ETHICAL HACKING

The digital world is Double Edged SWORD- while it brings convenience and connectivity ,

it can also be open doors to cyber threats.

Ethical Hacking is a Crucial practice of legally protecting the orgnaisation's and to identify vulnerabilities before malicious hackers exploit them.

What is Ethical Hacking Exactly??

Ethical Hacking is also known as Penetrating Test or White-Hat Hacking.

It is practice of legally breaking systems,networks and applications of organisation to strengthen their defenses.

Unlike Black-hat hackers(criminal hackers), White-hat hackers are good hackers.

One who do Ethical hacking is called anEthical Hacker.

THE ROLE OF AN ETHICAL HACKER:

Ethical Hackers job is to think like a cyber criminals -BUT act with Integrity.

Ethical hackers have some responsibilities includes:

1**.** Penetrating test: determing or discovering the weaknesss of the sytems.

2. Network and security audits: Accessing the firewalls,routers and security policies.

3. Social engineering testing: detecting how easily employees can be manipulated for revealing the sensitive information.

4. Reporting and fixing vulnerabilities:documenting and finding the threats and recommended the improvements in security.

Some important Tools and Technique used by an ethical hackers:

1. nmap: it is network scanning tool for discovering open ports and services.

2. metasploit: it is powerful framework for exploiting known vulnerabilities.

3. burp suite: it is web application security testing tool.

4. wireshark: it is network protocol analyser for capturing and analysing the data packets.

5. john the ripper: it is password cracking tool used to test the strength of the password.

Legal and Ethical aspects:

Ethical Hacking operates within the legal boundaries. Organisation grant ethical hackers a explicit permissions before testing their systems.

Unauthorized hacking, even it for the good event ,is considered as Illegal.

The Computer Fraud and Abuse Act(CFAA) in U.S, GDPR Regulations in Europe set some strict guidelines for cyber security professionals.

How to become an Ethical Hacker:

To be become an Ethical Hacker they must have strong foundation in Cybersecurity, Networkking and Programming.

They have to do some Certifications which are needed to become an Ethical Hacker.

1. Certified Ethical Hacker(CEH): It will cover Tools and Techniques of hacking.

2. Offensive security Certified Professionls(OSCP): It covers some skills of security policies and hands on penetration testing.

3.CompAIT Security++: Entry level Hacking certification.

4. Certified Information System Security Professionals (CISSP): It is a globally recogination certificate for the ethical hackers and advanced security management.

Conclusion:

Ethical Hacking is an important essential practice in todays's cyber-threats landscape. By proactively identifying and fixing vulnerabilities, ethical hackers help organisation by stay ahead of cybercriminals.

As Technology evolves Cyber Threats are also increasing so we need Ethical Hackers .