deerwalk training center

DTI-CSC-101

Ethical Hacking and Cybersecurity with AI

deerwalktrainingcenter.com

Program Information

Nature of the Course
Theory + Practical

Total Hours per Day
2 hours

Course Duration
9 Weeks

Course Summary

This course covers cyber security, ethical hacking, ethical hacking phases, and numerous attack vectors, preventing countermeasures, Bug Bunty Hunting, Penetration Testing, and Forensics, among other topics. This will give you an insight into how hackers think and act maliciously, allowing you to better build up your security infrastructure and protect against future attacks. Organizations can increase their system security measures by understanding system flaws and vulnerabilities, lowering the chance of an incident.

Completion Criteria

After fulfilling all of the following criteria, the student will be deemed to have finished the Module:

- Has attended 90% of all classes held
- Has received an average grade of 80% on all assignments
- Has received an average of 60% in assessments
- The tutor believes the student has grasped all of the concepts and is ready to go on to the second module.

Required Textbooks

- **Mary Aiken, "The Cyber Effect", Random House.**
- **Peter Kim, "The Hacker Playbook 3", Peter Kim.**
- **Helden Wong "Cyber Security: Law and Guidance", Bloomsbury Professional.**

Prerequisites

- Basic knowledge about programming, bits/bytes, procedures, classes, 1 computer architecture,etc. If you just have theoretical knowledge that is perfectly okay but you should have strong convictions on what programming is, and what you hope to achieve from this class.
- Willing and eager to spend at least 10-20 hours (varying from student-to-student) per week outside of the training class to read/write codes in JavaScript (self-study and practice).
- There is no prior educational level requirement for this course. Anyone from 10+2 student to someone who is doing her PHD in Genetic Engineering is welcome to take this course.
- If you are only interested in theory and have no interest/patience in spending at least 10 hours every week throughout the duration of the course, then this course might not be for you.
- If you have absolutely no idea about programming or do not see yourself doing programming in the next six - odd months, then this class may not be for you!

Course Details

Module 1: Networking Fundamentals & CCNA Essentials

Topic

- Networking & CCNA Basics

What You Will Learn

- OSI Model vs. TCP/IP Stack
- Network Topologies
- Ethernet
- Switching & Routing Essentials
- VLANs and Router/Switch
- Configuration Concepts

Time Allocation

- 5 Hours

Topic

- IP Addressing & Subnetting

What You Will Learn

- IPv4 & IPv6 Architecture
- Public vs. Private IPs
- Subnet Masks
- CIDR Notation
- Variable Length Subnet Masking (VLSM)
- IP Calculation

Time Allocation

- 5 Hours

Topic

- Network Infrastructure Services: DNS, DHCP & Domains

What You Will Learn

- DNS Architecture(Resolution, Records, Zones)
- DHCP Operation(DORA process, Scopes, Leases)
- Domain Infrastructure (Active Directory, Domain Controllers, Trusts)

Time Allocation

- 5 Hours

Module 2 : Operating Systems, Linux Essentials & Filesystems

Topic

- Linux Operating System Fundamentals

What You Will Learn

- Linux Command Line Interface (CLI)
- Shell Scripting Basics
- Package Management
- Process Control, User & Group Administration
- System Logging, and Sudo Privileges.

Time Allocation

- 6 Hours

Topic

- Filesystem Architecture & Permissions

What You Will Learn

- Linux Filesystem Hierarchy Standard (FHS: /etc, /var,/usr, /home)
- Windows Filesystems (NTFS,FAT32)
- File Permissions(Chmod, Chown, ACLs)
- Inodes
- Mounting
- File Integrity

Time Allocation

- 4 Hours

Module 3: Information Gathering, Footprinting & Scanning

Topic

- Chapter 1: InfoSec & Ethical Hacking Overview

What You Will Learn

- CEH v13
- Elements of Security
- Cyber Kill Chain
- MITRE ATT& CK
- Framework , Security Laws and AI in Ethical Hacking.
- **Activity:** Examining MITRE ATT& CK

Time Allocation

- 3 Hours

Topic

- Chapter 2: Footprinting & Reconnaissance

What You Will Learn

- OSINT Tools
- Whois
- DNS,Website, Email, and Social Network Footprinting
- **Activities:** Shodan, theHarvester, Google Hacking, WHOIS, DNS Enumeration, Traceroute

Time Allocation

- 5 Hours

Topic

- Chapter 3: Scanning Networks

What You Will Learn

- Discovery & Port Scans
- NMAP
- Firewall/IDS Evasion, Proxies, AI-
- Enhanced Scanning Tools.
- **Activity:** Port Scanning and Fingerprinting with NMAP

Time Allocation

- 4 Hours

Topic

- Chapter 4: Enumeration

What You Will Learn

- SMB
- NetBIOS
- WMI
- SNMP
- LDAP
- SMTP
- Website and Active Directory Enumeration.
- **Activities:** SMTP Enumeration, Enumerating Website Directories

Time Allocation

- 3 Hours

Module 4: Vulnerabilities, Exploitation & Malware

Topic

- Chapter 5: Vulnerability Analysis

What You Will Learn

- Vulnerability Scanning and AI-Assisted Assessment.
- **Activity:** Vulnerability Scanning with OpenVAS

Time Allocation

- 3 Hours

Topic

- Chapter 6: System Hacking

What You Will Learn

- OS Exploits, Buffer Overflows, Metasploit, Meterpreter, Keylogging, Windows Exploitation.
- **Activities:** Hacking with Metasploit, Having Fun with Meterpreter, Using Netcat

Time Allocation

- 6 Hours

Topic

- Chapter 7: Malware Threats

What You Will Learn

- Viruses
- Trojans
- Rootkits
- Malware Deployment
- Detection, Analysis
- Countermeasures.
- **Activities:** Creating a Malware Dropper and Handler, Analyzing SolarWinds Hack

Time Allocation

- 6 Hours

Module 5: Attacks, Defense Mechanisms & Web Security

Topics

- Chapter 8: Sniffing & Spoofing

What You Will Learn

- Network Sniffing,
- MAC/ARP Attacks
- Name Resolution Attacks
- **Activities:** Wireshark Data Interception, MITM with Ettercap, Spoofing with Responder

Time Allocation

- 4 Hours

Topic

- Chapter 9: Social Engineering

What You Will Learn

- Techniques, Insider Threats
- Social Media
- Identity Theft
- AI in Social Engineering
- **Activities:** Phishing for Credentials, OMG Cable Baiting

Time Allocation

- 3 Hours

Topic

- Chapter 10: Denial-of-Service

What You Will Learn

- DoS/DDoS Concepts
- Volumetric
- Fragmentation
- State Exhaustion
- Application Layer Attacks
- **Activity:** Conducting a Slowloris DDoS Attack

Time Allocation

- 3 Hours

Topic

- Chapter 11: Attack Detection & Prevention

What You Will Learn

- IDS (Snort)
- Firewalls
- Packet Filtering
- Split DNS
- NAC
- Endpoint Security
- Honeypots.
- **Activity:** Busting the DOM for WAF Evasion

Time Allocation

- 4 Hours

Topic

- Chapters 12-14: Web Server, Web App Security & SQLi

What You Will Learn

- Web Server Attacks
- OWASP Top 10
- XSS
- CSRF
- Parameter Tampering,
- Error/Union/Blind SQL Injection.
- **Activities:** Command Injection, SQLi on Live Website (Parts 1 & 2)

Time Allocation

- 6 Hours

Module 6: Wireless, Mobile & Applied Cryptography

Topic

- Chapter 15: Hacking Wireless Networks

What You Will Learn

- Wi-Fi Standards
- Discovery Tools
- WEP/WPA/WPA2/WPA3
- Password Cracking
- Bluetooth Hacking
- **Activity:** WPA2 KRACK Attack

Time Allocation

- 5 Hours

Topic

- Chapter 16: Cryptography & Course Conclusion

What You Will Learn

- Symmetric/Asymmetric Encryption
- Public Key Exchange
- PKI
- Digital Signatures Hashing.
- Activities:
- Symmetric/Asymmetric
- Encryption, Asymmetric
- Key Pair, Calculating
- Hashes

Time Allocation

- 5 Hours

Topic

- Chapter 17 : Project

What You Will Learn

- Two Team RED and BLUE working in VPS machine as group task.

Time Allocation

- 5 Hours

---

deerwalk training center

Sifal, Kathmandu, Nepal
Phone: +977 - 01 - 5913021 | 4567153
Mobile: +977 - 9765355167 | 9860422021
Email: training@deerwalkcompware.com
Website: deerwalktrainingcenter.com