Layer 2 Security

Protocols – Attacks – Countermeasures

Disclaimer

- The purpose of this document is informational only
- The author is not and could not be held responsible for your behavior

Part 1 - Today's work

- Layer 2 Switching - Sniffing tools - Exercise 0
- Attack 1: ARP spoofing - Exercise 1 - Counter 1
- Attack 2: CAM table overflow - Exercise 2 - Counter 2

Layer 2 switching

- **ARP** = IP – MAC resolution
- **ARP table** on the hosts, routers…
- ARP messages: requests, replies, gratuitous

- On the switch **CAM table** = MAC – Port bindings
- Built using frames source addresses

- Set the card to **promiscuous mode**

Sniffing tools

- **Wireshark** = easy, handy and powerful, but not so scalable
- Prefer CLI tools such as
  - Tshark (Wireshark CLI tool)
  - **Tcpdump**
- Possibility to script

Exercise 0

- Packet Tracer
  - Follow L2 information interactions in a simple network
- Wireshark
  - Analyze a frame
  - Observe the different ARP messages
- Related CLI commands (Windows/Linux/IOS)
  - Print the ARP table on Windows, Linux and Cisco IOS
  - Print the CAM table on a Catalyst switch

Attack 1: ARP spoofing

- ARP spoofing ⇔ ARP cache poisoning
- **Fake ARP information** in hosts tables (ARP table/cache)
- Man in the Middle (MitM) and Denial of Services (DoS)

Exercise 1

- ARP spoofing 1 – MitM
  - Realize a bidirectional ARP spoofing using arpspoof (dsniff)
  - Wiretap traffic with Wireshark
- ARP spoofing 2 – MitM
  - Realize a bidirectional ARP spoofing with forged frames using scapy
  - Wiretap traffic with Wireshark
- ARP spoofing 3 – DoS/Blackhole
  - Realize a bidirectional ARP spoofing
  - Redirect the entire subnet to a host that does not route the packets

Counter 1

- **Dynamic ARP Inspection** available on switches with security features. Examines all ARP requests.
- Necessity to set up DHCP snooping (create MAC – IP – port tables)
- Prevent gratuitous ARP
- Similar mechanisms available on end hosts (ARPWatch, ARPon, XARP, Kasperky…)

Attack 2: CAM table overflow

- Switch mode != Hub mode
- Switches have a MAC addresses limit
- When the CAM table reaches the limit, the switch goes in hub mode to ensure basic frame forwarding
- Hub mode = easy wiretapping

Exercise 2

- MAC overflow
  - Perform a MAC overflow with macof
  - Wiretap traffic flowing through the switch (wireshark)

Counter 2

- **Port security** features
- Set maximum number of MAC addresses per port
- Save the MAC address of the first device connected on the port
- Set a static MAC addresses