www.npti.gov.in

एन पी टी आई
NPTi
प्रावीण्यं परोपवृत्तिश्च

WHIZHACK
Securing Digital

Presents

India's First Experiential Post Graduate Diploma in Cyber Security(PGDCS) Program

2023

Course Starts
From 1st March

mail us at : query.npti@gov.in
info@whizhack.com

India today not only faces unprecedented opportunity of widespread digital adoption but also threat of sophisticated global cyber attacks.

NPTI has been at the forefront of nation building through training and capacity building. .NPTI has trained over 3,70,000 power professionals over the last 5 decades and Certified more than 1200 Power Professionals in its 2 Week's Basic Level course on Cyber Security .

NPTI Faridabad has specialised in joint initiatives with industry to meet modern technology needs of India. WhizHack Technology is incubating a Centre of Excellence in Cybersecurity at NPTI Faridabad with focus on developing technologies and training solutions to empower Indians to tackle next generation of Indian and global cyber challenges.

The PGDCS Program in Cyber Defense blends the best of Indian academicians, top industry experts and best practises lab to provide a unique learning experience to learners. Cyber security being a global issue, excelling in skillsets automatically would allow learners to access the best of Global and Indian careers.

Cyber Security an Emerging Need For Country's Power Grid

NEWS • LIVE TV INDIA TODAY APP

HOME MY FEED CORONA INDIA WORLD BUSINESS TECH MOVIES SPORTS HAPPINESS QUEST

News / India / Maharashtra cyber cell submits report on Mumbai power outage, confirms malware attack hit powe

Maharashtra cyber cell submits report on Mumbai power outage, confirms malware attack hit power grid

The Maharashtra cyber department on Monday submitted a provisional report to the Maharashtra government on the massive grid failure which hit Mumbai and surrounding areas on October 12 last year.

ADVERTISEMENT

WATCH Effective price starting at ₹38900

Inclusive of ₹3000* Cashback on cards of ICICI Bank kotak

PGDCS Program
from the Best of India

Cyber Defense Program

Get the Skills. Land the Job.

The explosion of high tech cyber attacks has led industry and Government to shift focus to "Proactive Cyber Defense". This means acting in anticipation to oppose an attack involving computers and network. This skillset has maximum potential demand from employers, currently .

The PGDCS Program at NPTI covers the hands-on and practical skills necessary for Students to land high-paying careers in cybersecurity, one of the world's fastest growing industries.

The PGDCS Program is an accelerated cybersecurity training program designed to successfully prepare people with little or no background in IT for entry level jobs in cybersecurity, a highly in-demand and lucrative career path. The Program is delivered completely online with both live video classroom sessions and online self-paced activities.

97% Employment rate

Career-ready skills

Affordable & accelerated

Why Cyber security and Cyber Defense?

Cybersecurity is the fastest growing market in technology with 30x growth over the last decade.

Not only is it a hot career path, but the field has had 0% unemployment for nearly a decade. With plentiful opportunities and competitive compensation, the only thing standing in your way of a lucrative, future-proof global career is skill and certification.

0% Unemployment rate since 2011

INR 500,000 / $80,000 Average entry level salary

350% Cyber job growth through 2021

Who it's For:

The Post Graduate Diploma Program is for anyone interested in becoming a Global Cyber Defense Expert. The training will ensure learners get the best blend of skill sets to tackle global cyber threats and also certification that's valued in India and beyond.

Qualifications:

Graduates from any discipline can apply with aptitude for cyber security

How it Works:

The certification program was developed around top international training methodology and live mentoring by top faculties. 50% of pedagogy comprises of hands on learning on live projects and simulated scenarios.

The NPTI PGDCS Course was developed around military training methodologies and hands-on learning. We know that everyone learns differently which is why NPTI offers student with two accelerated tracks:

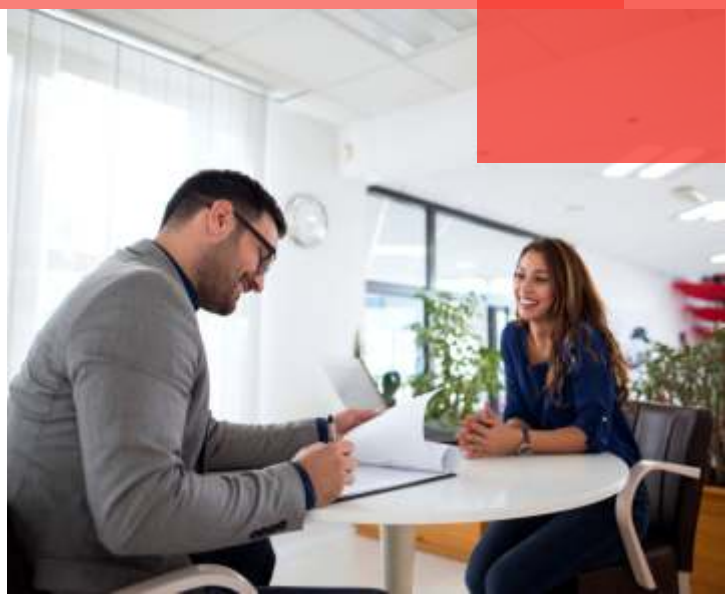
- **NPTI offers 6 month part-time 480 hrs** course with access to virtual labs and live online classes twice a week, 2hrs each day(evening).

During PGDCS

- Self-paced and flexible learning with instant feedback
- Curriculum based on National Initiative for Cybersecurity Education (NICE)
- Access to faculties and industry experts
- Guidance on job searching and resume building

Upon Graduation

- 12 months of continued access to online learning platform
- Connection to our alumni and career network
- **A new career in: Cyber Forensics Analyst, Network Operations Specialist, Cyber Analyst, Cyber Incident Responder, Cyber Infrastructure Support Specialist**



480 Hours of quality content

Learn from anywhere

Real-world simulations

Subject : Foundation of Networking

MODULE 1 : NETWORKING

- What is network/networking ?
- Types of network
- Network Topology
- What Network is Made off
- Networking devices
- OSI layers
- TCP/IP models
- IPV4/IPV6
- Sub-netting
- MAC address
- All about internet
- HTTP & HTTPS
- NAT
- Basics of Routing Protocol
- Static routing
- Dynamic routing
- Switching & VLAN
- Access List Controls (ACL)

TECH TOOLS USED

Cisco Packet tracer
GNS3
WireShark
Others

Subject : Operating System Essentials

MODULE 1 : OPERATING SYSTEM BASICS

- Introduction to Operating Systems
- 32-bit vs. 64-bit Operating Systems
- Mobile Operating Systems
- Compatibility Between Operating Systems

TECH TOOLS USED

Theory Only

MODULE 2 : VIRTUALIZATION BASICS

- What is Virtualization
- Hypervisor basics
- Need & Benefits of Virtualization
- Using Virtualization

TECH TOOLS USED

VmWare
Virtual Box

MODULE 3 : WINDOWS ESSENTIALS

- MS Windows Versions
- Prerequisites and compatibility
- Types of Installations
- Boot Methods
- Basic commandline
- File systems
- Basic Network Configuration & troubleshooting
- Users and Permissions
- Windows security basics

TECH TOOLS USED

Windows OS
Virtual Environment
Windows Tools

MODULE 4 : LINUX ESSENTIALS	TECH TOOLS USED
• Linux Distributions • Prerequisites and compatibility • Types of Installations • Boot Methods • Basic commandline & bash • File systems • Basic Network Configuration & troubleshooting • Users and Permissions	Linux OS Virtual Environment Linux Tools

Subject : Fundamentals of Information Security

MODULE 1 : BASIC CONCEPT OF INFORMATION SECURITY	TECH TOOLS USED
• Introduction to Cyber Security • CIA triad • Privacy • Identification • Authentication • Authorization • Accountability • Vulnearbilities, Threat, Attack • Physical & Environmental Security • Threat Modeling concepts • Security Policies, Procedure, standard & Guidelines	Theory Only

MODULE 2 : BASIC CONCEPT OF WEB	TECH TOOLS USED
• How the internet is works • Type of web applications • HTTP Protocol, HTTPS - TLS/SSL • HTTP Request Methods • Cookies • Sessions • Tokens • Brute force & other password related attacks	Browser wireshark netcat curl John the ripper hashcat hydra

MODULE 3 : BASICS OF CRYPTOGRAPHY	TECH TOOLS USED
• Cryptographic Basics • Symmetric Cryptography • Asymmetric Cryptography • Public Key Infrastructure (PKI) • Email Encryption • Disk Encryption • Cryptanalysis • hashing • Encoding • Digital Signatures • Cryptography attacks	Browser gnupg gpg4win kleopatra veracrypt Mailvelope HashCalc HashMyFiles HashID

MODULE 4 : LAWS AND COMPLIANCE	TECH TOOLS USED
• Computer based Crime • Cyber laws	Theory Only

Subject : Ethical Hacking and Cyber Security

MODULE 1 : INTRODUCTION

- Difference between Ethical Hacking & Cyber Security
- Cyber Kill Chain
- Information security Controls
- Information security Compliance and Standards

TECH TOOLS USED

Theory Only

MODULE 2 : INFORMATION GATHERING & OSINT ESSENTIALS

- Reconnaissance introduction
- What is OSINT
- Active and passive reconnaissance
- Builiding Sock-pupets and anonymizers
- Fingerprinting through Search Engines
- Fingerprinting through Social media
- Website Fingerprinting
- Whois Footprinting
- Network Footprinting
- Collecting locations and addresses
- Using Data breach for OSINT
- Company's Employee OSINT
- Organisation Technological OSINT

TECH TOOLS USED

Browser
internet
OSINT framework
TheHarvester
TOR, GIT
Sherlock
Darcy, Httrack
Ping, Whois, WDE
Cewl
Email Tracker
NSlookup
Path analyzer pro
Recon-ng
Foca
Maltego

MODULE 3 : SCANNING & ENUMERATION

- Network Scanning Basics
- Ping
- Host Discovery
- Ping Sweeping
- Nmap Ping Scan
- Nmap Scan Types
- Port and Service Discovery
- Version Detection with Nmap
- Specifying the Targets
- With an IP Addresses List
- By Using CIDR Notation
- By Using Wildcards
- Specifying Ranges
- OS Fingerprinting
- Banner Grabbing
- Scanning Beyond IDS and Firewall
- Enumeration Basics
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP and NFS Enumeration
- SMTP and DNS Enumeration
- Enumeration Countermeasures

TECH TOOLS USED

nbtstat
nmap
SNMP-check
RPCscan
dig
DNSrecon
enum4linux

Nmap
Zenmap
AngryIPscanner
Megaping
hping3
adv IP scanner
netdiscover
Wireshark

MODULE 4 : VULNERABILITY ASSESMENT

- Vulnerability Assessment Basics
- Diffrent types of Vulnerability Assessment
- Tools and techniques
- Vulnerability Rating
- CVE detail
- CVSS Score
- Making repots

TECH TOOLS USED

OpenVAS
Nessus
NIKTO
Acunetix
Nmap
MITRE
etc

MODULE 5 : PENETRATION TESTING

- Understanding different PC models & standard
- Planning and Scoping plan
- Pre-engagement interactions
- Requirement Gathering
- Defining Scope
- Methodology Selection
- Tool Selection
- Permission memo
- Rule of engagements
- Preparing and Signing Agreement

TECH TOOLS USED

Theory Only

MODULE 6 : SYSTEM HACKING

- System Hacking Basics
- Escalating Privileges
- Maintaining Access
- Cracking passwords
- Kali Tools for hacking
- cloning Github
- open source tools
- Types of windows hackings
- Metasploitable labs
- Clearing Logs

TECH TOOLS USED

Responder
L0phtcrack
metasploit
armitage
John the ripper
hashcat
hydra
theFATrat
etc etc

MODULE 7 : MALWARE THREATS & ANALYSIS

- Basic of malware
- Types of malware
- Working of malware
- Advanced persistent threat (APT)
- Virus and Worm Concepts
- Trojan and rootkits basics
- Mitre ATT&CK repository
- Malware Detection & Analysis
- Anti-malware solutions

TECH TOOLS USED

njrat
cryptors
prorat
theefRAT
JPSvirusmaker
Binwalk
IDA
Bintext
Process monitor
TCPview
etc etc

MODULE 8 : SNIFFING AND SPOOFING

- Sniffing Basics
- MAC Address sniffing attack
- DHCP sniffing attack
- ARP Poisoning
- DNS Poisoning
- Sniffing tools & techniques
- Detecting sniffing
- Spoofing Basics
- Spoofing HOST
- Spoofing E-mail
- Spoofing Contact numbers
- Spoofing Website
- Spoofing Video & Audio
- Spoofing System Files

TECH TOOLS USED

Macof
arpspoof
cain & abel
Mitmf
wireshark
betterCAP
tcpdump
etthercap
Dsniff
Spoofing toolkit
etc etc

MODULE 9 : STEGANOGRAPHY

- Steganography Basics
- What data can be used for Steganography
- Steganography Tools
- Detecting steganography
- Whitespace steganography

TECH TOOLS USED

Opensteg
Steghide
Online tools
Stego Suite
DeepSound

MODULE 10 : SOCIAL ENGINEERING

- Social Engineering Introduction
- Social Engineering Techniques
- Type of Social Engineerings
- Traits of Social Engineering
- Diffrent types of attacks
- Identity Theft
- Countermeasures
- Phishing Attacks
- PreTexting Attacks
- Vishing Attacks
- Smsing Attacks
- IVR Phishing

TECH TOOLS USED

All phising tools
SET
BeeF
Blackeye
SocailFish
etc

MODULE 11 : DoS/DDoS

- DoS/DDOS Concepts
- DoS/DDOS Attack Techniques
- DDOS Case Study
- DoS/DDOS Attack Tools
- DoS/DDOS Protection Tools

TECH TOOLS USED

Metasploit
hping3
HOIC
LOIC

MODULE 12 : SYSTEM HACKING

- System Hacking Introduction
- Scanning systems for existing Vulnerabilities
- Finding Exploits
- Checking Exploit Code
- Deploying Exploit code against Target
- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

TECH TOOLS USED

Nmap
Responder
L0phtcrack
metasploit
armitage
theFATrat
etc etc

MODULE 13 : PRIVILEGE ESCALATION

- Types Of Privilege Escalation Attacks
- Vertical Privilege Escalation
- Horizontal Privilege Escalation
- Linux Privilege Escalation
- Windows Privilege Escalation
- How To Prevent A Privilege Escalation Attack

TECH TOOLS USED

LinEnum
Find
LinPeas
Exploit suggester

MODULE 14 : WEB APPLICATION SECURITY

- Introduction
- Manual vs automated testing
- Web Application Hacking Methodology
- Web Testing Tools setup
- Owasp Top 10
- Top 25 application Risks

TECH TOOLS USED

WhatWeb
Owasp ZAP
Burpsuite
Vega
WPscan
Metasploit
weevely
sqlmap

MODULE 15 : BUG BOUNTY ESSENTIALS

- Bug-Bounty Introduction
- Bug-Bounty Platforms
- How to start with bug bounty
- How to test vulnerabilities
- Getting private programs
- Writing Reports

TECH TOOLS USED

Owasp ZAP
Burpsuite
browser

MODULE 16 : WIRELESS SECURITY

- Wireless Security Essentials
- Understanding Wi-Fi Standards
- Implementing wireless security
- Threats to wireless security
- Hand-on tools introduction
- Performing Wi-Fi attacks
- Other wireless technologies
- Attacks on other wireless technologies

TECH TOOLS USED

FernWi-Fi
Aircrack-ng
Wireshark
Vistumbler
BlueSnarf
Airgeddon
etc

MODULE 17 : MOBILE PLATFORM SECURITY

- Securing Mobile Devices
- Understanding Mobile Vulnerability
- SAST & DAST
- Exploiting Mobile OS's
- Mobile OWASP Top 10

TECH TOOLS USED

BurpSuite
MobSF

MODULE 18 : IOT HACKING

- IoT Basics
- Importance of IoT Security
- Shodan searches for IoT
- IoT Attacks
- IoT Hacking Toolkit

TECH TOOLS USED

Shodan
search engines
ZoomEYE

MODULE 19 : CLOUD SECURITY

- Introduction to Cloud
- Cloud Architecture Security
- Cloud Data Security
- Cloud Application Security
- Cloud Vulnerability Management

TECH TOOLS USED

AWS
BurpSuite
lazys3
s3scanner
etc etc

MODULE 20 : TRACKING & PRIVACY

- Introduction
- How Online Tracking Works
- Browser & Network based trackers
- Browser Leaks
- Iploggers
- Autofills
- How to protect against Internet Tracking

TECH TOOLS USED

Online Tracking applications

MODULE 21 : ANONYMITY & DARKWEB

- Introduction
- VPN, ProxyChains & anonymizers
- Darkweb Basics
- Introduction to TOR
- How TOR Works
- Perfect Forward Secrecy
- Understanding TOR Networking
- Risk & legals over using Darkweb
- What is TAILS OS
- Introduction to WHONIX OS
- Basics of Qubes OS

TECH TOOLS USED

TOR Browser
Qubes OS
TAILS OS
Belena Echer
WhoNix OS
ProxyChains
VPN
Etc...

MODULE 22 : DIGITAL FORENSICS

- Understanding Digital Forensics
- Type of investigations
- Different fields under Digital Forensics
- Environment setup
- Important terminologies
- Data Acquisition
- Data Analyzing
- Reporting

TECH TOOLS USED

Windows Forensic Toolchest
DumpReg
DumpSec
DumpEvt
Foundstone Forensic ToolKit
Sysinternals Suite
dig – DNS Lookup Utility
VisualRoute
Netstat Command

MODULE 23 : INCIDENT RESPONSE

- Importance of Incident Response
- Cyber Incident Statistics
- Role of Incident Handler
- Policy, Plan & Procedures
- Goals of Incident Response
- Identifying possible Incidents
- Preparing Incident Response Plans
- Incident Response and Handling Steps
- Incident Containment
- Eradications
- Incident Recovery Plan
- How to Report an Incident
- Writing incident reports

TECH TOOLS USED

Activity Monitor
Net Spy Pro
Spector Pro
SpyAgent
Handy Keylogger
Anti Keylogger
Actual Spy
IamBigBrother
007 Spy Software
SpyBuddy
SoftActivity Keylogger
Elite Keylogger
Spy Sweeper

MODULE 24 : RISK MANAGEMENT

- Introduction od Risk Management
- CIA Fundamentals
- Security Governance
- Legal & Compliance Risk
- Security Policies
- Business Continuity
- Risk Assessment
- Quantititative Risk Assessment
- Information Classification
- Risk Managment Framework
- Cloud legal and compliance risks
- Security Compliance & Governance Frameworks

TECH TOOLS USED

Theory Only

Fee Details

Program Fee : 80,000 + GST
Easy EMI options available

For more detail please visit : www.npti.whizhack.in
Email us : info@whizhack.com, query.npti@gov.in
Call us : +91-8447223249