



- Another tool for **MITM** attacks with basic but reliable features.
- Built-in sniffer.
- Supports plugins for dns spoofing ...etc.
- Supports custom **filters**.
- + more



# Ettercap

## BYPASSING HTTPS USING SSLSTRIP

- Use ettercap as a spoofer and a basic sniffer.
  - Run `sslstrip` manually to `downgrade` HTTPS requests to HTTP.
1. Flush iptables.
  2. Add iptables rule to redirect packets to sslstrip.
  3. Start sslstrip to downgrade https.
  4. Start ettercap to poison target(s).

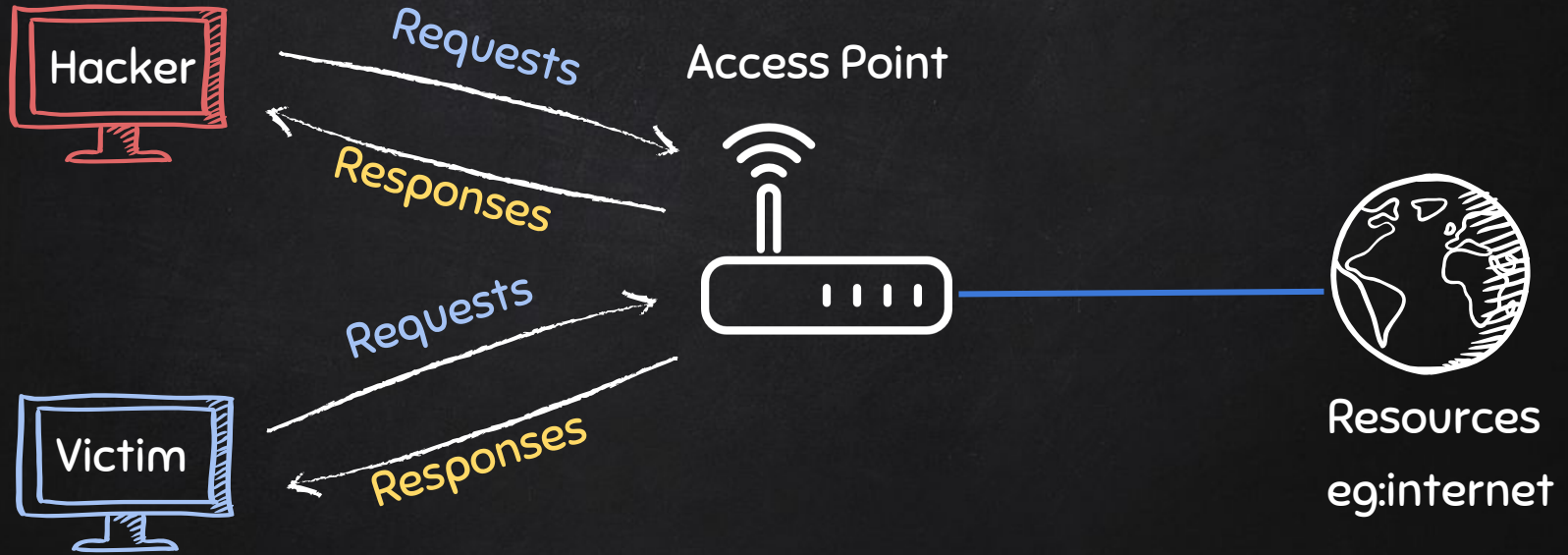


# Ettercap

## ETTERCAP PLUGINS

- Ettercap has a number of plugins.
- Plugins can be used to:
  - Auto-add new clients → `autoadd`.
  - Re-poison clients after arp broadcasts → `repoison_arp`.
  - DNS spoof targets → `dns_spoof`.
  - + more.

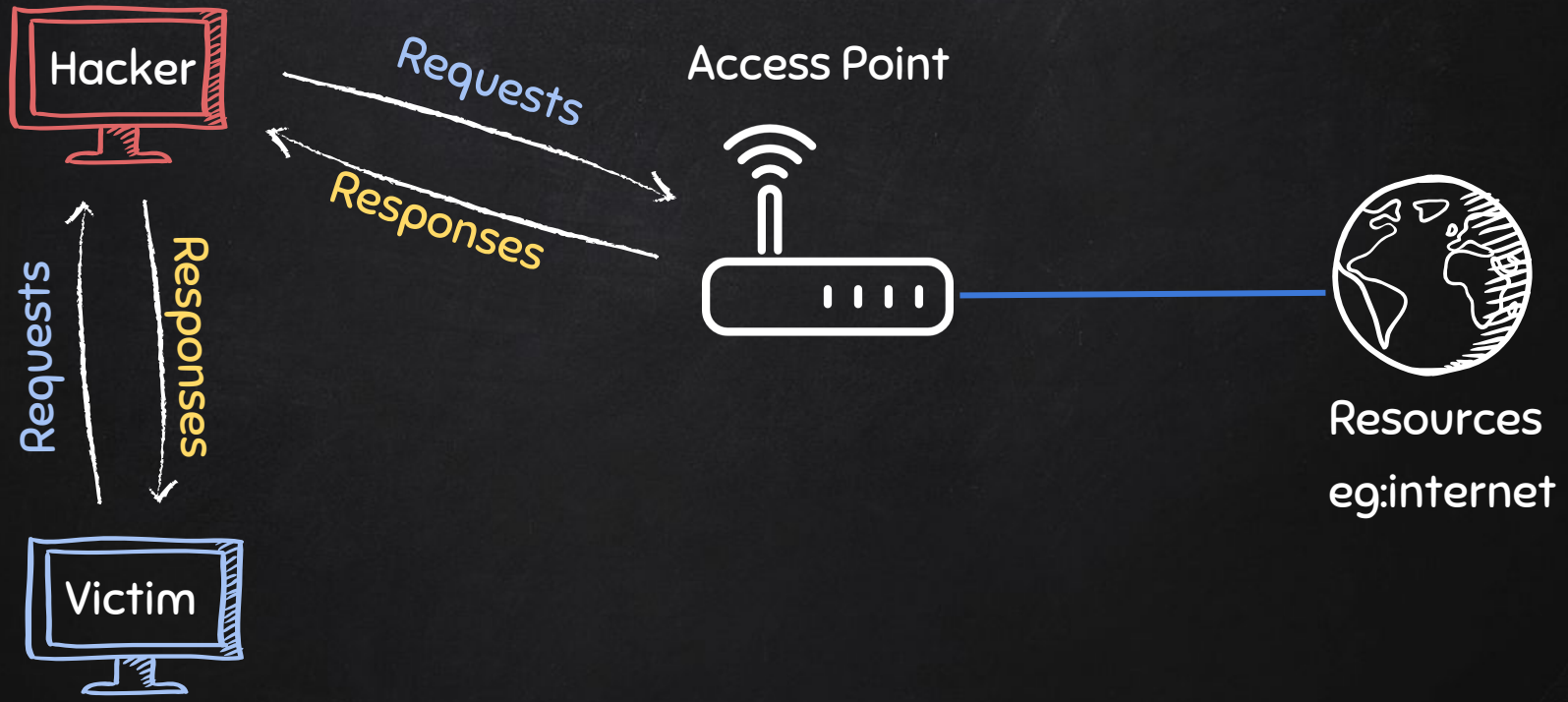
# TYPICAL NETWORK



# ARP SPOOFING



# ARP SPOOFING



# ONE WAY ARP SPOOFING

