Networking

G.Filosofi 2018

- Blockchain: a network distributed database of peer-to-peer transactions (of any kind, e.g. a payment, a google search, voting, etc.) where all the participants share a consensus. Any new transaction added at any point of the network gets spreaded over the entire network. It cannot be removed or changed anymore.
- SEO (Search Engine Optimisation): the art of making your web content more relevant in google search. An important factor is the number of input links, i.e. links to your web pages found in other web sites
- Telnet: client-server protocol used for bidirectional interactive text-oriented communication. For secure use SSH is preferred. Every time users 'hit' a key a packet is sent. Users authenticate with a clear-text username and password.

Exposed on TCP port ????.
host $ telnet <ipaddr>

- FTP (File Transfer Protocol): client-server protocol used for file transfer. Users authenticate with a clear-text username and password. For secure transmission FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP)
- SSH (Secure Shell): client-server remote terminal for operating network services securely over an unsecured network. The best known example application is for access to computer systems by remote users. Username and password are sent encrypted over the network. SSH is a recommended alternative to Telnet because it is encrypted. However, it is susceptible to sniffing using MITM techniques
- SMTP (Simplified Mail Transport Protocol): the Internet standard for email. The secure version is S/SMTP. SMTP is a clear-text protocol. In addition to that, emails inherently do not have

any authentication mechanism. In other words, the protocol does not provide a secure way of authenticating whether a received email is indeed from the listed sender

- The Domain Name System (DNS) is a translation service that translates hostnames to IP addresses
- The Pup (PARC Universal Packet) format created for Alto (1973) influenced the TCP/IP protocol suite developement
- IPv4 sono 32 bit, IPv6 sono 128 bit. Questo significa tantissimi ip address per ogni metro quadro sulla terra. Oggi il traffico IPv6 è al 14%, in crescita. La latenza di IPv6 è inferiore a IPv4
- url: ns2.ntc.com
- IPv4: 205.251.198.137
- IPv6: 2600:9000:5306:8900:0:0:0:1
- IPv6: an IP address consisting of 8 groups of 16-bit hexadecimal numbers (for a total of 128 bits). If several groups in a row are all zero, you can omit those groups and replace them with a double

colon (but only once per IP address). For example, the IPv6 address for example.com is 2001:500:88:200::10.

- pfSense: piccola distribuzione FreeBSD con un sw che funge da router, firewall e proxy. Si può creare una VPN con la quale ci si può collegare alla rete domestica dall'esterno, si può creare una rete ospiti nella rete domestica, impostare traffic shaping, fare logging, monitorare l'utilizzo di banda dei vari device connessi, ecc.
- ntop: comando di sistema per avere statistiche di rete
- Tunneling SSH: Una volta stabilita una connessione sicura SSH con un server remoto, si può stabilire un tunnel per accedere ad alcune risorse presenti nella rete locale del server remoto ma che non hanno indirizzo pubblico
- VPN (Virtual Private Network): it is the client-server protocol of choice to establish a secure connection over the internet
- Switch: Layer 2 device that routes MAC

addresses

- Router: Layer 3 device that routes IP addresses
- Proxy: Layer 4 server that performs access to web sites on clients behalf. A client makes a query to the Proxy he want to visit a specific URL. The Proxy establishes a brand new connection toward that URL. This will guarantee anonymization for the client. Moreover the Proxy caches the web pages, which will reduce internet traffic for repeated browsing sessions.
- WAN: é la porta di connessione alla internet pubblica
- RAID: *Redundant Array of Indipendent Disks*
- NAS: Network Attached Storage
- NAT/PAT: Network/Port Address Translation. The majority of NATs map multiple private hosts to one publicly exposed IP address. In a typical configuration, a local network uses one of the designated IP subnets. A router on that network has a private address in

that address space and a "public" WAN address assigned by an ISP. As traffic passes from the local network to the Internet, all the source private addresses in each packet are translated on the fly by the router to its public address. For different source addresses the router overwrites different source ports. The router tracks basic data about each active connection. When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase (source address and port) to determine the private address and port on the internal network to which to forward the reply. NAT/PAT are considered Level 3 protocols

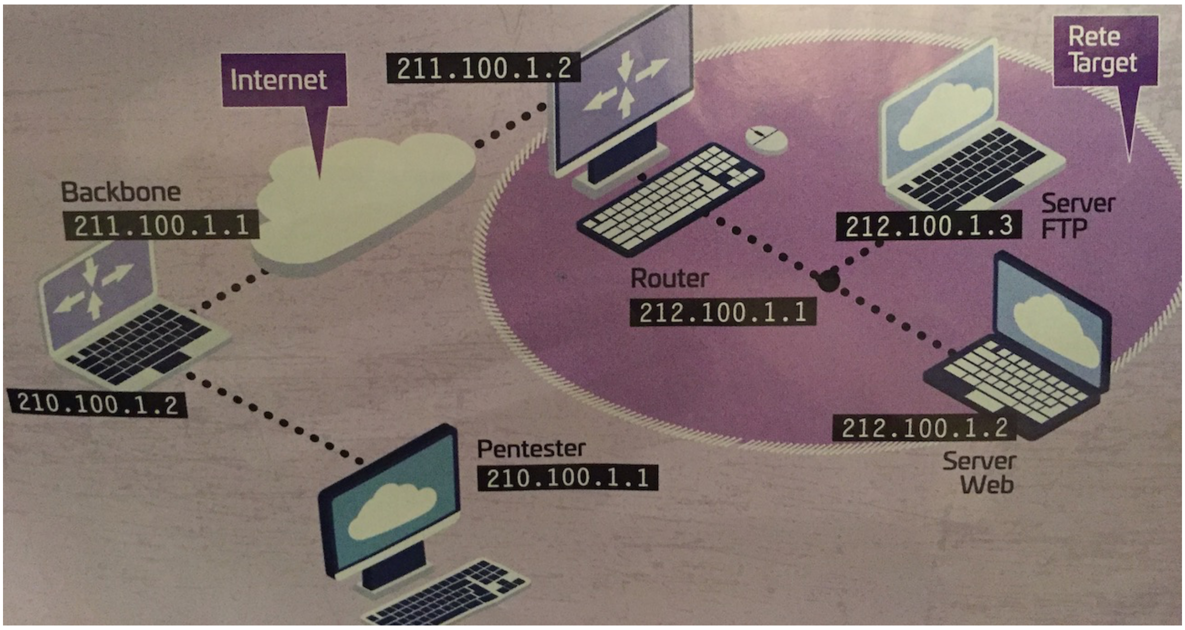
- Firewall: a wall of fire that protects a local network form incoming connections.
- If you go to the WhatIsMyIPAddress.com home page, you can see your public IP address. Now is 87.18.216.169
- Wireshark is a powerful free packet

sniffer for monitoring and analyzing network traffic

- nettop is a shell command to monitor network activity
- netsynt: a shell command to ..
- nmap is a tool to scan the network. Nmap was created in 1997 by *Gordon Lyon* (aka Fyodor)
- TTL (Time To Live): numero massimo di hops di un pacchetto ip prima che venga eliminato

How To

- To inspect incoming network connections
  $ w
- To change the port of SSH from 22 to 2233
  $ sudo vim /etc/ssh/sshd_config
  $ sudo service ssh restart
- To configure static IP and routes
  Consider two networks connected through the Internet



Pentester deve consegnare a Backbone tutti i pacchetti non destinati alla sottorete di appartenenza

```
Pentester $ ifconfig eth0 210.100.1.1 netmask 255.255.255.0 up
Pentester $ route add default gw 210.100.1.2
```

Backbone ha due interfacce di rete

```
Backbone $ ifconfig eth0 210.100.1.2 netmask 255.255.255.0 up
Backbone $ ifconfig eth1 211.100.1.1 netmask 255.255.255.0 up
```

Quello che è destinato alla sottorete 212.100.1.x deve essere inoltrato a Router

```
Backbone $ sysctl -w net.ipv4.ip
```

```
forward=1
Backbone $ route add -net
212.100.1.0/24 gw 211.100.1.2
```

Router ha due interfacce di rete

```
Router $ ifconfig eth0 212.100.1.1
netmask 255.255.255.0 up
Router $ ifconfig eth1 211.100.1.2
netmask 255.255.255.0 up
```

Quello che è destinato alla sottorete 210.100.1.x deve essere inoltrato a Backbone

```
Router $ sysctl -w net.ipv4.ip
forward=1
Router $ route add -net 210.100.1.0/24
gw 211.100.1.1
```

Server Web deve consegnare a Router tutti i pacchetti non destinati alla sottorete di appartenenza

```
ServerWeb $ ifconfig eth0 212.100.1.2
netmask 255.255.255.0 up
ServerWeb $ route add default gw
212.100.1.1
```

Server FTP deve consegnare a Router tutti i pacchetti non destinati alla sottorete di appartenenza

```
ServerFTP $ ifconfig eth0 212.100.1.3 netmask 255.255.255.0 up
ServerFTP $ route add default gw 212.100.1.1
```

hping

- To send a TCP message to a web server (port 80 http) with ip 8.8.8.8, come farebbe inizialmente qualsiasi web browser
  ```
  host $ hping3 -S -p 80 -c 1 8.8.8.8
  ```
  dove -S significa che solo il flag SYN è attivo
  Altre opzioni sono -SA (SYN +ACK) e -A (solo ACK)
  L’opzione –t 1 forza il TTL a 1, quindi dopo il primo hop il messaggio viene scartato
  L’opzione -T invia pacchetti con TTL crescenti
  L’opzione –tr–stop ferma l’invio dei pacchetti alla ricezione di una risposta
- To install hping on macOS
  ```
  host $ ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/
  ```

```
install/master/install)" < /dev/null 2> /dev/null
host $ brew install hping
```

Add /usr/local/sbin/ to PATH

```
host $ export PATH="/usr/local/sbin:$PATH"
```

nmap

A network exploration tool and port scanner

- Install nmap on mac

  ```
  host $ ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
  host $ brew install nmap
  ```

- To scan all 1000 ports on my LGTV

  ```
  $ sudo nmap -A 192.168.1.14
  ```

```
Port Scanning host: 192.168.1.14

    Open TCP Port:     1094        rootd
    Open TCP Port:     1097        sunclustermgr
    Open TCP Port:     1563        cadabra-lm
    Open TCP Port:     1636        cncp
```

```
    Open TCP Port:     1775
    Open TCP Port:     3000        hbci
    Open TCP Port:     3001        redwood-broker        nodemon
    Open TCP Port:     9955
    Open TCP Port:     9998        distinct32
    Open TCP Port:     18181       opsec-cvp
    Open TCP Port:     36866
Port Scan has completed…
```

wget

A utility for downloading files from the Internet

- To download all files and subfolders in ddd directory of a HTTP web site with index.html

  ```
  host $ wget -r -np -nH --cut-dirs=3 -R index.html http://hostname/aaa/bbb/ccc/ddd/
  ```

  -r : recursively

  -np : not going to upper directories, like ccc/…

  -nH : not saving files to hostname folder

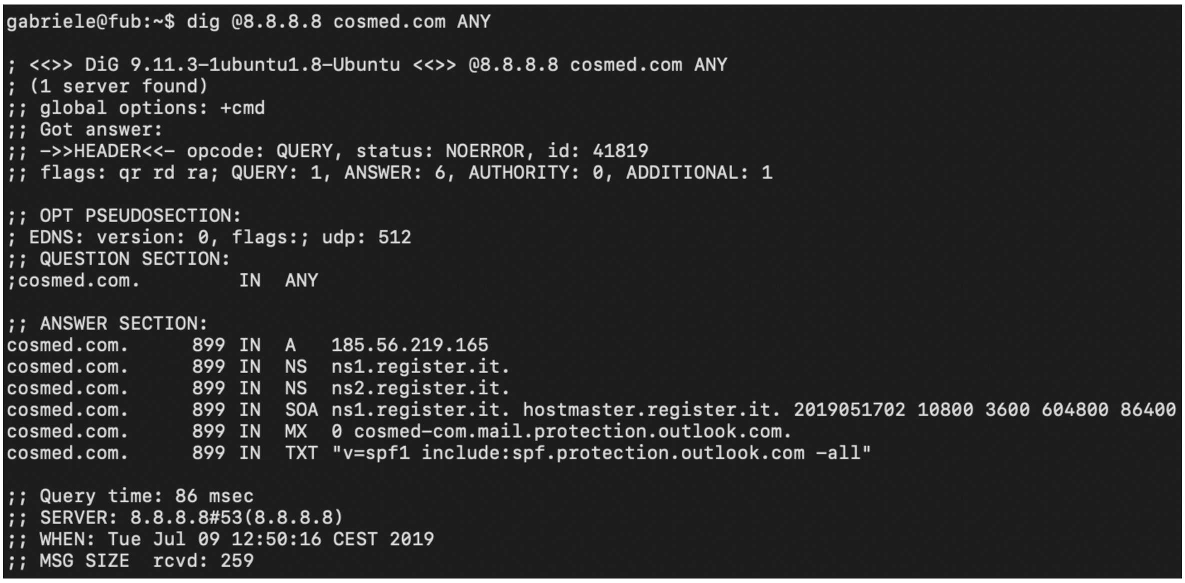
  --cut-dirs=3 : but saving it to ddd by

omitting first 3 folders aaa, bbb, ccc
-R index.html : excluding index.html files

dig

A tool for interrogating DNS servers

- To ask for a specific record
  host $ dig @<dnsserver> <recordname> <querytype> +<option>
  If no <dnsserver> is provided, it is supplied by /etc/resolv.conf
  <querytype> can be ANY, A (default), MX, SIG, TXT, SOA, MS, etc.
  <option> can be trace, norecurse, etc.
  Example:



```
gabriele@fub:~$ dig @8.8.8.8 cosmed.com ANY

; <<>> DiG 9.11.3-1ubuntu1.8-Ubuntu <<>> @8.8.8.8 cosmed.com ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41819
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cosmed.com.            IN   ANY

;; ANSWER SECTION:
cosmed.com.      899 IN  A    185.56.219.165
cosmed.com.      899 IN  NS   ns1.register.it.
cosmed.com.      899 IN  NS   ns2.register.it.
cosmed.com.      899 IN  SOA  ns1.register.it. hostmaster.register.it. 2019051702 10800 3600 604800 86400
cosmed.com.      899 IN  MX   0 cosmed-com.mail.protection.outlook.com.
cosmed.com.      899 IN  TXT  "v=spf1 include:spf.protection.outlook.com -all"

;; Query time: 86 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Jul 09 12:50:16 CEST 2019
;; MSG SIZE  rcvd: 259
```

- To ask for IP corresponding to a domain
  host $ dig @192.168.0.241 google.com

- To ask for reverse DNS lookup of a given IP
  host $ dig -x <ipaddr>