Nexus Infosec
Red Team as a Service

WE ARE NOW IN INDIA

Nexus Infosec USA has expanded to Nagpur, Maharashtra, offering cybersecurity training for students and professionals and expertise to businesses. The corporation has established a subsidiary, Apex Cyber Pvt Ltd, to enhance operations across India.

APEX CYBER
REGENCY OF DIGITAL DEFENCE

+

Nexus Infosec
Red Team as a Service

OUR INSTRUCTORS

SHUBHAM KHICHI
FOUNDER & CEO, NEXUS INFOSEC
Prof. Adversary Simulation
10+ years exp
Offensive Security

LIN AUNG
Prof. Network Security
10+ years exp
Network Hacking

SUNNY SAHOTA
Prof. Web Application Security
10+ years exp
British Govt. (7 yrs)

Our instructors are working professionals from Fortune 100 American companies.

More than 30 years of combined experience in Corporate Cybersecurity and Training

800+ Students Trained in Cyber
500+ Students Landed 6 Figure Jobs
300+ Called onsite to work in USA

Get a comprehensive Cybersecurity education with our three-course program. For a small investment of ₹ 25,000 per course, get access to Hands-On Labs, Career Services, Internship Certificate, and a Diploma Certificate.

Nexus Infosec
Red Team as a Service

AMERICAN CYBER TRAINING

RECOGNITION

We are excited to collaborate with Rashtrasant Tukadoji Maharaj Nagpur University's Board of Lifelong Learning & Extension, providing cybersecurity education to its students. The partnership demonstrates the university's dedication to equipping students with necessary skills to excel in the digital world.

100% PLACEMENT ASSISTANCE

Our program offers customized career guidance, job preparation, and ongoing support, including the development of a professional resume and LinkedIn profile. We'll provide you with vital skills that are relevant to the best job opportunities we've identified with potential industry leaders.

wipro · MasterCard · SOPHOS · ALSTOM · mobility by nature
Sterling · JPMorgan Chase & Co. · HSBC
KPMG · standard chartered

ADMISSION ELIGIBILITY
1. B.Tech/B.E (Pref 2nd & 3rd Yr or Passout)
2. B.Sc in Computer Sc/Data Sc/IT/Cyber Security (Pref 2nd & 3rd Yr or Passout)
3. BCA (Pref 2nd & 3rd Yr or Passout)
4. MCA (Pursuing & Passout)
5. High End IT Admins, Working Professionals in Govt, Corporates, etc

---

What we Offer

- 23 Week Hands-On **Live Online** Cyber training from the best American Cyber Professionals.
- Complete specialization of Network Security, Web Security, Red Teaming
- Internship & Diploma Certificate in Cybersecurity from Deptartment of Lifelong Learning and Extension, RTM Nagpur University and Nexus Infosec, USA available to all enrolled students.

Our Priority is Quality

Our Expert instructors with more than 30 years of experience from the USA and UK, top quality education in cybersecurity, renowned lab providers like **TryHackMe and HackTheBox** and a stellar internship with certificate. You are set for success and can outsmart the competition.

Find out more about our training program, diploma, syllabus, and success stories by scanning the QR code.

+91 70205 92900

Address: 403, Gomti Apartment, Law College Square, Dharampeth, Nagpur – 440010

Email: info@apexcyber.in
www.nexusinfosec.com
www.apexcyber.in

ACSE Course Syllabus

Learning Module	Learning Units	Learning Objectives
Network Security	Intro to Networking	Understand the basics of computer networks and their components
	IP Address, IP Classes	Learn about IP addressing schemes and classes
	Common Networking Commands	Master essential networking commands
	Common Ports and Protocols	Identify and understand standard ports and associated protocols
	Subnetting	Learn how to perform subnetting
	Installing Virtual Machines, Setting up Kali Linux	Set up a virtual lab environment for practice
	Linux File System	Understand the Linux file system hierarchy
	Hands-on: Linux commands in the terminal	Master basic Linux commands
	Text Editing Tools, Git Cloning, Permission and Files	Learn text editing, file permissions, and how to clone repositories
	Penetration Testing Methodology	Understand the phases and methodology of penetration testing
	Nessus, OpenVAS, Researching Public Exploits	Learn to use vulnerability scanning tools and research public exploits
	OSINT Fundamentals	Understand the basics of Open Source Intelligence
	Port Scanning, Nmap	Learn to use Nmap for port scanning
	Enumerating and Exploiting Common Ports	Learn techniques for exploiting common open ports
	Kernel, Shell, Payloads	Understand the Linux Kernel, Shell, and how to create payloads
	MSFVenom, File Transfers and Download	Learn to use MSFVenom for payload generation and methods for file transfers
	Metasploit Framework	Master the Metasploit Framework for exploitation
	Pivoting, Local Privilege Escalation	Learn techniques for network pivoting and escalating privileges locally
	Password Attacks, Cracking Hashes	Understand different types of password attacks and how to crack hashes
	CVSS Calculator, Covering Tracks	Learn to use the CVSS calculator and techniques to cover tracks
	Firewall Evasion Techniques	Learn techniques to bypass firewalls

	Wireless Network Attacks	Understand vulnerabilities in wireless networks and how to exploit them
	VPN and Tunneling	Learn how VPNs and tunneling can be exploited or bypassed
Web Security	Introduction to Web App Security	Understand the basics of web application security
	Information Gathering	Learn techniques for gathering information about a target web application
	Scanning & Spidering Web Apps	Learn to use tools for scanning and spidering web applications
	Directory Discovery and Fuzzing	Learn techniques for directory discovery and fuzzing
	Information Disclosure	Understand how to identify and exploit information disclosure vulnerabilities
	Authentication and Usernames	Learn about authentication mechanisms and how to exploit weaknesses
	Sessions and Bypassing Authentication	Learn how to hijack sessions and bypass authentication mechanisms
	Command Injection	Understand and exploit command injection vulnerabilities
	File Inclusion & Directory Traversal	Learn to exploit file inclusion and directory traversal vulnerabilities
	SQL Injection	Understand and exploit SQL injection vulnerabilities
	XXE and DOM	Learn about XXE and DOM-based vulnerabilities and how to exploit them
	Cross-Site Scripting	Understand and exploit Cross-Site Scripting vulnerabilities
	BeEF Framework	Learn to use the BeEF framework for client-side attacks
	WordPress Attack Demo	Understand common WordPress vulnerabilities and how to exploit them
	Apache Attack Demo	Learn about vulnerabilities in Apache web servers and how to exploit them
	Web Application Firewalls	Understand Web Application Firewalls and how to bypass them
	API Security	Learn about API vulnerabilities and how to secure them
	OAuth and SSO Attacks	Understand OAuth and Single Sign-On vulnerabilities and how to exploit them
Adversary	Adversary Simulation vs	Understand the difference between adversary

Simulations	Emulation	simulation and emulation
	Frameworks and Methodologies	Learn about frameworks and methodologies used in adversary simulations
	Unified Kill Chain Attack Methodology	Understand the Unified Kill Chain and how to use it in simulations
	Phases of Red Team Engagement	Learn about the different phases involved in a red team engagement
	Threat Intelligence	Understand the role of threat intelligence in adversary simulations
	Resource Development	Learn about developing resources for an engagement
	Initial Access	Understand techniques for gaining initial access to a target system
	Execution of attacks	Learn various attack execution techniques
	Persistence	Understand techniques for maintaining access
	Domain Privilege Escalation	Learn techniques for escalating privileges within a domain
	Defense Evasion	Understand techniques for evading detection
	Credential Access	Learn methods for obtaining credentials
	Discovery	Understand techniques for internal reconnaissance
	Domain Lateral Movement, Domain Trust Attacks	Learn techniques for lateral movement and exploiting domain trusts
	Collection	Understand methods for collecting data
	Exfiltration	Learn techniques for data exfiltration
	Impact, Engagement Closure	Understand how to assess the impact of an engagement and how to close it
	Building a Discord C2, Using Covenant	Learn to build and use custom Command and Control servers
	C2 Comparison - C2 Matrix, Using Caldera C2	Understand different C2 frameworks and their use-cases
	Social Engineering Attacks	Learn about social engineering techniques and how to simulate them
	Endpoint Security Bypass	Understand how to bypass endpoint security solutions
	Purple Teaming	Learn about the collaboration between red and blue teams for improved security