INGI2347 : Exercises*

Lab session 4

Xiao Chen, Marco Canini

March 14, 2016

Exercise 1: Amplification Attack

Steve Pirate noticed that a DNS zone transfer request (used for example to provide to a slave DNS server the information it has to know regarding the zone(s) it serves) is always 27 bytes long, and the DNS server `dns.thingummy.com` response is 745 bytes. Let us assume that the communications are based on UDP. Steve Pirate is able to use source address spoofing when it connects to the `dns.thingummy.com`.
1. How can S. Pirate carry out a denial of service attack against the server `poor.victim.com` ?
2. If Steve Pirate has a bandwidth of 256 Kbps and is able to use 100% of it for his attack, how much of the bandwidth belonging to `poor.victim.com` will be used by the attack?

Exercise 2: Network Traffic Analysis

Simon Osterwald, a computer engineer working for a Swiss bank, is responsible for the proper working and security of the employer's network. One morning, during a routine control, he notices suspicious traffic on the server that manages the database of the customers bank accounts. Below is a portion of this traffic.

```
02:01:27 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:27 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 100.20.94.1 is-at 0:3:47:48:5c:ee
```

[*] 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. Knowing that `100.20.94.1` is the gateway's address, give a short interpretation of this traffic.

2. Explain how you can protect against ARP spoofing.

Exercise 3: ARP/DNS Spoofing

Let us consider a local area network (LAN) composed of two workstations and separated from the outside by a router (gateway) as represented in Figure 1. The workstations are configured to use the DNS server at `128.178.33.38`, outside the LAN and do not use an internal DNS cache. Finally, let us consider two HTTP servers outside the LAN, `www.site.ch` and `www.fakesite.ch`. The objective of this exercise is to propose an attack based on *DNS spoofing*, such that when `station1` user (victim) tries to reach the site `www.site.ch`, he will transparently end on the site `www.fakesite.ch`. The attack will be carried out from `station2`.

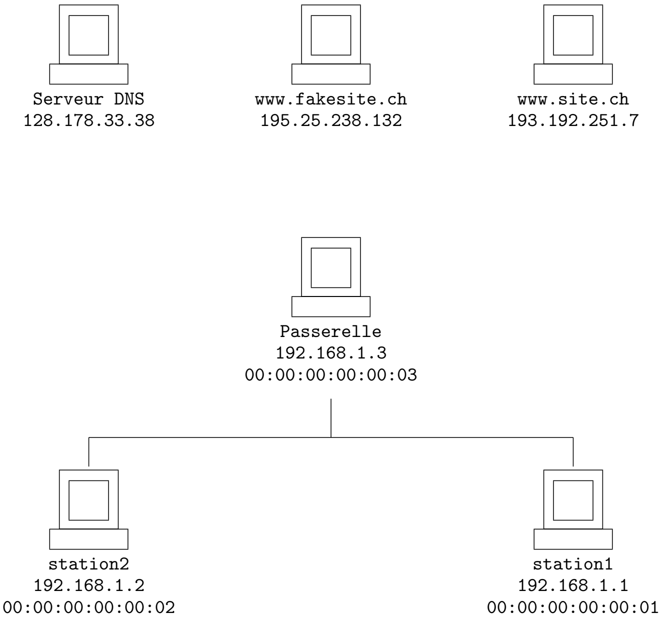

Figure 1: Architecture of the network to be attacked by ARP spoofing

When a workstation wants to communicate with the outside of the LAN, it uses, as destination MAC address the MAC address of the gateway. The gateway receives the packet and retransmits it towards its destination (which is outside the LAN); the destination address in the IP packet remains unchanged. For now, let us suppose that none of the computers on the LAN (including the gateway) know the MAC addresses of the other computers and that the ARP protocol is used to obtain the MAC addresses.

1. The user on computer `station1` executes the command `ping 192.168.1.2`. Write down the ARP and IP messages exchanged on the LAN as well as the destination and source address (MAC, and IP when relevant) of these until the ping packet can actually be sent.

2. The same question for `ping 128.178.33.38`.

3. The same question for `ping www.site.ch`.

4. We suppose that `station2` has launched an ARP spoofing attack to impersonate the gateway and to replace `www.site.ch` by `www.fakesite.ch`. Draw in Figure 1 the paths taken by the

packets transiting on the LAN when `station1` executes the command `ping www.site.ch` (do not draw the ARP requests and replies).

Exercise 4: DHCP Vulnerabilities

DHCP schematically works in the following way: when a computer needs an IP address to connect to a network, it sends a `DHCPDISCOVER` request to all computers of the network located on the same segment. A DHCP server is then responsible to listen to the network in order to allocate IP addresses to the different computers. The pool of available IP addresses is a limited resource. When the server receives a request from a computer, it returns a `DHCPOFFER` packet containing an IP address along with a validity period, as well as other information, such as for example, the gateway's IP address, or those of the DNS servers. Distinct source MAC addresses receive distinct IP addresses. These communications are unfortunately not secure.
1. Describe a simple attack that allows a pirate to prevent the clients from obtaining IP Addresses.

2. How is it possible to extend the previous attack for the pirate to be able to intercept the outbound LAN communications of a targeted computer?

Exercise 5: Ethernet frame

Suppose the following Ethernet frame contains confidential data, which however was not sent securely. Can you find it?

```
00 05 73 a0 00 00 e0 69 95 d8 5a 13 86 dd 60 00
00 00 00 9b 06 40 26 07 53 00 00 60 2a bc 00 00
00 00 ba de c0 de 20 01 41 d0 00 02 42 33 00 00
00 00 00 00 00 04 96 74 00 50 bc ea 7d b8 00 c1
d7 03 80 18 00 e1 cf a0 00 00 01 01 08 0a 09 3e
69 b9 17 a1 7e d3 47 45 54 20 2f 20 48 54 54 50
2f 31 2e 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74
69 6f 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a
6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d
0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73
61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74
3a 20 77 77 77 2e 6d 79 69 70 76 36 2e 6f 72 67
0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d
0a
```

Hint: What tool can we use when we analyze a packet? What can we get from this Ethernet frame? Which encoding method can we use to decode?
Go to this webpage `http://www.root-me.org/en/Challenges/Network/ETHERNET-frame` to perform the challenge and validate your exploit and solution.

Exercise 6: Twitter authentication

A Twitter authentication session was made in cleartext and a corresponding packet trace has been captured. Your goal is to retrieve the password.
You will download the .pcap file on `http://www.root-me.org/en/Challenges/Network/Twitter-authentication-` by clicking "Start the challenge" button. Go to this webpage to perform the challenge and validate your solution.

Exercise 7: IP Time To Live

Find the TTL used to reach the targeted host in this ICMP exchange.
Hint: What is TTL? How can you find in Wireshark?
You will download the .pcap file on `http://www.root-me.org/en/Challenges/Network/IP-Time-To-Live` by clicking “Start the challenge” button. Go to this webpage to perform the challenge and validate your solution.