Hidden Networks

- A hidden network is one that does not broadcast its name or ESSID.
- Hidden networks still broadcasts their existance (channel, BSSID).

Problem:

Can't connect or even attempt to crack its password.

Solutions:

- Airodump-ng can determine the ESSID if the network is active.
- Deauth one of the connected clients for a short period of time.

Mac Filtering

- Mac address is unique to each network device.
- Routers can use mac filtering to allow/deny devices from connecting based on their mac address.

2 Implementations:

1. Using a blacklist – allow all MACs to connect except the ones in the list.
2. Using a whitelist – deny all MACs from connecting except the ones in the list.

Security

1. Deauthentication Attacks

- No proper way to secure against it.
- Can't prevent clients from sending deatuh frames.

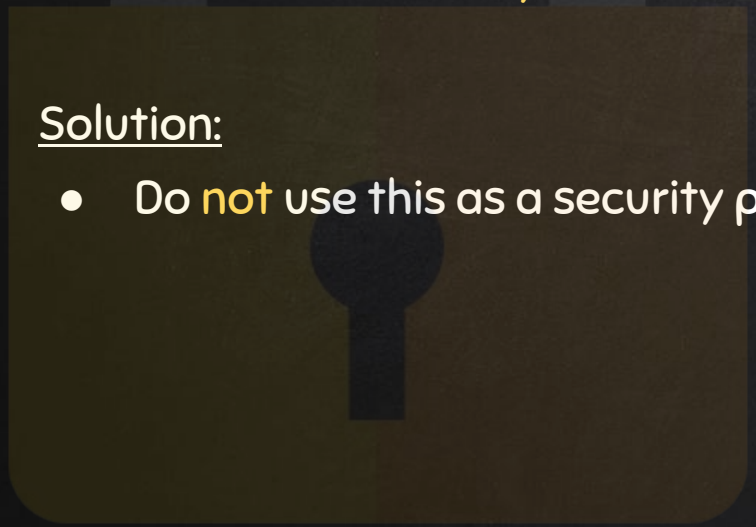
Solution:

- Switch to 802.11w.
- Uses protected management frames.
- Can detect and prevent deauth attack.

Security

2. Hidden Networks

- Only SSID is hidden.
- Network Has to broadcast its existence.
- ESSID can be easily discovered.



Solution:

- Do not use this as a security precaution.

Security

3. Mac Filtering

- Relies on Mac Address.
- Mac address can be changed easily.
- Therefore it is not secure.

Solution:

- Do not use Mac Filtering.
- Use WPA/WPA2 Enterprise instead.

Security

Summary

1. Switch to 802.11w.
2. Hiding network will not secure network from hackers.
3. Do not rely on MAC for access control.