Identify Common Threats

You **first** check for **ARP scans** since ARP scan helps identifying the connected devices in the system.

lots of ARP broadcast requests looking for different IP addresses. Here, be careful, sometimes scanning tools send 2 ARP request for the same IP address one with padding (18 bytes of 0) and one without.

secondly ICMP ping Sweeps since it helps identify the IP stack in the system for the attacker.

a Layer-3 scan where your system is sweeped with bunch of ICMP pings.

many of the systems are configured not to respond to ICMP ping sweeps. but there comes **TCP SYN**s to common ports

a weird TCP SYN packet is the one which does not have timestamp, SACK, big window etc.

Also, TCP syn sweep causes lots of TCP resets since many of the ports are not open. tcp reset packets are also an indicator.

of course the biggest indicator is searching whole netwotk or subnet with different ports using syns.

With **UDP** getting more and more pervasive also they do UDP scans.