.1 Discovering the Vulnerability
- 11.1.1 Fuzzing the HTTP Protocol
- 11.2 Win Buffer Overflow Exploitation
- 11.2.1 A Word About DEP, ASLR, and CFG
- 11.2.2 Replicating the Crash
- 11.2.3 Controlling EIP
- 11.2.4 Locating Space for Our Shellcode
- 11.2.5 Checking for Bad Characters
- 11.2.6 Redirecting the Execution Flow
- 11.2.7 Finding a Return Address
- 11.2.8 Generating Shellcode with Metasploit
- 11.2.9 Getting a Shell
- 11.2.10 Improving the Exploit

- 11.2.3 Controlling EIP
- 11.2.4 Locating Space for Our Shellcode
- 11.2.5 Checking for Bad Characters
- 11.2.6 Redirecting the Execution Flow
- 11.2.7 Finding a Return Address
- 11.2.8 Generating Shellcode with Metasploit
- 11.2.9 Getting a Shell
- 11.2.10 Improving the Exploit

11.3 Wrapping Up

12 Linux Buffer Overflows
- 12.1 About DEP, ASLR, and Canaries
- 12.2 Replicating the Crash
- 12.3 Controlling EIP
- 12.4 Locating Space for Our Shellcode
- 12.5 Checking for Bad Characters
- 12.6 Finding a Return Address
- 12.7 Getting a Shell
- 12.8 Wrapping Up

13 Client-Side Attacks

13.1 Know Your Target
13.1.1 Passive Client Information Gathering
13.1.2 Active Client Information Gathering
13.2 Leveraging HTML Applications
13.2.1 Exploring HTML Applications
13.2.2 HTA Attack in Action

13.3 Exploiting Microsoft Office
13.3.1 Installing Microsoft Office
13.3.2 Microsoft Word Macro
13.3.3 Object Linking and Embedding
13.3.4 Evading Protected View
13.4 Wrapping Up

14 Locating Public Exploits

14.1 A Word of Caution
14.2 Searching for Exploits
14.2.1 Online Exploit Resources
14.2.2 Offline Exploit Resources
14.3 Putting It All Together
14.4 Wrapping Up

15 Fixing Exploits
15.1 Fixing Memory Corruption Exploits
15.1.1 Overview and Considerations
15.1.2 Importing and Examining the Exploit
15.1.3 Cross-Compiling Exploit Code
15.1.4 Changing the Socket Information
15.1.5 Changing the Return Address
15.1.6 Changing the Payload
15.1.7 Changing the Overflow Buffer

15.2 Fixing Web Exploits

- 15.2.1 Considerations and Overview
- 15.2.2 Selecting the Vulnerability
- 15.2.3 Changing Connectivity Information
- 15.2.4 Troubleshooting the “index out of range” Error

15.3 Wrapping Up

16 File Transfers

- 16.1 Considerations and Preparations
- 16.1.1 Dangers of Transferring Attack Tools
- 16.1.2 Installing Pure-FTPd
- 16.1.3 The Non-Interactive Shell

16.2 Transferring Files with Windows Hosts

- 16.2.1 Non-Interactive FTP Download
- 16.2.2 Windows Downloads Using Scripting Languages
- 16.2.3 Windows Downloads with exe2hex and PowerShell
- 16.2.4 Windows Uploads Using Windows Scripting Languages
- 16.2.5 Uploading Files with TFTP

16.3 Wrapping Up

17 Antivirus Evasion

- 17.1 What is Antivirus Software
- 17.2 Methods of Detecting Malicious Code
- 17.2.1 Signature-Based Detection
- 17.2.2 Heuristic and Behavioral-Based Detection
- 17.3 Bypassing Antivirus Detection
- 17.3.1 On-Disk Evasion
- 17.3.2 In-Memory Evasion
- 17.3.3 AV Evasion: Practical Example
- 17.4 Wrapping Up

18 Privilege Escalation

18.1 Information Gathering

18.1.1 Manual Enumeration

18.1.2 Automated Enumeration

18.2 Windows Privilege Escalation Examples

18.2.1 Understanding Windows Privileges and Integrity Levels

18.2.2 Introduction to User Account Control (UAC)

18.2.3 User Account Control (UAC) Bypass: fodhelper.exe Case Study

18.2.4 Insecure File Permissions: Serviio Case Study

18.2.5 Leveraging Unquoted Service Paths

18.2.6 Windows Kernel Vulnerabilities: USBPcap Case Study

18.3 Linux Privilege Escalation Examples

18.3.1 Understanding Linux Privileges

18.3.2 Insecure File Permissions: Cron Case Study

18.3.3 Insecure File Permissions: /etc/passwd Case Study

18.3.4 Kernel Vulnerabilities: CVE-7-2 Case Study

18.4 Wrapping Up

19 Password Attacks

19.1 Wordlists

19.1.1 Standard Wordlists

19.2 Brute Force Wordlists

19.3 Common Network Service Attack Methods

19.3.1 HTTP htaccess Attack with Medusa

19.3.2 Remote Desktop Protocol Attack with Crowbar

19.3.3 SSH Attack with THC-Hydra

19.3.4 HTTP POST Attack with THC-Hydra

- 19.4 Leveraging Password Hashes
    - 19.4.1 Retrieving Password Hashes
    - 19.4.2 Passing the Hash in Windows
    - 19.4.3 Password Cracking
    - 19.5 Wrapping Up

20 Port Redirection and Tunneling

- 20.1 Port Forwarding
    - 20.1.1 RINETD
- 20.2 SSH Tunneling
    - 20.2.1 SSH Local Port Forwarding
    - 20.2.2 SSH Remote Port Forwarding
    - 20.2.3 SSH Dynamic Port Forwarding
    - 20.3 PLINK.exe
- 20.4 NETSH
- 20.5 HTTPTunnel-ing Through Deep Packet Inspection
- 20.6 Wrapping Up

21 Active Directory Attacks

- 21.1 Active Directory Theory
- 21.2 Active Directory Enumeration
- 21.2.1 Traditional Approach
- 21.2.2 A Modern Approach
- 21.2.3 Resolving Nested Groups
- 21.2.4 Currently Logged on Users
- 21.2.5 Enumeration Through Service Principal Names
- 21.3 Active Directory Authentication

21.3.1 NTLM Authentication

21.3.2 Kerberos Authentication
21.3.3 Cached Credential Storage and Retrieval
21.3.4 Service Account Attacks
21.3.5 Low and Slow Password Guessing
21.4 Active Directory Lateral Movement
21.4.1 Pass the Hash
21.4.2 Overpass the Hash
21.4.3 Pass the Ticket
21.4.4 Distributed Component Object Model
21.5 Active Directory Persistence
21.5.1 Golden Tickets
21.5.2 Domain Controller Synchronization
21.6 Wrapping Up

22 The Metasploit Framework

22.1 Metasploit User Interfaces and Setup
22.1.1 Getting Familiar with MSF Syntax
22.1.2 Metasploit Database Access
22.1.3 Auxiliary Modules
22.2 Exploit Modules
22.2.1 SyncBreeze Enterprise

22.3 Metasploit Payloads
22.3.1 Staged vs Non-Staged Payloads
22.3.2 Meterpreter Payloads
22.3.3 Experimenting with Meterpreter
22.3.4 Executable Payloads
22.3.5 Metasploit Exploit Multi Handler
22.3.6 Client-Side Attacks
22.3.7 Advanced Features and Transports
22.4 Building Our Own MSF Module

- 22.5 Post-Exploitation with Metasploit
    - 22.5.1 Core Post-Exploitation Features
    - 22.5.2 Migrating Processes
    - 22.5.3 Post-Exploitation Modules
    - 22.5.4 Pivoting with the Metasploit Framework

- 22.6 Metasploit Automation

- 22.7 Wrapping Up

- 23 PowerShell Empire
    - 23.1 Installation, Setup, and Usage
        - 23.1.1 PowerShell Empire Syntax
        - 23.1.2 Listeners and Stagers
        - 23.1.3 The Empire Agent
    - 23.2 PowerShell Modules
        - 23.2.1 Situational Awareness
        - 23.2.2 Credentials and Privilege Escalation
        - 23.2.3 Lateral Movement
    - 23.3 Switching Between Empire and Metasploit

    - 23.4 Wrapping Up

- 24 Assembling the Pieces: Penetration Test Breakdown
    - 24.1 Public Network Enumeration
    - 24.2 Targeting the Web Application
    - 24.2.1 Web Application Enumeration
    - 24.2.2 SQL Injection Exploitation
    - 24.2.3 Cracking the Password
    - 24.2.4 Enumerating the Admin Interface
    - 24.2.5 Obtaining a Shell
    - 24.2.6 Post-Exploitation Enumeration
    - 24.2.7 Creating a Stable Pivot Point

- 24.3 Targeting the Database
    - 24.3.1 Enumeration
    - 24.3.2 Attempting to Exploit the Database
- 24.4 Deeper Enumeration of the Web Application Server
    - 24.4.1 More Thorough Post Exploitation
    - 24.4.2 Privilege Escalation
- 24.4.3 Searching for DB Credentials
- 24.5 Targeting the Database Again
    - 24.5.1 Exploitation
    - 24.5.2 Post-Exploitation Enumeration
    - 24.5.3 Creating a Stable Reverse Tunnel

- 24.6 Targeting Poultry
    - 24.6.2 Enumeration
    - 24.6.3 Exploitation (Or Just Logging In)
    - 24.6.4 Post-Exploitation Enumeration
    - 24.6.5 Unquoted Search Path Exploitation
    - 24.6.6 Post-Exploitation Enumeration

- 24.7 Internal Network Enumeration
    - 24.7.1 Reviewing the Results

- 24.8 Targeting the Jenkins Server
    - 24.8.1 Application Enumeration
    - 24.8.2 Exploiting Jenkins
    - 24.8.3 Post Exploitation Enumeration
    - 24.8.4 Privilege Escalation
    - 24.8.5 Post Exploitation Enumeration

- 24.9 Targeting the Domain Controller
    - 24.9.1 Exploiting the Domain Controller

24.10 Wrapping Up
25 Trying Harder: The Labs
- 25.1 Real Life Simulations
- 25.2 Machine Dependencies
- 25.3 Cloned Lab Machines
- 25.4 Unlocking Networks
- 25.5 Routing
- 25.6 Machine Ordering & Attack Vectors
- 25.7 Firewall / Routers / NAT

25.8 Passwords

CYBRON– OFFENSIVE
PENETRATION TESTING
CERTIFIED PROFESSIONAL

TERMS & CONDITIONS

WITHDRAWAL FROM THE DIPLOMA/CERTIFICATION

Students are not allowed to withdraw from the Diploma. If a student cannot continue the Diploma his/her fee will be forfeited.

CONDUCT AND DISCIPLINE

A disciplinary action, leading to rustication, will be taken against students whose conduct is found objectionable at any time during the course of study. Reference will be made to 3D Educators code of conduct.

EVALUATION AND GRADING

The performance of students is evaluated through continuous observation of a student’s performance in the Diploma – class participation, submission of assignments, quizzes and exercises.

The student will be examined through three hourly exams conducted at the midterm and a final exam at the end of the program. Total marks for passing the Diploma will be 60 out of a total of 100.

Students who do not meet the attendance or any other eligibility criteria will not be allowed to appear in the final examination.

The following grading plan will be applicable for the Certification:

A	87 - 100
B+	81 -86
B	72 - 80
C+	66 - 71
C	60 - 65
F	below 60

Students who are unable to appear for the final exam/assessment and are required to submit a written application stating the reason for not appearing for the exam. 3D Educators reserves the rights to approve or deny such applications. If approved, the student will be allowed to sit for the exam within one month. Failure to do so, the student will be resubmit the examination fee (if applicable) and sit the future schedule exam.

Without passing of the exams no certification will be awarded.

CYBRON– OFFENSIVE PENETRATION TESTING CERTIFIED PROFESSIONAL

ONLINE LIVE CLASSES FACILITY AVAILABLE

- Instructor Led Training
- Real Time Presentations
- Interactive Classes
- Complete Notes and Other Stuff shall be provided through our Secure Student Login Member's Area
- For Online Live Classes, you may please download the Admission Form through our website http://www.3deducators.com. Fill it properly and attached the required document along with Picture and send back to info@3deducators.com with scanned fee submitted voucher in the bank.
- For Pakistan you may submit the fee at any MCB Branch with the title of "3D EDUCATORS-TRAINERS & CONSULTANTS".
- If you are outside Pakistan then you may transfer via Bank to Bank or any western union, Fast Track, Money Gram or else International Transfer Body.
- After Admission, if you don't have GMAIL Account then you are requested to kindly make one GMAIL Account and shared it info@3deducators.com. Then further correspondence shall be made by our institute official.
- Extra Bandwidth Charges shall be incurred.

100,000+ Students have been Trained

since 1997

CYBRON– OFFENSIVE
PENETRATION TESTING
CERTIFIED PROFESSIONAL

PRECAUTIONARY MEASURES

- During Classes, you are requested to make sure that you are in isolated room, where no noise should be there except your voice.
- Kindly Switch Off your Cell Phone during the class, because it will disturb the quorum of class.
- If you have taken the admission in the course online lonely, then ethically it is recommended and suggested that you alone in the class.
- Recording of Lectures are not allowed at your end.

This world is emerging and growing in the 21st Century very rapidly because of latest and remarkable technologies and its advancement. Due to advancement of technology, we 3D EDUCATORS offer Live Interactive class sessions

3D EDUCATORS believe on Information Technology and its systems. Now you can also avail this facility at your home.

DISTANCE NOT MATTER

You can join in the live classes Sessions of 3D EDUCATORS – TRAINERS & CONSULTANTS from anywhere of the world.

CONTACT US

021-34141329, 0333-2402474
021-34857148

info@3deducators.com
http://www.3deducators.com

Get the Admission Form

Download Form

MANAGEMENT
3D EDUCATORS
TRAINERS & CONSULTANTS