Introduction on Low level Network tools

Georges Da Costa
dacosta@irit.fr

`http://www.irit.fr/~Georges.Da-Costa/cours/addis/`

1 Introduction

2 Aircrack-ng

3 Wireshark

Low level tools

Hacking tools

- Aircrack-ng (ex Aircrack, ex Airsnort)
    - WEP/WPA cracking program
- Wireshark (ex ethereal)
    - Capture and analyze network frames

1 Introduction

2 Aircrack-ng

3 Wireshark

Aircrack-ng

- 802.11a/b/g WEP/WPA cracking program
- Can recover a 40-bit, 104-bit, 256-bit or 512-bit WEP key
- Method:
  - Gather encrypted frames
  - Once enough frames are acquired (10th of thousand) determines the key
  - Can inject dummy packet to acquired frames
- Can attack WPA1/2 networks with some advanced methods or simply by brute force.

Webpage: `http://www.aircrack-ng.org/`

Wireshark

- Packet sniffer
- Packet analyzer
- It provides multi-level analyze of frames
- It provides semantics for large number of protocols
- It can save sniffed packet for later analyze

Webpage: `http://www.wireshark.org/`

Interface

Three main parts

- Filter
- Frame list
- Content of the current frame

Filter can be used on protocol (*http*, *bootp* or *ftp*) or combination of them (*http or ftp*) or on other frame fields. We will start with **ethereal.cap**.

DHCP

Filter on *bootp*

- DHCP messages are send over UDP or TCP ?
- Draw temporal diagram of communications between dhcp client and server
- What is the DHCP server IP ?
- Which message contains the new client IP ? Which is this IP ?
- What is the time life of this IP ?

Telnet

- How to filter on the telnet messages ?
- Telnet messages are send over UDP or TCP ?
- What is the login used ? What is the password ?
- What is the remote command ? What is the result ?
- Draw temporal diagram of communications between client and server.

DNS

Filter on *dns*, we will focus on request 113 (on **ftp.kernel.org**)

- Filter on dns, are messages send over UDP or TCP ?
- What is the IP of the dns server used ?
- What is the *type* of DNS request ? Are there *answers* in the requests ?
- Look closely on the answers, how many answers are given ? Why ?
- Draw temporal diagram of communications between client and server.

Ping

Two ping command are issued. The first (*ping 204.152.191.37*) starts message 101, the second (*ping ftp.kernel.org*) message 113.

- Which protocol is used ?
- How to filter on the ping messages ?
- Why those frames do not have a local or remote port ?
- Remove filters and explain the difference between the two pings
- For the two pings, draw temporal diagram of communications between client and server for the first round.

ftp

- Find the filter to show the 44 messages of the ftp session. Is ftp based on UDP or TCP ?
- What is the login used ? What is the password ?
- What is the name of the file transferred ?
- What is the content of the file ?
- Draw temporal diagram of communications between client and server.

Http, part 1

- HTTP requests comes from two requests: One single image and one complete web page.
- For the single image (request frame 236)
  - Which is the version of the HTTP protocol asked by the client ?
  - Which is the version of the HTTP protocol used by the server for answering ?
  - Which is the status replied by the server ?
  - What is the date of last modification ?
  - What is the size of the answer ? (at the different levels)
  - This file is large, how do the transfer occurs at the different levels ?
  - Draw temporal diagram of communications between client and server.

Http, part2

For the whole web site (frame 274)

- What is the Operating system of the client ?
- What is the maximum number of files requested at the same time ?
- The image of the first part is displayed but not requested, why ?

traceroute

For this part, switch to **ethereal_traceroute.cap**

- traceroute allows to obtain information on routers on a IP path between a client and a server.
- It uses TTL (Time To Live)
- When a server receive an IP message with a TTL of 0, it answers back that the remote host could not be attained.

traceroute, bis

- What is the name of the server ?
- What are the values of TTL ?
- What is the protocol used ? Why ?
- What else occurs than knowing IP of routers ? Why ?