**Module 6 Sniffing**

**6.0 Sniffing**

**Sniffing**

1. Capture & scan traffic flowing across network
   1. Active – monitor & alter
   2. Passive – listening only
2. Protocols for easy sniffing
   1. telnet – keystrokes easily sniffed (usernames, passwords)
   2. HTTP – designed to send cleartext
   3. SMTP (Simple mail Transfer Protocol) – no protection against sniffing
   4. NNTP (Network News Transfer Protocol) – data sent cleartext
   5. POP (Post Office Protocol) – passwords & usernames can be intercepted
   6. FTP (File Transfer Protocol) – transmissions sent in cleartext
   7. IMAP (Internet Message Access Protocol) – similar to SMTP
3. Sniffing tools
   1. Wireshark
   2. Tcpdump
   3. Windump
   4. Omnipeek
   5. Dsniff
   6. Netwitness NextGen

**Wireshark**

1. Filters
   1. == - equal
   2. Eq - equal
   3. != - not equal
   4. Ne – not equal
   5. Contains – contains specific value
2. CLI tools
   1. Tshark – CLI ver of wireshark
   2. Dumpcap – small with sole intent of capturing traffic
   3. Capinfos – reads capture & returns statistics on that file
   4. Editcap – edits/translates format of capture files
   5. Mergecap – combines multiple capture files into 1
   6. Text2cap – creates capture file from ASCII hex dump of packets

**SECTOOLS – GOOD WEBSITE FOR FINDING GOOD TOOLS**

**MAC Flooding**

1. Goal is to convert switch to act like hub
2. Attacker floods switch with MAC addresses
3. Switch unable to write to own CAM (Content Addressable Memory) table, which causes it to act like a hub (fail open)
4. Not seen much with newer switches

**ARP (Address Resolution Protocol) Poisoning**

1. Contaminate network with improper gateway mapping
2. ARP maps IP addresses to MAC addresses
3. Attacker feeds network hosts & gateway with incorrect mappings
4. Tools
   1. Ettercap
   2. Cain & Abel
   3. Arpspoof

**Switched Port Analyser (SPAN) port**

1. Generally requires physical access to machine
2. Sends copy of every network packet on 1 switchport to another for monitoring

**Sniffing Defense**

1. Encrypt sensitive traffic (SSH, IPsec)
2. Use hardware-switched network for most sensitive parts of network to isolate traffic to single segment
3. Implement IP DHCP snooping on Cisco switches to prevent ARP poisoning
4. Implement policies preventing promiscuous mode on network adapters