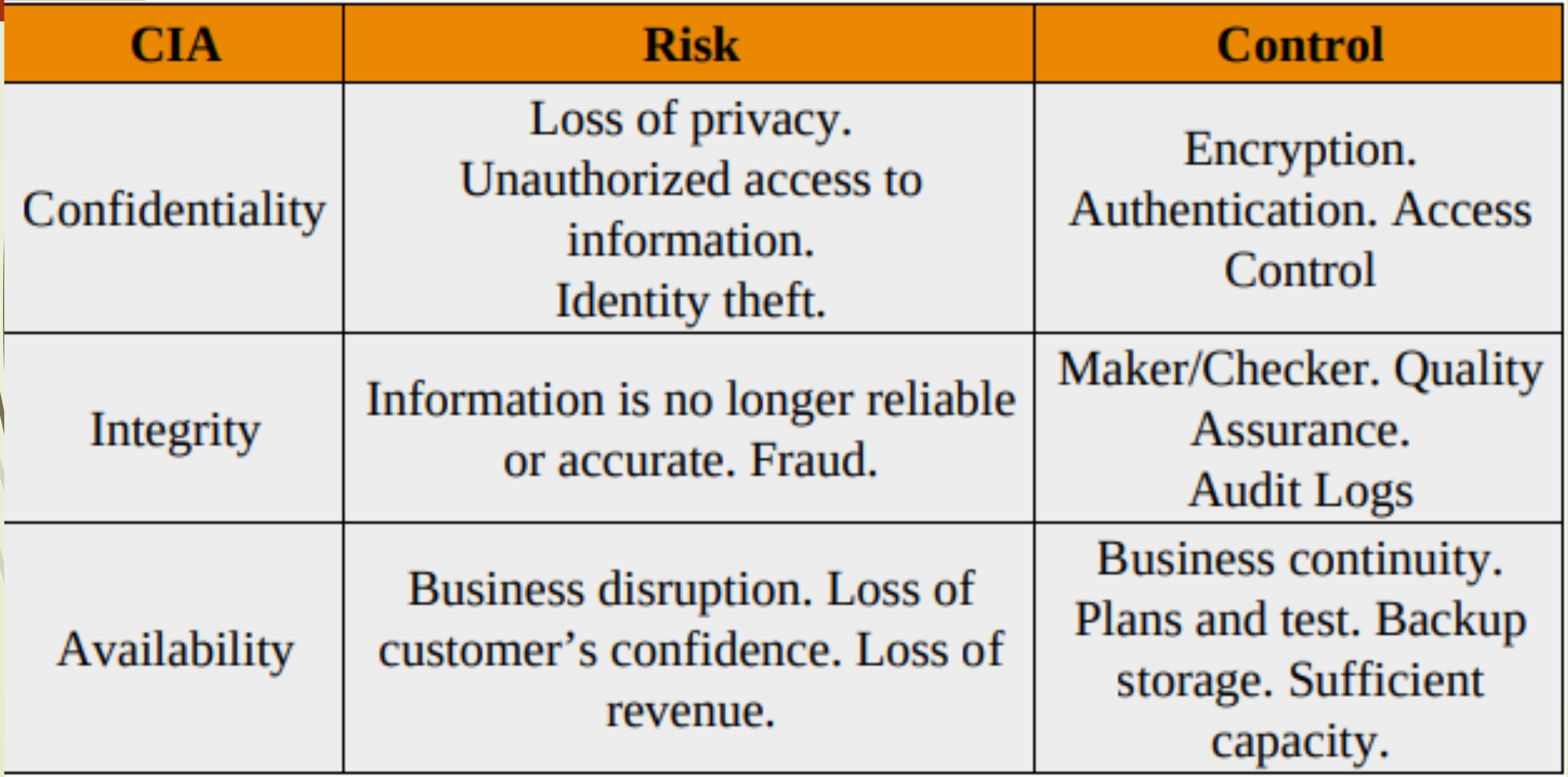
Welcome to
Cyber Security Training

Topic Outline

- Introduction to Ethical Hacking
- Introduction of Kali Linux
- Footprinting and Reconnaissance
- Enumeration / Scanning Networks
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Social Engineering
- Hacking Web Servers
- Steganography

CIA Triad



CIA	Risk	Control
Confidentiality	Loss of privacy. Unauthorized access to information. Identity theft.	Encryption. Authentication. Access Control
Integrity	Information is no longer reliable or accurate. Fraud.	Maker/Checker. Quality Assurance. Audit Logs
Availability	Business disruption. Loss of customer's confidence. Loss of revenue.	Business continuity. Plans and test. Backup storage. Sufficient capacity.

Information Security Threat Categories

Network Threats

Information gathering
Man-in-the-Middle Attack

- Sniffing & Eavesdropping
- Spoofing Session hijacking
- DNS & ARP Poisoning

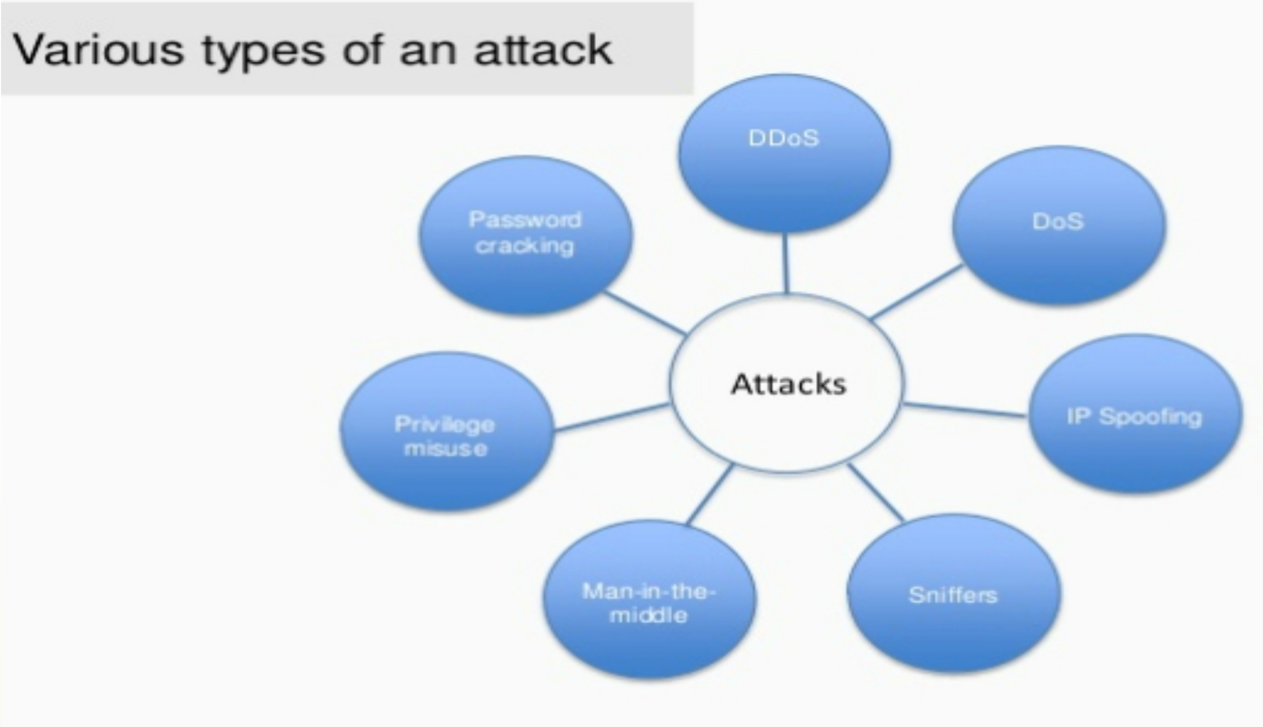
Password-based Attacks
Denial-of-Services Attacks
Firewall & IDS Attacks

Host Threats

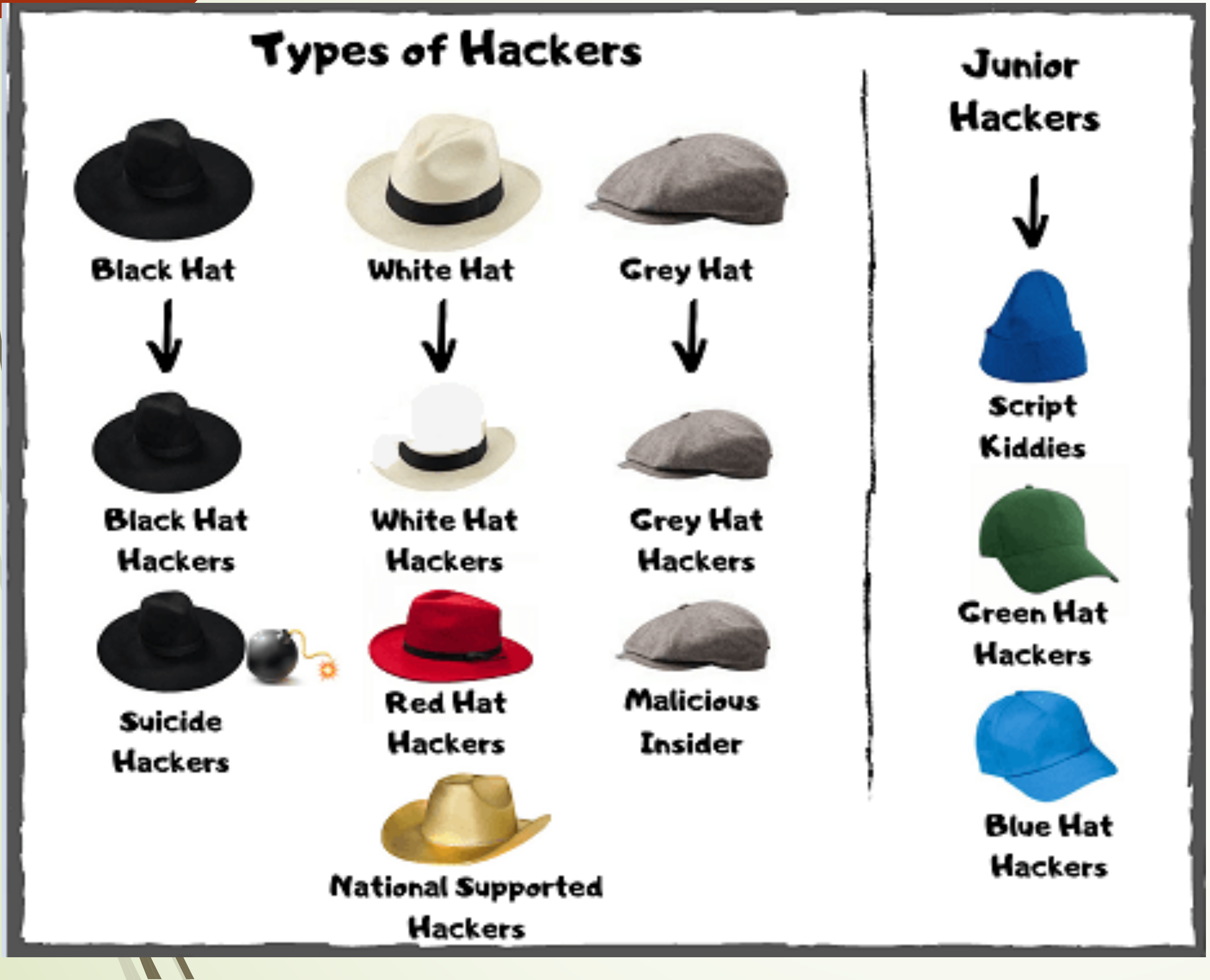
Malware Attacks
Password Attacks
Denial-of-Services Attacks
Arbitrary code execution
Unauthorized Access
Privilege Escalation
Backdoor Attacks
Physical Security Threats

Application Threats

Improper Data / Input Validation
Authentication & Authorization Attack
Security Misconfiguration
Information Disclosure
Broken Session Management
Buffer Overflow Issues
Cryptography Attacks
SQL Injection Improper


Various types of an attack

Hacking Concepts, Types, and Phases



Types of Penetration Testing

Three types of Penetration testing are important to be differentiated because a penetration tester may have asked to perform any of them.

Black Box: The black box is a type of penetration testing in which the pentester is blind testing or double-blind testing, i.e. provided with no prior knowledge of the system or any information of the target. Black boxing is designed to demonstrate an emulated situation as an attacker in countering an attack.

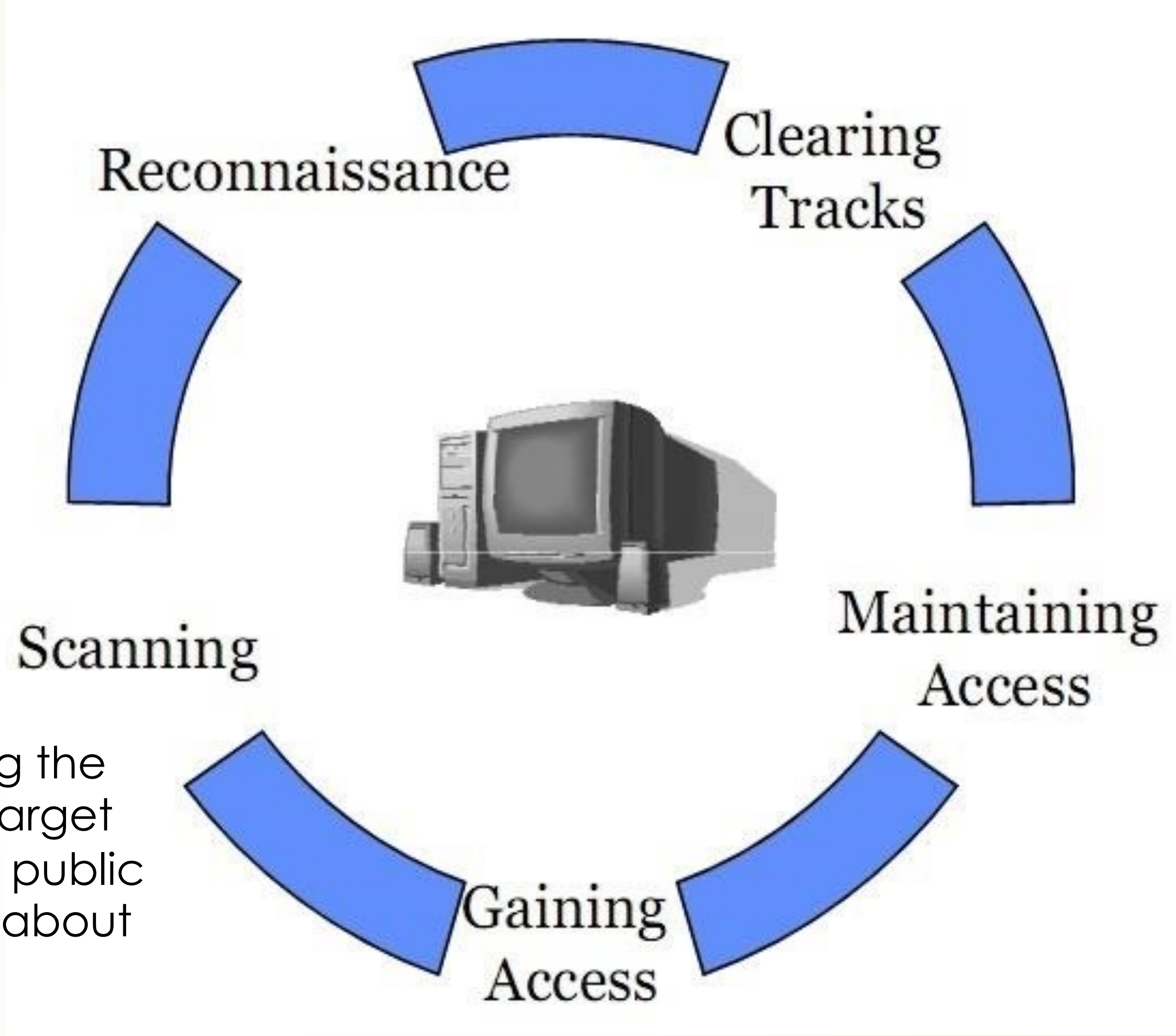
Gray box: Gray box, is a type of penetration testing in which the pentester has very limited prior knowledge of the system or any information of targets such as IP addresses, Operating system or network information in very limited. Gary boxing is designed to demonstrate an emulated situation as an insider might have this information and to counter an attack as the pentester has basic, limited information regarding target.

White box: The white box is a type of penetration testing in which the pentester has complete knowledge of system and information of the target. This type of penetration is done by internal security teams or security audits teams to perform auditing.

Hacking Phases

The following are the five phases of hacking:

- ✓ **Reconnaissance**
- ✓ **Scanning**
- **Passive Reconnaissance**
- **Active Reconnaissance**
- ✓ **Gaining Access**
- ✓ **Maintaining Access**
- ✓ **Covering Tracks**



In **Passive Reconnaissance**, the hacker is acquiring the information about target without interacting the target directly. An example of passive reconnaissance is public or social media searching for gaining information about the target.

Active Reconnaissance is gaining information by acquiring the target directly. Examples of active reconnaissance are via calls, emails, help desk or technical departments