Network training

Maël Auzias

Fall 2014

Contents

1 HTTP example

1.1 Who are you? Where are you?

What is your own IP address? What is your own MAC address? What is your network mask? What do theses commands display?

```
#ifconfig
$curl ifconfig.me
$netstat -at
```

1.1.1 How to get out?

Before we can access the Internet we need to know who/what is the gateway. What is a gateway? What do theses commands display?

```
#route -n
#arp -a
```

1.1.2 What's your number?

As explained before, humans can easily remember name such as news.ycombinator.comor root-me.orgbut it is not as easy to remind `198.41.191.47` or `212.129.28.16`. We need a way to *translate* a domain name into an IP address. This is role of DNS[1]. You can query DNS using `nslookup`.

1.1.3 Wait! What direction?

The (IP) address is of the website you want to visit is now known. The next step is to know how to *GET*[2] there. Try to trace the route using... `traceroute` (or `tracepath`) to see packets' path. Do you know any town on the path from where you are to `www.ethicalhacker.net` server? Note that sometimes, for security reasons, IMCP protocol is blocked. If this is the case you can use an option to use TCP SYN for probes. How does `traceroute` work ?

1.1.4 Go GET it!

What does `wget 95.215.16.43 80` do?

1.1.5 Capture it

Use `wireshark` to capture:

- a GET through HTTP (selfoss.aditu.dedoes not have valid HTTPS certificate).
- a GET through HTTPS (micahflee.comforce redirection to HTTPS).

What differences can you see? How can you explain theses differences?

[1] DNS: Domain Name Server, if you needed to read this footnote keep in mind that you should remember it from now on

[2] that's not a HTTP verb, but a word play!

1.1.6 "Security" *without* HTTPS

Some methods allow web-master to secure some part of the website. Then the website requires a user and a password to enter. You can test on the webpage: http://teaching.auzias.net/http-auth/

- user: test
- pass: p4ssw0rd

Use `wireshark` and verify if you had captured the user:password encrypted or not. RFC 2617could be handful.

2 Chat

`netcat (or ncat)` is a "network swiss army knife". By checking its man page how can you use it as a chat server/client (two nodes only).

2.0.7 TCP

Use the mode TCP of `netcat` and try it. Can `netstat` could, somehow, be handful for anything while waiting for connection? Can `telnet` be used to chat?

2.0.8 UDP

Use the mode UDP of `netcat` and try it. Explain a situation within the server could not receive every packet. Try to produce this situation by implementing it using Java langage. (`InetAddress` and `DatagramPacket` should be useful...)

More example of netcat