

CAPTIVE PORTALS

- Captive portals usually refer to **open** wifi networks.
- Widely used in hotels, airports, coffee shopsetc
- Allow users to access the internet after logging in.
- Users login using a **web interface**.



BYPASSING CAPTIVE PORTALS

There are a number of ways to bypass captive portals depending on the way it is implemented:

1. Change **MAC address** to one of a connected client.
2. Sniff logins in **monitor** mode.
3. Connect and sniff logins after running an **arp spoofing** attack.
4. Create a **fake AP**, ask users to login.



BYPASSING CAPTIVE PORTALS

SNIFFING CREDENTIALS IN MONITOR MODE

- Since captive portals are **open**.
- IE: they do NOT use encryption;
- We can sniff data sent to/from it using airodump-ng.
- Then use **Wireshark** to read this data including passwords.



BYPASSING CAPTIVE PORTALS

SNIFFING CREDENTIALS USING ARP SPOOFING

- Since captive portals are **open**;
 - Therefore we can connect to the target without a password;
 - We can then run a normal **arp spoofing** attack;
- Clients will **automatically** lose their connection and will be asked to login again
- Data sent to/from router including **passwords will be directed to us.**



BYPASS CAPTIVE PORTALS

USING SOCIAL ENGINEERING

- When everything fails we target **the users**.
- Clone the login page used by the captive portal.
- Create a fake AP with the same/similar name.
- Deauth users to use the fake network with the cloned page.
- Sniff the login info!



BYPASS CAPTIVE PORTALS

USING SOCIAL ENGINEERING

- When everything fails we target **the users**.
- **Clone the login page used by the captive portal.**
- Create a fake AP with the same/similar name.
- Deauth users to use the fake network with the cloned page.
- Sniff the login info!



BYPASS CAPTIVE PORTALS

USING SOCIAL ENGINEERING

- When everything fails we target **the users**.
- Clone the login page used by the captive portal.
- **Create a fake AP with the same/similar name.**
- Deauth users to use the fake network with the cloned page.
- Sniff the login info!



CREATING FAKE AP

The main components of a wifi networks are:

1. A router broadcasting signal → use wifi card with **hostapd**.
2. A DHCP server to give IPs to clients → use **dnsmasq**.
3. A DNS server to handle dns requests → use **dnsmasq**.



BYPASS CAPTIVE PORTALS

USING SOCIAL ENGINEERING

- When everything fails we target **the users**.
- Clone the login page used by the captive portal.
- Create a fake AP with the same/similar name.
- **Deauth users to use the fake network with the cloned page.**
- Sniff the login info!



BYPASS CAPTIVE PORTALS

USING SOCIAL ENGINEERING

- When everything fails we target **the users**.
- Clone the login page used by the captive portal.
- Create a fake AP with the same/similar name.
- Deauth users to use the fake network with the cloned page.
- **Sniff the login info!**

