**Vulnerability Research-Legal implication of hacking, Impact of hacking-**

**Vulnerability Research-**

Vulnerability research is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.

Vulnerability Research is the process of analyzing a product, protocol, or algorithm - or set of related products - to find, understand or exploit one or more vulnerabilities.

**Types of vulnerability**-

* Network vulnerabilities
* Operating system vulnerabilities
* Process (or procedural) vulnerabilities
* Human vulnerabilities

**Network vulnerabilities** are weaknesses within an organization’s hardware or software infrastructure that allow cyber attackers to gain access and cause harm. These areas of exposure can range from poorly-protected wireless access all the way to misconfigured firewalls that don’t guard the network at large.

**Operating system (OS) vulnerabilities** are exposures within an OS that allow cyber attackers to cause damage on any device where the OS is installed. An example of an attack that takes advantage of OS vulnerabilities is a Denial of Service (DoS) attack, where repeated fake requests clog a system so it becomes overloaded. Unpatched and outdated software also creates OS vulnerabilities, because the system running the application is exposed, sometimes endangering the entire network.

**Process vulnerabilities** are created when procedures that are supposed to act as security measures are insufficient. One of the most common process vulnerabilities is an authentication weakness, where users, and even IT administrators, use weak passwords.

**Human vulnerabilities** are created by user errors that can expose networks, hardware, and sensitive data to malicious actors. They arguably pose the most significant threat, particularly because of the increase in remote and mobile workers. Examples of human vulnerability in security are opening an email attachment infected with malware, or not installing software updates on mobile devices.

**Legal implication of hacking -**

**It is legal as long as it is done with the owner's permission to find loopholes in the system and offer solutions to improve it. Also, it protects the system from further damage caused by the hacker.**

* **Hacking crosses the criminal line when a hacker accesses someone else's computer system without such consent or authority. For example, a hacker can be charged with a crime if they lack consent or any lawful authorization to enter another's computer system.**
* **If hackers attack your website, they will view, leak or damage the information. And data breaches can make your business shut down. Of course, you are the one who will pay for it. Besides, you might be a victim of a ransom attack if your website contains users' private data.**
* **Identity theft creates financial problems for both organizations and individuals. When cyber criminals acquire a victim's financial information, they can steal money from his account or take loans in his name. This can cause the victim a lot of financial problems.**

**Impact of hacking-**

**Hacking can create a variety of damages to people, groups and systems of broad spectrum. Negative Hacking Interactions: Identity Theft – Some hackers can gain access to sensitive information which could be used to fuel identity theft.**

**Impact of hacking on society-**

**It can leak sensitive user data and risk user privacy. Hacking exposes confidential information of the user. Identity theft online is another important hacking effect. Hacking may also danger your national security and fraud also is another major effect of computer hacking.**

**Hackers use a variety of techniques to achieve their aims. Some of the most common methods include:**

* **Social engineering**

**Social engineering is a manipulation technique designed to exploit human error to gain access to personal information. Using a fake identity and various psychological tricks, hackers can deceive you into disclosing personal or financial information. They may rely on phishing scams, spam emails or instant messages, or even fake websites to achieve this.**

* **Hacking passwords**

**Hackers use different ways to obtain passwords. The trial and error method is known as a brute force attack, which involves hackers trying to guess every possible combination to gain access. Hackers may also use simple algorithms to generate different combinations for letters, numbers, and symbols to help them identify password combinations. Another technique is known as a dictionary attack, which is a program that inserts common words into password fields to see if one works.**

* **Infecting devices with malware**

**Hackers may infiltrate a user’s device to install malware. More likely, they will target potential victims via email, instant messages and websites with downloadable content or peer-to-peer networks.**

* **Exploiting insecure wireless networks**

**Rather than using malicious code to infiltrate someone’s computer, hackers may simply take advantage of open wireless networks. Not everyone secures their router, and this can be exploited by hackers driving around looking for open, unsecured wireless connection. This is an activity known as wardriving. Once hackers are connected to the unsecured network, they only need to bypass basic security to gain access to devices connected to that network.**

* **Gaining backdoor access**

**Hackers may create programs that search for unprotected pathways into network systems and computers. Hackers may gain backdoor access by infecting a computer or system with a Trojan horse, created by hackers to acquire and steal important data without the victim noticing.**

* **Spying on emails**

**Hackers can create code which allows them to intercept and read emails. Most email programs today use encryption formulas which mean that even if hackers intercept a message, they can't read it.**

* **Logging keystrokes**

**Some programs allow hackers to track every keystroke a computer user makes. Once installed on a victim's computer, the programs record each keystroke, giving the hacker everything, they need to infiltrate a system or steal someone’s identity.**

* **Creating zombie computers**

**A zombie computer, or bot, is a computer that a hacker can use to send spam or commit Distributed Denial of Service (DDoS) attacks. After a victim executes a seemingly innocent code, a connection opens between their computer and the hacker's system. The hacker can then secretly control the victim’s computer, using it to commit crimes or spread spam.**

Cybersecurity hacking can cause real havoc. Whatever technique hackers use, once they have gained access to your data or devices, they can:

* Steal your money and open credit card and bank accounts in your name
* Destroy your credit rating
* Request new account Personal Identification Numbers (PINs) or additional credit cards
* Make purchases on your behalf
* Add themselves or an alias that they control as an authorized user so it’s easier to use your credit
* Obtain cash advances
* Use and abuse your Social Security number
* Sell your information to others who will use it for malicious purposes
* Delete or damage important files on your computer
* Obtain sensitive personal information and share it, or threaten to share it, publicly