**Activity – Threats to organisations**

**Task:**

1. Describe the various types of threat/problems to organisations, systems and data
2. Advanced Persistent Threats

* It is the time spent on probing your system.

Very costly and intelligent which is very important resource from hackers view. These are lower risk tolerance than other hackers and are carefully planned and find out the users vulnerabilities.

1. Cyber-attacks (groups)

* These are groups with gather information from organisations and users by hacking into devices or software.

1. Nation sponsored hackers –

These are hackers which hack into other nations to gain information about the nation’s strategies and plans to

1. Power Loss –

It is used to cause power outages to impact business and cause an imbalance in the stock market.

1. Rogue scanners –

These are wireless access points which are installed on a secure network without permission of the authorities.

1. Social engineering –

It’s the manipulation of people into performing acts of getting confidential information.

1. Human errors-

* These are basically mistakes in data entry by humans which affects the whole organisation from a simple error.

1. Robbery –

* These are cybercrimes where hackers steal money by hacking banks and organisations.

1. For each type above, what are their impacts to society/people in the working industry?

* These impact the organisations by :
* Sales
* Economy
* Bankruptcy
* Business
* Loss in assets

1. What are the following types of hackers and what are their intentions.

* 1. **Script Kiddlie-**

They copy code and use it for a virus or a SQLi or something else.

**2. White Hat** –

Also known as ethical hackers, White Hat hackers are the good guys of the hacker world.

3. Black Hat –

Also known as crackers, these are the men and women you hear about in the news.

4. Gray Hat –

Nothing is ever just black or white; the same is true in the world of hacking.

5. Green Hat –

These are the hacker “n00bz,” but unlike Script Kiddies, they care about hacking and strive to become full-blown hackers.

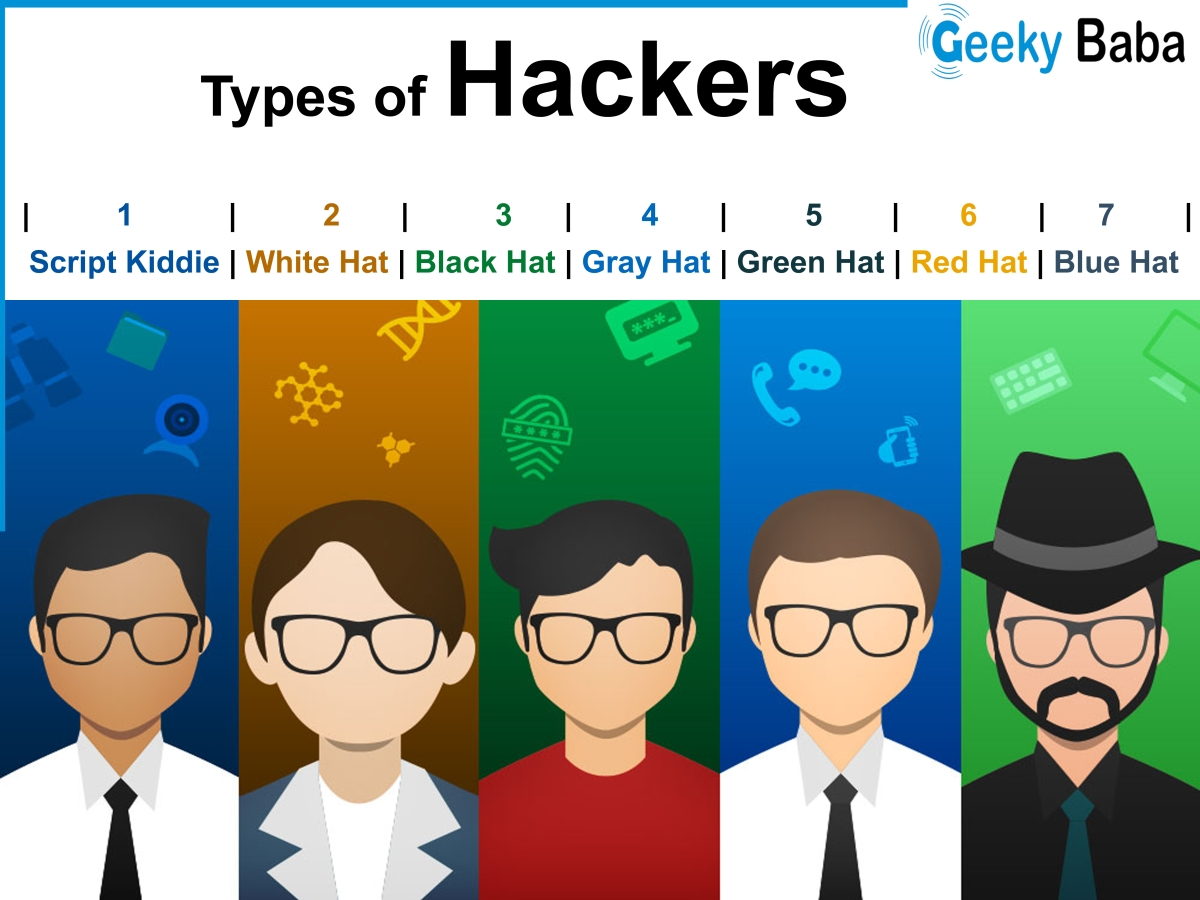
6. Red Hat –

These are the vigilantes of the hacker world. They’re like White Hats in that they halt Black Hats, but these folks are downright SCARY to those who have ever tried so much as Pen Test.

7. Blue Hat –

If a Script Kiddie took revenge, he/she might become a Blue Hat. Blue Hat hackers will seek vengeance on those who’ve them angry.

1. What are the tools being used by these types of hackers and why?



* 1 – Metasploit Framework. The tool that turned hacking into a commodity when it was released in 2003, the Metasploit Framework made cracking known vulnerabilities as easy as point and click. ...

2 – Nmap. ...

3 – OpenSSH. ...

4 – Wireshark. ...

5 – Nessus. ...

6 – Aircrack-ng. ...

7 – Snort. ...

8 – John the Ripper.

9 – Google

10 – L0phtCrack