**Module 9 Session Hijacking**

**9.1 Session Hijacking Lab Intro**

**Address Resolution Protocol (ARP)**

1. ARP resolves IP addresses to physical MAC address

**Man-in-the-Middle Attack**

1. Attacker secretly monitors traffic between 2 machines that believe they are just communicating with ea other
2. Great way to harvest user login credentials

**Network-level Session Hijacking**

1. Use Ettercap to poison ARP cache of target then do MitM attack to capture login credentials
2. For test environment, enable DVWA apache service
3. Go to Ettercap graphical under sniffing & snooping (GUI ver)
4. ARP Poisoning
   1. Select Sniff at top > Unified Sniffing
   2. Make sure eth0 network interface
   3. Scan for hosts
      1. Hosts > scan for hosts & add to host list
   4. in host list, can select hosts as targets
   5. go MitM panel > ARP Poisoning
      1. under optional parameters check sniff remote connections
      2. ARP cache poisoned
5. Capture user credentials
   1. In Ettercap, Start > Start Sniffing
   2. When target types username and password in DVWA apache server
      1. http://192.168.0.1/dvwa
      2. Shld be in Ettercap, review at bottom