INGI2347 : Exercises[*]

Lab session 4

Xavier Carpent, Xiao Chen

March 17, 2015

Solution 1: Amplification Attack (5 min)

1. Steve Pirate can just forge zone transfer requests (UDP packet) to `dns.thingummy.com` with a source IP address of `poor.victim.com`. The DNS server will then send replies directly to `poor.victim.com`.
2. Steve Pirate will thus be able to generate useless traffic with a bandwidth equal to $256 \times \frac{745}{27} \approx 7$ Mbps at `poor.victim.com`, which is approximately 27.6 times more that what he has himself.

Solution 2: Network Traffic Analysis (5 min)

1. The logs presented in this exercise are characteristic of an ARP Spoofing attack. We recall briefly how ARP works. When a computer on a LAN (for example `100.20.94.2`) wants to send a message to another computer on the same LAN (for example `100.20.94.1`), it must indicate in the message, the MAC address of the destination computer (that could be `00:00:00:00:00:01` in this example). Computers do not permanently store the MAC addresses of all other computers on the LAN. Thus `100.20.94.2` does not know the MAC address of `100.20.94.1`. It will then broadcast the following question on the LAN: "what is the MAC address of `100.20.94.1`?" (`[ARP who-has? 100.20.94.1]`). This packet will reach all the computers on the LAN, but only computer `100.20.94.1` will respond saying: "the MAC address of `100.20.94.1` is `00:00:00:00:00:01`" (`[ARP is-at 00:00:00:00:00:01]`).
For efficiency reasons, many operating systems keep in memory the answers to recent ARP requests. In a more debatable manner, a majority also store the answers to the requests which they see passing by, even if they did not make a request themselves.
This behavior allows a pirate to flood a targeted server (here, the server that manages the database of the clients' bank accounts) with answers `[ARP reply 100.20.94.1 is-at 00:03:47:48:5c:ee]` and hoping that the next time that the server will want to send a packet to the gateway `100.20.94.1`, it will use the MAC address `00:03:47:48:5c:ee`, which is probably that of a computer he controls. This will allow the pirate to place himself between the targeted computer and the real gateway, and thus intercept or even modify traffic before directing it towards the real gateway.

2. Some configurable switches have some features to prevent ARP Spoofing. One of these is to keep an up-to-date list of ARP/IP mapping by looking at the DHCP requests and responses sent on each port.

Solution 3: ARP/DNS Spoofing (10 min)

1.

[*] A part of these exercises comes from the book "Computer System Security". The reproduction and distribution of these exercises or a part of them are thus forbidden.

1- 192.168.1.1 sends [ARP who-has? 192.168.1.2] to the entire LAN.

2- 192.168.1.2 replies [ARP is-at 00:00:00:00:00:02] to 00:00:00:00:00:01.

3- 192.168.1.1 sends the ping packet to 192.168.1.2.

Destination address in the ping packet	
IP destination	192.168.1.2
MAC destination	00:00:00:00:00:02

2.

1- 192.168.1.1 sends [ARP who-has? 192.168.1.3] to the entire LAN.

2- 192.168.1.3 replies [ARP is-at 00:00:00:00:00:03] to 00:00:00:00:00:01.

3- 192.168.1.1 sends the ping packet to 128.178.33.38.

Destination address in the ping packet	
IP destination	128.178.33.38
MAC destination	00:00:00:00:00:03

3.

1- 192.168.1.1 sends [ARP who-has? 192.168.1.3] to the entire LAN.

2- 192.168.1.3 replies [ARP is-at 00:00:00:00:00:03] to 00:00:00:00:00:01.

3- 192.168.1.1 sends [DNS who-is? www.site.ch] @ 128.178.33.38.

4- 192.168.1.3 sends [ARP who-has? 192.168.1.1] to the entire LAN.

5- 192.168.1.1 replies [ARP is-at 00:00:00:00:00:01] to 00:00:00:00:00:03.

6- 128.178.33.38 replies [DNS is-at 193.192.251.7] @ 192.168.1.1.

7- 192.168.1.1 sends [ARP who-has? 192.168.1.3] to the entire LAN.

8- 192.168.1.3 replies [ARP is-at 00:00:00:00:00:03] to 00:00:00:00:00:01.

9- 192.168.1.1 sends the ping packet to 193.192.251.7.

Destination address in the DNS request	
IP destination	128.178.33.38
MAC destination	00:00:00:00:00:03

Destination address in the ping packet	
IP destination	193.192.251.7
MAC destination	00:00:00:00:00:03

4. The answer to question 4 is shown in Figure 1.

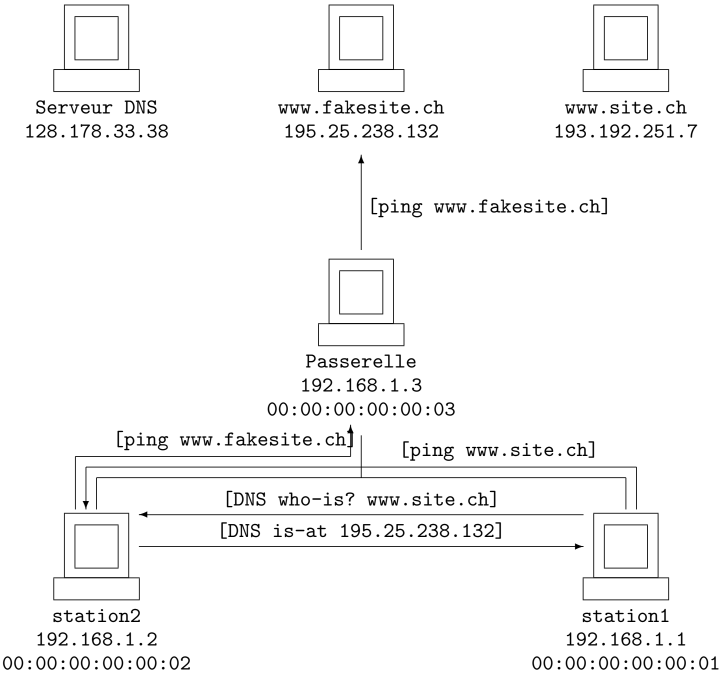

Figure 1: Architecture of a network attacked by ARP spoofing

Solution 4: DHCP Vulnerabilities (5 min)

1. A very simple attack that allows a pirate from preventing clients from obtaining an IP address consists in exhausting the DHCP server's IP addresses stock. To do this, it suffices for a pirate to forge (by indicating a fake MAC address) a sufficiently large number of `DHCPDISCOVER` packets until all the addresses available are allotted. Thus, other clients will be unable to obtain an IP address during the validity period of the addresses that were distributed.

2. If, initially, a pirate succeeds in exhausting the DHCP server's IP address stock, it can no more answer to client's requests. Thus it will be easy for the pirate to set up a false DHCP server that will re-allocate "stolen" IP addresses to the clients and will provide, by the same occasion, erroneous information regarding the gateway and the DNS servers. The pirate will then be able to intercept any client's communications.

Solution 5: TCP session Hijacking (10 min)

As indicated in Figure 2, after the first exchange, Philippe will pretend being Gildas and send a packet to Pascal which must arrive before Gildas' reply. Pascal will accept this packet and then receive Gildas' legitimate packet, which he will not accept as the sequence number will not match. An infinite loop may follow, its outcome depending on Gildas' and Pascal's TCP/IP stack implementation. The exchanges are represented in Figure 2.

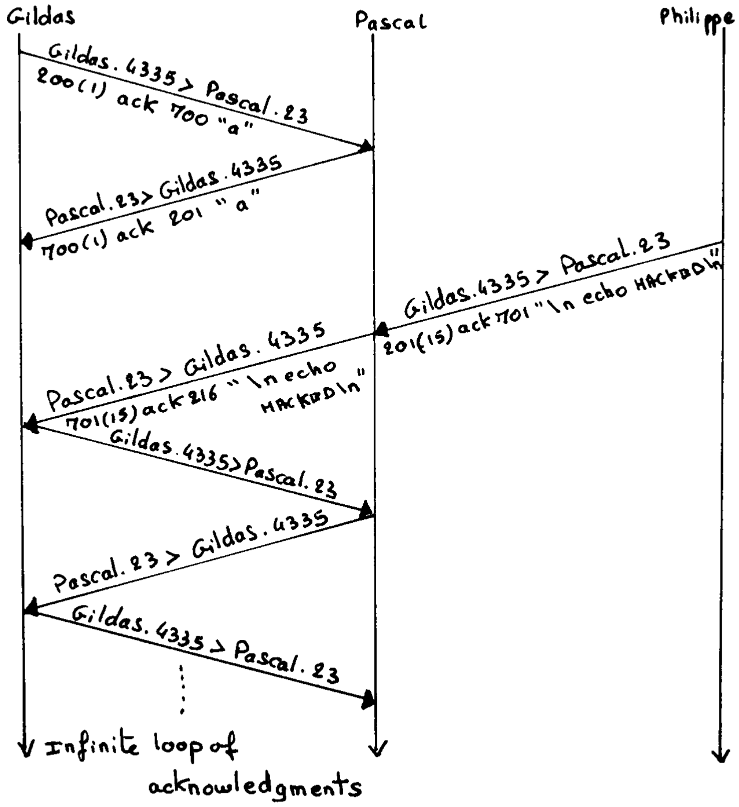

Figure 2: TCP hijacking