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 ..
- 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

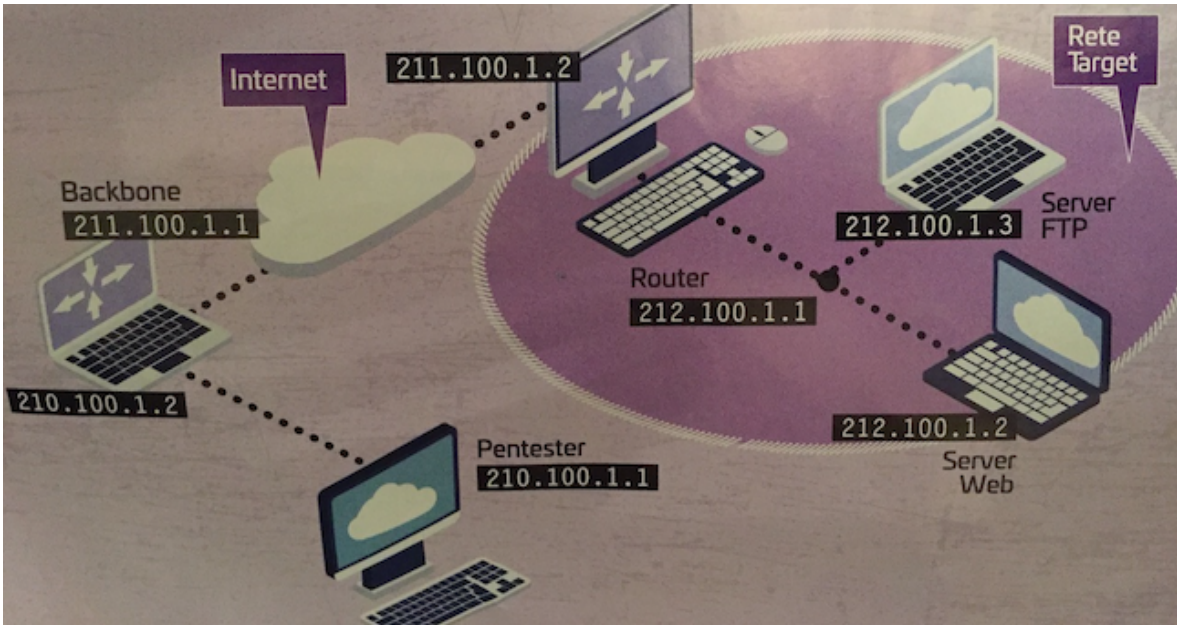
  ```
  Backbone $ sysctl -w net.ipv4.ip forward=1
  Backbone $ route add -net 212.100.1.0/24 gw 211.100.1.2
  ```
  Router ha due interfacce di rete

  ```
  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
  ```

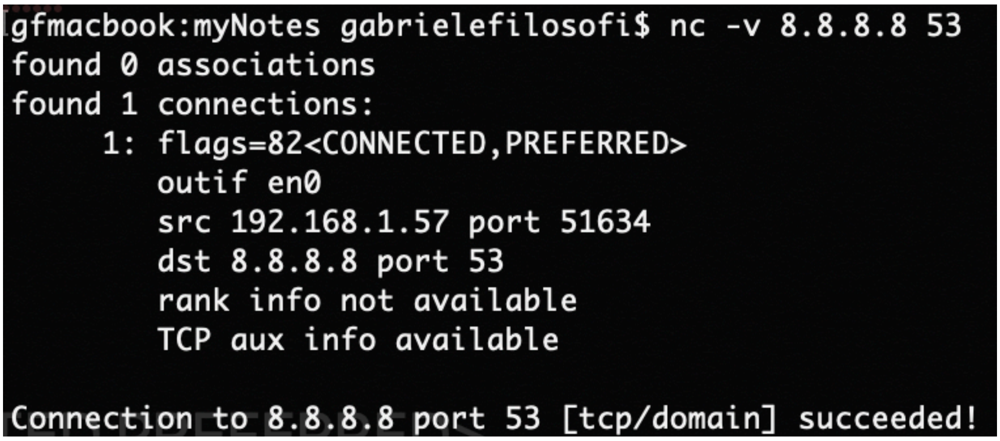
ServerWeb $ route add default gw 212.100.1.1
Server FTP deve consegnare a Router tutti i pacchetti non destinati alla sottorete di appartenenza
ServerFTP $ ifconfig eth0 212.100.1.3 netmask 255.255.255.0 up
ServerFTP $ route add default gw 212.100.1.1



nc

A command to open TCP/UDP connections and listen. It works with IPv4/6

- Example: using nmap over 8.8.8.8 you find out there two open ports
  53/tcp open tcpwrapped
  443/tcp open ssl/https sffe
  Then try to connect to the port
  host $ nc -v 8.8.8.8 53



```
gfmacbook:myNotes gabrielefilosofi$ nc -v 8.8.8.8 53
found 0 associations
found 1 connections:
     1: flags=82<CONNECTED,PREFERRED>
        outif en0
        src 192.168.1.57 port 51634
        dst 8.8.8.8 port 53
        rank info not available
        TCP aux info available

Connection to 8.8.8.8 port 53 [tcp/domain] succeeded!
```

-v : shows not only the open ports, but also the ports that were checked and found to not be open

- With -e option you can make any process a network server
  Example: on host computer with IP add <hostip>
  host $ nc -l -p 1234 -e /bin/sh
  Then on client computer
  client $ nc <hostip> 1234

hping2/3

A command to send custom TCP packets and display replies

- To send a TCP message to a web server (port 80 http) with IP <ip>
  host $ hping3 -S -p 80 -c 1 <ip>
  -S significa che solo il flag SYN è attivo
  -SA (SYN +ACK) e -A (solo ACK)
  -t 1 forza il TTL a 1, quindi dopo il primo hop il messaggio viene scartato
  -T invia pacchetti con TTL crescenti
  -tr-stop ferma l'invio dei pacchetti alla ricezione di una risposta
- To install on macOS
  host $ brew install hping
  Add /usr/local/sbin/ to PATH
  host $ export PATH="/usr/local/sbin:$PATH"

nmap

A network scanning tool and created in 1997 by *Gordon Lyon* (aka Fyodor)

- To install on macOS
  host $ brew install nmap
- Examples
  $ sudo nmap -sS -Pn -sV <ip>
  -sV option displays the protocol versions
  -Pn bypasses ping blocking
- To display also SSL/TLS certificates and RSA public keys
  $ sudo nmap -n -vv -A <ip> --min-parallelism=50 --max-parallelism=150 -PN -T2 -oA <ip>
- To scan ports from 1 to 1000
  $ sudo nmap -A <ip>
- To scan protocol versions active on UDP ports from 1 to 65535 of any target IP 192.168.0.1 to 192.168.0.3
  $ nmap -n -sU -sV 192.168.0.1-3 -p 1-65535
- To search for directory structures and files on a http server
  $ nmap -sV -p 80 <serverip> --script=http-enum

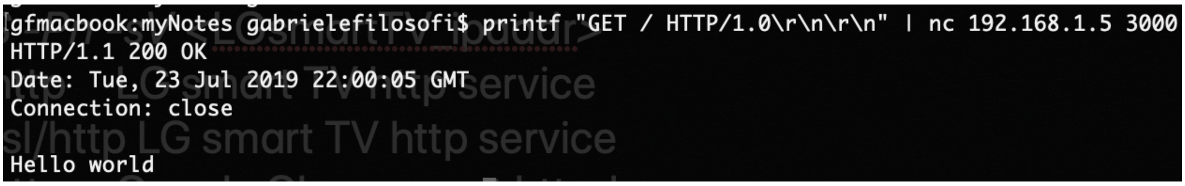
hacking SmartTV

Let's make some practice with the Smart TV
Name: LGwebOSTV
Model: LG 55UH850V
OS: webOS 3.0
https://www.displayspecifications.com/en/model/a38c46c

host $ sudo nmap -sS -Pn -sV <LGsmartTV_ipaddr>

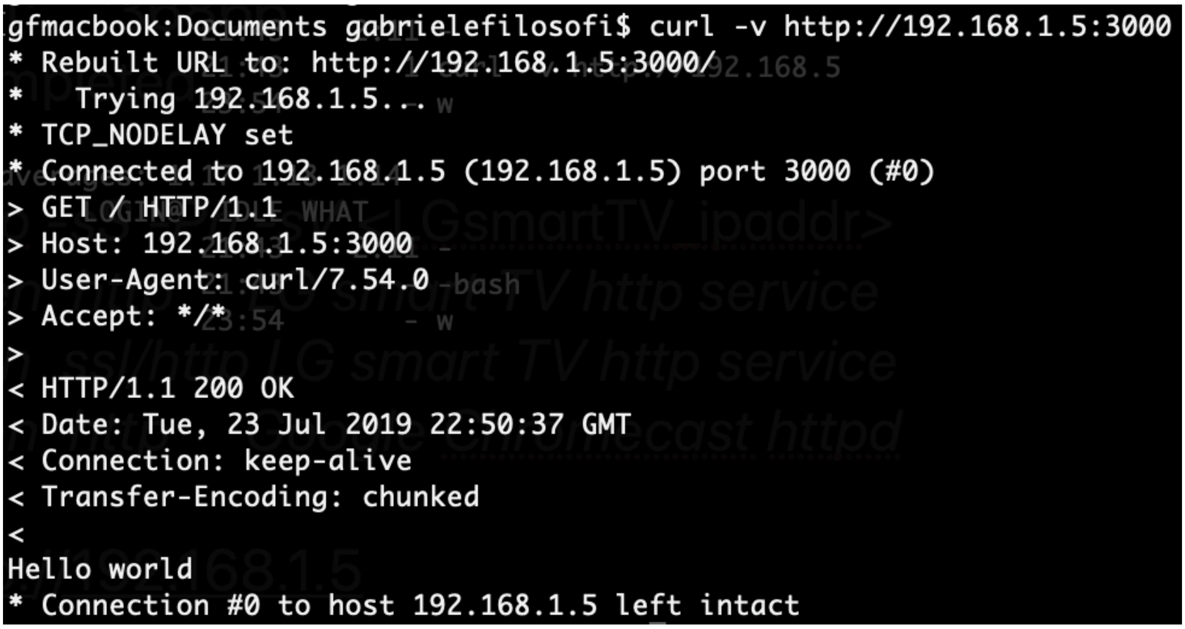
```
      3000/tcp open  http     LG smart TV http service
      3001/tcp open  ssl/http LG smart TV http service
      9998/tcp open  http     Google Chromecast httpd
```

We want to interact with HTTP server
host $ printf "GET / HTTP/1.0|r|n|r|n" | nc -n -i 1 192.168.1.5 3000



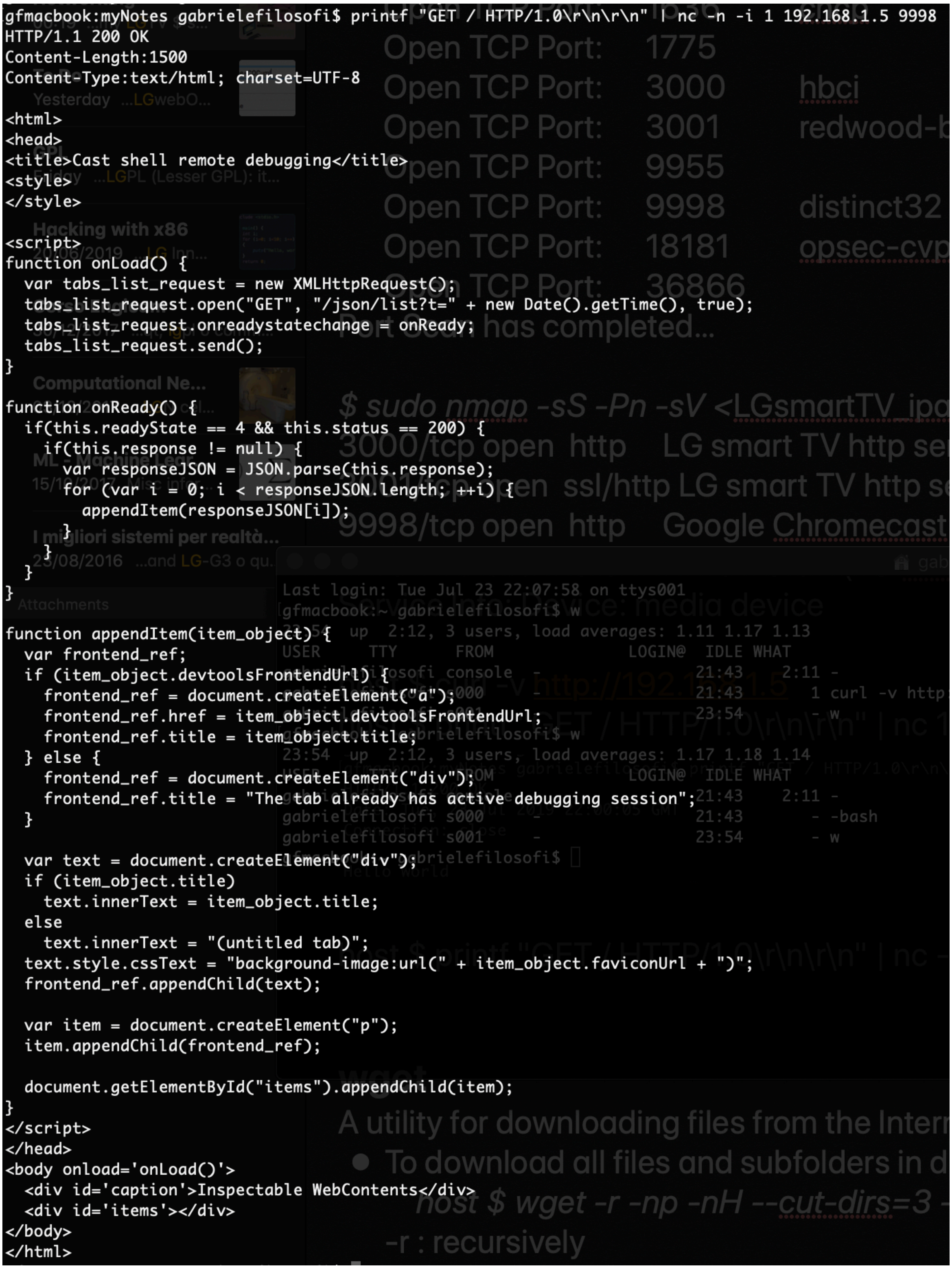
```
gfmacbook:myNotes gabrielefilosofi$ printf "GET / HTTP/1.0\r\n\r\n" | nc 192.168.1.5 3000
HTTP/1.1 200 OK
Date: Tue, 23 Jul 2019 22:00:05 GMT
Connection: close

Hello world
```

host $ curl -v http://192.168.1.5:3000
where -v is the verbose option



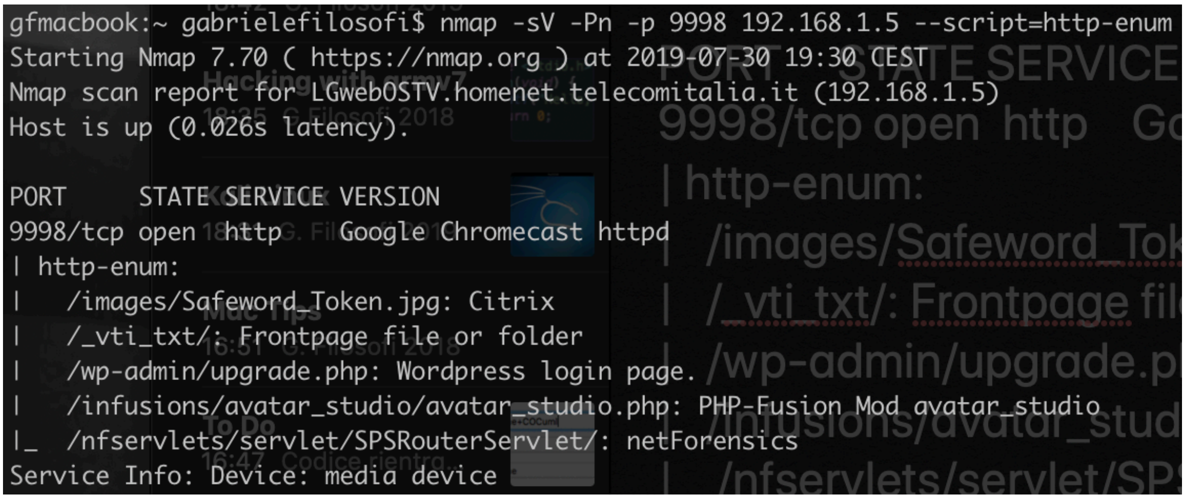
```
gfmacbook:Documents gabrielefilosofi$ curl -v http://192.168.1.5:3000
* Rebuilt URL to: http://192.168.1.5:3000/
*   Trying 192.168.1.5...
* TCP_NODELAY set
* Connected to 192.168.1.5 (192.168.1.5) port 3000 (#0)
> GET / HTTP/1.1
> Host: 192.168.1.5:3000
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 23 Jul 2019 22:50:37 GMT
< Connection: keep-alive
< Transfer-Encoding: chunked
<
Hello world
* Connection #0 to host 192.168.1.5 left intact
```

host $ printf "GET / HTTP/1.0\r\n\r\n" | nc -n -i 1 192.168.1.5 9998



```
gfmacbook:myNotes gabrielefilosofi$ printf "GET / HTTP/1.0\r\n\r\n" | nc -n -i 1 192.168.1.5 9998
HTTP/1.1 200 OK
Content-Length:1500
Content-Type:text/html; charset=UTF-8

<html>
<head>
<title>Cast shell remote debugging</title>
<style>
</style>

<script>
function onLoad() {
  var tabs_list_request = new XMLHttpRequest();
  tabs_list_request.open("GET", "/json/list?t=" + new Date().getTime(), true);
  tabs_list_request.onreadystatechange = onReady;
  tabs_list_request.send();
}

function onReady() {
  if(this.readyState == 4 && this.status == 200) {
    if(this.response != null) {
      var responseJSON = JSON.parse(this.response);
      for (var i = 0; i < responseJSON.length; ++i) {
        appendItem(responseJSON[i]);
      }
    }
  }
}

function appendItem(item_object) {
  var frontend_ref;
  if (item_object.devtoolsFrontendUrl) {
    frontend_ref = document.createElement("a");
    frontend_ref.href = item_object.devtoolsFrontendUrl;
    frontend_ref.title = item_object.title;
  } else {
    frontend_ref = document.createElement("div");
    frontend_ref.title = "The tab already has active debugging session";
  }

  var text = document.createElement("div");
  if (item_object.title)
    text.innerText = item_object.title;
  else
    text.innerText = "(untitled tab)";
  text.style.cssText = "background-image:url(" + item_object.faviconUrl + ")";
  frontend_ref.appendChild(text);

  var item = document.createElement("p");
  item.appendChild(frontend_ref);

  document.getElementById("items").appendChild(item);
}
</script>
</head>
<body onload='onLoad()'>
  <div id='caption'>Inspectable WebContents</div>
  <div id='items'></div>
</body>
</html>
```

host $ nmap -sV -p 9998 192.168.1.5 --script=http-enum



```
gfmacbook:~ gabrielefilosofi$ nmap -sV -Pn -p 9998 192.168.1.5 --script=http-enum
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-30 19:30 CEST
Nmap scan report for LGwebOSTV.homenet.telecomitalia.it (192.168.1.5)
Host is up (0.026s latency).

PORT     STATE SERVICE VERSION
9998/tcp open  http    Google Chromecast httpd
| http-enum:
|   /images/Safeword_Token.jpg: Citrix
|   /_vti_txt/: Frontpage file or folder
|   /wp-admin/upgrade.php: Wordpress login page.
|   /infusions/avatar_studio/avatar_studio.php: PHP-Fusion Mod avatar_studio
|_  /nfservlets/servlet/SPSRouterServlet/: netForensics
Service Info: Device: media device
```

PORT   STATE SERVICE VERSION
9998/tcp open http   Google Chromecast httpd
| http-enum:
| /images/Safeword_Token.jpg: Citrix
| /_vti_txt/: Frontpage file or folder
| /wp-admin/upgrade.php: Wordpress login page.
| /infusions/avatar_studio/avatar_studio.php: PHP-Fusion Mod avatar_studio
|_ /nfservlets/servlet/SPSRouterServlet/: netForensics
Service Info: Device: media device

hacking router

host $ sudo nmap -sS -Pn -sV 192.168.1.1
53/tcp   open domain   (generic dns response: NOTIMP)
80/tcp   open http   Mbedthis-Appweb (Thomson Technicolor broadband router http admin)
443/tcp open ssl/http   Mbedthis-Appweb (Thomson Technicolor broadband router http admin)
5001/tcp open commplex-link?

wget

A utility for downloading files from the Internet

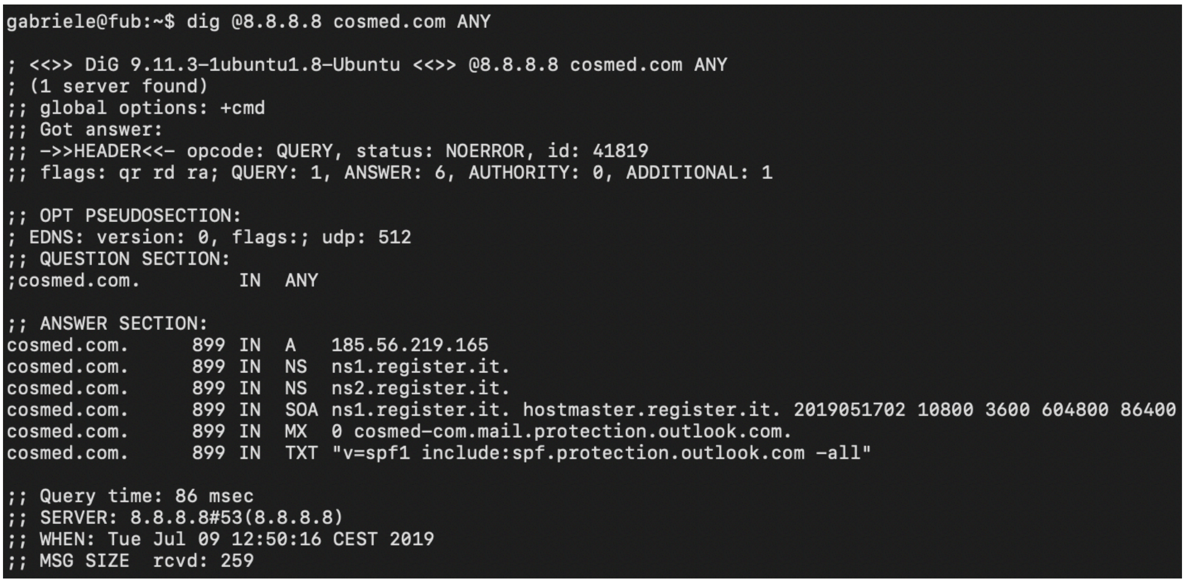
- To download all files and subfolders in ddd directory of a HTTP web site with index.html
  host $ wget -r -np -nH --cut-dirs=3 -R index.html http://hostname/aaa/bbb/ccc/ddd/
  -r : recursively
  -np : not going to upper directories, like ccc/…
  -nH : not saving files to hostname folder
  --cut-dirs=3 : 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>