

Vulnerabilità e Difesa dei Sistemi Internet

A.K.A. ETHICAL HACKING

FRANCESCO MANCINI - francesco.mancini@uniroma2.it

PASQUALE CAPORASO - pasquale.caporaso@uniroma2.it

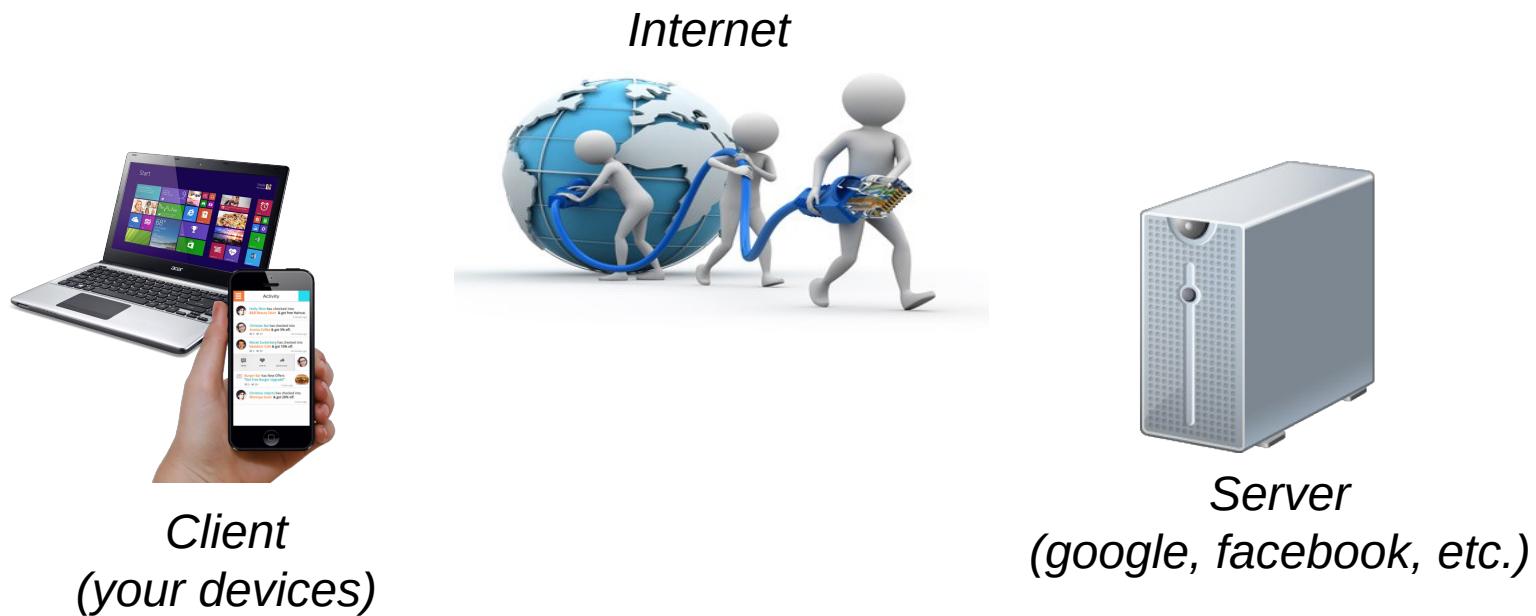
SARA DA CANAL - sara.da.canal@uniroma2.it

PIERCIRO CALIANDRO - pierciro.caliandro@uniroma2.it

Vulnerabilità e Difesa dei Sistemi Internet

UNDER THE HOOD OF APPLICATIONS

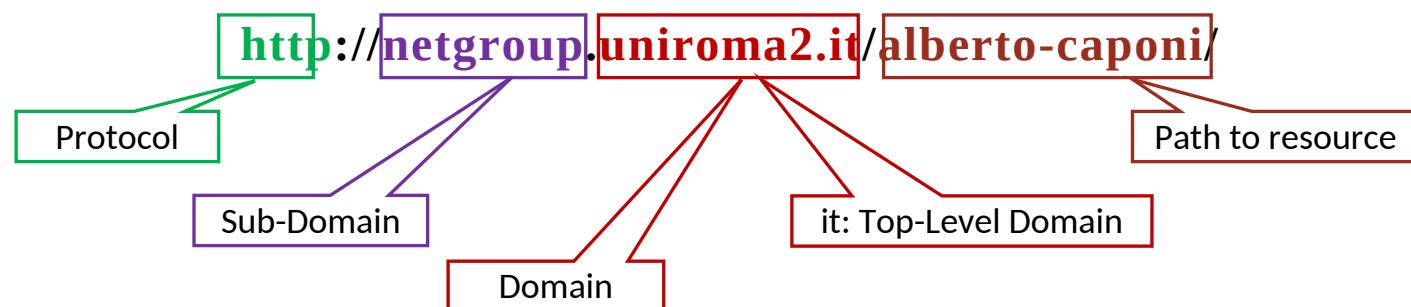
What does it happen really on Internet?



What a web page is?

a resource (i.e a file), specified by a
URL: Uniform Resource Locator.

e.g. my home page:



URL's components

Protocol (also called “scheme”)

- How can the web resource be accessed?

http, https, ftp, ...

Domain name

- Where is the page located?

google.com, ...

Sub-Domain

- In which specific host of the domain?

netgroup, www, ...

Resource Path

- Which is the specific path/name of the resource?

index.html, home.php, ...



URL Parameters: /login.php?user=alberto&pass=1234

What a protocol is?

- A common language between client and server that defines:
 - A common set of rules & messages that allow the client to be understood by the server:
 - Web → HTTP
 - E-mail → SMTP
 - File Transfer → FTP
 - ...

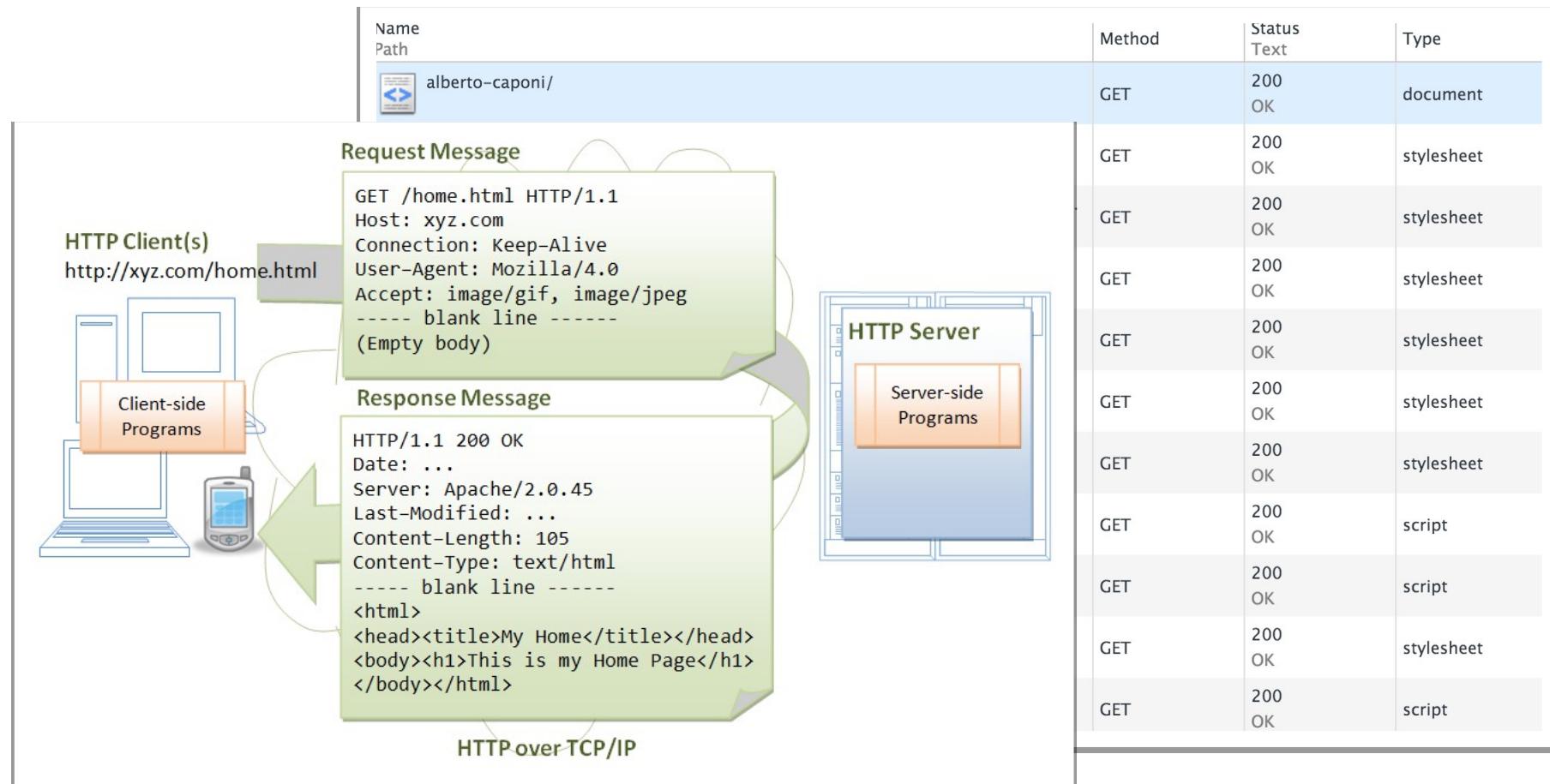


HTTP Protocol

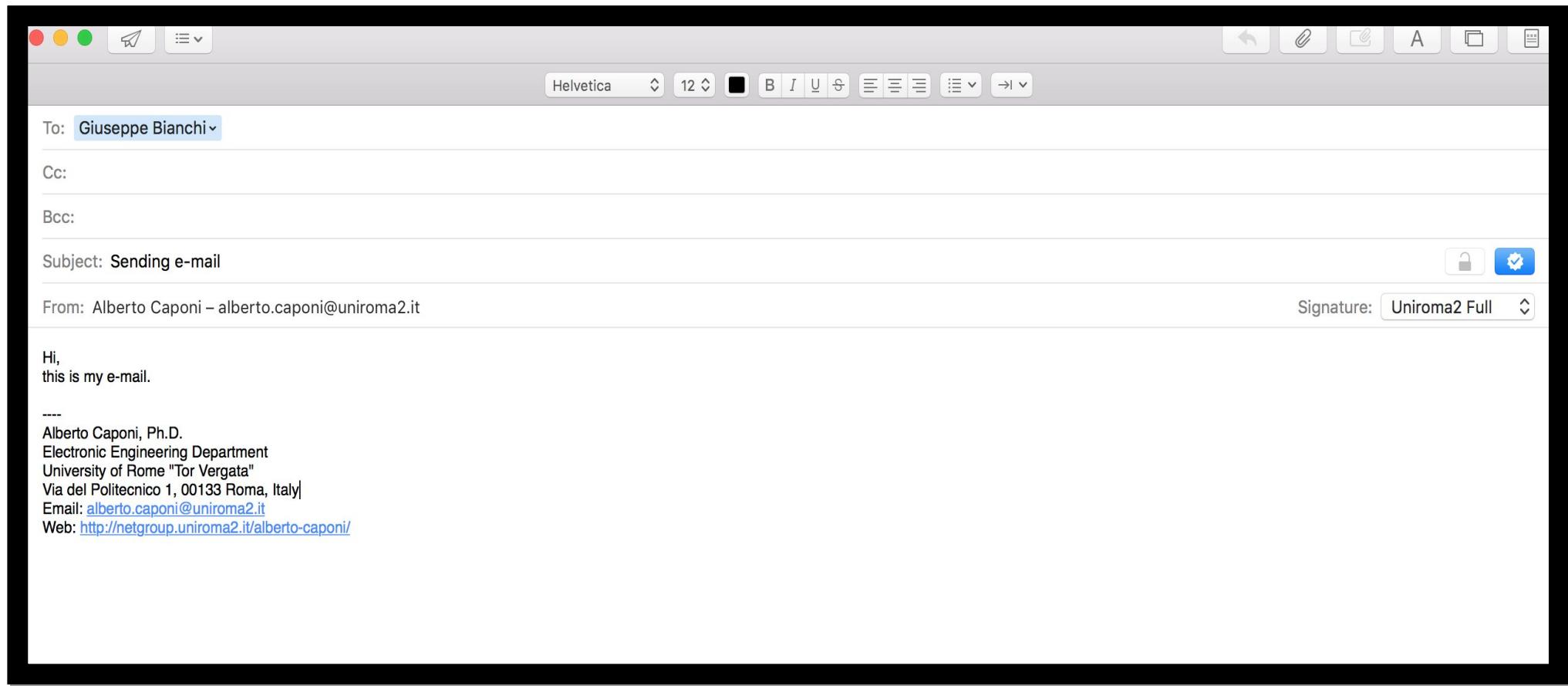
The screenshot shows a web browser window with the following details:

- Title Bar:** Alberto Caponi | netgroup
- Address Bar:** netgroup.uniroma2.it/alberto-caponi/
- Toolbar:** Security Courses, Hacking, Learning, Altri, Inglesi, Google Translate Pro, XDCC, "Common" by Alberto, Coursera, BitBucket, FilesOverMiles, Google Students, CodiceSconto.com, Other Bookmarks.
- Header:** University of Rome Tor Vergata, Department of Electronic Engineering, NETWORKING GROUP
- Navigation:** HOME, PEOPLE, TEACHING, PROJECTS/RESEARCH, EVENTS, INFO, SEARCH
- Profile Section (Left):**
 - Alberto Caponi:** Profile picture of a man in a suit.
 - PostDoc:**
 - Contacts:**
 - e-mail: alberto.caponi – at – uniroma2.it
 - telephone: +39 067259-7773
 - skype: caponi.alberto86
 - Netgroup Lab ([map](#))
 - Research Interests:**
 - Network & Computer Security
 - Data-Centric Security: Identity & Attribute Based Cryptography
 - Information Centric Networks (ICN) | Named Data Networks (NDN): caching efficiency and resilience to attacks ([more...](#))
 - Publications:**
 - N. Blefari-Melazzi, G. Bianchi, A. Caponi, A. Detti, "A General, Tractable and Accurate Model for a Cascade of LRU Caches", IEEE Communications Letters 18(5), 877-880 (2014). ([pdf](#))
 - A. Detti, A. Caponi, G. Tropea, G. Bianchi, N. Blefari-Melazzi, "On the Interplay among Naming, Content Validity and Caching in Information Centric Networks", IEEE GLOBECOM 2013, Atlanta, USA, 9-13 December 2013. ([pdf](#))
- Netgroup Section (Right):**
 - Home
 - People
 - Faculties
 - Postdoc
 - PhD Students
 - Cooperating Personnel
 - Teaching
 - Projects/Research
 - Events
 - Info
 - Links

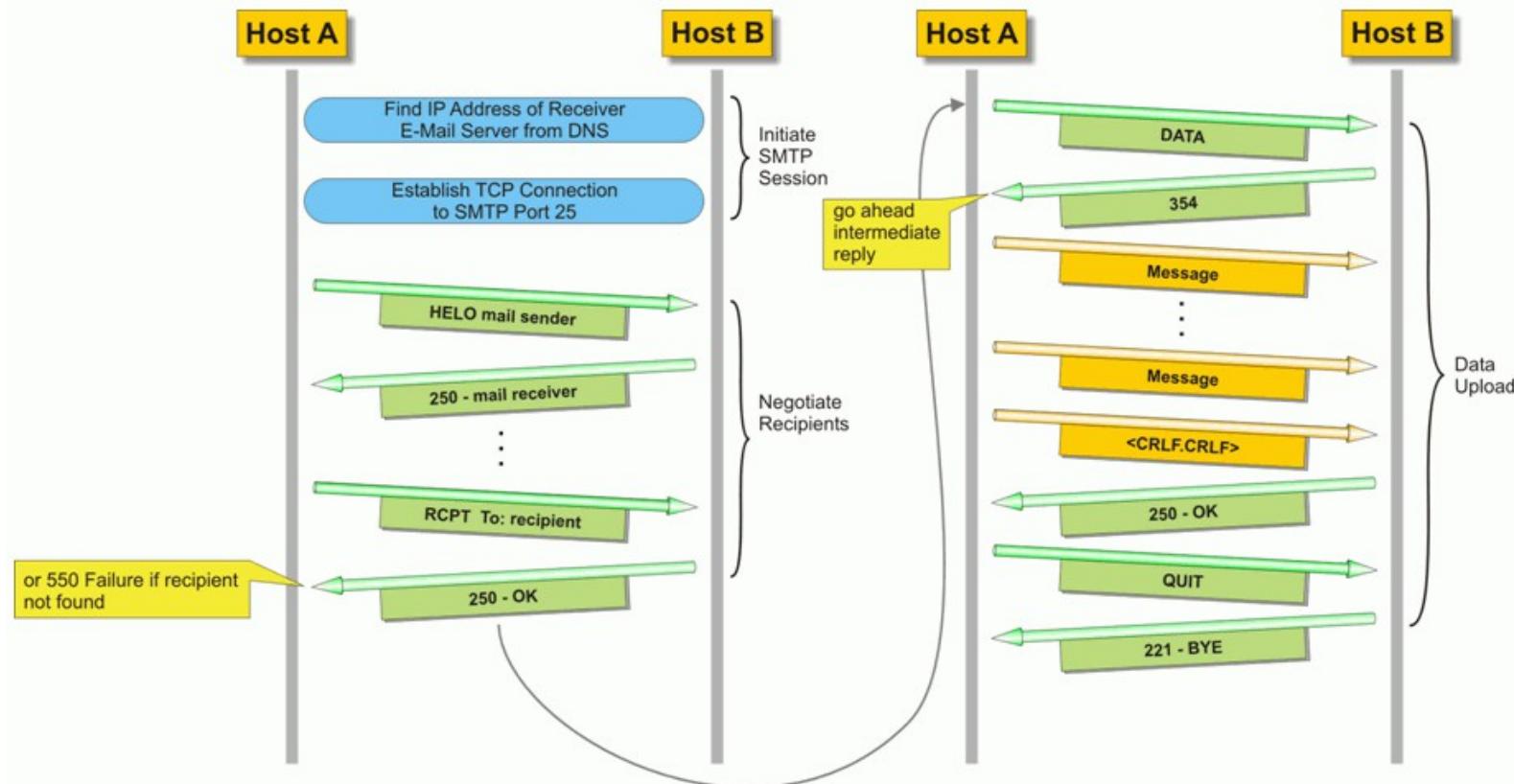
HTTP Protocol: under the hood



SMTP Protocol



SMTP Protocol: under the hood



Applications manage protocols

```
macbook-markin:~ markin$ telnet netgroup.uniroma2.it 80
Trying 160.80.221.15...
Connected to netgroup.uniroma2.it.
Escape character is '^]'.
GET /alberto-caponi/ HTTP/1.1
Host: netgroup.uniroma2.it
```

Applications manage protocols

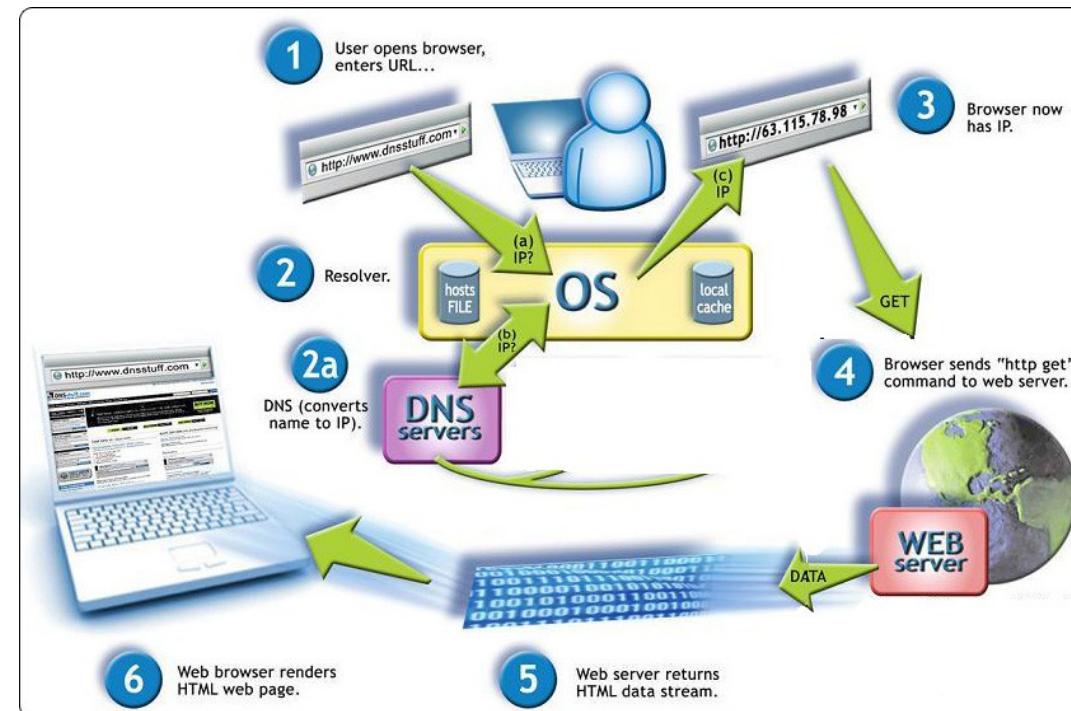
```
[macbook-markin:~ markin$ telnet smtp.uniroma2.it 25
Trying 160.80.6.23...
Connected to smtp.uniroma2.it.
Escape character is '^].
220 smtp-2015.uniroma2.it ESMTP Sendmail 8.14.4/8.14.4/Debian-8; Mon, 15
IL)-[160.80.103.191]
HELO uniroma2.it
250 smtp-2015.uniroma2.it Hello [160.80.103.191], pleased to meet you
MAIL FROM:<giuseppe.bianchi@uniroma2.it>
250 2.1.0 <giuseppe.bianchi@uniroma2.it>... Sender ok
RCPT TO:<alberto.caponi@uniroma2.it>
250 2.1.5 <alberto.caponi@uniroma2.it>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
FROM: Giuseppe Bianchi <giuseppe.bianchi@uniroma2.it>
TO: Alberto Caponi <alberto.caponi@uniroma2.it>
Reply-To: Giuseppe Bianchi <attacker@foo.com>
SUBJECT: [URGENT] I lost my Credit Card!
Please Alberto,
send me your credit card data. I lost mine and need it urgently!

Best Regards,
GB
.
250 2.0.0 u1FHxP8000719 Message accepted for delivery
quit
221 2.0.0 smtp-2015.uniroma2.it closing connection
Connection closed by foreign host.
macbook-markin:~ markin$
```

Domain name is translated to number

We need the exact address of the resource's server

- Should be unique in the World!
- Humans remembers strings but...machines likes numbers!



Domain name is translated to number

```
[macbook-markin:~ markin$ dig www.uniroma2.it

; <>> DiG 9.8.3-P1 <>> www.uniroma2.it
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56193
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

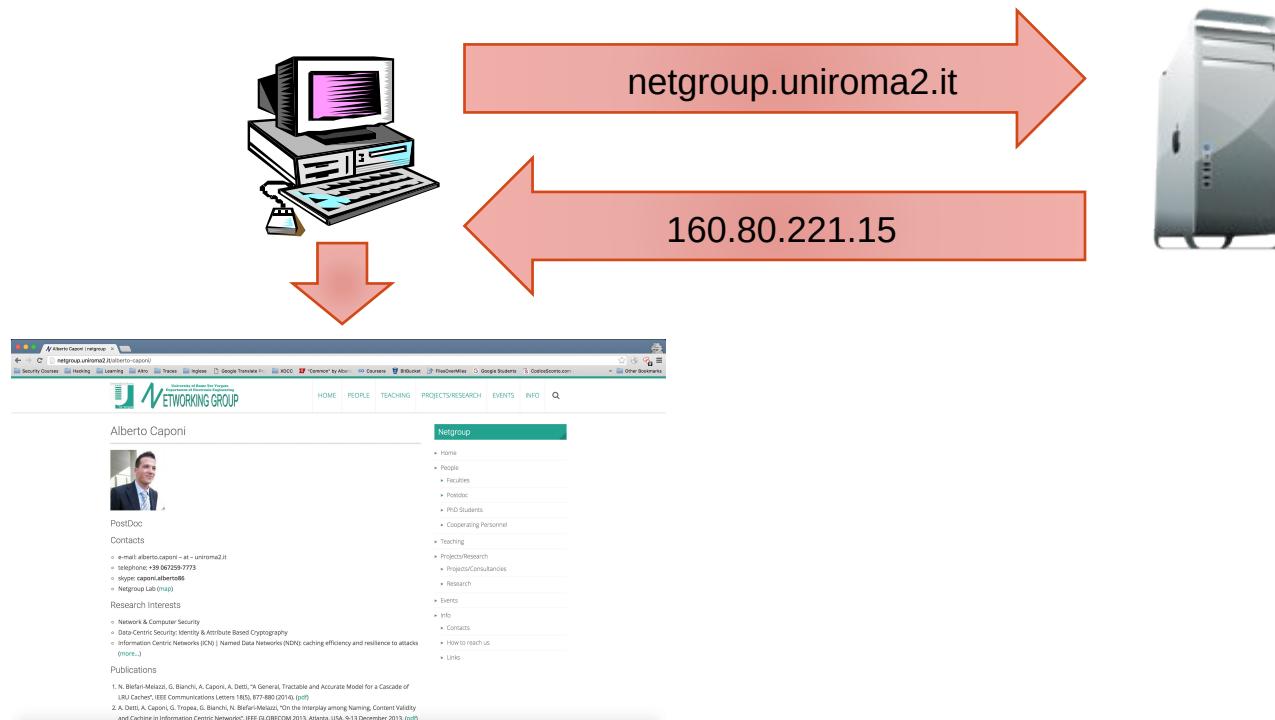
;; QUESTION SECTION:
;www.uniroma2.it.           IN      A

;; ANSWER SECTION:
www.uniroma2.it.      1776    IN      CNAME   webhouse01.ccd.uniroma2.it.
webhouse01.ccd.uniroma2.it. 2426    IN      A       160.80.2.46

;; Query time: 14 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Feb 16 12:23:36 2016
;; MSG SIZE  rcvd: 78

macbook-markin:~ markin$
```

Domain Name System

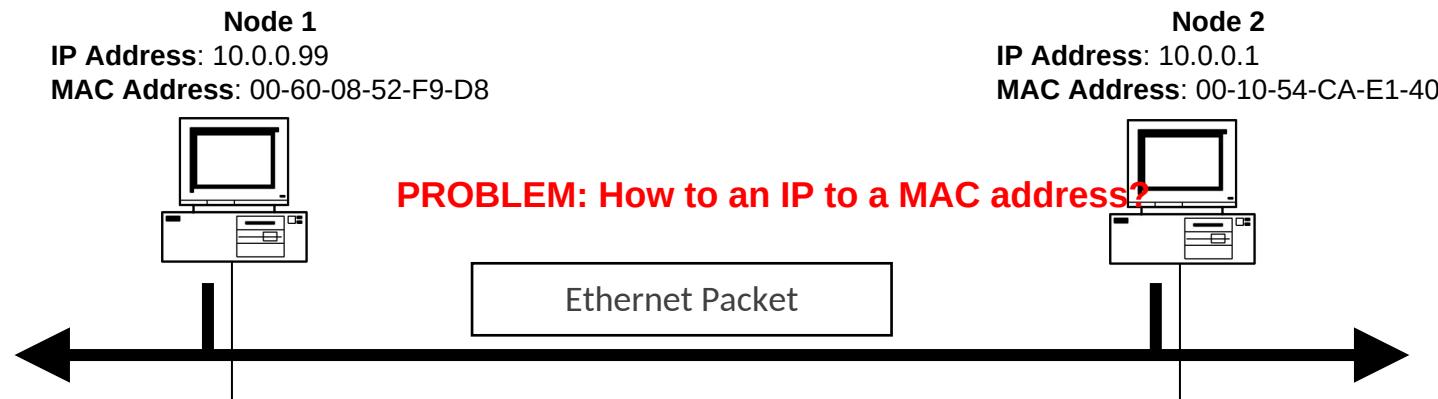


IP or MAC addresses?

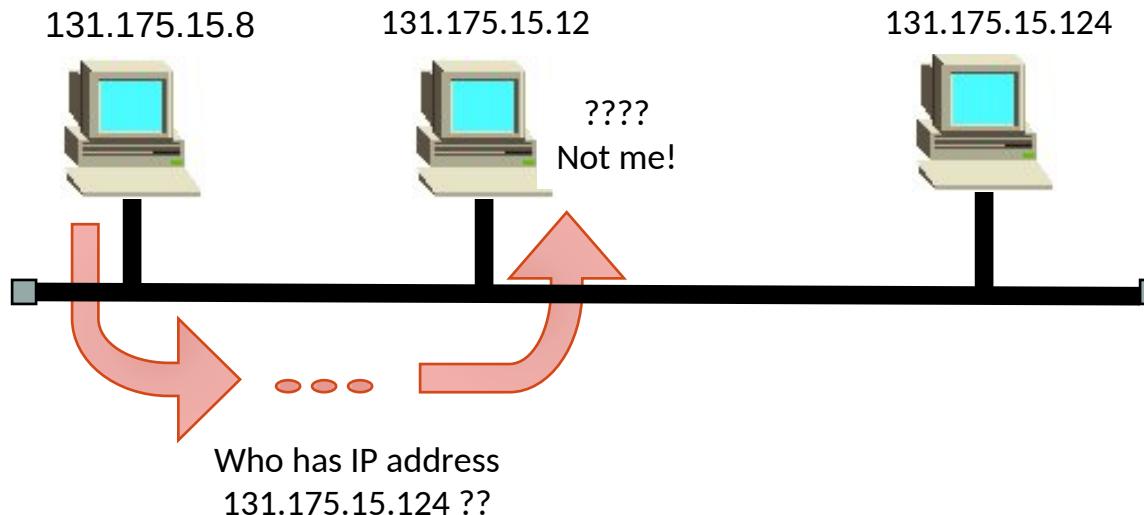
Physical Networks don't uses IP addresses

- IP address depends on the network you are connected to!
- What if you move from that network to another one?

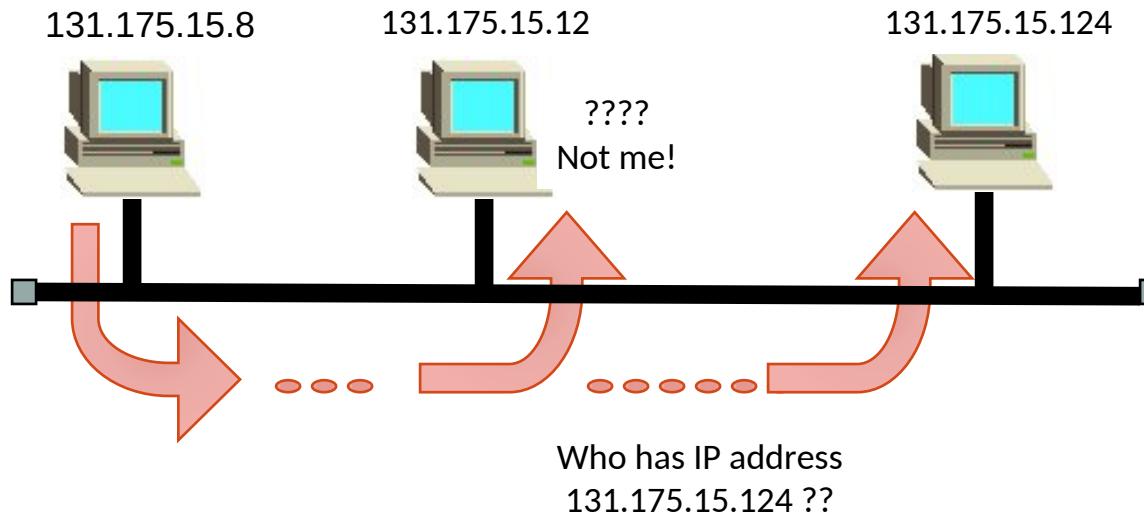
Needs to use the pre-stamped address of your network card: MAC address!



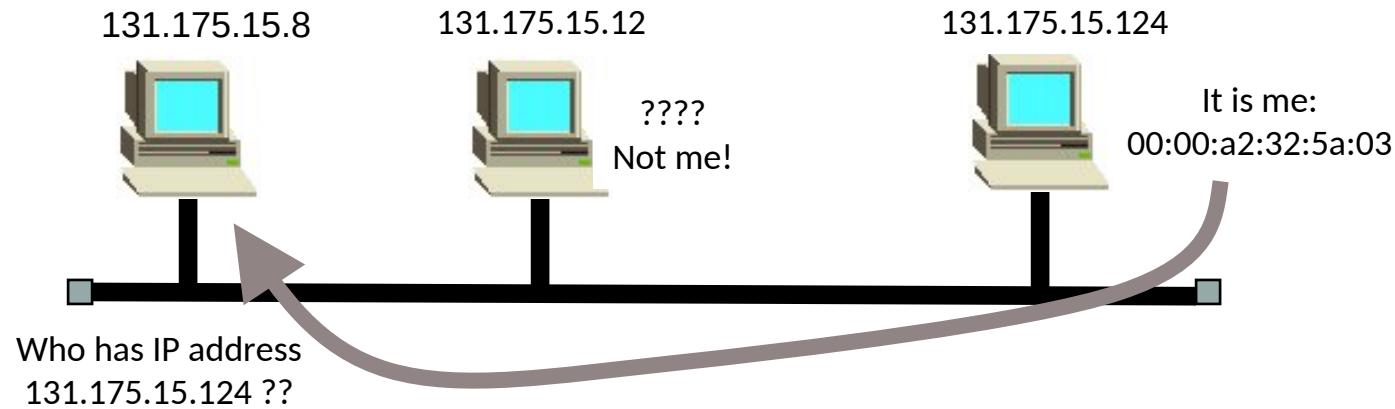
Address Resolution Protocol



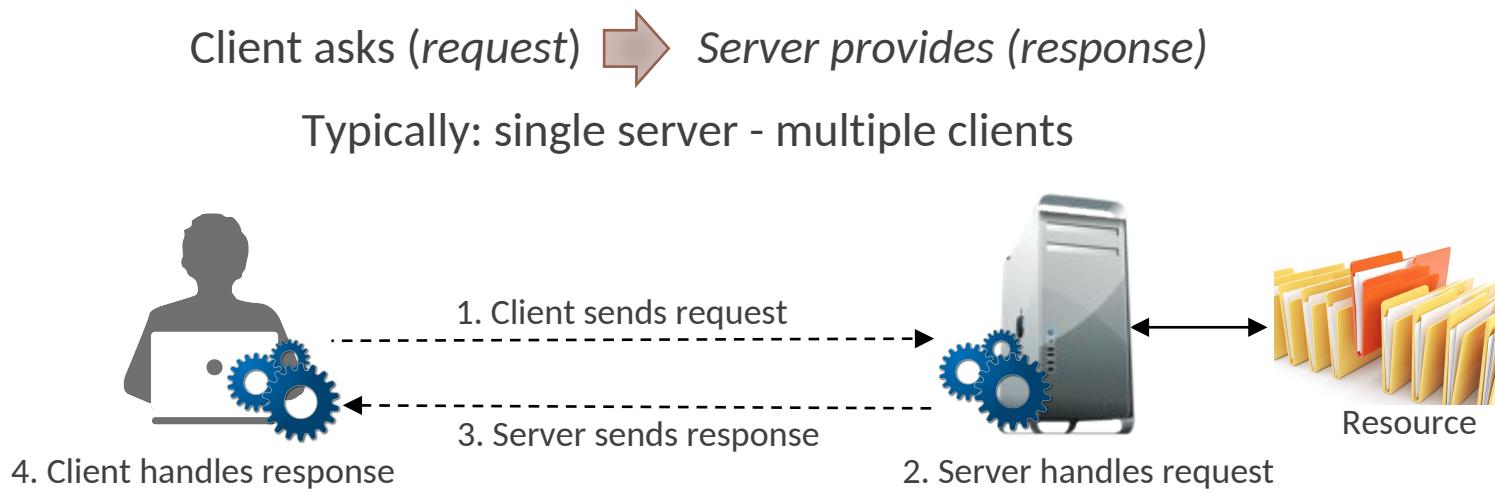
Address Resolution Protocol



Address Resolution Protocol



Client-Server Model Overview



Clients and servers are processes running on physical host machines

Client-Server Model Overview

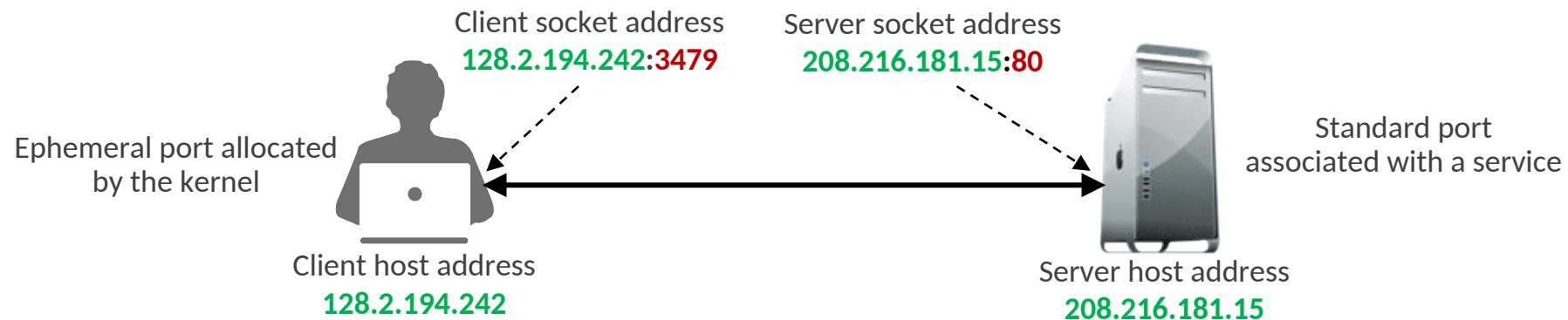
Address the machine on the network

- By IP address

Address the process

- By the “port” number

The pair of IP-address + port – makes up a “socket-address”



Client

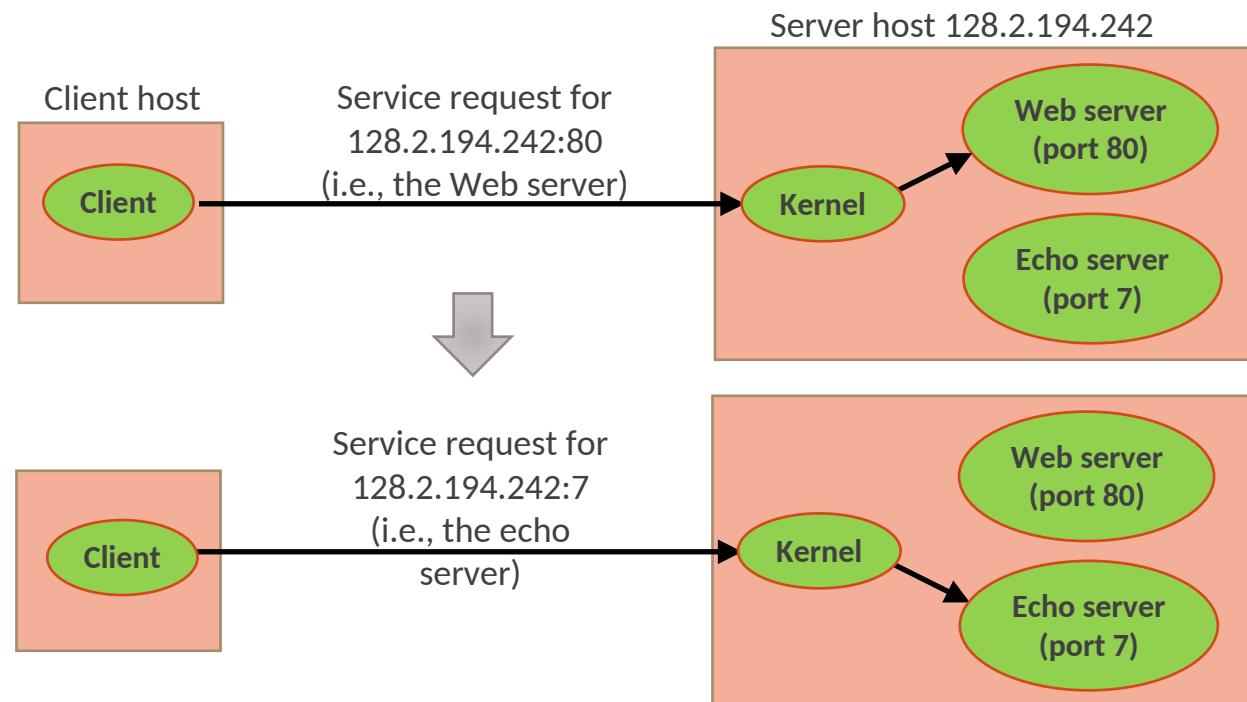
Examples of client programs

- Web browsers, ftp, telnet, ssh

How does a client find the server?

- The IP address in the server socket address identifies the physical host
- The (well-known) port in the server socket address identifies the service
 - Implicitly identifies the server process that performs that service
- Examples of well known ports:
 - Port 7: Echo server
 - Port 23: Telnet server
 - Port 25: Mail server
 - Port 53: DNS
 - Port 80: Web server

Using Ports to Identify Services



Vulnerabilità e Difesa dei Sistemi Internet

FIRST HANDS-ON TO KALI & LINUX

Booting up Kali Linux

You can find Kali Linux Virtual Machines [at this link](#)

Kali Linux contains over 300 forensics and penetration testing tools

- finding your way around them can be a daunting task at times

The default credentials for the Kali VM are:

- **Username:** kali
- **Password:** kali

The Kali Linux menu presents a large number of tools

- It helps to understand the context and usage of a tool
- Familiarize yourself with the available tools and their categories

Find, Locate, and Which

Prior to using the **locate** utility, we must run **updatedb**

- It builds a local database of all files on the filesystem
- Once the database has been built, **locate** can be used to easily query this database when looking for local files

```
root@kali:~# updatedb
root@kali:~# locate sbd.exe
/usr/share/windows-binaries/backdoors/sbd.exe
```

The **which** command searches through the directories that are defined in the **\$PATH** environment variable

- If a match is found, **which** returns the full path to the file as shown below

```
root@kali:~# which sbd
/usr/bin/sbd
```

Find, Locate, and Which

The **find** command is a more aggressive search tool than **locate** or **which**.

- Find is able to recursively search any given path for various files
- It has a lot of options for files attributes
 - E.g. permissions, owner

```
root@kali:~# find / -name sbd*
/usr/share/doc/sbd
/usr/share/windows-binaries/sbd.exe
/usr/share/windows-binaries/backdoors/sbd.exe
/usr/share/windows-binaries/backdoors/sbdbg.exe
/usr/bin/sbd
/var/lib/dpkg/info/sbd.md5sums
/var/lib/dpkg/info/sbd.list
```

Find, Locate, and Which

Programs that are configured for SetUID:

- `find / -perm -4000 -print`

Programs that are configured for SetGID:

- `find / -perm -2000 -print`

Files that are readable by anyone in the world:

- `find / -perm -2 -type f -print`

Hidden files:

- `find / -name "./*"`

bash

Imagine you are tasked with

- finding all of the subdomains listed on the *cisco.com* index page
- find their corresponding IP addresses.

Start by downloading the *cisco.com* index page using the **wget** command

```
root@kali:~# wget www.cisco.com
--2013-04-02 16:02:56--  http://www.cisco.com/
Resolving www.cisco.com (www.cisco.com)... 23.66.240.170,
Connecting to www.cisco.com (www.cisco.com)|23.66.240.170|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23419 (23K) [text/html]
Saving to: `index.html'

100%[=====] 23,419      --.K/s   in 0.09s
2013-04-02 16:02:57 (267 KB/s) - `index.html' saved [23419/23419]

root@kali:~# ls -l index.html
-rw-r--r-- 1 root root 23419 Apr  2 16:02 index.html
```

bash

```
root@kali:~# grep "href=" index.html | cut -d "/" -f 3 | grep "\." | cut -d
'"' -f 1 | sort -u
blogs.cisco.com
communities.cisco.com
csr.cisco.com
developer.cisco.com
grs.cisco.com
home.cisco.com
investor.cisco.com
learningnetwork.cisco.com
newsroom.cisco.com
secure.opinionlab.com
socialmedia.cisco.com
supportforums.cisco.com
tools.cisco.com
www.cisco.com
www.ciscolive.com
www.meraki.com
```

netcat

Connecting to a TCP/UDP port can be useful in several situations:

- To check if a port is open or closed
- To read a banner from the port
- To connect to a network service manually

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [127.0.0.1] from (UNKNOWN) [10.0.2.15] 35336
hi my name is John!
hi my name is Anne!
```

```
root@kali:~# nc 127.0.0.1 1234
hi my name is John!
hi my name is Anne!
```

netcat

```
root@kali:~# nc -lvp 1234 < .ssh/authorized_keys
listening on [any] 1234 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [127.0.0.1] from (UNKNOWN) [10.0.2.15] 35330
```

```
root@kali:~# nc 127.0.0.1 1234
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCu8Ghr7LPQPp0e2yxN+2ALq/LVN3CgGpdwYQ8Yd2/s
GexxCjtWIJM0Q0T7/bIAAR3/UQMwjXV+rGtsDgqEc tyEBBEIevzE1CmY2Vp13sSWFKxDVvEBBtMD07Ud
vshzF68TRVMMWZwVOGzDoZZd7mVNgjz6lldSnKtv8rx5SL/uHKQja9SyGuR9JoKa2eNGzrF0KRZLXwwl
HXN5GwmJLA8wIbjQM962IYGhDDjG1xSFfG015xjabCh7bHtNk3Qb5WRNBBRmTEvlJG6eMokIsW6u6H/9
2sKazemx8MYc+qS88EeYZsy+fW8MyAT0od0m9surajf+tmYim9Rpvn/gu3T7  pentest-env
```

netcat

- Netcat can be used for file transferring too:
 - Sender side:** nc -w 3 [destination] [port] < [file]
 - Receiver side:** nc -l -p [port] > [file]

```
(root㉿kali)-[~/kali]
# nc -w 3 192.168.6.209 1234 < linpeas.sh

└── hola.php.jpeg      master
    └── (kali㉿kali)-[~]
        $ sudo su
[sudo] password for kali:
(root㉿kali)-[~/kali]
# nc -l -p 1234 > out.file
```

netcat

```
root@kali:~# nc -lvp 1234 -e /bin/bash
listening on [any] 1234 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [127.0.0.1] from (UNKNOWN) [10.0.2.15] 35338
[]
```

```
root@kali:~# nc 127.0.0.1 1234
whoami
root
ls
bettercap
Desktop
Documents
Downloads
index.html
Music
Pictures
Public
Templates
Videos
[]
```

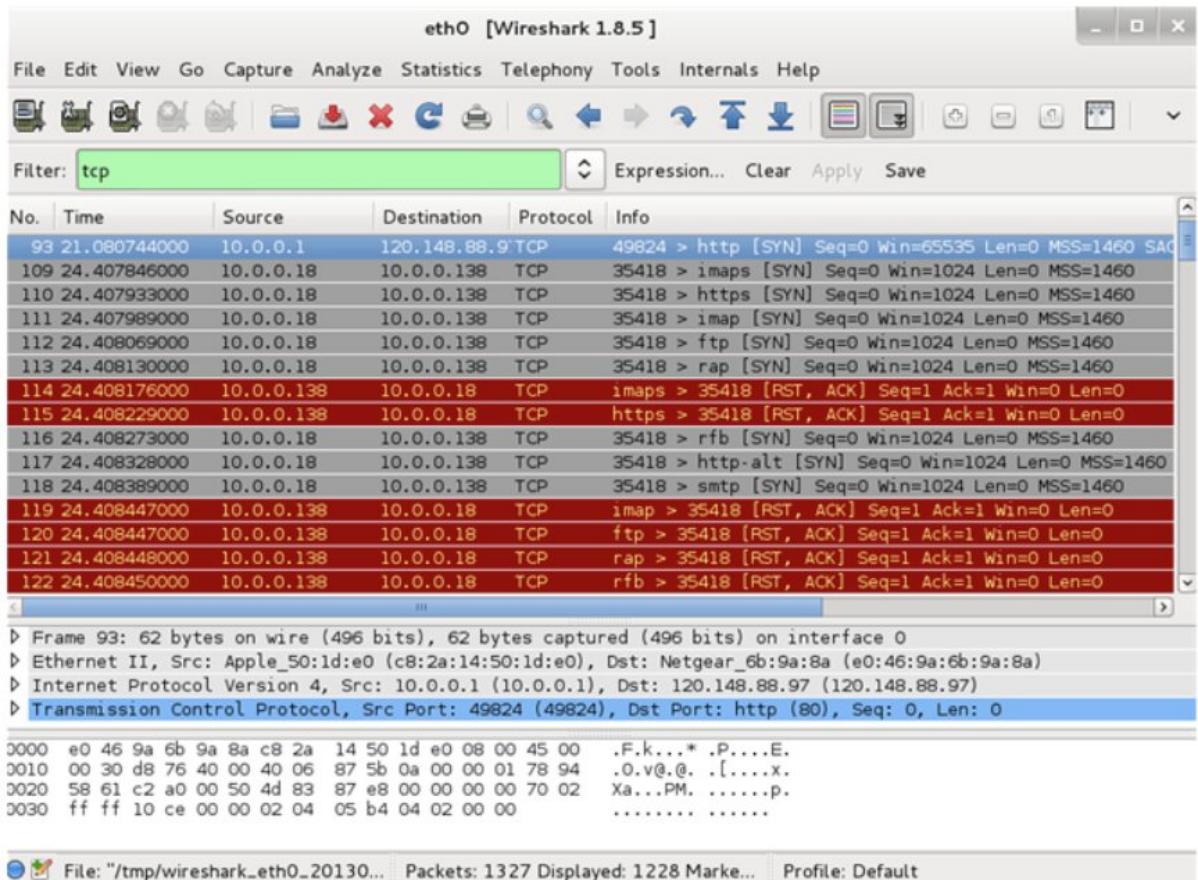
wireshark

Network sniffer like wireshark are useful to:

- Understand a protocol
- Debug a network client
- Analyze traffic in your network

Explore wireshark:

- Capture filters
- Display filters
- Follow streams



tcpdump

We might not have access to GUI network sniffers such as Wireshark:

- We can use the command line **tcpdump** utility
- `tcpdump -r password_cracking_filtered.pcap`
- `tcpdump -n -r password_cracking_filtered.pcap | awk -F" " '{print $3}' | sort -u | head`
- `tcpdump -n src host 172.16.40.10 -r password_cracking_filtered.pcap`
- `tcpdump -n dst host 172.16.40.10 -r password_cracking_filtered.pcap`
- `tcpdump -n port 81 -r password_cracking_filtered.pcap`
- `tcpdump -nX -r password_cracking_filtered.pcap`
- `tcpdump -A -n 'tcp[13] = 24' -r password_cracking_filtered.pcap`
- `tcpdump -A -n -r password_cracking_filtered.pcap | grep "HTTP/1.1 "`

What happened?

Vulnerabilità e Difesa dei Sistemi Internet

PENTEST FRAMEWORKS - INTRODUCTION

Metasploit framework

- Well known framework, used to generate *payloads* that can be used to exploit a particular vulnerability
- Supports payloads and exploits for several protocols, languages and frameworks such as:
 - HTTP/s
 - MySQL
 - SSH
- Furthermore, it allows the generation of automatic artifacts such as *bind/reverse shell* for Linux/Windows etc...
- **Won't be allowed at the exam!**



Metasploit

SQL Map

- Useful framework for the testing and automation of *SQL injections*
- Support for more or less every known database (both commercial and none):
 - MySQL
 - Oracle
 - PostgreSQL
 - Microsoft SQL Server
 - ...
- Open source, can be downloaded [here](#)
- **Won't be allowed at the exam!**

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
[!] H {1.3.4.44#dev}
[!] http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:44:53 /2019-04-30/

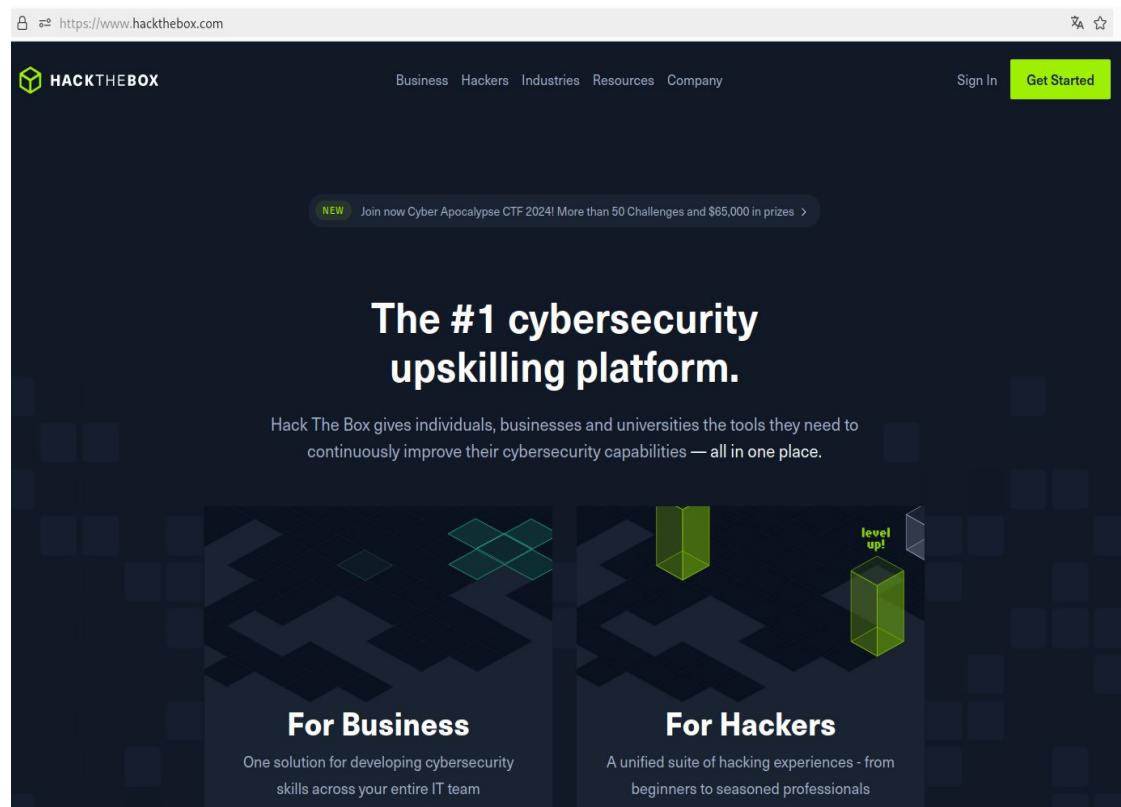
[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'ascii'
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:54] [INFO] testing if the target URL content is stable
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```

Vulnerabilità e Difesa dei Sistemi Internet

TRAINING PLATFORM

Hack the box

- The most well known platform for penetration testing training
- In the last years, it also offers an *academy program*
- Where to register:
 - [Hack the box](#)
 - [Hack the box academy](#): you can find training modules under “All modules”



Try hack me

- Similar to hack the box
- Certification program, certificates can be earned (there's a fee to pay for exam access)
- Where to register:
 - [Try hack me registration](#)



FYI

- At the end of the course, your Hack the box and Try hack me profiles will be evaluated
- If you did enough training and machine solves, there could be **bonus points** on the final exam
vote 😊

Conclusion

THAT ALL FOLKS!

Thank you for your attention 😊 !