

*(Building Futures Through Digital Knowledge and Innovation)*

## Geek Certified Cyber Security Professional (GCCSP) (12 Months)

### 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 Text 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
- ✓ Analysing 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. 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
- Analysing file metadata and timestamps
- Introduction to Network Forensics
- Network traffic analysis and capture using Wireshark
- Analysing network logs and packet data
- Identifying and tracking network-based attacks
- Malware Analysis and Forensics
- Types of malwares (viruses, worms, ransomware)
- Techniques for analysing malware behaviour
- Tools for malware analysis (gdb, redare2, Ghidra, IDA Pro, OllyDbg, x64dbg, AndroGuard)

## 14. 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 Redirection and Tunnelling
- ✓ Power Shell Empire
- ✓ Lab Solving (HackTheBox, VulnHub, TryHackMe, PortSwigger, OWASP JuiceShop and WebGoat etc.)

## 15. Network Penetration Testing

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

## 16. Advanced Exploitation Techniques

- ✓ Kernel-level vulnerabilities and exploitation
- ✓ Advanced memory corruption attacks
- ✓ Writing custom exploits and payloads

- ✓ Mitigations and defences against advanced attacks

## **17. 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

## **18. 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

## **19. Internet of Thing (IOT) Penetration Testing**

- ✓ Introduction To IoT
- ✓ Sensor Network & Wireless Protocol
- ✓ Review of Electronic Platform, Production and Cost Projection
- ✓ Mobile App Platform and Middleware for IoT
- ✓ Machine learning for Intelligent IoT
- ✓ Analytic Engine for IoT

## **20. Blockchain and Cryptocurrency Security**

- ✓ Understanding blockchain technology
- ✓ Cryptocurrency vulnerabilities and risks
- ✓ Smart contract security and auditing

## **21. Programming Languages**

- ✓ C/C++ Programming
- ✓ x86\_64 Assembly Language Programming & Binaries Reversing/Debugging
- ✓ PHP Programming for Vulnerable Web Apps Development

## **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., TensorFlow, Scikit-learn, OpenAI, IBM Watson)