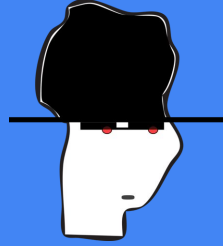
More websec

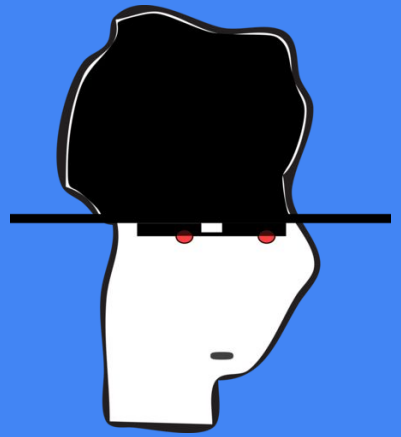


Less Known Web Application Vulnerabilities

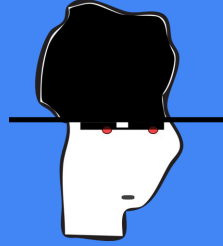
- PHP Object Injection
- Java deserialization
- Expression Language Injection
- NoSQL Injection
- XML External Entities
- XPATH Injection
- LDAP Injection
- Web Cache Deception Attack
- Host Header Injection
- HTTP Header Injection
- HTTP Parameter Pollution
- DNS Rebinding
- Server Side Template Injection
- CSS Injection
- CSS History Hijacking
- Path-Relative Stylesheet Import
- Reflective File Download
- JSONP Injection
- Session fixation
- Session puzzling
- Password Reset MitM Attack
- ECB/CBC Crypto tokens
- Padding oracle attack
- Server Side Request Forgery
- SMTP Command Injection
- On Site Request Forgery
- Cross Site Script Inclusion (XSSI)
- XSSJacking

Pentesting (intro)

Seguridad Ofensiva



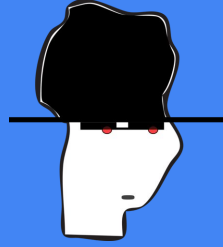
Introducción a las pruebas de intrusión



Definición
Llamaremos Pentest / Test de intrusión al proceso llevado a cabo dentro de la vida de un sistema, en el cual se procede a planificar, analizar y verificar distintas características involucradas con la seguridad del mismo.

Objetivos
Todo esto con el objetivo de analizar el nivel de seguridad y la exposición de los sistemas ante posibles ataques. (Encontrar y corregir vulnerabilidades)

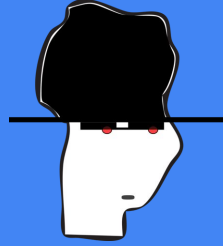
Propiedades de interés:
Integridad, confidencialidad, disponibilidad, control, etc.



Pentest vs Vuln Scan

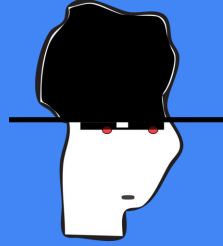
	Vulnerability Scan	Penetration Test
Purpose	Identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.	Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components.
When	At least quarterly or after significant changes.	At least annually and upon significant changes. (Refer to Section 2.6 of this document for information on significant changes.)
How	Typically a variety of automated tools combined with manual verification of identified issues.	A manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.

Tipos

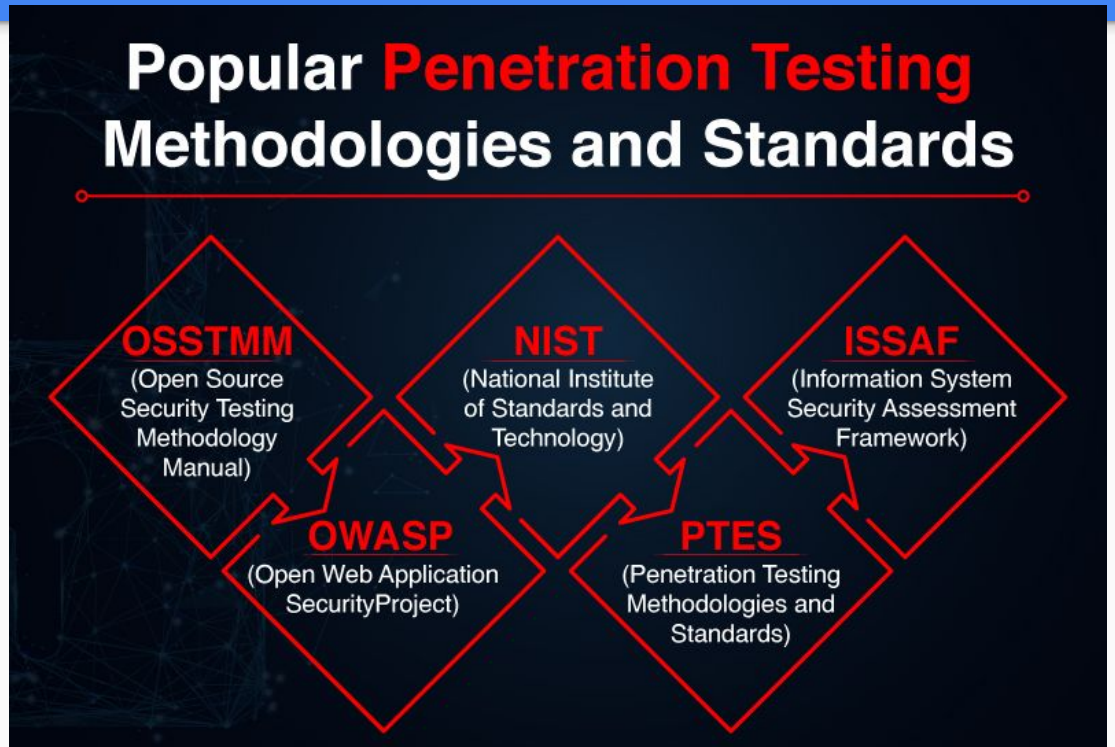


- Network services test
- Client-side test
- Web Application test
- Remote dial-up war dial test
- Wireless security test
- Social engineering test
- Physical security test
- Crypto-Test
- ...

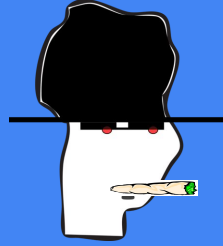
Tests de Intrusión



Metodologías



Fases (I , II)



- Planning
- Scanning
- Exploitation
- Wireless Attack
- Web App Attack
- Password Attack
- …
- Analysis & Report

Conducting a Penetration Test on an Organization
conducting-penetration-test-organization-67.pdf

Abstract

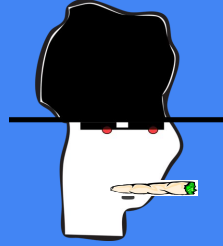
What is a Penetration Test?

The Process and Methodology
- Planning and Preparation
- Information Gathering and Analysis
- Vulnerability Detection
- Penetration Attempt
- Analysis and Reporting
- Cleaning Up

Fases (III, IV)

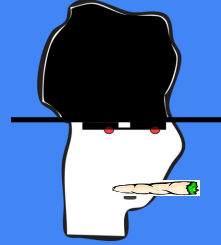
- Reconnaissance
- Scanning and Enumeration
- Gaining Access
- Escalation of Privileges
- Maintaining Access
- Covering Your Tracks

Antes de empezar



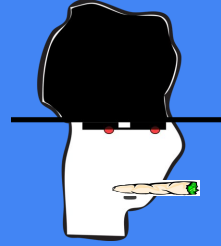
- Rango de tiempo – disponibilidad horaria
- Entornos – (tst, stg, prod, IP, servidores, dominios)
- Tipo de aplicación
- Tipo de pentest
- Visibilidad del pentest (caja negra, caja blanca)
- Posicionamiento (interno, externo)
- Perfiles - Acceso
- Preparación por parte del cliente
- Etapas – actividades
- Funcionalidades (scope)
- Limitaciones técnicas – de negocio
- Documentación a entregar

Reconocimiento / Reconnaissance



Esta fase es el enfoque sistemático en el que se intenta localizar y recopilar información sobre el objetivo.

Reconocimiento / Reconnaissance



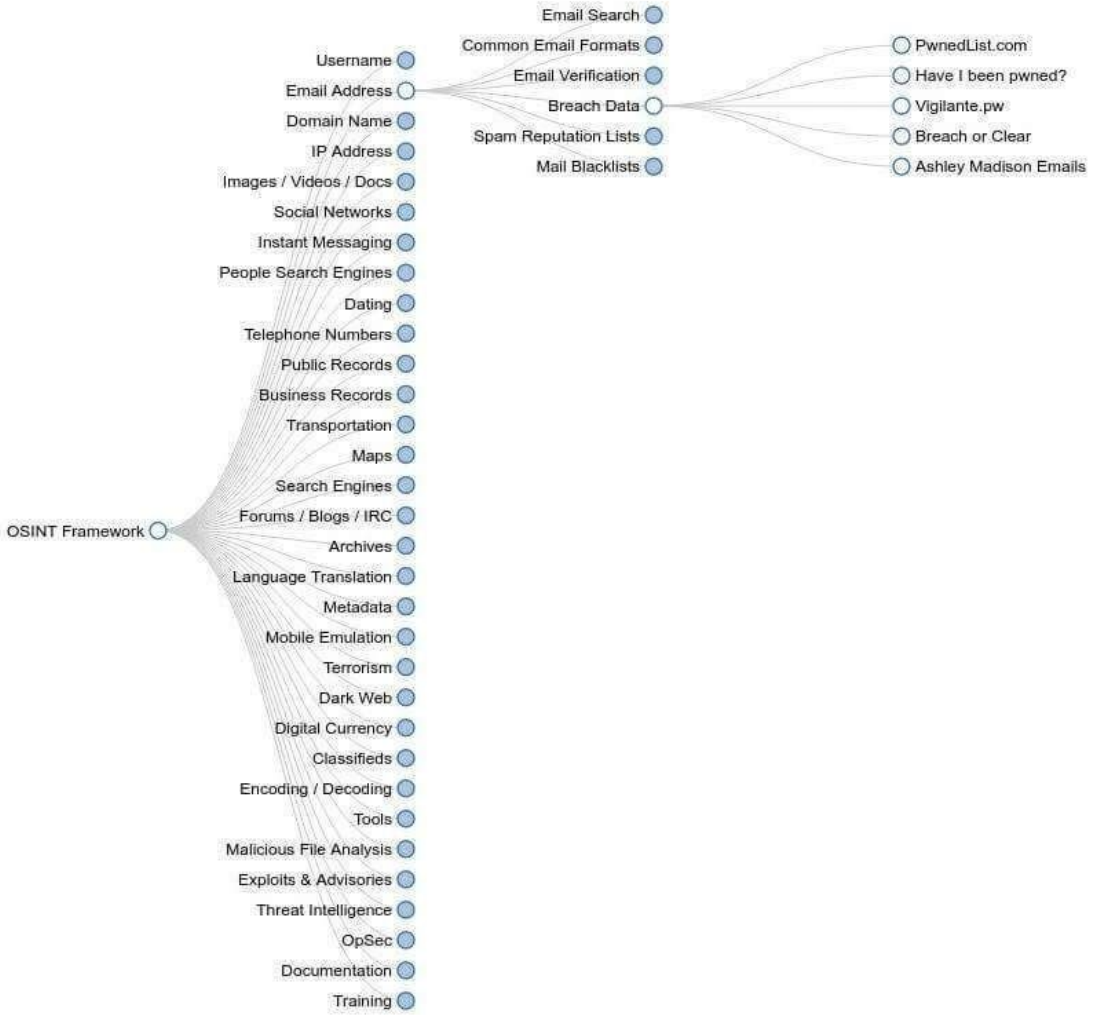
Que buscar?

- nombres
- mails
- telefonos
- direcciones ip de servidores (www, mail, ..)
- codigo (fuente y no)

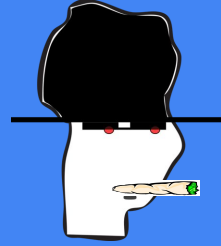
Reconocimiento

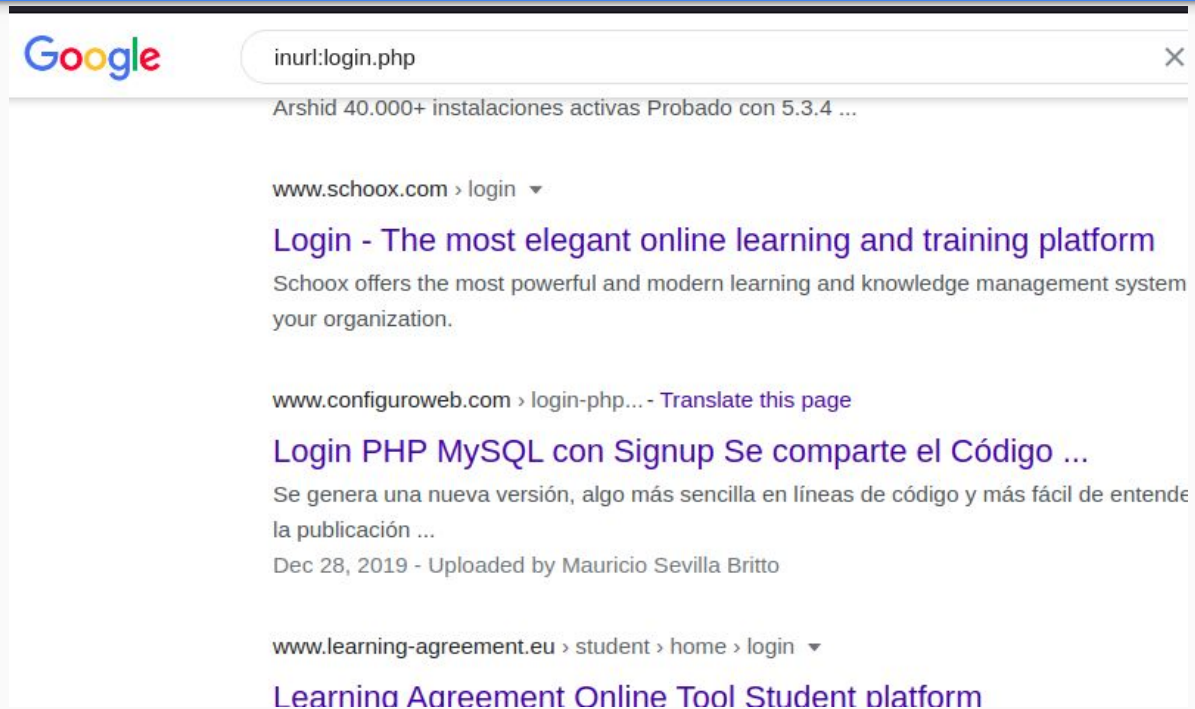
Cómo buscar?

- OSINT
- Google
- HavelbeenPwned
- Recon-Ng
- Maltego
- Shodan
- Jigsaw
- SpiderFoot ...

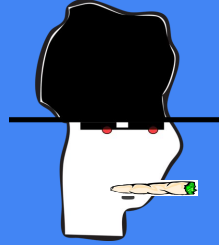


Reconocimiento / Reconnaissance



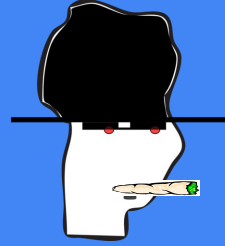


Scanning / Enumeration



Es la primer fase práctica activa en el proceso de pentesting.

Consiste en obtener toda la información relevante posible según la infraestructura que estemos analizando.

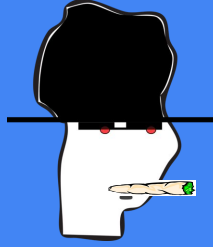


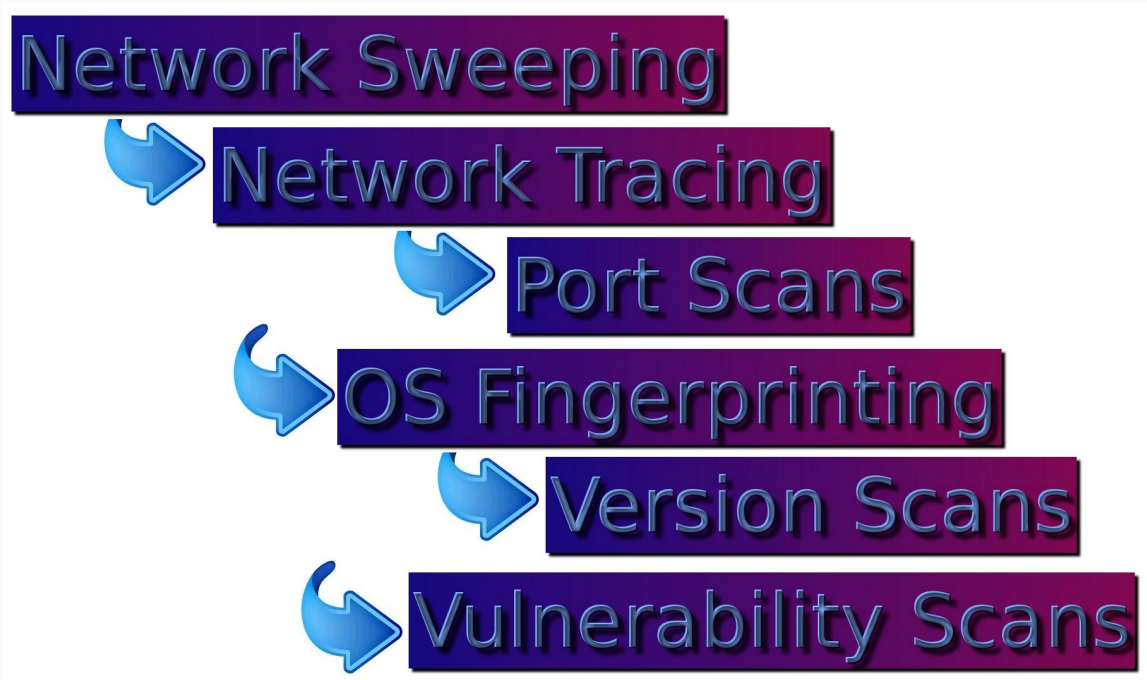
Scanning / Enumeration

***Pasivo**:
Analizar paquetes de un host en la red sin inyectar ninguna clase de tráfico.

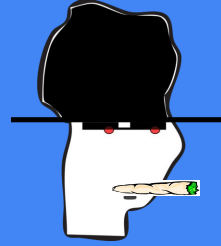
***Activo**:
Transmitir paquetes a uno o más host y analizar las correspondientes respuestas.

Workflow del scanning





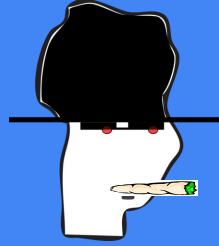
Objetivos del scanning



Conocer más de nuestro/s objetivos buscar entradas a través de interacción con el entorno

- Determinar hosts "vivos", firewalls, routers
- Topología de la red
- Puertos y servicios abiertos
- SO's (tipos) / Infra
- Listar posibles vulnerabilidades

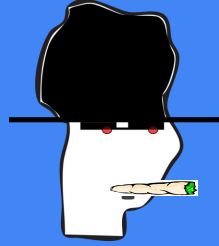
Network Sweeping - Como?



`Ping` || `Nmap` . Obvio!

```
:-\$ ping -c1 8.8.8.8\newline
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.\newline
64 bytes from 8.8.8.8: icmp\_req=1 ttl=57 time=10.8 ms

--- 8.8.8.8 ping statistics ---\newline
1 packets transmitted, 1 received, 0\% packet loss, time 0ms
rtt min/avg/max/mdev = 10.887/10.887/10.887/0.000 ms
```

Network Sweeping - Como?



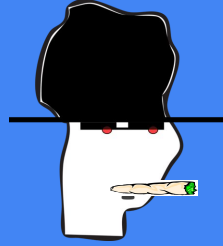
Pero también están:

- Hping
- Hping3

```
:-\$ sudo hping3 8.8.8.8 --syn -p 80 --count 1
HPING 8.8.8.8 (eth0 8.8.8.8): S set, 40 headers + 0 data bytes
len=46 ip=8.8.8.8 ttl=63 DF id=0 sport=80 flags=SA seq=0
win=14600 rtt=1.0 ms
--- 8.8.8.8 hping statistic ---
1 packets transmitted, 1 packets received, 0\% packet loss
round-trip min/avg/max = 1.0/1.0/1.0 ms
```

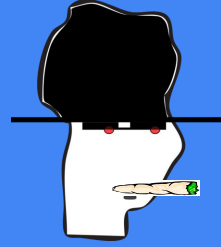
- Custom Scripts

Network Tracing - Como?

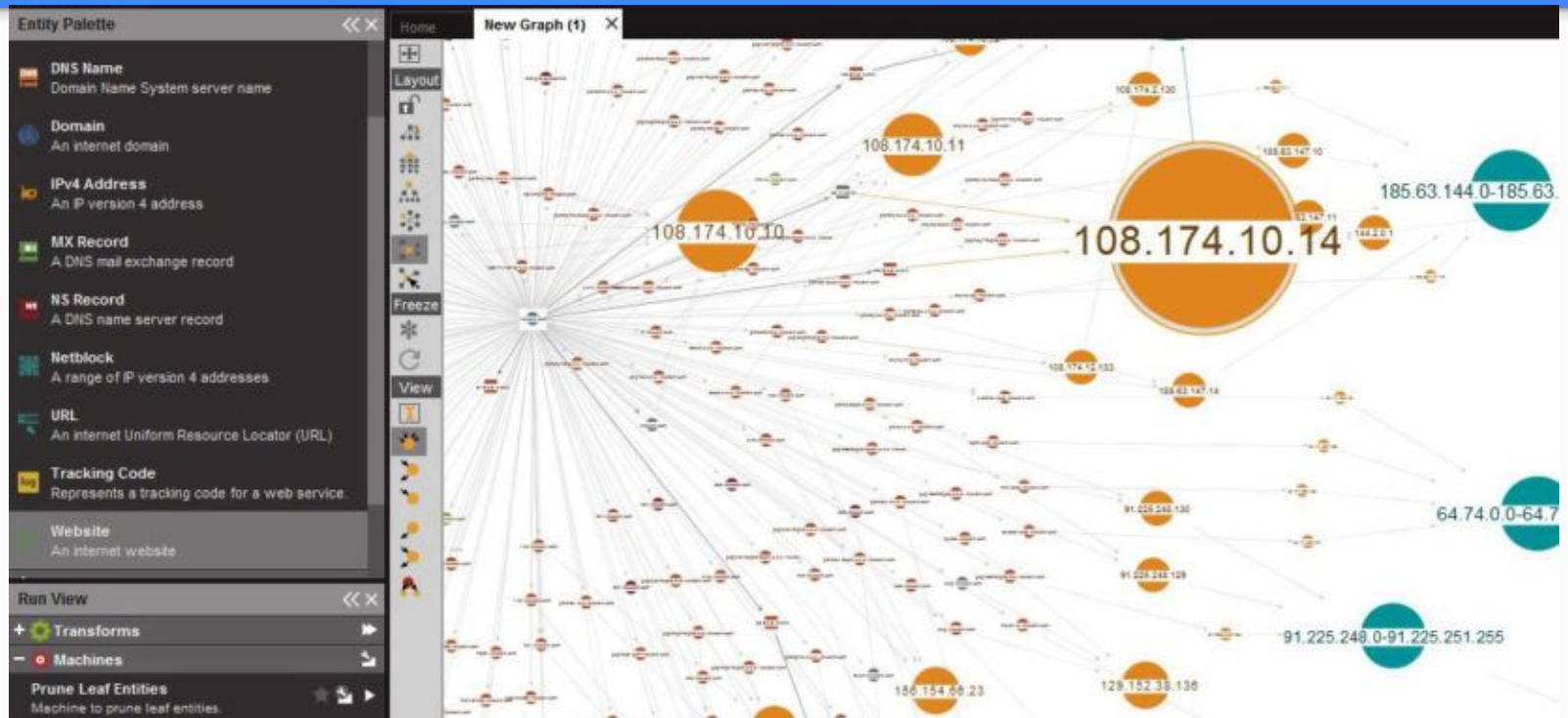


```
tracer*t* ||  mtr || nmap

:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (192.168.64.247)  0.380 ms  0.607 ms  0.588 ms
 2  * * *
 3  * * *
 4  209-165-89-200.fibertel.com.ar (200.89.165.209)  46.069 ms  ...
 5  222-165-89-200.fibertel.com.ar (200.89.165.222)  49.987 ms  ...
 6  200.49.159.254 (200.49.159.254)  26.731 ms  26.724 ms  26.702 ms
 7  74.125.242.209 (74.125.242.209)  28.132 ms ...
 8  74.125.37.15 (74.125.37.15)  21.223 ms ...
 9  google-public-dns-a.google.com (8.8.8.8)  27.228 ms  ...
```

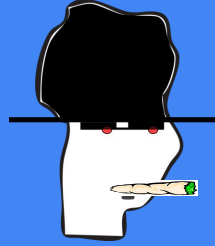
Network Tracing - Como?

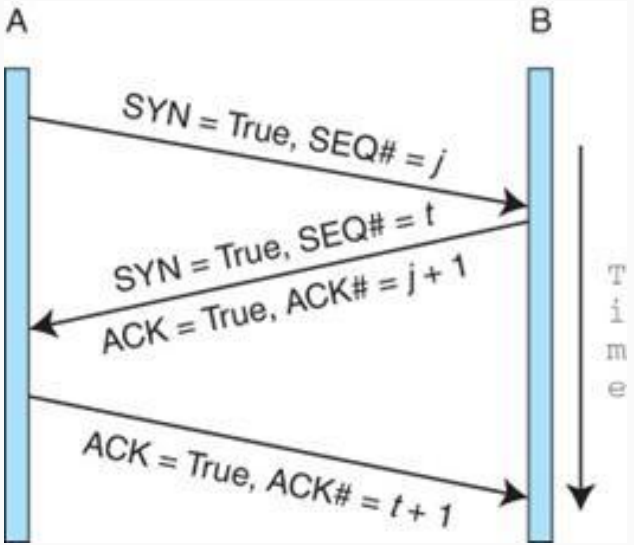


Network Tracing - Como?

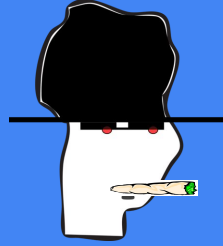


Port Scanning - Como?



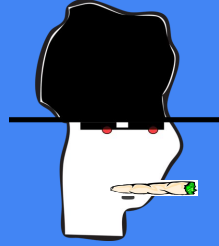


Port Scanning - Como?



```
nmap …

:~$ nmap -p53 8.8.8.8
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-06 19:13 -03
Nmap scan report for google-public-dns-a.google.com (8.8.8.8)
Host is up (0.022s latency).

PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

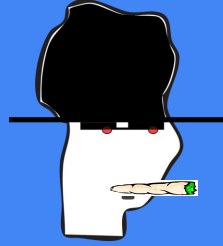
OS Fingerprinting - Como?



nmap …

```
MAC Address: 00:0C:29:3A:07:03 (VMware)
Device type: general purpose|WAP|specialized|firewall
Running (JUST GUESSING): FreeBSD 6.X|7.X|8.X (92\%), OpenBSD 4.X
(91\%),...
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:openbsd:openbsd:4.0 ...
Aggressive OS guesses: FreeBSD 6.2-RELEASE (92\%), FreeBSD
6.3-RELEASE (92\%)...
No exact OS matches for host (test conditions non-ideal).\newline
Network Distance: 1 hop
OS detection performed.
Please report any incorrect results at ...
```

http://phrack.org/issues/54/9.html#article (1998)



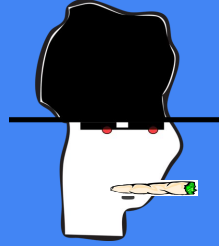
OS Fingerprinting - Como?

Pero también está

Xprobe2 (2001 - BlackHat , Ofir Arkin, Fyodor Yarochkin)

“La máxima cantidad de paquetes necesaria para identificar exitosamente un sistema operativo es 4 enviados y 4 recibidos.”

OS Fingerprinting - Como?

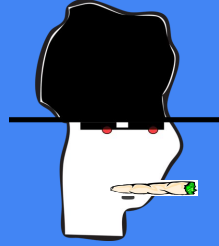


Nmap compara fingerprints:

- Sequence generation (SEQ, OPS, WIN, and T1)
- ICMP echo (IE)
- TCP explicit congestion notification (ECN)
- UDP (U1)
- TCP (T2–T7)
- TCP ISN greatest common divisor (GCD)
- TCP ISN counter rate (ISR)
- TCP ISN sequence predictability index (SP)
- IP ID sequence generation algorithm (TI, CI, II)

https://nmap.org/book/osdetect-methods.html

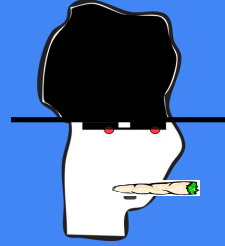
OS Fingerprinting - Como?



Nmap compara fingerprints:

- TCP timestamp option algorithm (TS)
- TCP options (O, O1–O6)
- TCP initial window size (W, W1–W6)
- Responsiveness (R)
- Don't fragment (ICMP) (DFI)
- IP initial time-to-live (T)
- IP initial time-to-live guess (TG)
- ...

https://nmap.org/book/osdetect-methods.html



Version Scans - Como?

Dependiendo el servicio/protocolo/puerto que se haya "encontrado" uno podría intentar conexiones, requests menos obvios y obtener información interesante o al menos relevante sobre el servicio en cuestión.

Por ej:

:-$ telnet www.famaf.unc.edu.ar 80 y luego GET / HTTP/1.9

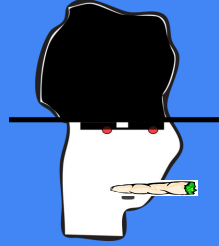
o

:-$ telnet webmail.sanatorionosti.com.ar 22

```
joe@zoidberg:~$ telnet webmail.sanatorionosti.com.ar 22
Trying 162.243.173.15 ...
Connected to mail.sanatorionosti.com.ar.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10
```

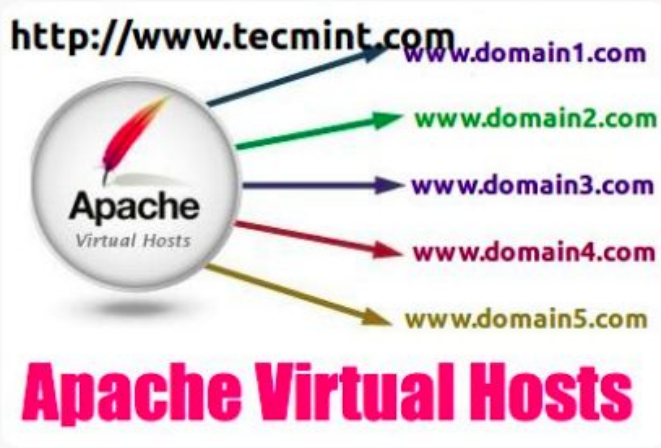
```
joe@zoidberg:~$ telnet www.famaf.unc.edu.ar 80
Trying 200.16.17.123 ...
Connected to ratri.famaf.unc.edu.ar.
Escape character is '^]'.
GET / HTTP/1.9

HTTP/1.1 400 Bad Request
Server: nginx/1.10.3
Date: Mon, 28 Sep 2020 15:11:14 GMT
Content-Type: text/html
Content-Length: 173
Connection: close
```

Version Scans - OJO



tecmint.com/apache-ip-based-and-name-based-virtual-hosting/

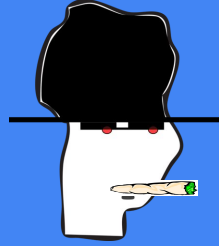
Linux Foundation LFCS and LFCE Certification Pr



Apache Virtual Hosting in Linux

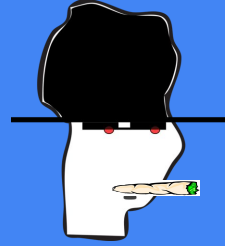
```
<VirtualHost 192.168.0.100:80>
    ServerAdmin webmaster@example1.com
    DocumentRoot /var/www/html/example1.com
    ServerName www.example1.com
ErrorLog logs/www.example1.com-error_log
CustomLog logs/www.example1.com-access_log common
</VirtualHost>

<VirtualHost *:80>
    ServerAdmin webmaster@example2.com
    DocumentRoot /var/www/html/example2.com
    ServerName www.example2.com
ErrorLog logs/www.example2.com-error_log
CustomLog logs/www.example2.com-access_log common
</VirtualHost>
```

Vuln Scans - Como?



- Google / duckduckgo
- Mitre DB
- NIST NVD
- Exploit-db / 0day.today
- Security focus
- Nikto
- Nessus / OpenVAS / Acunetix
- Pompem
- NSE/Nmap
- w3af
- wpscan
- Manual Scripts
- Deep Web
- ....

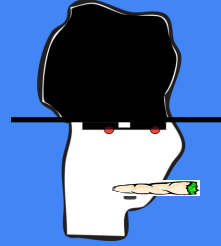
- Importante *-*



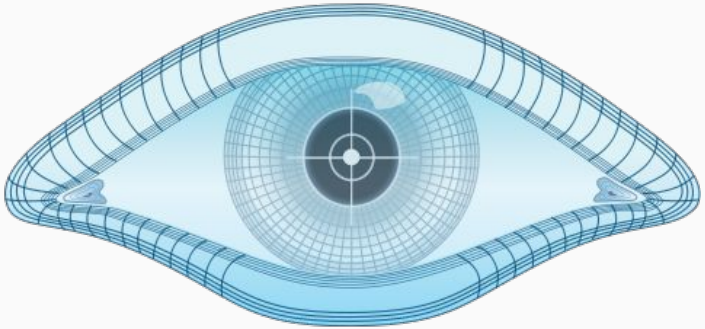
Es importante “al menos” tener una idea general de cuales son a grandes rasgos las clases de vulnerabilidades que nos vamos a encontrar y cómo generar el mejor "pipeline" para aprovechar esa debilidad.

- Inyecciones, XSS, CSFR, Overflow, Path Traversal, DoS, XXE, etc.
- RWX?

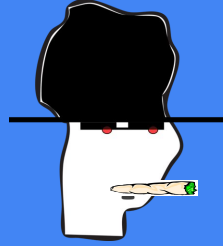
NMAP (Network Mapper)



La tool que ya conocíamos.
www.nmap.org



NMAP

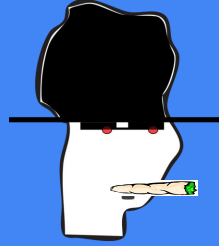


Es una herramienta de software libre(GPL) para realizar escaneos de seguridad en una red.
Nació en 1997, como un proyecto personal desarrollado por Gordon Lyon, a.k.a Fyodor.

Originalmente corría en linux, y todo el soft eran 3 archivos
(nmap.c, nmap.h & Makefile, Phrack #51).

```
Makefile:
     nmap: nmap.c nmap.h
     gcc -Wall -O6 -o nmap nmap.c -lm
```

NMAP



#basico
```
nmap IP
```

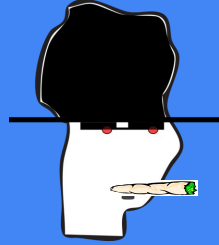
#TCP SYN scan
```
nmap -sS IP
```

#custom flags
```
nmap --scanflags ACKURGRST IP
```

#skip portscan
```
nmap SEGMENT -sP
```

#source port setting
```
nmap --source-port PORT IP
```

NMAP



#skip portscan
```
nmap SEGMENT -sP
```

#IPs from file
```
nmap -iL IPS.txt
```

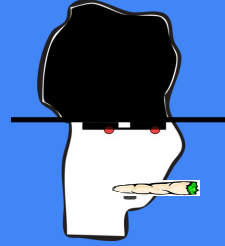
#mac spoofing
```
nmap IP -spoof-mac MAC
```

#version & OS detect
```
nmap IP -sV
nmap -O IP
```

https://nmap.org/docs/nmap-mindmap.pdf

Lo que estábamos esperando

Caso practico (Google)



Google Vulnerability Reward Program (VRP) Rules

We have long enjoyed a close relationship with the security research community. To honor all the cutting-edge external contributions that help maintain a Vulnerability Reward Program for Google-owned web properties, running continuously since November 2010.

Services in scope

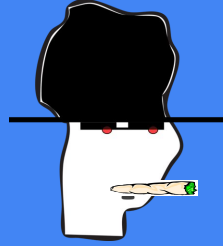
In principle, any Google-owned web service that handles reasonably sensitive user data is intended to be in scope. This includes virtually all domains:

- *.google.com
- *.youtube.com
- *.blogger.com

Bugs in Google Cloud Platform, Google-developed apps and extensions (published in Google Play, in iTunes, or in the Chrome Web Store), hardware devices (Home, OnHub and Nest) will also qualify. See our Android Rewards and Chrome Rewards for other services and devices

+Recon

https://pentest-tools.com/alltools#information-gathering



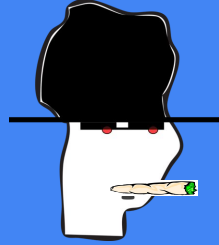
```
[1] Recon modules
[1] Discovery modules

[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > options set SOURCE google.com
SOURCE => google.com
[recon-ng][default][hackertarget] >
```

```
[recon-ng][default][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' t
th the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  google.com     yes       source of input (see 'info' for detail

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT
  <string>       string representing a single input
```

```
[recon-ng][default][hackertarget] > run

GOOGLE.COM

[*] Country: None
[*] Host: google.com
[*] Ip_Address: 172.217.13.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------------
[*] Country: None
[*] Host: google-proxy-74-125-210-0.google.com
[*] Ip_Address: 74.125.210.0
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------------
[*] Country: None
```

+Recon

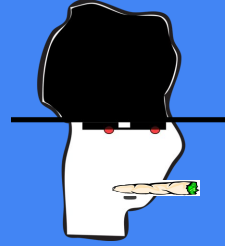
https://pentest-tools.com/alltools#information-gathering



```
[recon-ng][default] > marketplace search
```

Path	Version	Status	Updated	D	K
dev/spyse_subdomains	1.0	not installed	2020-07-07		*
discovery/info_disclosure/cache_snoop	1.0	not installed	2019-06-24		
discovery/info_disclosure/interesting_files	1.1	outdated	2020-01-13		
exploitation/injection/command_injector	1.0	not installed	2019-06-24		
exploitation/injection/xpath_bruter	1.2	not installed	2019-10-08		
import/csv_file	1.1	not installed	2019-08-09		
import/list	1.1	not installed	2019-06-24		
import/masscan	1.0	not installed	2020-04-07		

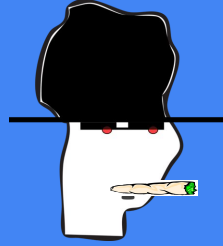
dnsenum google.com



```
Brute forcing with /usr/share/dnsenum/dns.txt:
_____________________________________________

about.google.com.                       86400   IN    CNAME     www3.l.google.c
om.
www3.l.google.com.                      262     IN    A         172.217.162.14
accounts.google.com.                    173     IN    A         172.217.172.109
admin.google.com.                       23      IN    A         216.58.222.46
ads.google.com.                         216     IN    A         172.217.172.110
america.google.com.                     60      IN    CNAME     www3.l.google.c
om.
www3.l.google.com.                      250     IN    A         172.217.172.46
ap.google.com.                          604800  IN    CNAME     www2.l.google.c
om.
www2.l.google.com.                      222     IN    A         172.217.30.228
apps.google.com.                        485997  IN    CNAME     www3.l.google.c
om.
www3.l.google.com.                      267     IN    A         172.217.173.14
archive.google.com.                     300     IN    A         172.217.172.174
asia.google.com.                        300     IN    A         216.58.222.36
blog.google.com.                        60      IN    CNAME     www.blogger.com
```

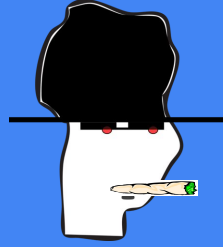
```
google.com class C netranges:
_____________________________

8.8.4.0/24
8.8.8.0/24
64.9.224.0/24
64.233.184.0/24
142.250.4.0/24
172.217.30.0/24
172.217.162.0/24
172.217.172.0/24
172.217.173.0/24
172.217.192.0/24
172.217.218.0/24
209.85.233.0/24
216.58.202.0/24
216.58.222.0/24
216.239.32.0/24
216.239.34.0/24
216.239.36.0/24
216.239.38.0/24
```

whois 8.8.8.8



```
NetRange:       8.0.0.0 - 8.127.255.255
CIDR:           8.0.0.0/9
NetName:        LVLT-ORG-8-8
NetHandle:      NET-8-0-0-0-1
Parent:         NET8 (NET-8-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Level 3 Parent, LLC (LPL-141)
RegDate:        1992-12-01
Updated:        2018-04-23
Ref:            https://rdap.arin.net/registry/ip/8.0.0.0


OrgName:        Level 3 Parent, LLC
OrgId:          LPL-141
Address:        100 CenturyLink Drive
City:           Monroe
StateProv:      LA
PostalCode:     71203
Country:        US
RegDate:        2018-02-06
```

```
joe@zoidberg:~/Soft/assetfinder$ ~/go/bin/assetfinder google.com | wc -l
27680
```



assetfinder google.com

```
*.sites.sandbox.google.com
docs.google.com
*.mail.google.com
*.talkgadget.google.com
fra-da.ext.google.com
code.google.com
*.developers.google.com
appengine.google.com
*.cloud.google.com
*.google.com
google.com
*.google.com.af
```

```
www.freezone.google.com
clients.google.com
*.docs.google.com
*.drive.google.com
*.photos.google.com
*.upload.google.com
upload.google.com
upload.video.google.com
dg.video.google.com
*.vp.video.l.google.com
friendconnect.google.com
```

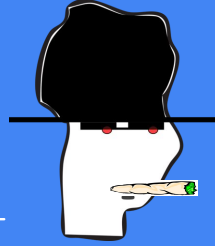
```
joe@zoidberg:~/Soft/assetfinder$ host wprj11.hot.corp.google.com
Host wprj11.hot.corp.google.com not found: 3(NXDOMAIN)
```

```
devconsole-testers.sandbox.google.com
*.docs.sandbox.google.com
*.drive.sandbox.google.com
*.prom-qa.corp.google.com
*.prom-qa.sandbox.google.com
*.prom-test.corp.google.com
*.prom-test.sandbox.google.com
*.sandbox.google.com
sandbox.google.com
*.sandbox.google.com.au
*.sandbox.google.com.br
*.sandbox.google.com.hk
*.script.sandbox.google.com
*.sites.sandbox.google.com
accounts.flexpack.google.com
accounts.freezone.google.com
flexpack.google.com
freezone.google.com
gaiastaging.flexpack.google.com
gaiastaging.freezone.google.com
```

```
*.dasher.corp.google.com
*.dasher-qa.corp.google.com
*.demetrius-codespot.corp.google.com
*.demetrius.corp.google.com
*.demetrius-googlecode.corp.google.com
*.dfa7.corp.google.com
*.docs-dev.corp.google.com
*.docs-platinum.corp.google.com
*.docs-qa.corp.google.com
*.drive-test.corp.google.com
```

```
wprj12.hot.corp.google.com
wprj11.hot.corp.google.com
wprj10.hot.corp.google.com
wprj9.hot.corp.google.com
wprj8.hot.corp.google.com
```

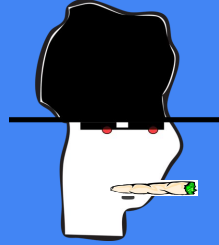
```
./patator.py dns_forward name=FILE0.google.com
0=../SecLists/Discovery/DNS/subdomains-top1milli
on-5000.txt -x ignore:code=3 --threads 20
```



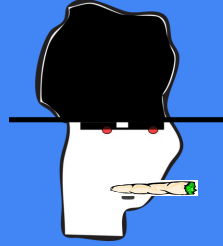
```
                    api.google.com
                   www.blogger.com ?
                   blog.google.com
                 images.l.google.com ?
                  images.google.com
                 video.l.google.com ?
                  video.google.com
                 ipv4.l.google.com ?
                  ipv4.google.com
Domains ──────────────────────────────────────────
                        google.com 86
Networks ─────────────────────────────────────────
                                  8.8.4.4
                                  8.8.8.8
                                  64.9.224.x
                                  64.233.190.x
                                  172.217.192.x
                                  216.239.32.10
                                  216.239.34.10
                                  216.239.36.10
                                  216.239.38.10
                                  2001:4860:4802:32::a
                                  2001:4860:4802:34::a
                                  2001:4860:4802:36::a
                                  2001:4860:4802:38::a
```

```
* telnet_login   : Brute-force Telnet
* smtp_login     : Brute-force SMTP
* smtp_vrfy      : Enumerate valid users using the SMTP VRFY comma
* smtp_rcpt      : Enumerate valid users using the SMTP RCPT TO co
* finger_lookup  : Enumerate valid users using Finger
* http_fuzz      : Brute-force HTTP/HTTPS
* rdp_gateway    : Brute-force RDP Gateway
* ajp_fuzz       : Brute-force AJP
* pop_login      : Brute-force POP
* pop_passd      : Brute-force poppassd (not POP3)
* imap_login     : Brute-force IMAP
* ldap_login     : Brute-force LDAP
* dcom_login     : Brute-force DCOM
* smb_login      : Brute-force SMB
* smb_lookupsid  : Brute-force SMB SID-lookup
* rlogin_login   : Brute-force rlogin
* vmauthd_login  : Brute-force VMware Authentication Daemon
* mssql_login    : Brute-force MSSQL
* oracle_login   : Brute-force Oracle
* mysql_login    : Brute-force MySQL
* mysql_query    : Brute-force MySQL queries
* rdp_login      : Brute-force RDP (NLA)
* pgsql_login    : Brute-force PostgreSQL
* vnc_login      : Brute-force VNC
* dns_forward    : Brute-force DNS
* dns_reverse    : Brute-force DNS (reverse lookup subnets)
* ike_enum       : Enumerate IKE transforms
```

dnsrecon



```
joe@zoidberg:~$ dnsrecon -d  google.com
[*] Performing General Enumeration of Domain: google.com
[-] DNSSEC is not configured for google.com
[*]      SOA ns1.google.com 216.239.32.10
[*]      NS ns4.google.com 216.239.38.10
[*]      NS ns4.google.com 2001:4860:4802:38::a
[*]      NS ns2.google.com 216.239.34.10
[*]      NS ns2.google.com 2001:4860:4802:34::a
[*]      NS ns3.google.com 216.239.36.10
[*]      NS ns3.google.com 2001:4860:4802:36::a
[*]      NS ns1.google.com 216.239.32.10
[*]      NS ns1.google.com 2001:4860:4802:32::a
[*]      MX aspmx.l.google.com 172.217.192.26
[*]      MX alt4.aspmx.l.google.com 172.253.118.26
[*]      MX alt1.aspmx.l.google.com 64.233.184.26
[*]      MX alt3.aspmx.l.google.com 209.85.233.26
[*]      MX alt2.aspmx.l.google.com 172.217.218.26
[*]      MX aspmx.l.google.com 2800:3f0:4003:c01::1a
[*]      MX alt4.aspmx.l.google.com 2404:6800:4003:c05::1b
[*]      MX alt1.aspmx.l.google.com 2a00:1450:400c:c0b::1a
[*]      MX alt3.aspmx.l.google.com 2a00:1450:4010:c03::1b
[*]      MX alt2.aspmx.l.google.com 2a00:1450:4013:c08::1a
[*]      A google.com 172.217.172.110
```



whatweb

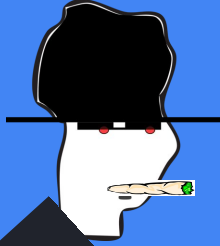
```
joe@zoidberg:~$ whatweb www.google.com
http://www.google.com [200 OK] Cookies[1P_JAR,NID], Country[UNITED STATES][US],
HTML5, HTTPServer[gws], HttpOnly[NID], IP[172.217.173.4], Script, Title[Google]
 X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]
```

```
http://developers.google.com [301 Moved Permanently] Country[UNITED STATES][US],
 HTTPServer[Google Frontend], IP[172.217.172.110], RedirectLocation[https://deve
lopers.google.com/], UncommonHeaders[x-cloud-trace-context]
https://developers.google.com/ [200 OK] Country[UNITED STATES][US], HTML5, HTTPS
erver[Google Frontend], IP[172.217.172.110], Open-Graph-Protocol[website], OpenS
earch[https://developers.google.com/s/opensearch.xml], Script[application/json,a
pplication/ld+json], Strict-Transport-Security[max-age=31536000; includeSubdomai
ns], Title[Google Developers], UncommonHeaders[x-content-type-options,x-cloud-tr
ace-context,alt-svc], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]
```

```
https://www.famaf.proed.unc.edu.ar [200 OK] Content-Language[es], Cookies[Moodle
Session,idunc,route,serverid], Country[ARGENTINA][AR], Google-Analytics[Universa
l][UA-8153017-9], HTML5, HTTPServer[Tengine], IP[200.16.16.170], Moodle, PHP[7.2
.24-0ubuntu0.18.04.6], PasswordField[password], Script[text/css,text/javascript]
, Tengine-Web-Server, Title[Facultad de Matemática, Astronomía y Física], Uncomm
onHeaders[content-script-type,content-style-type,front-end-https], X-Frame-Optio
ns[sameorigin], X-Powered-By[PHP/7.2.24-0ubuntu0.18.04.6], X-UA-Compatible[IE=ed
ge]
```

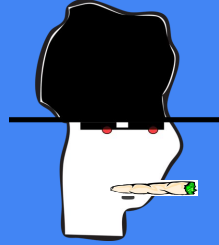
dirb

```
START_TIME: Mon Sep 28 13:01:14 2020
URL_BASE: http://www.google.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_________________


GENERATED WORDS: 4612

---- Scanning URL: http://www.google.com/ ----
+ http://www.google.com/2001 (CODE:301|SIZE:239)
+ http://www.google.com/2002 (CODE:301|SIZE:239)
+ http://www.google.com/2003 (CODE:301|SIZE:239)
+ http://www.google.com/2004 (CODE:301|SIZE:239)
+ http://www.google.com/2005 (CODE:301|SIZE:239)
+ http://www.google.com/2006 (CODE:301|SIZE:239)
+ http://www.google.com/2007 (CODE:301|SIZE:239)
+ http://www.google.com/2008 (CODE:301|SIZE:239)
+ http://www.google.com/2009 (CODE:301|SIZE:239)
+ http://www.google.com/2010 (CODE:301|SIZE:239)
+ http://www.google.com/2011 (CODE:301|SIZE:239)
+ http://www.google.com/2012 (CODE:301|SIZE:239)
+ http://www.google.com/2013 (CODE:301|SIZE:239)
+ http://www.google.com/2014 (CODE:301|SIZE:239)
+ http://www.google.com/about (CODE:301|SIZE:218)
==> DIRECTORY: http://www.google.com/accessibility/
+ http://www.google.com/account (CODE:302|SIZE:227)
+ http://www.google.com/accounts (CODE:302|SIZE:210)
+ http://www.google.com/activity (CODE:301|SIZE:0)
==> DIRECTORY: http://www.google.com/ads/
+ http://www.google.com/advanced_search (CODE:301|SIZE:235)
+ http://www.google.com/advertise (CODE:301|SIZE:224)
+ http://www.google.com/advertisers (CODE:301|SIZE:236)
+ http://www.google.com/advertising (CODE:301|SIZE:224)
+ http://www.google.com/adview (CODE:204|SIZE:0)
+ http://www.google.com/af (CODE:301|SIZE:227)
+ http://www.google.com/africa (CODE:302|SIZE:231)
+ http://www.google.com/alerts (CODE:302|SIZE:226)
+ http://www.google.com/analytics (CODE:301|SIZE:250)
```



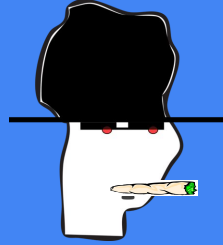
```
---- Entering directory: http://www.google.com/answers/ ----
+ http://www.google.com/answers/.swf (CODE:302|SIZE:270)
+ http://www.google.com/answers/browse (CODE:301|SIZE:231)
+ http://www.google.com/answers/browser (CODE:301|SIZE:231)
^[[B
+ http://www.google.com/answers/player.swf (CODE:302|SIZE:276)
+ http://www.google.com/answers/ratings (CODE:301|SIZE:231)
```

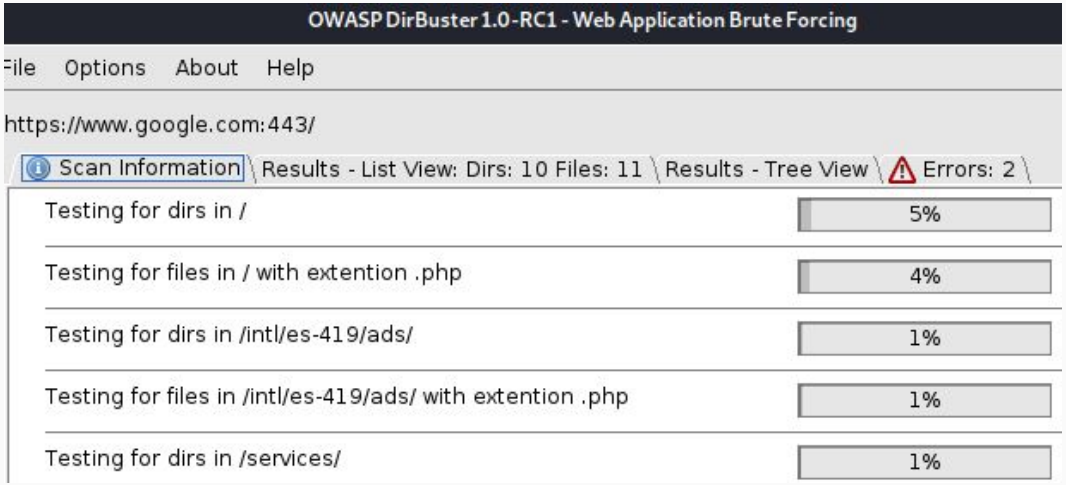
gobuster



```
joe@zoidberg:~$ gobuster vhost  -w Soft/SecLists/Discovery/Web-Content/apache.txt  -u www.google.com
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://www.google.com
[+] Threads:      10
[+] Wordlist:     Soft/SecLists/Discovery/Web-Content/apache.txt
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
2020/09/28 18:46:25 Starting gobuster
===============================================================
Found: .web.www.google.com (Status: 400) [Size: 1555]
Found: .htaccess.www.google.com (Status: 400) [Size: 1555]
Found: .meta.www.google.com (Status: 400) [Size: 1555]
Found: .htpasswd.www.google.com (Status: 400) [Size: 1555]
Found: ~bin.www.google.com (Status: 400) [Size: 1555]
Found: ~root.www.google.com (Status: 400) [Size: 1555]
Found: ~nobody.www.google.com (Status: 400) [Size: 1555]
Found: ~ftp.www.google.com (Status: 400) [Size: 1555]
===============================================================
2020/09/28 18:46:25 Finished
```

dirbuster




OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
https://www.google.com:443/
Scan Information
Results - List View: Dirs: 10 Files: 11
Results - Tree View
Errors: 2
Testing for dirs in /
5%
Testing for files in / with extention .php
4%
Testing for dirs in /intl/es-419/ads/
1%
Testing for files in /intl/es-419/ads/ with extention .php
1%
Testing for dirs in /services/
1%

detecting virtual hosts:

https://pentest-tools.com/information-gathering/find-virtual-hosts/

Find Virtual Hosts for Any IP Address Report (Light)

✔ developer.google.com

Found 4 virtual hosts

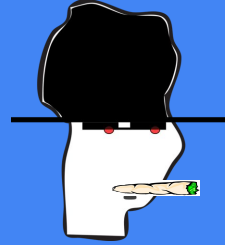
Virtual Host	IP Address
android.clients.google.com	216.58.204.14
archive.google.com	216.58.204.14
lhr35s07-in-f14.1e100.net	216.58.204.14
lhr48s21-in-f14.1e100.net	216.58.204.14

Scan parameters

Target: developer.google.com

NMAP

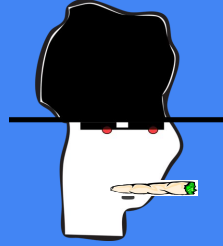
```
Warning: OSScan results may be unreliable because we could not find at least 1 open and
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 8.82 seconds
```



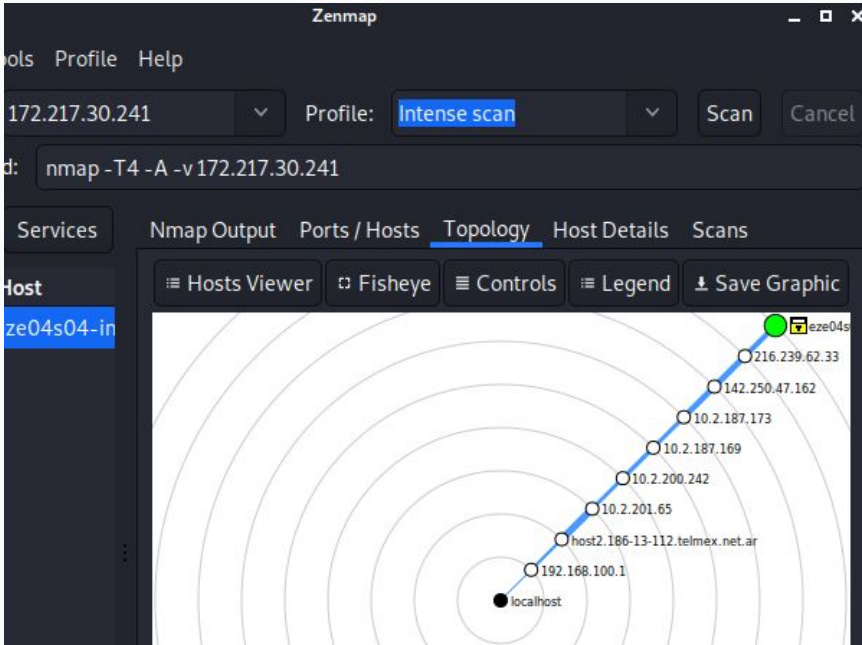
```
joe@zoidberg:~$ nmap -sP 172.217.30.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 17:45 -03
Nmap scan report for rio01s23-in-f0.1e100.net (172.217.30.0)
Host is up (0.067s latency).
Nmap scan report for rio01s23-in-f1.1e100.net (172.217.30.1)
Host is up (0.057s latency).
Nmap scan report for rio01s23-in-f2.1e100.net (172.217.30.2)
Host is up (0.056s latency).
Nmap scan report for rio01s23-in-f3.1e100.
Host is up (0.058s latency).
Nmap scan report for rio01s23-in-f4.1e100.
Host is up (0.058s latency).
Nmap scan report for rio01s23-in-f5.1e100.
Host is up (0.057s latency).
Nmap scan report for rio01s23-in-f6.1e100.
Host is up (0.058s latency).
Nmap scan report for rio01s23-in-f7.1e100.
```

```
joe@zoidberg:~$ nmap -sV 172.217.30.240-245
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 17:49 -03
Stats: 0:00:24 elapsed; 0 hosts completed (6 up), 6 undergoing Service Scan
Service scan Timing: About 8.33% done; ETC: 17:52 (0:02:01 remaining)
Nmap scan report for eze04s04-in-f16.1e100.net (172.217.30.240)
Host is up (0.019s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE   VERSION
80/tcp  open  http      UploadServer
443/tcp open  ssl/https UploadServer
2 services unrecognized despite returning data. If you know the service/vers
ervice :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.80%I=7%D=9/28%Time=5F724C83%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,23D,"HTTP/1\.0\x20404\x20Not\x20Found\r\nX-GUploader-UploadID:\x
SF:20ABg5-Uw7JZf1-cgpgALPbU-Jes5SfEB4K1juLvWsY8XfKf9cblWpvDqo1MnWzusu-zhO7
SF:9nJUId23hKIsLBv1vQyZ5g\r\nContent-Type:\x20application/xml;\x20charset=
```

NMAP



```
joe@zoidberg:~$ sudo nmap -script vuln 172.217.30.240
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 17:56 -03
Nmap scan report for eze04s04-in-f16.1e100.net (172.217.30.240)
Host is up (0.016s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp open  https
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_sslv2-drown:
```

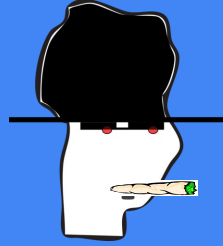


Otras tools

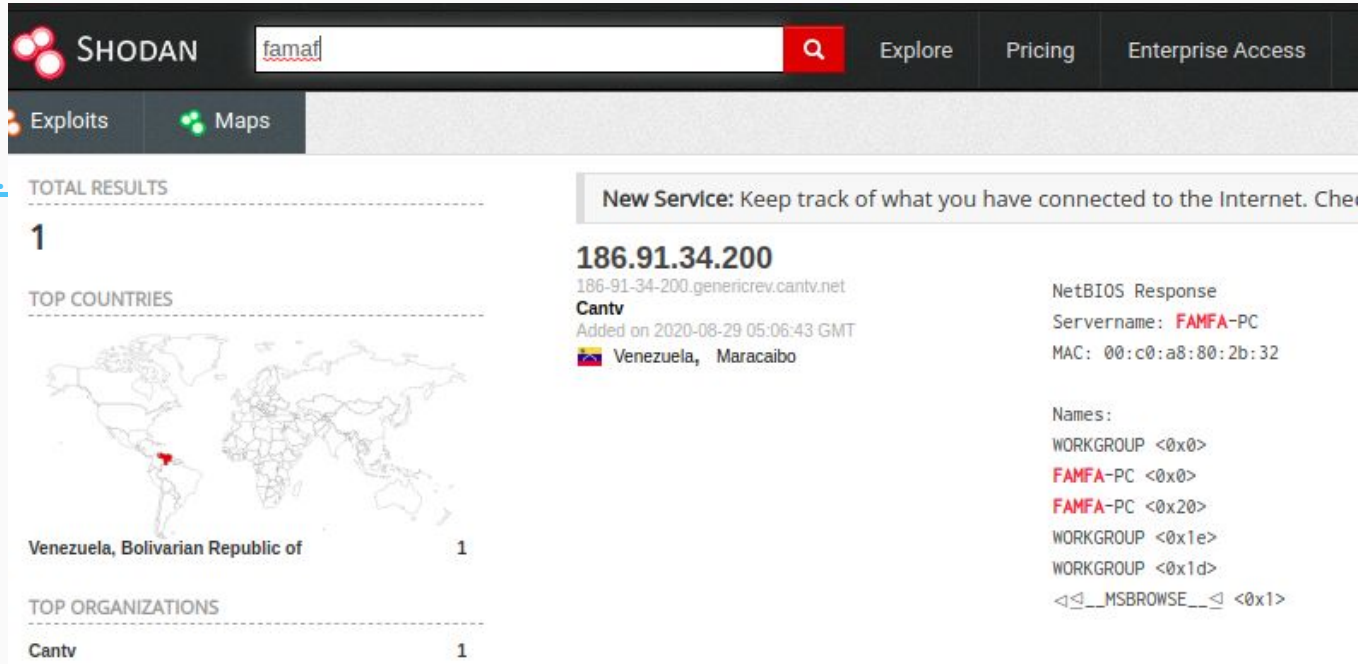
Shodan.io
Censys
https://haveibeenpwned.com/
Wfuzz
Burp Scans
httpx
masscan

```
[*] Using auxiliary/scanner/http/dir_scanner
msf5 auxiliary(scanner/http/dir_scanner) > options

Module options (auxiliary/scanner/http/dir_scanner):

   Name        Current Setting
   ----        ---------------
   DICTIONARY  /usr/share/metasploit-framework/data/wmap/wmap_dirs.txt
   PATH        /
   Proxies
   RHOSTS
   RPORT       80
   SSL         false
   THREADS     1
   VHOST

msf5 auxiliary(scanner/http/dir_scanner) > set RHOSTS 172.217.30.241
RHOSTS => 172.217.30.241
msf5 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 172.217.30.241
[+] Found http://172.217.30.241:80/accounts/ 302 (172.217.30.241)
[+] Found http://172.217.30.241:80/ads/ 200 (172.217.30.241)
[+] Found http://172.217.30.241:80/archivesearch/ 301 (172.217.30.241)
[+] Found http://172.217.30.241:80/blogsearch/ 301 (172.217.30.241)
[+] Found http://172.217.30.241:80/bookmarks/ 302 (172.217.30.241)
[+] Found http://172.217.30.241:80/books/ 302 (172.217.30.241)
[+] Found http://172.217.30.241:80/calendar/ 301 (172.217.30.241)
[+] Found http://172.217.30.241:80/careers/ 301 (172.217.30.241)
[+] Found http://172.217.30.241:80/checkout/ 301 (172.217.30.241)
[+] Found http://172.217.30.241:80/dl/ 302 (172.217.30.241)
[+] Found http://172.217.30.241:80/finance/ 301 (172.217.30.241)
```

Otras tools



Shodan.io
Censys
https://haveibeenpwned.
Wfuzz
Burp Scans
httpx
masscan
gau



Otras tools

Shodan.io
Censys
https://haveibeenpwned.com/
Wfuzz
Burp Scans
httpx
masscan
gau