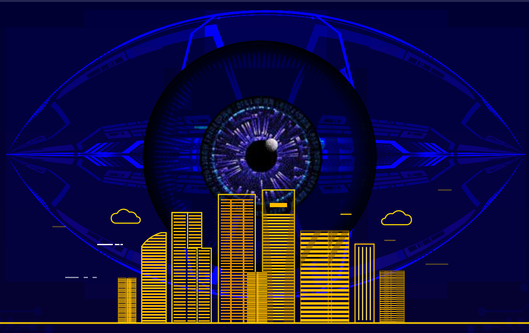
RECONNAISSANCE



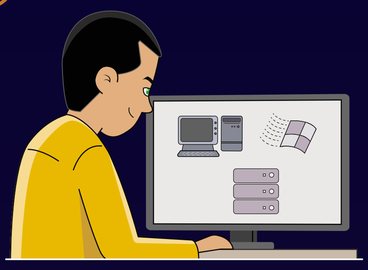
The information gathering mission

Every heist begins with surveying the premises of the intended attack. A cyberheist is no different. Reconnaissance is the first step of the cyber kill chain, during which hackers like Mr. Gene, look for various points of entry into a network and want to discover vulnerabilities that can be targeted. Here are five ways it can be done.

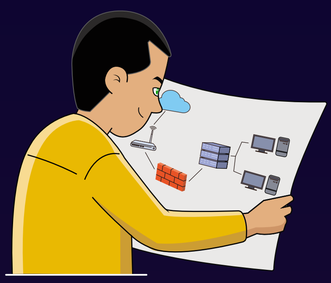
1

Looking for vulnerabilities

Mr. Gene can look for vulnerable hosts and applications to deploy exploits in a target organization.



2



Snooping around the network

He can gather network information along with specifics on cyberdefense appliances such as firewalls, bastion hosts, and anti-malware programs.

3

Studying the victim

Mr. Gene can launch phishing campaigns and analyze social media accounts to get ahold of personal data of networked users.

4

Surveilling the organization

Mr. Gene can survey the physical location of the organization to identify where critical resources are housed.

5

Reconnaissance phase complete

- Stale accounts
- IP ranges
- Domain names
- ISP
- Hierarchy
- Departments
- Business operations
- Security measures