THE GEEK INSTITUTE OF CYBER SECURITY

Geek Certified Cyber Security Professional (GCCSP)

www.geekinstitute.org

Dear Esteemed Learner,

At The Geek Institute of Cyber Security, we recognize the profound impact we have on shaping your future, and we approach this responsibility with utmost dedication.

As the founder of The Geek Institute of Cyber Security, I am committed to providing you with unparalleled training enriched by hands-on projects and promising opportunities.

With us, your journey towards a successful and prosperous career begins.

Wishing you every success!

Warm regards,

Mani Kumar
Founder, The Geek Institute of Cyber Security

Course Description

Duration : 12 Months

This intensive course is designed to equip participants with a deep understanding of cyber security principles, practices, and ethical hacking techniques. The curriculum covers a wide range of topics, from foundational concepts to advanced penetration testing skills, while emphasizing the ethical and responsible use of hacking methodologies.

Prerequisites:

Strong understanding of computer networks, operating systems, and programming languages

Familiarity with basic cyber security concepts

Proficiency in using computers and the internet

Who can Enroll ?

Information Technology (IT) Professionals: IT professionals, including network administrators, system administrators, and IT managers, often enroll in GCCSP course to enhance their skills in securing their organization's systems and networks.

Computer Science and Engineering Students: Students pursuing degrees in computer science, computer engineering, or related fields often take GCCSP course to supplement their education and gain practical cyber security skills.

Cyber security Enthusiasts: Individuals with a strong interest in cyber security, even without a formal IT background, can enroll in GCCSP course as a starting point to learn about hacking techniques and how to defend against them.

Network Security Analysts: People working in network security roles or those aspiring to enter this field find GCCSP course valuable for improving their knowledge and skills.

Penetration Testers and Ethical Hackers: Those who want to become professional penetration testers or ethical hackers can take GCCSP course to acquire the knowledge and skills necessary for conducting authorized security assessments.

Security Researchers: Individuals interested in security research and discovering vulnerabilities in systems and software can benefit from GCCSP course to deepen their understanding of security concepts.

Course Objectives

Understanding Cyber Security Fundamentals: The course aims to educate students about the fundamental concepts of cybersecurity, including the importance of information security, the threat landscape, and the need for ethical hacking.

Ethical Hacking Skills: One of the primary goals is to teach students how to ethically hack and assess the security of computer systems, networks, and applications. This includes learning penetration testing techniques, vulnerability assessment, and exploitation.

Defensive Security Knowledge: Students learn how to defend against various cyber threats, such as malware, phishing, and social engineering. Defensive security topics may include firewall configuration, intrusion detection systems (IDS), and incident response.

Security Tools and Technologies: The course introduces students to a range of cyber security tools and technologies used in both offensive and defensive roles. This includes tools for scanning, enumeration, exploitation, and monitoring.

Cyber Security Best Practices: The course covers best practices for securing computer systems, networks, and data. This includes topics like access control, encryption, and secure coding

Job Profiles

GCCSP course can open up a range of job opportunities in the field of Cyber Security and Ethical hacking.

Information Security Analyst: These professionals are responsible for monitoring an organization's computer networks and systems for security breaches, implementing security measures, and responding to incidents.

Network Security Engineer: Network security engineers design, implement, and manage security measures to protect an organization's network infrastructure from cyber threats.

Penetration Tester (Ethical Hacker): Penetration testers, also known as ethical hackers, simulate cyberattacks to identify vulnerabilities in systems and applications, helping organizations strengthen their security.

Security Consultant: Security consultants work for consulting firms or independently to provide expert advice to organizations on how to enhance their cybersecurity posture and address vulnerabilities.

Forensic Analyst: Forensic analysts investigate cybercrimes and security incidents, collecting and analyzing digital evidence to determine the extent of the breach and identify perpetrators.

Cyber Security Researcher: Researchers work in academia, government agencies, or private organizations to advance knowledge in the field of cybersecurity, develop new tools, and discover vulnerabilities.

Course Syllabus

1. Introduction to Cyber Security & Ethical Hacking

- The evolution of cyber threats and attacks
- Principles of cyber security: confidentiality, integrity, availability
- Risk management and threat modelling
- Legal and ethical considerations in cyber security

2. Networking Fundamentals

- OSI model and TCP/IP stack review
- IP addressing and subnetting
- Network protocols and vulnerabilities
- Network topologies and architecture
- Network architecture and segmentation for security
- Intrusion Detection and Prevention Systems (IDS/IPS)

3. Linux Fundamentals

- Getting Started with Linux Operating System
- Accessing the Command Line
- Managing Files from the command Line
- Creating, Viewing & Editing Test Files
- Managing Local Users and Groups
- Controlling Access to Files
- Monitoring and Managing Linux Process
- Controlling Services and Daemons
- Configuring and Securing SSH
- Configuring Network File Sharing
- Samba Server Configuration

- FTP Server Configuration
- Virtual Host Configuration (Apache2 & Nginx)
- Dark web Server Configuration
- Analyzing and Storing Logs
- Archiving and Transferring Files
- Managing Networking
- Firewall Configurations
- Accessing Linux File System
- Installing and Updating Software Packages

4. Operating System Security

- Operating system concepts and types
- Common OS vulnerabilities and exploits
- User authentication mechanisms and access controls
- Securing operating systems: Windows, Linux, macOS and Android
- Patch management and system hardening

5. Web Application Security

- Web application architecture and components
- OWASP Top Ten vulnerabilities
- Secure coding practices and frameworks
- Web application firewalls and security tools

6. Ethical Hacking Methodology

- Understanding ethical hacking and penetration testing
- Principles of ethical hacking and penetration testing
- Information gathering and reconnaissance techniques
- Scanning and enumeration: tools and methodologies
- Vulnerability assessment and reporting

7. Network Security

- Firewalls, VPNs, Intrusion Detection Systems (IDS)
- Virtual Private Networks (VPNs) and encryption
- Wireless network security: WEP, WPA, WPA2, WPA3
- Network monitoring and incident response
- Network architecture design for security

8. Cryptography and Secure Communications

- Cryptographic algorithms and protocols
- Public key infrastructure (PKI) and digital certificates
- Secure communication channels: SSL/TLS, SSH
- Implementing encryption in various applications

9. Ethical Hacking

- Introduction to Ethical Hacking
- Foot-printing Active & Passive Approach
- In-depth Network Scanning
- Enumeration User Identification
- System Hacking & Password Cracking
- Malware, Viruses, Worms, Trojan and backdoor
- Sniffers MITM with Kali Linux
- Bots and Botnets
- Social Engineering Techniques with Practical
- Denial of Service DOS & DDOS Attack
- Hacking Web servers Server Rooting
- Hacking Wireless Networks (Wi-Fi, Bluetooth and RF)
- Honeypots
- Evading IDS, Firewall
- Buffer Overflow

- Computer and Mobile Hacking

10. Advanced Web Application Security

- Advanced SQL injection techniques
- Cross-Site Scripting (XSS) variants
- Understanding the vulnerabilities and way of Exploiting:
    - SQL Injection (SQLi)
    - SQL Authentication Bypass
    - Cross-Site Scripting (XSS)
    - Cross-Site Request Forgery (CSRF)
    - Remote Code Execution (RCE)
    - File Inclusion Vulnerabilities (LFI/RFI)
    - Server-Side Request Forgery (SSRF)
    - XML External Entity (XXE) Attacks
    - Web Session Hijacking
    - File Upload Vulnerability
    - Security Misconfigurations
    - Insecure Deserialization
    - Broken Authentication
    - JWT Token Attack
    - Insecure Direct Object References (IDOR)
    - Sensitive Data Exposure
    - Multi Factor Authentication Bypass
    - HTTP Request Smuggling
    - Source Code Disclosure
    - Directory Path Traversal
    - HTML Injection
    - Host Header Injection

    - Clickjacking
    - Unvalidated Redirects and Forwards
    - Server-Side Template Injection (SSTI)
    - Flood Attack on Web
- Application security assessments: Source code review, DAST, SAST
- Secure DevOps and continuous security testing
- Vulnerability assessment and reporting

11. Cloud and Virtualization Security

- Cloud computing models and security challenges
- Cloud service provider security features
- Securing virtual environments and containers
- Identity and access management in the cloud

12. Mobile and IoT Security

- Mobile app security assessments
- Securing mobile devices and APIs
- IoT security challenges and best practices
- Security implications of wearable technology

13. Advanced Penetration Testing

- Bash Shell Scripting
- Practical Tools
- Using Public Exploits
- Antivirus Evasion Techniques
- Windows Privilege Escalation
- Payload Deployments and File Transfers
- Password Attacks
- Linux Privilege Escalation
- Active Directory Attacks
- Port Forwarding and Tunnelling
- Power Shell Empire
- Lab Solving (HackTheBox, VulnHub, TryHackMe, PortSwigger etc.)

14. Network Penetration Testing

- In-depth network penetration testing methodologies
- Advanced reconnaissance and OSINT techniques
- Exploiting complex network vulnerabilities
- Reporting and communicating findings effectively

15. Advanced Exploitation Techniques

- Kernel-level vulnerabilities and exploitation
- Advanced memory corruption attacks
- Writing custom exploits and payloads
- Mitigations and defenses against advanced attacks

16. Exploitation and Post-Exploitation

- Exploiting vulnerabilities: Metasploit, Exploit-DB
- Privilege escalation and maintaining access
- Covering tracks and post-exploitation activities
- Legal and ethical aspects of penetration testing

17. Mobile Application Penetration Testing

- Introduction to Mobile Penetration testing
- Lab Setup
- Android Architecture
- APK File Structure
- Reversing Application with Apktool
- Static Analysis
- Scanning Vulnerability
- Insecure data storage
- Insecure Communication
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Code Tempering
- Reverse Engineering

- SSL Pinning
- Intercepting network traffic

18. Cyber Forensics

- Key terminology and concepts
- Chain of custody and evidence handling
- Digital Evidence Fundamentals
- Types of digital evidence (files, logs, metadata)
- Evidence collection methods
- Tools and software for evidence acquisition
- Techniques for creating forensic images
- Tools for imaging (autopsy, guymager, bulk-extractor, metagoofill , FTK Imager, EnCase , NetworkMiner)
- Understanding file systems (NTFS, FAT32, ext4)
- File recovery techniques
- Analyzing file metadata and timestamps
- Introduction to Network Forensics
- Network traffic analysis and capture using Wireshark
- Analyzing network logs and packet data
- Identifying and tracking network-based attacks
- Malware Analysis and Forensics

- Types of malware (viruses, worms, ransomware)
- Techniques for analysing malware behaviour
- Tools for malware analysis (gdb, redare2, Ghidra, IDA Pro, OllyDbg, x64dbg, AndroGuard)

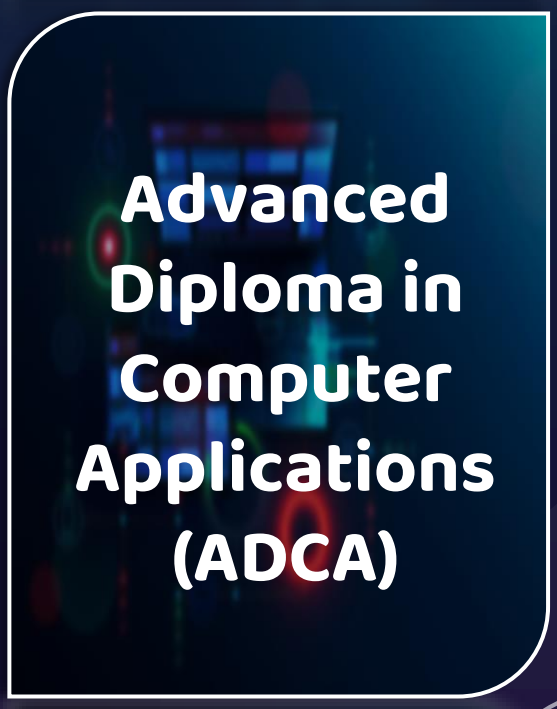
21. Programming Languages

- C/C++ Programming
- x86_64 Assembly Language Programming & Binaries Reversing/Debugging

22. Artificial Intelligence in Cyber Security and Ethical Hacking

- ✓ Overview of AI and Machine Learning in Cyber Security
- ✓ AI-powered threat detection and prediction systems
- ✓ Using AI for malware classification and anomaly detection
- ✓ Building intelligent intrusion detection systems (IDS) using ML models
- ✓ Deep learning for phishing and spam detection
- ✓ Automated vulnerability scanning and exploitation with AI
- ✓ Using AI in digital forensics: pattern recognition and timeline correlation
- ✓ ChatGPT and Copilot for cyber operations, scripting, and reporting
- ✓ Ethical considerations and adversarial machine learning
- ✓ Introduction to popular tools and frameworks (e.g.,

Our Popular Courses



Contact Information

Ready to unlock a secure future? Reach out to us and let's code the path to success together!

Call Now To Get Fee Details

Call Now to Book 3-Days of FREE Demo Classes

+91 8882618533

info@geekinstitute.org

www.geekinstitute.org

Kapashera, New Delhi
Pincode-110097

/TheGeekInstitute

@geekinstitute

/Geek_Institute

@TheGeekInstitute