Hacking-Terminologies

1. `Threat ⇒`

> An entity or action that has the capacity to exploit a vulnerability

OR

> A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.

2. `Vulnerability ⇒`

> A `bug` or `error` or `weakness` in software, operating systems, or firmware that can be exploited, which can lead to a system compromise

3. `Risk ⇒`

> The probability of a threat exploiting a vulnerability

> So, **RISK** is defined as exposure to harm or loss resulting from breaches of or attacks on information systems

4. `Security ⇒`

> Security is keeping **unauthorized entities** from **doing** things you **don't want** them to do

5. `Attack ⇒`

> The action of a threat exploiting a vulnerability on a system or network

6. `Target (of Evaluation) ⇒`

> A `system, program, or network` that is the subject of a security analysis or attack

7. `Exploit ⇒`

> A `procedure` or `code` that takes advantage of a vulnerability in software, an operating system, or firmware

OR

> `Exploits` is the methods of using vulnerabilities to hack security perimeters.

8. `Remote Exploit ⇒`

> An exploit that executes over a network,
> ⇒
> without physical access to the target system

OR

> Remote exploits are exploits that you can run on an external machine.

> A remote exploit may be on a host inside an intranet, accessible only by few people, but also inside the internet, accessible by everyone.

9. `Local Exploit⇒`

> An exploit that executes directly on a target system due to previous access to the target system

OR

> Local exploits are exploits that you can run only with access to the machine

10. `Zero-Day Attack⇒`

> In this attack ⇒ the attacker exploits vulnerabilities in a computer application before the software developer can release a patch for them.

OR

> It is an attack that exploits the PC vulnerability before software engineer releases a patch

11. `Confidentiality ⇒`

> Ensuring information is only available to those authorized to have access to the information

12. `Integrity ⇒`

> Only authorized person can alter,modify,delete information and those **unauthorized person have no rights**

13. `Availability ⇒`

> The ability to use the information or resource when it is needed

14. `VIRUS ⇒`

> A virus is a **malicious program or a piece of code** which is **capable** of `copying itself` and typically has a `detrimental/harmful` effect, such as corrupting the system or destroying data.

OR

> A virus is a malicious program written in code that copies itself into a
> larger program, modifying that program.
>
> A virus executes only when its host program begins to run.
>
> The virus then replicates itself, infecting other programs as it reproduces.

15. `Worms ⇒`

> A worm is a `self-replicating virus` that does **not alter files** but `resides in active memory and duplicates itself`.

16. `MALWARE ⇒`

> Malware is an *umbrella term* used to refer to a **variety of forms of hostile or intrusive software**, including `computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.`

> In very simple word ⇒ **Malware** is ⇒ any type of **malicious software** ⇒ which is designed to harm or exploit any `programmable device, service or network`

17.. `Phishing ⇒`

> **Phishing** ⇒ is any type of **fraud method** ⇒ in which hacker sends out **legitimate-looking** emails,website etc ⇒ in an attempt **to gather personal and financial information from recipients or victim users.**

18. `Social engineering ⇒`

> Social engineering implies `deceiving someone` with the **purpose** of *acquiring sensitive and personal information*, like `credit card details or user names and passwords.`

19. `Brute force attack ⇒`

> A brute force attack is an automated and the simplest kind of method to gain access to a system or website.
>
> It tries different combination of usernames and passwords, over and over again, until it gets in

20. `Denial of service attack (DoS) and DDoS ⇒`

> A `denial of service (DoS)` attack is a **malicious attempt** to make a server or a network resource `unavailable to users`, usually `by temporarily interrupting` or `suspending the services of a host connected to the Internet`.

> DDoS ⇒ Distributed denial of service attack.

5. `Attack ⇒`

> The action of a threat exploiting a vulnerability on a system or network