chapter 8

Sniffing

Concepts

Sniffer - turns NIC → promiscous mode

Types:

- Passive (use of hub)
- Active (use of switch)
  - inject ARP Flood
  - Switch CAM table.

Active Sniffing Techniques

- MAC Flooding
- DHCP Attack
- DNS Flood
- ARP Flood
- Spoofing attack
- Switch Port stealing

Vulnerable Protocols

Telnet, Rlogin

HTTP

POP

IMAP

SMTP, NNTP

FTP

Passwords in clear Text.

Hardware Protocol Analyzer

- captures signals without altering traffic
- identify usage & find malicious traffic
- predetermined rules
- Voyager M4x, N2X N5540A

SPAN Port

- Port to receive a copy of every packet

Wiretapping

- monitoring telephone, Internet conversation by third party.
- using listening device
- Monitor, intercept, access, record information

Active – monitors into communication/traffic

Passive – collects knowledge reg. data.

Lawful Interception

- legal Interception of data communication.
- telecomm, VoIP, multiservice networks

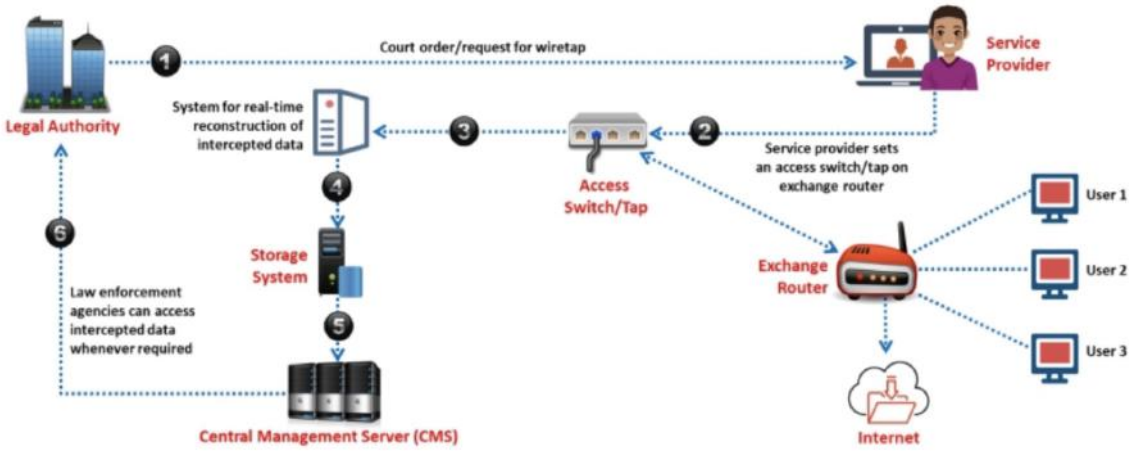
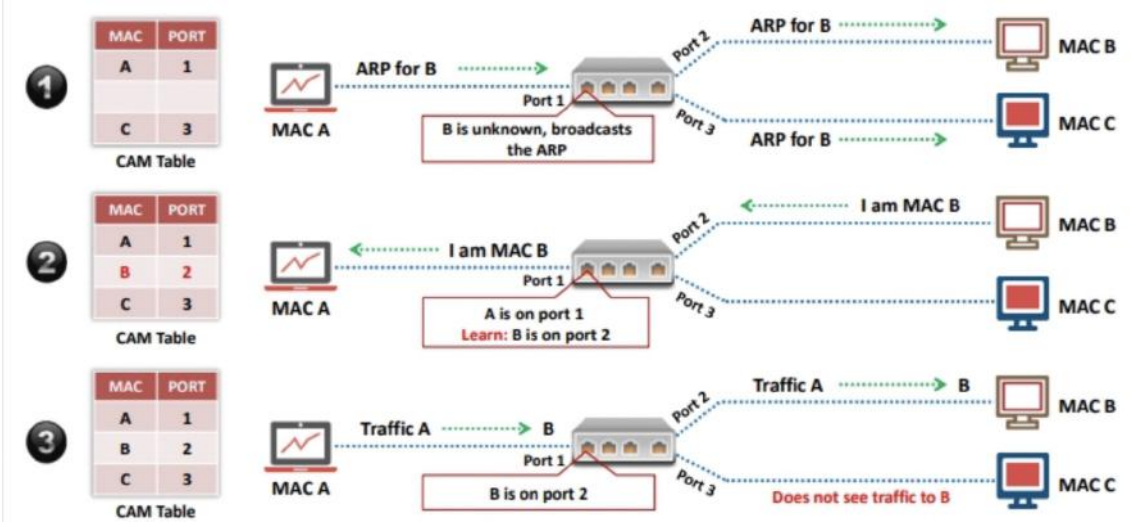


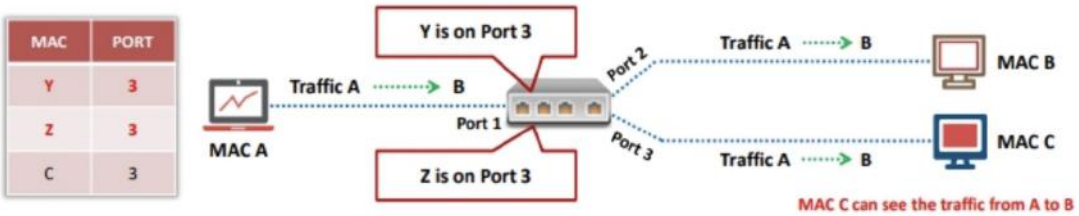
Figure 8.14: Telco/ISP lawful solution

Techniques

CAM stores MAC addresses & VLAN Parameters.



- once CAM is full, additional ARP is flooded
- This resets learning mode, broadcasts every port, fills adjacent switches.



MAC Flooding

- Flooding of CAM with fake MAC address
- Once full, CAM acts as a hub and broadcasts to all machines
- attacker sniffs traffic easily.

macof (dsniff) - random source MAC

↳ unix/linux

Switch Port Stealing

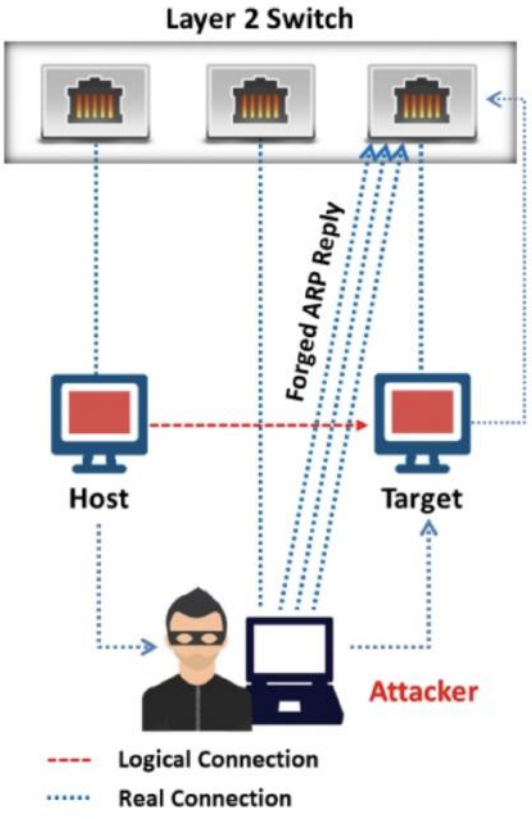


Figure 8.22: Switch port stealing

- attacker spoofs target IP & MAC addr.
- He turns NIC → Promiscuous mode.
- when ARP requested by host, attacker

quickly responds it by having dos attack for target.

- Now ARP cache is updated with spoof
- system forward all packets to attacker.

How to defend?

- configure Port Security (cisco)

DHCP starvation Attack

- Denial of Service on DHCP Servers.
- broadcast forged DHCP requests
- Tools: Yersinia, Gobbler.

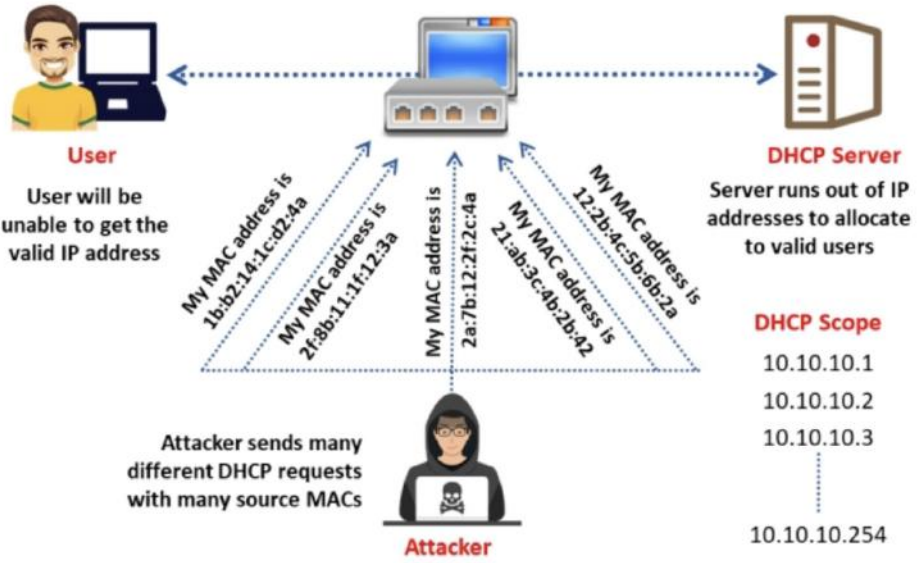
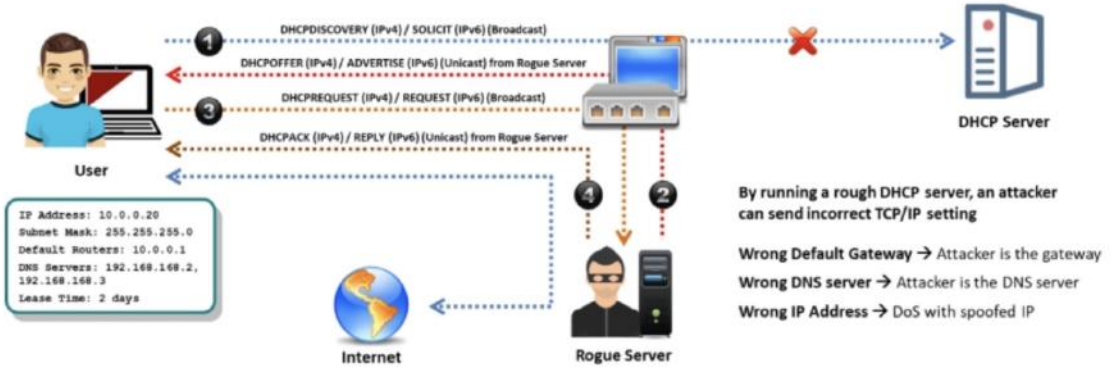


Figure 8.27: DHCP starvation attack

attacker perform Rogue DHCP Server attack with bogus IP address in conjuction with DHCP starvation attack.



defend :

- Port Security
- DHCP Snooping

ARP Poisoning

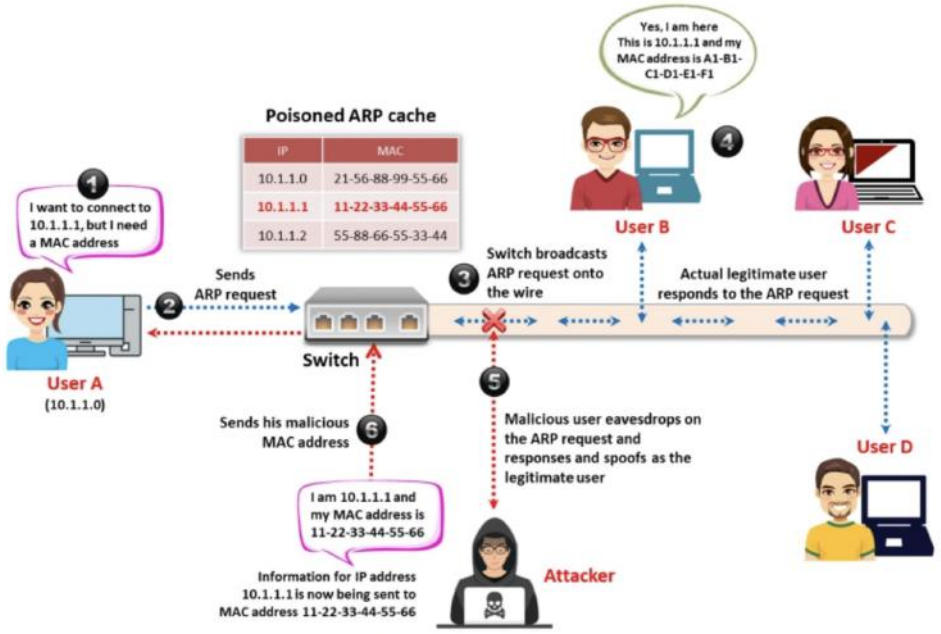


Figure 8.34: Working of an ARP spoofing attack

- arpspoof
- dsniff
- Ettercap
- BetterCap

} Tools

defend:

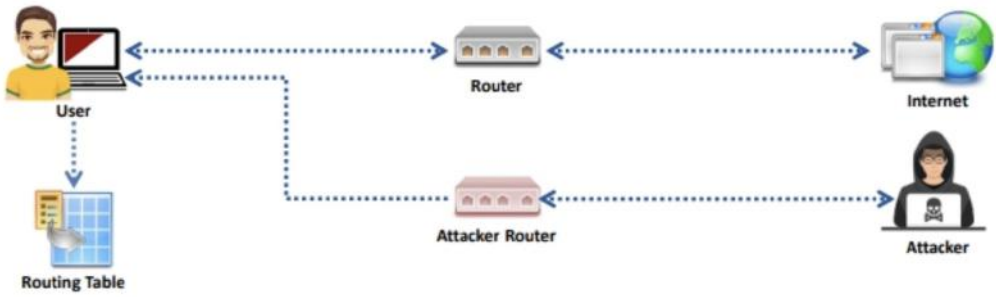
- ARP dynamic Inspection.

X Arp - Detect ARP

IRDP Spoofing

ICMP router discovery protocol

- allows host to discover IP of active router on the subnet
- Sends spoofed IRDP advertisement message to change default router.



VLAN hopping

- target resources on VLAN

Switch Spoofing

- connects rogue switch
- creates trunk link between them

Double tagging

- adds another tags in ethernet frame
- Outer & Inner VLAN.

STP Attack (Priority less of any switch)

- connects rogue switch to network
- changes operation of STP Protocol
- it configures as "root switch" to sniff all traffic.

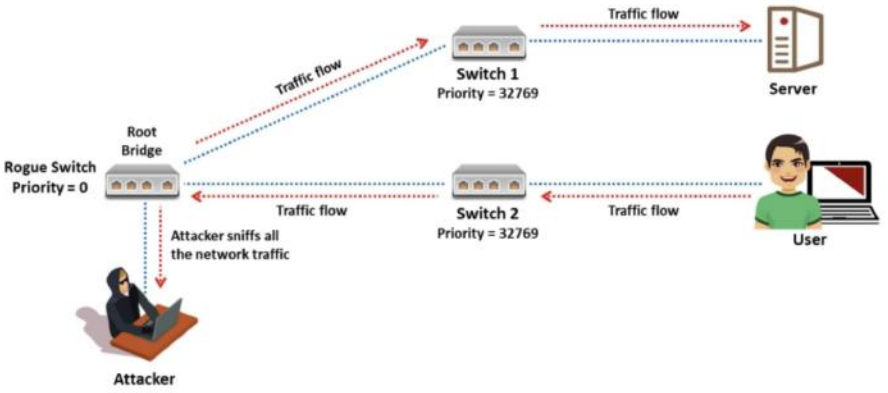


Figure 8.45: Illustration of an STP attack

Defend - Hopping

- configure not to negotiate trunks.

  switchport mode access / negotiate

- ensure each VLAN assigned with access port.

  switchport access vlan 2.

defend - STP

- BPDU Guard, Loop Guard, Root Guard

DNS Poisoning

- replace IP entries of attackers' DNS server

  Intranet (local) LAN

  Internet (remote) → Trojan

  Proxy Server → Trojan → IE

  DNS Cache (Internal DNS Server)

- Tools: DerpNSpoof

defend:

- Implement DNSSEC, IDS
- Use SSL, static ARP的IP, SSH
- NXDomain rate limit

Tools:

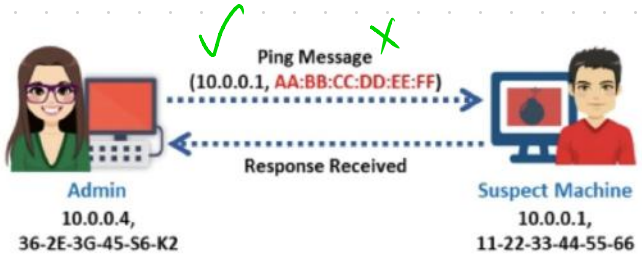
- Wireshark.
  - Follow TCP stream
  - Display Filters (protocol, Port, address, other)
- Capsa Network Analyser
- OmniPeek, Steel Central.
- Sniffer WiCap } Mobile
- FaceNiff
- Packet Capture

Detection Techniques

- check devices (promiscuous mode)

- Run IDS
- Run Network tools

Ping:



(FOUND)

Figure 8.61: Promiscuous mode

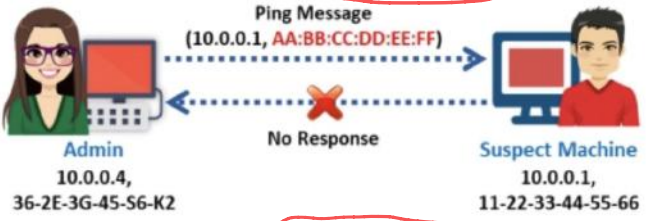
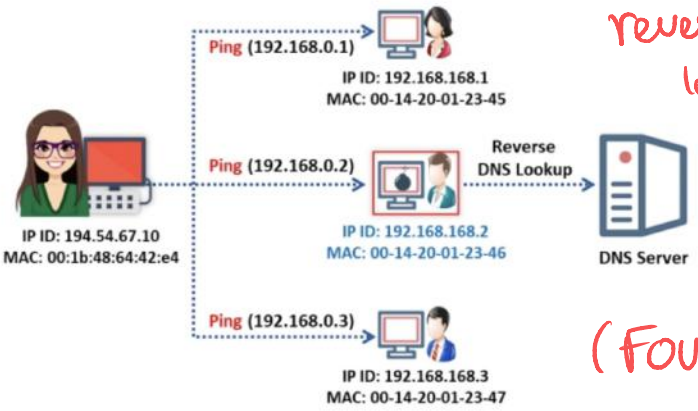


Figure 8.62: Non-promiscuous mode

DNS:

if responds reverse DNS lookup



(FOUND)

Figure 8.63: Sniffing detection using the DNS method

ARP :

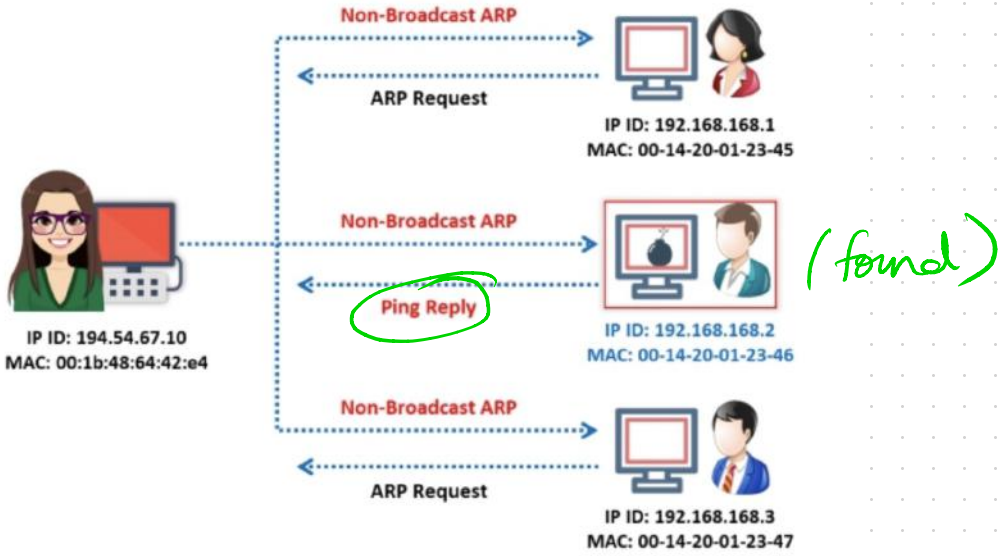


Figure 8.64: Detecting sniffing via the ARP method

only Promiscuous mode responds to ARP

- Nmap
- Net Scan Tools Pro