

1. Malware



SPYWARE



VIRUS



TROJAN HORSE



WORMS



ADWARE



RANSOMWARE



BACKDOOR



SCAREWARE



ROOTKIT

- replicates itself and spreads from one computer to another through the network.
- encrypting data and then demands the owners to pay money for the data to be decrypted.
- works in the background of a computer system and can remotely access the resources
- secretly collects data and sends to another person without the awareness owner.
- infects a computer when executed and then replicates itself to pass to another computer by USB drives, network shares or email.
- found in image files, audio files or games and do not self-replicate but carry out malicious operations.
- designed to modify the operating system
- designed to deliver advertisements to a user on a web browser automatically.
- is warn the user that the system is at risk and needs to run a specific program. If the user accepts the computer system infected

Column A

1. Fake prize message

2. Fake login page

3. Stranger asking for login details C. Stealing login credentials

Column B

A. Asking for a password

B. Promising a prize to trick students

3. Denial-of-service



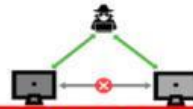
Distributed DoS

1



Botnet

2



On-Path-Attack

3



SEO poisoning

4



Attackers use popular **search terms** and use SEO to **push malicious sites** to higher up the ranks of search results.



Through system commands, **attackers control** a **group of bots** in hundreds of thousands of bots connected through the internet.



The attack is designed to **deny service** to legitimate users by overwhelming the target with traffic, causing it to slow down or crash.



This attack intercepts or modifies **communications between two devices**, such as a web browser and a web server, to collect information from the devices.

4. Wi-Fi password cracking

Match: the words:

1. Password spraying  	2. Dictionary 
3. Rainbow 	4. Traffic interception 
5. Brute-force  	

-  1. Trying **numerical values** of passwords from a large dictionary.
-  2. Trying a **few commonly** used passwords
-  3. Trying every possible **combination** of **letters, numbers, and symbols**
-  4. Trying every **word** in a dictionary
-  5. Trying read plain **text** or unsecured passwords.