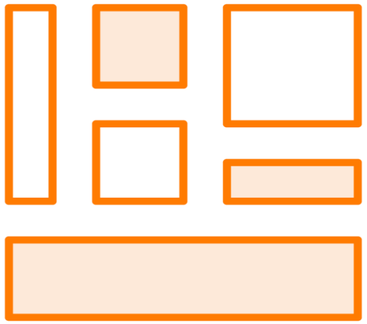
Establish a Foothold in a Host

Malek Mohammad
Information Security Consultant
https://github.com/malek-mohammad
www.linkedin.com/in/malekmohammad

Maintain Presence Inside the Host

Presence

Undetected

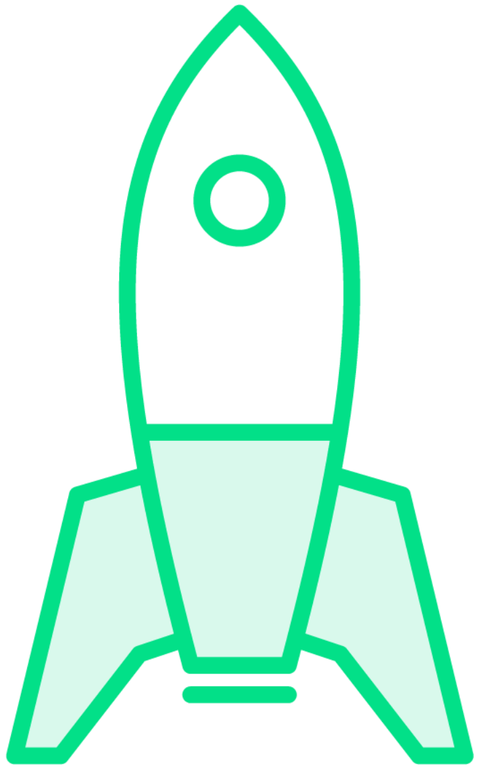


Gather

How to Maintain Presence

Persistence is key

Using backdoors or malware



Escalate privileges

Malicious activities start:

- Data exfiltration
- Lateral movement

Risk on attacker:

- Might be detected
- Tricky process

Sudoers File

Privilege configuration

Elevates privileges

Can be useful but with risk

Write access is dangerous

NOPASSWD poses a threat

Set User Id

SUID, the special permission

Runs with owner's privileges

Elevates privileges if the owner is root

Not properly secured

Input manipulation

Bash Makes You Able

Gained access

Elevate privileges