## **Introduction to Hacking**

## 

## **What Is Hacking? - Hacking is the process of identifying and exploiting weakness in a system or a network to gain unauthorized access to**

## **data and system resources by compromising the security.**

## 

## **Example of Hacking: Exploiting the weakness of default password to gain access to the data stored**

## **inside the system.**

## 

## **What is Ethical Hacking? -**

## 

## **Ethical Hacking sometimes called as Penetration Testing is an act of intruding/penetrating into system or networks to find out threats,**

## **vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages.**

## 

## **What is the Purpose of Ethical Hacking? - The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found**

## **during testing.**

## 

## **Who is an Ethical Hacker - An Ethical Hacker is a skilled professional who has excellent technical knowledge and skills and knows how to identify**

## **and exploit vulnerabilities in target systems. He works with the permission of the owners of systems.**

## 

## 

## 

## 

## **Types of Hackers -**

## 

## **1. Black Hat Hackers - Black-hat Hackers are also known as an Unethical Hacker or a Cracker. These people hack the system illegally to steal**

## **money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can**

## **also modify or destroy the data as well. Black hat hacking is illegal.**

## 

## **2. White Hat Hackers - White Hat hackers are also known as Ethical Hackers. They never intent to harm a system, rather they try to find out weaknesses**

## **in a computer or a network system as a part of penetration testing and vulnerability assessments. Companies hire them to test their system.**

## 

## **3. Grey Hat Hackers - Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a**

## **security weakness in a computer system or network without the owner’s permission or knowledge.**

## **Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.**

## 

## **4. Suicide Hackers - Suicide hackers are those who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any**

## **other kind of punishment. Suicide hackers are similiar to suicide bombers who sacrifice their life for an attack and are thus not concerned with the**

## **consequences of their actions.**

## 

## **5. Script Kiddies - Script Kiddies are amateurs in the field of hacking. They try to hack the system with scripts from other fellow hackers. They try**

## **to hack the systems, networks, or websites. The intention behind the hacking is just to get attention from their peers. Script Kiddies do not have complete**

## **knowledge of the hacking process.**

## 

## **6. State-Sponsored/Country-Sponsored Hackers - State-sponsered hackers are those individuals employed by the government to penetrate, gain top-secret information**

## **and damage the information systems of other governments.**

## 

## **7. Hacktivist - Hactivist breaks into government or corporate computer systems as an act of protest.**

## **In general, most hacktivism involves website defacement or denial of-service attacks.**

## 

## **Rules for Ethical Hacker :**

## **1. Get a written permission from the owner/organization before performing the hacking.**

## **2. Maintain the privacy of that organization.**

## **3. Transparently report to the owner/organization about the weakness.**

## **4. Inform the related issue to the software and hardware vendor.**

## 

## **Type of Cyber Crime :**

## **1. Spam - Fake Mailing System etc.**

## **2. Privacy Violation - Exposing the data over the internet.**

## **3. Identity Theft - Stealing information from the system/network**

## **4. Sharing Copyrighted files/informtion - leaking the confidential files**

## **5. Eletronic Money Transfer - Net Banking - Transaction Procedure**

## **6. Electronic Money Laundering - Convert Black money to white**

## **7. ATM Fraud - Cloning of atm card**

## **8. DOS Attack - Denial of Service Attack (Router/ Server)**

## **9. MITM Attack - Man in the Middle Attack (Capturing packets)**

## 

## **TYPES OF INFORMATION :**

## **1. Confidentials Information - Aadhar Cards, Votar card, Birth Certificates, PAN Cards etc.**

## **2. Financial Information - Financial Statements, Bank Details, Login Credentials for banking poractices etc.**

## **3. Health Information - Policies, Diseases etc.**

## **4. Personal Information - Address, Phone Numbers, DOBs etc.**

## 

## **Motive for hacking :**

## **1.Hobby**

## **2.Defame/Revenge**

## **3.Stealing information**

## **4.Leaking information**

## **5.Security Reasons(Penetration Testing)**

## **6.Just For Fun**

## 

## **Essential Terminology :**

## 

## **Hack value**

## **It is a notion among hackers that something is worth doing or is interesting.**

## 

## **Vulnerability**

## **Existence of a weakness, design, or Implementation error that can lead to an unexpected event**

## **compromising.**

## 

## **Payload**

## **Payload is the part of an exploit code that performs the intended malicious action,**

## **such as destroying creating backdoors, and hijacking computer.**

## 

## **Exploit**

## **A Breach of IT system through vulnerabilities.**

## 

## **Zero-Day Attack**

## **An attack that exploits computer application vulnerabilities before the software**

## **developer releases a patch for the vulnerability. Basically they don't have patch of this vulnerability, hackers can**

## **exploit this vulnerability regularly.**

## 

## 

## 

## **Some Important Characterstics Of Information Security -**

## 

## **CIA Traid = Confidentility - Integrity - Availability - A concept that focuses on the balance between the confidentiality, integrity and availability of data**

## **under the protection of your in**

## 

## 

## 

## **information security program.**

## 

## **Confidentility - Confidentiality ensures that an Information is accessible to only an authorized user. The main purpose of confidentiality is to protect the**

## **sensitive information from reaching the wrong hands.It is used to maintain the privacy of the people. Encryption is a good example of confidentiality.**

## 

## **Integrity - Integrity maintains the correctness or accuracy of the information while the data is in transit, storage or processing. It is the guarantee that**

## **information is trust worthy and not tampered. This attribute ensures that an unauthorised person will not be able to modify the data.**

## **RSA digital signature, SHA1 hash codes are good examples.**

## 

## **Availability - Information should be available to an authorised person when it is requested for. It is the guarantee of access to the authorised individual**

## **to information. Keeping all the hardware and software up to date and keeping back up, taking proper recovery measures will ensure availability of data.**

## **horizontal line**