



Basics Of Hacking

@Ishan Jogalekar :

<https://www.linkedin.com/in/ishan-jogalekar-1708421a5>

Hacking :-

Hacking is method to find computer data and use it for breaching defenses and exploiting weaknesses in a computer system or network.

Basically there are different techniques in hacking to find weaknesses of computer security.

It is mainly related to cyber security.

Bypass limitation on product or software (like applying patch on software and use it as pirated) is also consider as form of hacking.

Information Security :-

Information security is field that deals with being protected against unauthorized usage of information especially from aspects of technology.

It relies of its three principles that must be sustained.

1. Confidentiality
2. Availability
3. Integrity

Cyber Security :-

Cyber security deals with specifically with defending , security system & network against cyber attacks.

In world cyber security , the term usually associated with obtaining unauthorized access to remote or local system.



Cyber security is divided into two main parts :

- **Defensive side :- Blue team**
- **Offensive side :- Red team**

Responsibility Distributions :

1. **Red team** : Security experts responsible for **a. Active investigations b. Probing of the system** Also for **a. Bench Test b. Tests on live system**
2. **Blue team** : Composed of InfoSec + Cyber security experts
Deal with -
 - a. Defending systems by changing with settings.
 - b. Configuring & Maintaining security measures on perimeter and outside.
3. **Purple team** : Not officially belong to any team but deals with works of red & blue team both.

Types of Hackers :

1.  **White Hat** :
 - Ethical hackers .
 - Experts in compromising computer.
 - Use there ability for good purpose.
2.  **Black Hat** :
 - Illegal hackers.
 - Violate system for personal gain like money , power , politics , revenge or causing damage .

- Operate on their own or in small groups .
- Black hat hackers' activities are mostly criminal & illegal .

3. Grey Hat :

- Between Black hat & white hat hackers .
- Sometimes hacking for good purpose and legal .
- But mostly works as underground groups and commit some criminal activity .

So, always hack as ethical and with permission



Hackers - State of Mind :-

- Basic thought that there is always " WAY IN " for any software , database and any other system.
- Hackers are seek the challenges , competitive & constantly developing , changing their techniques for hacking .
- Hacker need to find only 1 flow or error , loophole .



Terminology :-

1. Vulnerability :

A security flow that attacker can exploit to gain access into network , system or application.

2. Exploit :

Implementation of vulnerability in the form of code or poc (proof of concept) that can be used to achieve goal of remote access , privilege of escalation etc.

3. Threat :

Possible danger that asset might be compromised due to breach & cause harm to the system.

4. Malware :

Piece of software that carries a payload that can exploit a vulnerability within system & perform different actions on site and software.

5. Virus :

Virus is type of malicious software that when it is executed , replicates itself by modifying other computer programs & inserting its own program in other program of system

eg : Virus infecting other files in computer modifying them and deleting them etc.

6. **Worm :**

Computer worm is type of malware that spreads of copies of itself from one computer to other also through network , it does not need to attach itself to any software or need to be execute by user . It is automatically starts affecting system once get downloaded or pushed into system.

It mainly cause lesser damage than viruses.

7. **Trojan :**

Software that usually arrives from email or pushed to users when they visited infected websites. Trojan is like covered malicious program with some normal working program. Trojan must be executed by victim & typically provide remote access to attacker.

8. **Ransomware :**

Type of malware programs that encrypts the systems data & holds it hostage waiting for crypto currency or any other payment.

9. **Scareware :**

For of malware which uses social engineering that tricks users to believe their computer is infected with fictional malware & suggest fake malicious software as solution.

Attacks Now days :-

- Despite modern improvements in security , attack statistics keep growing.
- 300 + attacks in US in 2015-16.
- About 1 link in every 13 URLs on web is malicious link.
- [Recent attacks :](#)

1. New vulnerabilities on both old & new softwares.

2. There is usually a time window between when vulnerability is discovered until get patched.

3. 1/3 computers facing some security issues even though vulnerability is patched before.

4. Facebook data leak about 533 million accounts .

<https://haveibeenpwned.com/> : Website to check your data is leaked publicly or not.



Data Breaches :-

- Not all attacks brought to public knowledge.
- Main idea behind this is to get victims name , emails , passwords etc.

Common Attack Flow :-

Reconnaissance → Weaponization & Delivery → Exploitation & Installation → Escalation & Spreading → Remote actions

Attack Domains :-

- Applications : Through websites
- Infrastructure & Hardware
- Password attacks : Using Remote keylogger
- Mobile phones
- IOT devices hacking to create data breaches.
- System hacking , changing OS preferences.
- Hacking emails other social media platforms.

Mainly used OS for Hacking :

1. **Kali Linux** : Debian based , many tools , most used

Link : <https://www.kali.org/>

2. **Parrot OS** : Debian based , more customizable , less configured than kali

Link : <https://www.parrotsec.org/>

Mostly these OS installed in virtual environment

1. **Virtual box** : Most used , advance , free

Link : <https://www.virtualbox.org/>

2. **VMware** : Commonly used with MAC PC , mostly free but some features paid

Link : <https://www.vmware.com/in.html>