

Ethics & Hacking



What they are ??

- Ethics :
 - Moral principles that govern a person's or group's behavior
- Hacking :
 - Practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose

Hacking : How it all began ??

- been around for more than a century
- 1870s, several teenagers were flung off the country's brand new phone system by enraged authorities

Hacking in the past 40 years

- 1960s – MIT's artificial intelligence lab, became staging grounds for hackers.
- 1970s – John Draper makes a long-distance call for free



Hacking in the past 40 years

- 1980s – Kevin Mitnick, secretly monitors the e-mail of MCI and Digital Equipment security officials
- 1990s – Hackers break into and deface federal Web sites, including the U.S. Department of Justice, U.S. Air Force, CIA, NASA and others.



Why is security needed ??

- information is a strategic resource
- a significant portion of organizational budget is spent on managing information
- have several security related objectives
 - confidentiality - keep info secret
 - integrity - protect info accuracy
 - availability - ensure info delivery

Ethical Hacking

- Process of legally hacking the information that is considered to be confidential
- a.k.a Intrusion Testing, Penetration Testing or Red Teaming
- CEH, by EC-Council

continued...

Ethical Hacking

- Ethical Hacker :
 - An expert hired by an organization, to attempt to attack their network and computer system, the same way a hacker would
 - Uses same techniques & tactics used by the hackers
 - End result is the company's ability to prevent an intrusion, before it occurs

Ethical Hacker	Hacker
1. Done legally with permission of the respective organization.	1. Done illegally without the consent of the respective organization.
2. Done in an attempt to prevent malicious attacks from being successful.	2. Done in an attempt to make malicious attacks possible.
3. Discloses any vulnerabilities discovered.	3. Exploit discovered vulnerabilities.

Types of Hackers

- Script Kiddies :
 - Amatuers, copy others codes to attack
- White Hat Hackers :
 - Professional term for ethical hackers
- Black Hat Hackers :
 - Professional term for malicious hackers
- Gray Hat Hackers :
 - Combination of both, hack to learn
 - Self-proclaimed ethical hackers

Types of Hackers

- Hacktivists :
 - Hacker + Activists
- State Sponsored Hackers :
 - Limitless time & funding by govt.
- Spy Hackers :
 - Hired hackers by corporations
- Cyber Terrorists:
 - Motivated by religious / political beliefs
 - Spread fear, terror, and commit murders

Steps Involved :

- Footprinting / Information Gathering :
 - Gathering potential information about target system
 - A good hacker consumes 90% of time for this phase
- Scanning :
 - Network is scanned for any vulnerabilities

Steps Involved :

- System Hacking :
 - Involves actual hacking
 - Taking advantage of vulnerabilities found during scanning, & penetrate the victim's system
- Maintaining Access :
 - Making provisions by planting backdoors
- Covering Tracks :
 - Removing all the traces of his presence in system by removing log files & event logs

Thank you!!