Module 17
(Network Discovery)

- At the end of this module you'll know a little bit about the Address Resolution Protocol and ARP scans on local networks. You'll have been introduced to nmap for ARP scanning. You'll also find out about ping scans and look at a tiny bit of bash scripting.
What Systems Can I Reach?

- Determining what systems can be reached from any given host is an important capability when trying to gain control over hosts in a network.
- The security of every network is preserved only if the individual devices on that network are secure.
- All intrusion is, in the end, based on interaction with some kind of host even if that host is a simple device.
Identifying Hosts with ARP

- The Address Resolution Protocol (ARP) is used to translate a device's OSI Layer 3 IP address into an OSI layer 2 Media Access Control (MAC).

- Devices on a physically local (unrouted) network segment will respond to ARP requests. Thus, to find out all the devices on the local network, one can sweep through all IP addresses expected to be found on the local network asking for their associated MAC addresses.

- This is known as an ARP scan.
Using nmap for ARP Scans

- nmap is an extremely versatile network scanner. It provides numerous different ways to scan the devices on a network.
- One function that nmap supports is ARP scanning.
- To carry out an ARP scan, one provides nmap with the following flags:
  - -PR perform ARP discovery
  - -sn no port scan
- In addition one must specify the range of IP addresses to scan:
  - 172.16.28.0/24 (CIDR notation)
  - 172.16.28.0-255 (arbitrary range notation)
  - 0-255.0-255.3.37
Sample nmap Scan

- I run several VMs inside my own machine and do an ARP scan using nmap to identify the available hosts.
Discovering Hosts with ICMP Echo

- The ICMP Echo Request (message type 8) will be satisfied by most machines. They will respond with an ICMP Echo Reply (message type 9).
- Ping scans (unlike ARP scans) can reach beyond the unrouted local network across routers (because uses OSI layer 3 IP packets, which are routed).
- You can use ping to send ICMP echo packets. Ping's parameters vary from system to system. Check local listings. Your mileage may vary.
- On kali, -c tells how many packets to send: ping -c 1 172.16.28.132
Writing a bash program to do a Ping sweep

- Shell programming is extremely useful to penetration testers. I will not be testing your shell programming ability, but you will be well served in future examples if you know how to do it.

```
i=0;
while [ $i -le 255 ]; do
  ping -c 1 -W 1 172.16.28.$i
  let i+=1
done
```
What Does That Bash Script Do?

- `man bash`

- On the other hand, here are a few hints:
  - Variables can be assigned in bash with `var=value`
  - Variables can be referenced with `$var`
  - `[` is a way to run the program called `test`
    Do either `man [` or with `man test`
    Alternate syntax: `$(test $i -le 255)`
  - Let is another way to assign variables
    Alternate syntax: `i=$(expr $i + 1)`
    Alternate alternate syntax: `i=`expr $i + 1`