**MAC Flooding Attack**

* Attack
  1. dsniff on kali
  2. macof -n 5
* Defence (port security)
  1. Dynamic:
     + switchport port-security
  2. Maximum:
     + switchport port-security
     + switchport port-security maximum 8
  3. Sticky
     + switchport port-security
     + switchport port-security mac-address sticky
  4. Static
     + switchport port-security
     + switchport port-security mac-address 0000.0000.0000
  5. Recovery
     + errdisable recovery cause ?

Table

Description automatically generated

**Switch Spoofing Attack**

* Attack
  1. Yersinia on kali
* Defence
  1. Disable DTP negotiations and manually configure ports as access or trunk explicitly
     + switchport mode access
     + switchport access vlan 10
     + switchport nonegotiate
  2. shutdown all unused ports and place them in an unused VLAN
     + switchport mode access
     + switchport access vlan 100 (unused vlan)
     + shutdown
     + switchport trunk allowed vlan remove 100 (remove unused vlan)

**Double-Tagging Attack**

* Attack
  1. Yersinia on Kali
* Defence
  1. configure dedicated native VLAN, e.g., VLAN 500, for all trunk ports which should not be assigned to any access ports.
     + switchport trunk native vlan 500
     + vlan dot1q tag native

**STP Attack**

* Attack
  1. Use a rogue cisco switch and plug it in (Lab 2, pg 16 notes)
* Defence
  1. apply BPDU guard feature available
     + spanning-tree bpduguard enable
  2. BPDU guard may simply be enabled globally on all PortFast-enabled ports since these ports should not receive BPDU.
     + spanning-tree portfast
     + spanning-tree portfast bpduguard default
  3. root guard feature to enforce the placement of root switches, preventing them from being taken over by rogue root switch.
     + spanning-tree guard root

Table

Description automatically generated

Graphical user interface, text, application

Description automatically generated

**CDP Information Leakage**

* Attack
  1. Capture with wireshark
* Defence
  1. disable CDP individually on all access ports, except ports supporting VoIP which require CDP to function.
     + no cdp enable
  2. disabled globally on all interfaces of the device
     + no cdp run

**DHCP Starvation and Spoofing Attack that may lead to DNS and website spoofing**

* Attack
  1. Yersinia on Kali (DHCP Starvation Attack)
  2. Metasploit on Kali (DHCP Server Spoofing Attack)
  3. XAMPP on Windows (Spoof Website Attack)
  4. DNSChef on Kali (DNS Server Spoofing Attack)
* Defence
  1. DHCP Snooping
     + ip dhcp snooping
     + ip dhcp snooping vlan *vlan-id*
     + ip dhcp snooping verify mac-address (DHCP snooping MAC address verification)
     + ip dhcp snooping limit rate *rate* (DHCP snooping rate-limiting (from 1 – 2048 DHCP pps) can also be configured. If exceeded, the port is put into err-disabled state.)
     + ip dhcp snooping trust (ports connected to authorized DHCP servers)
     + ip dhcp relay information trust-all
     + ip dhcp relay information trusted
     + no ip dhcp snooping information option

Table

Description automatically generated with medium confidence

Diagram

Description automatically generated

**ARP Poisoning and MITM Attacks**

* Attack
  1. Bettercap in Kali (ARP Poisoning)
  2. Driftnet in Kali (MitM Eavesdropping Attack)
* Defence
  1. Dynamic ARP Inspection (DAI)
     + ip arp inspection trust
     + ip arp inspection limit rate *rate* (ARP rate-limit (default is 15 ARP pps). If exceeded, the port will transit to err-disabled state)
     + ip arp inspection validate ([src-mac] [dst-mac] [ip]) (validate contents of ARP reply matching layer 2 Ethernet addresses)
     + ARP ACL (Refer to pic)

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text

Description automatically generated

**IP and MAC Address Spoofing Attacks**

* Attack
  1. Set same ip or mac as the victim
* Defence
  1. IP source guard
     + ip verify source (Against IP spoof)
     + ip verify source port-security (Against IP and MAC spoof)
     + ip source binding *mac-address* vlan *vlan-id ip-address* interface *type number/number* (Binds static ip and mac to a port)