INTRODUCTION TO ETHICAL HACKING

By HackitTech

What is Hacking

- Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized access to the system.

  Eg:- Stealing, disclosure of Sensitive information.

Why Hack Happens?

- ATTACKS = MOTIVE(GOAL) + METHOD + VULNERABILITY
- MOTIVE:- Information theft, manipulating data, Financial loss, Revenge, Ransom, Damaging Reputation.

HackitTech

Ethical Hacking

- Ethical Hacking involves the use of hacking tools, tricks, and techniques to identify vulnerability so as to ensure system security.

- Ethical Hackers performs security assessment of their organization with the permission of concerned authorities

Why?

* To prevent hackers from gaining access

* To uncover vulnerabilities

* To strengthen the organization

* To safeguard the data

* To avoid security Breaches

* To enhance security awareness

Who can be an Ethical Hacker?

- Knowledge of Security areas
- Ability to learn
- Strong work ethics
- Forensic and Security people

HackitTech

Type of Hackers

- Black Hat
- White Hat
- Gray Hat
- Suicide Hackers
- Script Kiddies
- Cyber Terrorists
- State Sponsored hackers
- Hacktivists

Attack Vectors

- Virus & Worms
- Ransomware
- Mobile Threats
- Botnets
- Phishing
- Insider Attacks
- Cloud threats

Terminologies

- Hack Value
- Vulnerability
- Payload
- Exploit
- Zero-Day-Attack
- Daisy Chaining
- Doxing
- Bot

Phases of Hacking

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks or Logs

Zones

- Internet zone
- DMZ
- Production Network Zone
- Intranet Zone
- Management network Zone

HackitTech

Security Policies

- Access Control Policy
- Firewall Management Policy
- Password Policy
- Email Security Policy
- Information protection policy
- Special access Policy
- User account policy

HackitTech

Physical Security

- Preventive controls – Security Guard
- Detective controls – CCTV, Motion Detectors
- Deterrent controls – Warning Signs
- Recovery controls – Backup systems, recovery plans.

Penetration Testing

- Penetration Testing is a method of evaluating the security of an information system or network by simulating an attack to
- find vulnerability
- Security Measures
- Documentation and Report Preparation

Need?

1)Identification of threats

2)Security Protections and controls

3)Assessment of Organization's Security

4)Evaluation of Network Security

5)Upgradation of Infrastructure.

Types of Pentesting:

- 1)Black Box - No prior Knowledge
- 2)White Box - Complete Knowledge
- 3)Grey Box - Limited Knowledge

Standards and Compliances

1) Payment Card Data Security Standard (PCI DSS)

2) ISO/IEC 27001:2013

3) Health Insurance Portability and Accountability Act(HIPPA)

4) Sarbanes Oxley Act(SOX) – To prevent fraudulent Financial Activities(shares)

5) The Digital Millennium Copyright Act(DMCA) – Copyrights

6) Federal Information Security Management Act(FISMA) – Natural and Man Made threats

7) Governance, Risk Management and Compliance (GRC)

8) General Data Protection Regulation (GDPR) – EU and Transfer outside EU

HackitTech

Cyber Laws

- Section 43 - Damage to computer System
- Section 65 – Tampering of Computer Source Documents
- Section 66 – Computer Related Offences
- SECTION 66 A – Sending offensive Messages
- SECTION 66 B – Smuggling goods
- SECTION 66 C – Identity theft
- SECTION 66 D – False Personation(Telecallers)
- SECTION 66 E – Violation of Privacy
- SECTION 66 F – Cyber Terrorism

Cyber Laws – Cont’d

- SECTION 67 – Transmitting Obscene Material
- SECTION 71 - Misrepresentation
- SECTION 72 – Breaching of Confidentiality and Privacy
- SECTION 73 – Publishing Electronic Signatures

HackitTech

THANK YOU