12-5-2025

Ethical hacking

Indr[redacted] Sengupta

Lecture - 01 Week - 1

what is ethical hacking

-> It refers to the act of locating weakners & vulnerabilities of Computer & information System by replicating the intent & actions of malicious hackers.

-> ethical hacker mimics the same as an hacker.

-> It is also known as penetration testing, intrusion testing & red teaming.

Ethical hacking

↳ employed by Companies to perform penetration testing.

Penetration testing

↳ legal attempt to break into the Company's network to find the weak links.

- Testers only report findings, does not provide Solutions.

Security tester:-

↳ also include Company Security policies & procedures

- Testers offer Solutions to Secure or protect the network

Some terminologies

- Hacking :- Showing computer expertise.
- Cracking :- breaching security of Software & System
- Spoofing :- Faking the originating IP address in datagram.
- Denial of Service (DOS) → flooding a host with sufficient network traffic so that it cannot respond anymore.
  - one or collection of computers/nodes they can flood host with most numbers of packets
  - so server will get more time to clear out junk data
- Port Scanning → Searching Vulnerabilities
  ~~ports indicate some entry points where~~
  in pc there are many programs running so they are already associated with some port numbers they are basically the entry points to the hacker.

Gaining Access

Front Door

- Password guessing (guess valid pass)
- password / key Stealing

Back door → are some entry points which are kept by developers, such as root pass of router of house

- often left by original developers as debug and diagnostic tools.

Trojan Horses → Software code hidden inside an other big Software

- usually hidden inside a Software that we download & install from the net.
- Mainly install backdoors which help hackers to gain ~~ghost entry point~~ in PC

Software Vulnerability exploitation

- often advertised by OEMs website along with Security patches.
- fertile ground for Script kiddies, looking for something to do. → new hackers (noob)

Once inside, the hacker can

- Modify logs (keeps tracks who did login at
  - ~~to track their track~~
  - to cover their tracks

So hackers delete their logs to developer cannot track that actually hacking happened or not.

- Steal files.
  - Sometimes destroy after stealing
  - An expert hacker would steal & cover their tracks to remain undetected

---

- Modify files.
- To let you know they were there.
- To cause Mischief.

- Install back doors.
  - more dangerous and the user cannot actually know that there data is been shared.
  - So they can get in again when they want.

The Role of Security & penetration Testers.

- Script Kiddies or packet Monkeys.
  - young or inexperienced hackers.
  - Copy Code & techniques from knowledgeable hackers.

- Experienced penetration testers write program or scripts using Perl, C, C++, Python, JavaScript,

Penetration testing Methodologies

- Tiger box
  - Collection of OSs and hacking tools.
  - usually on a laptop
  - Helps penetration testers & Security testers Conduct Vulnerability assessments & attacks.

- White box model
  - They are told everything about network topology & technology.
  - Testers is authorized to interview the IT personnel & Company employee.
  - That actualy makes the testers' job easier.

- Black box mode
  (reverse of white box mode)

- Tester is not given details about network.
- Burden is on the tester to find details.

- grey box model

  Hybrid of white & black box.
  given testers the partial information because some information might not be available with company too.

What You Can legally do

- laws involving technology change rapidly as technology itself.
- laws what is legal for you locally
  - laws change from place to place.
- Be aware of what is allowed & what is not allowed

Laws of the land.

↳ Tools on your Computer might be illegal to possers.

- Access a Computer without permission
- installing Viruses or worms.
- DOS attacks are illegal
- Denying users access to network resources.

Ethical hacking in Nutshell

→ what it takes to be Security tester

- Knowledge of [networks] & [Computer technology]
- ability to [Communicate with management] & IT personell
- understanding of the laws.
- Ability to use [necessary tools]