Network Administration HW2

B04705003 資工三 林子雋

1 Reference

1.1 Flamestrike

1. 了解交換器如何傳遞
2. https://www.youtube.com/watch?v=se-pVwapTic
3. https://www.wikiwand.com/en/Spanning_Tree_Protocol

1.2 MAC Pro

1. (a) Address Resolution Protocol (ARP) Explained
   (b) How does a packet travel from one computer to another over the Internet based on OSI model
   (c) How are IP Packets Routed on a Local Area Network?
   (d) How IP Packets are Routed on a Local Area Network
2. MAC Address Table Attack 媒體存取控制位址表攻擊
3. How IP Packets are Routed on a Local Area Network
4. Arp Poisoning Explained + Kali Tutorial

1.3 Let's IPv6

1. Neighbor Discovery Protocol
2. As above
3. Netcat (nc6) - Minimal IPv6 only TCP Server and Client

2 Problem

2.1 Flamestrike

(a) Broadcast storm is caused by infinite loop of broadcast packet between two switches. For example, if a server wants to send ARP packet(with destination MAC address FF:FF:FF:FF:FF:FF) to find IP-MAC mapping, the switch that receive this packet will need to send it out of all ports every time because FF:FF:FF:FF:FF:FF is always an unknown destination. However, if the topology of this network has an loop, this kind of broadcast packets will be generated more and more within such loop.

(b) I will quickly disable the redundant link in the switches loop so that the looping broadcast packets won't continue looping.

(c) STP will create a spanning tree within the network, disabling those links that are not part of the spanning tree(leave just one active path between any two nodes in the network).

2.2 MAC Pro

(a) Since arp tables and mac address table are all empty, Mario will need to first determine the gateway's mac address, and then send ICMP packet to gateway. After gateway receives Mario's ICMP packet, gateway will need to broadcast ARP request on interface 1 to 3 to figure out the MAC address of Zelda and send out the ICMP packet to it.

(1) ARP request, 10.0.0.1 -> 10.0.0.254, fa:ce:b0:00:00:0c -> FF-FF-FF-FF-FF-FF (determine default gateway MAC address)

(2) ARP reply, 10.0.0.254 -> 10.0.0.1, ba:aa:aa:ad:c0:de -> fa:ce:b0:00:00:0c

(3) ICMP, 10.0.0.1 -> 10.0.0.2, fa:ce:b0:00:00:0c -> ba:aa:aa:ad:c0:de (send to gateway)

(4) ARP request, 10.0.0.254 -> 10.0.0.2, ba:aa:aa:ad:c0:de -> FF-FF-FF-FF-FF-FF (gateway needs to figure out Zelda MAC address)

(5) ARP reply, 10.0.0.2 -> 10.0.0.254, de:ad:be:ee:ee:ef -> ba:aa:aa:ad:c0:de

(6) ICMP, 10.0.0.254 -> 10.0.0.2, ba:aa:aa:ad:c0:de -> de:ad:be:ee:ee:ef

(b) After Zelda reply back to Mario, the table will look like

Mac address	Interface Number
fa:ce:b0:00:00:0c	Interface 1
de:ad:be:ee:ee:ef	Interface 2

Table 1: Mac address table of gateway

(c) Assume all tables are empty. Packets sent by Mario are below.

(1) ARP request, 10.0.0.1 -> 10.0.0.254, fa:ce:b0:00:00:0c -> FF-FF-FF-FF-FF-FF

(2) ICMP, 10.0.0.1 -> 140.112.30.28, fa:ce:b0:00:00:0c -> ba:aa:aa:ad:c0:de (send to gateway)

(d) We can use "ARP spoofing" or "ARP poisoning" to do this. Just run the following code and you can use wireshark to sniff packet and get the PTT password, because "arpspoof" command will send "ARP reply" to Mario and gateway to let Mario thinks that Sonic is the gateway and let gateway thinks that Sonic is Mario.

```
sudo arpspoof -i [interface] -t 10.0.0.1 -r 10.0.0.254
```

2.3 Let's IPv6

(a) ICMPv6

(b) ff02::2

(c) 526b2837+6244832f19c525445d71fcb843f0fe7b