CYBER SECURITY & ETHICAL HACKING

COURSE CODE: MOOCCSE-A11 **DURATION: 8 Weeks**

Course Outcomes:

1. BASICS OF SECURITY
2. WINDOWS & AD FUNDAMENTALS
3. TCP/IP & NETWORK SERVICES
4. BASICS OF ETHICAL HACKING
5. SCANNING OF SYSTEMS/APPLICATIONS
6. SECURING WEB APPLICATIONS

COURSE DESCRIPTION:

Build Your Career With the Most In-Demand field.

The Cyber Security & Ethical Hacking Program will equip you with the skills needed to become familiar in this rapidly growing domain. You will learn hacking tools, methodologies and techniques and learn how to secure them from these hackers.

COURSE DETAILS

MODULE 1: (Title of the Module)

TOPIC 1: (Introduction)

Lecture 1.1: Cyber space
Lecture 1.2: Encryption
Lecture 1.3: Email security
Lecture 1.4: Antiviruses
Lecture 1.5: Career in cyber sec

MODULE 2: (Microsoft OS)

TOPIC 1: (Windows)

Lecture 1.1: File System
Lecture 1.2: System Configuration
Lecture 1.3: Computer Management
Lecture 1.4: System Information
Lecture 1.5: Resource Monitor
Lecture 1.6: Command Prompt
Lecture 1.7: Registry Editor

TOPIC 2: (Active Directory)

Lecture 2.1: Domain Controller
Lecture 2.2: Forest
Lecture 2.3: Users & Groups
Lecture 2.4: Domain Authentication

MODULE 3: (Networking)

Lecture 1.1: TCP/IP
Lecture 1.2: Layers in TCP/IP
Lecture 1.3: Ports & Sockets
Lecture 1.4: Firewall

Lecture 1.5: Network Services
Lecture 1.6: DNS, Telnet, SSH
Lecture 1.7: Video Forensic

MODULE 4: (Ethical Hacking)

Lecture 1.1: What is Hacking?
Lecture 1.2: Types of Hackers
Lecture 1.3: Google Dorks as Hacking Tools
Lecture 1.4: Phases of Hacking
Lecture 1.5: Passive Reconnaissance
Lecture 1.6: Active Reconnaissance
Lecture 1.7: Port Scanning
Lecture 1.8: NMAP as Scanning Tool
Lecture 1.9: NMAP Scripting Tool
Lecture 1.10: Exploit Searching
Lecture 1.11: Video Password Cracking

MODULE 5: (Websites)

Lecture 1.1: Working of Website
Lecture 1.2: HTML
Lecture 1.3: HTTP
Lecture 1.4: HTTP Methods
Lecture 1.5: Headers & Cookies

MODULE 6: (Web Applications)

Lecture 1.1: Walking a Application
Lecture 1.2: Browser Developer Tools

RESOURCES:

- OWASP Installation - Vulnerable Web Application
- DIRB & Whatweb For Website Identification
- Hydra - Bruteforcing Any Login Page
- Burpsuite Introduction & Configuration
- Command Injection & Target Exploitation
- Combining Our Python Tool With Command Injection Vulnerability
- XSS Attack Theory
- Finding XSS Vulnerability On A Webpage
- Solving XSS Challenges On An Online Lab
- HTML Character Encoding To Exploit an XSS Vulnerability

MODULE 7: (Web Applications Security Risks)

Lecture 1.1: Injection

RESOURCES:

- HTML Code Injection Vulnerability
- What is SQL & SQL Injection Theory
- Stealing Database Passwords With Advance Manual SQL Injection
- Broken Access Control
- Sensitive Data Exposure
- Security Misconfigurations

MODULE 8: (Hacking)

Lecture 1.1: Password Tool John the Ripper
Lecture 1.2: Hacking Video