CERTIFICATE IN ETHICAL HACKING (Advanced):

About Us:

Alagappa University - HebeSec Research & Development Centre,Karaikudi Provides Skills Training, Assessment and 15 days Internship Program in Cyber Security as Certification In Ethical Hacking Course for the duration of 2 Months for only the person who has fulfilled all requirements in AU-HRC's Fundamentals in Cyber Security Course.

About This Program:

The role of ethical hacker and penetration tester has emerged as one of the most important in the information security industry. Discovering system vulnerabilities internally before the bad guys exploit them can save companies millions of dollars and prevent the exposure of highly sensitive information.

In this Course certificate program, we'll cover the foundations and advancements of ethical hacking, including reconnaissance, exploitation and the rules of engagement. You'll discover how to perform password, Wireless, Web, Mobile and cloud application attacks. Don your white hat and protect your organization's valuable information with the latest industry skills and knowledge.

ADMISSION REQUIREMENTS:

To apply, you must have:

- Experience administering an operating system such as Windows or Linux
- Experience with networking and a basic understanding of networking concepts and protocols

Those who need help meeting the network administration requirements should consider enrolling in our **Fundamentals in Cyber Security** course.

TIME COMMITMENT:

- Including time in class, you should expect to spend about 5 to 7 hours each week on coursework.

TECHNOLOGY REQUIREMENTS:

- Access to a computer with a recent operating system and web browser
- High-speed internet connection
- Headset and webcam (recommended)

EARNING THE CERTIFICATE:

- You earn the certificate by adhering to the program's attendance and successfully completing all required courses. For more information, Contact us.

WHAT YOU'LL LEARN:

- How to conduct and support penetration testing on enterprise network assets
- Planning and assessment of a security profile and posture
- Analysis of an organization's computer network defense policies
- Evaluation of regulatory compliance and organizational directives

GET HANDS-ON EXPERIENCE:

- Practice various real-world hacking techniques using a virtual server
- Participate in a Capture the Flag practicum exercise

Alagappa University - HebeSec

Research and Development Centre
(AU-HRC)
Karaikudi-630001

HEBESEC TECHNOLOGIES

Duration: 2 Months(60hrs training + 60 Hrs Assessment + 15 days Internship)

Cost Per Student: Rs.8000 for 2 Months.

Course Agenda:

1	**Application Security Assessment / Audit including** • Web Application Security • Manual and Automated Assessment
2	**Network Penetration Testing & Vulnerability Assessment**

Web Application Security

1	Fundamentals and Essentials
2	**Introduction to OWASP top 10** Injection Flaws
3	Broken Authentication and Session Management
4	Sensitive Data Exposure
5	XML External Entity (XXE)
6	Broken Access Control
7	Insecure Direct Object Reference
8	Security Misconfiguration
9	Cross Site Scripting (XSS)
10	Insecure Deserialization
11	Using Components with Known Vulnerabilities
12	Insufficient Logging & Monitoring
13	Cross Site Request Forgery
14	Unvalidated Redirects and Forwards
15	Cryptography Based Attacks
16	Password Related Vulnerabilities
17	Phishing Attack
18	Tools Demo and Hands-on for Web Application Vulnerability detection i. Nikto ii. Xenu iii. DirBuster iv. SQL Map (exploitation) v. Burp Pro Components vi. Web inspect
19	Other General Topics i. Offensive & Defensive face of Penetration Testing ii. OSINT Penetration Testing Methodology iii. OWASP Penetration Testing Methodology iv. NIST Security Testing & Standards v. Penetration Testing Plan Template vi. Security Assessment Plan Template vii. Exploit & CVE Expose Tools

Network Penetration Testing

I	Network Security Fundamentals and Essentials Common PT methodologies i. OSSTMM ii. SANS 20 CSC iii. PTES iv. MITRE attack framework Protocol Introductions (http, https, FTP, SMTP etc) Introduction to Penetration testing
II	Introduction to Networking and Network Security Introduction to different network Components Introduction to Kali Linux Getting used to Linux CLI and hands-on
III	Deep-Dive on the OSI Model / TCP IP Stack
IV	Introduction to Nmap Port scanning commands and hands on of Nmap commands OS Detection Techniques through Nmap Service Fingerprinting through Nmap
V	Vulnerability Scanning and detection (NSE, Nessus & Nexpose) Vulnerability Exploitation and Penetration Testing Post Exploitation using Metasploit
VI	Analysis & Reporting Defense Mechanisms

Note:

- This Certification Course is Based on AU-HRC's Fundamentals In Cyber Security Course
- Certificates Will be Provided only after the completion of Assessment.
- You Will Receive Both AU-HRC's Completion Certificate and Internship Certificate

If Any Questions, Please Contact 9566022629