Establish a Foothold in a Network

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

Hackers want more

Techniques to spread

Steal password hashes

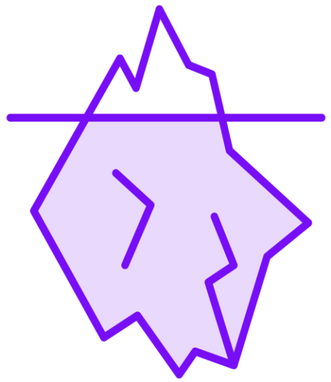
Using a compromised machine as a base

Tools used

- Netcat
- Bash

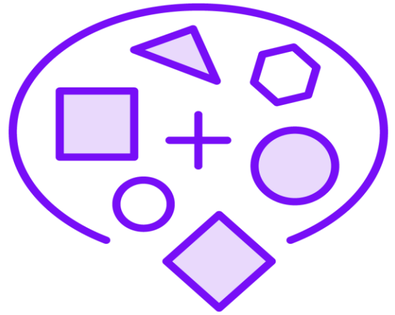
Techniques used

- ARP spoofing
- MAC spoofing



A tool with potential

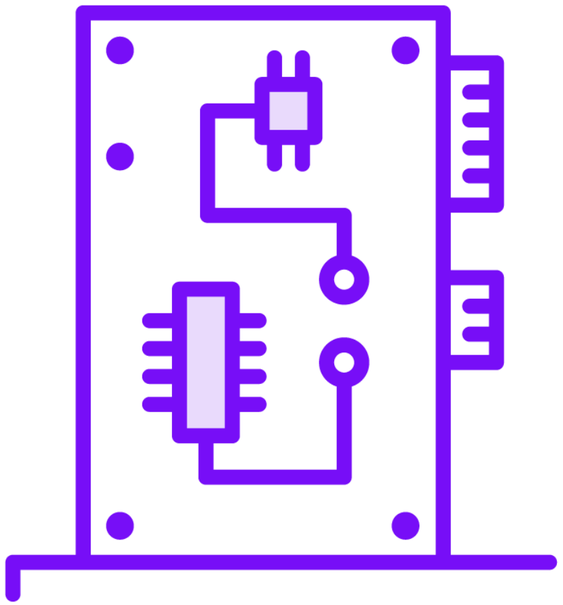
Uses TCP and UDP for connections



It provides versatile usecases

Hackers rely on netcat a lot

Combined in bash scripts to automate attacks



Bash supports networking

Not versatile

Bash has

- TCP file handle
- UDP file handle

How to

- echo
- cat

MAC address can be manipulated

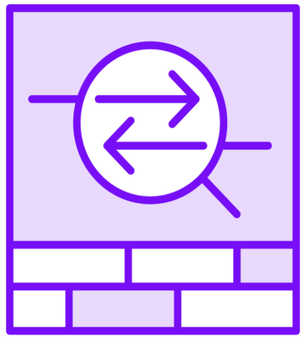
ARP maps an IP to a MAC

Communication is carried out

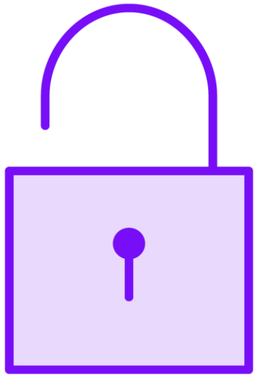
Change the MAC

Done by software

Bypass blacklisting

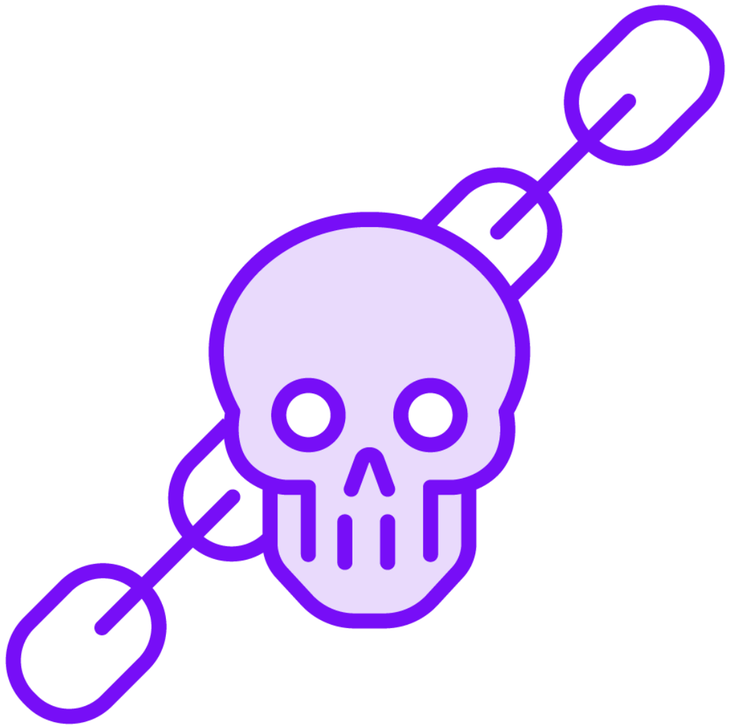


Blacklist



Bypass

Malicious



Intercept communication

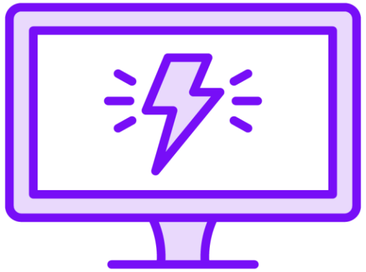
ARP spoofing leads to MiTM

Attacker forges ARP requests

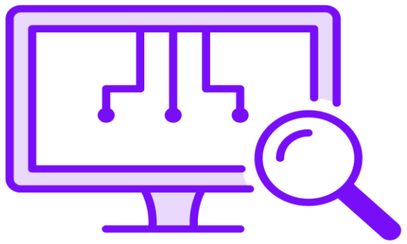
Diverts the traffic

Can be a base for other attacks

Cross functional



Automation



Focus