
CLUB DE
HACK1NG
{HARDWARE}

Pentest

Test de intrusión

Son las pruebas que se realizan a un sistema con el objetivo de evaluar sus líneas de defensa.

- **Extraer información**
- **Determinar la posibilidad de la denegación de servicio.**
- **Detectar vulnerabilidades no conocidas.**

Pentest

Test de intrusión

Los alcances de un *pentest* se deben negociar con el cliente. Existen tres tipos de análisis que dependen de la cantidad de información que se tenga del objetivo

- **Caja negra**
- **Caja blanca**
- **Caja gris**

Pentest

Metodologías de pentest

National Institute of Standars and Technology (NIST).

https://csrc.nist.gov/Publications

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Open Web Application Security Project (OWASP)

Open Source Security Testing Methodology Manual (OSSTMMM)

Pentest

Reconocimiento: obtener información del objetivo. *Pasivo*, no hay interacción, es decir, la información se puede obtener de medios externos. *Activo*, se interactúa con el objetivo, por ejemplo, ingeniería social.

Enumeración: el objetivo es hacer un mapeo de la arquitectura del objetivo ya sea utilizando herramientas como Nmap y hping3.

Pentest

Análisis: reconocimiento de las vulnerabilidades. Algunas herramientas, Nmap, Nessus, Acunetix, AppScan.

Explotación: se utilizan *exploits* contra los servicios y aplicaciones vulnerables detectados en las previas etapas. Elevación de privilegios e intentar mantener el acceso (por ejemplo, backdoors, rootkits)

Pentest

Documentación: Se describen paso a paso el proceso realizado y los resultados obtenidos. Finalmente, el documento debería tener los consejos para dar solución a las vulnerabilidades detectadas y cómo mejorar la línea de defensa del sistema.

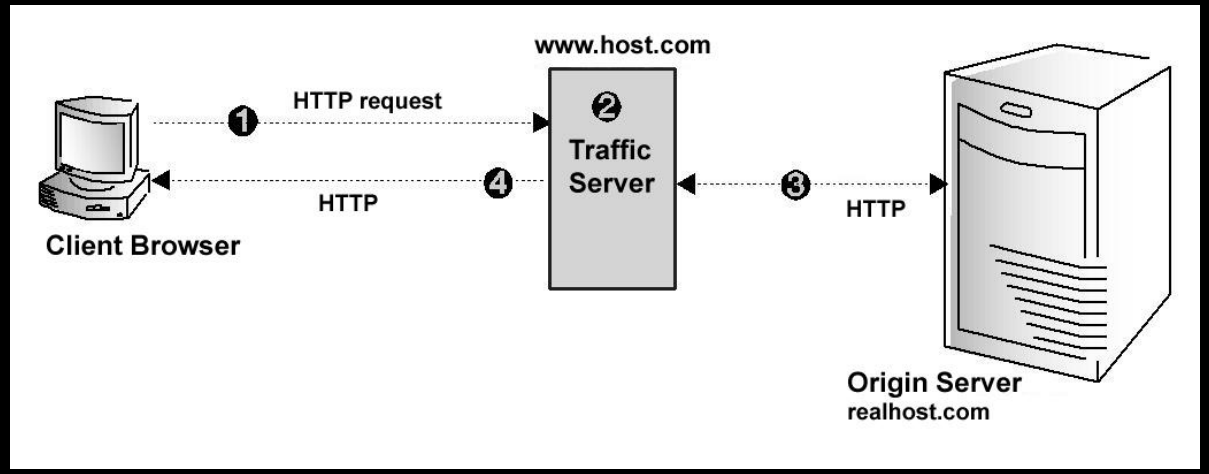
What does a hacker do?

Clasificación de redes

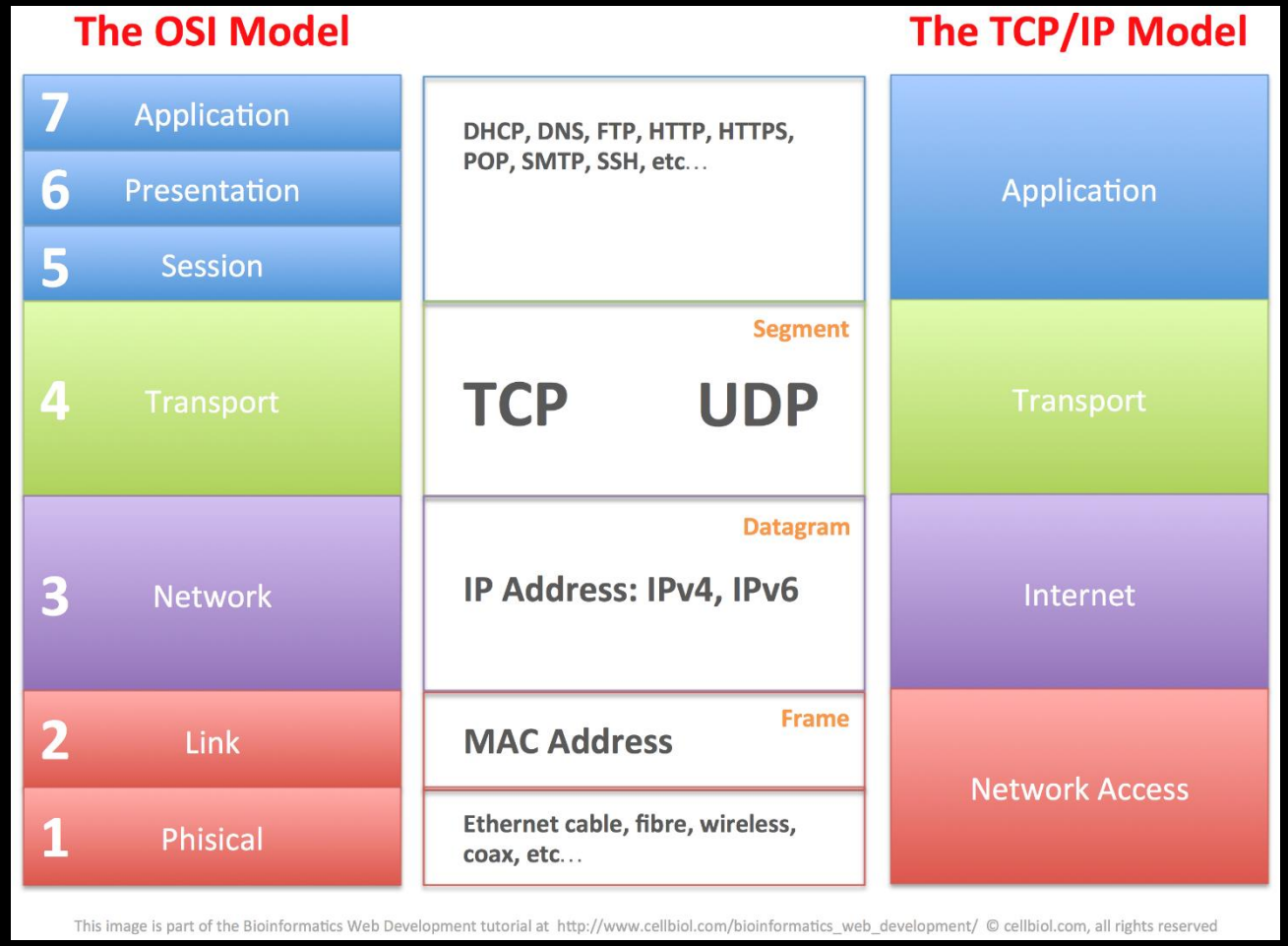
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WIDE (Wide Area Network)
- PAN (Personal Area Network)
- WLAN (Wireless Local Network)
- WMAN (Wireless Metropolitan Network)
- WWMAN (Wireless Wide Area Network)

HTTP

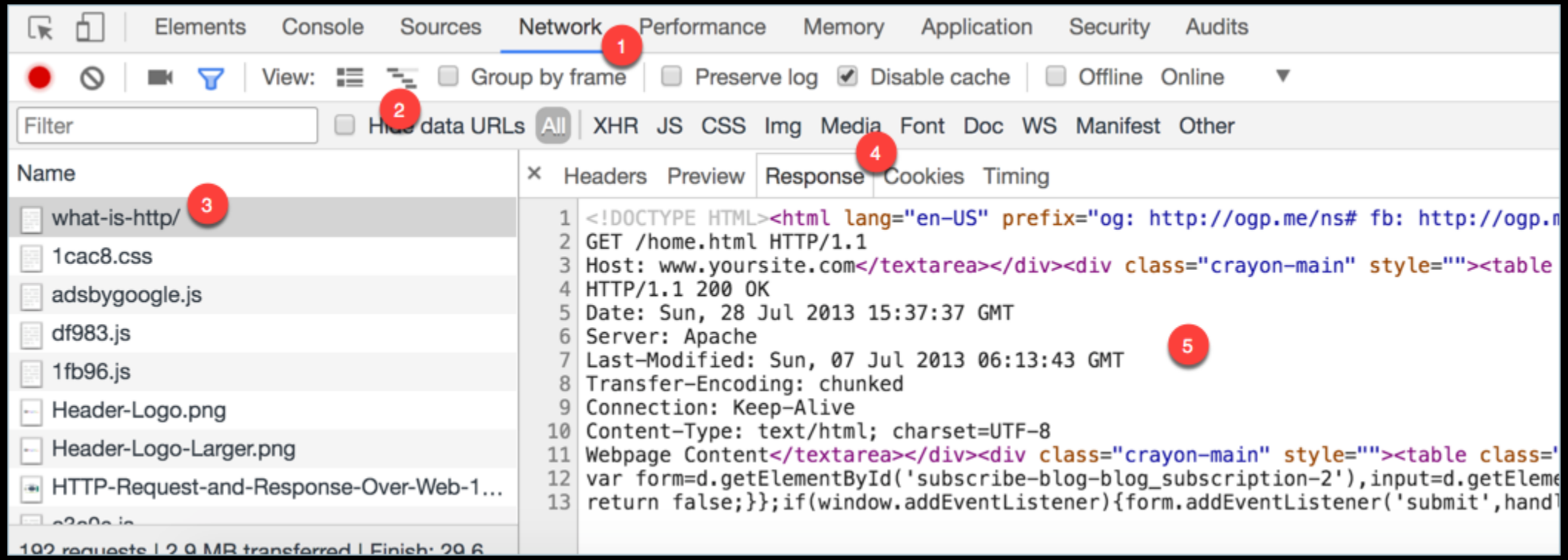
HyperText Transfer Protocol, es un protocolo de la capa de aplicación del modelo OSI y TCP/IP



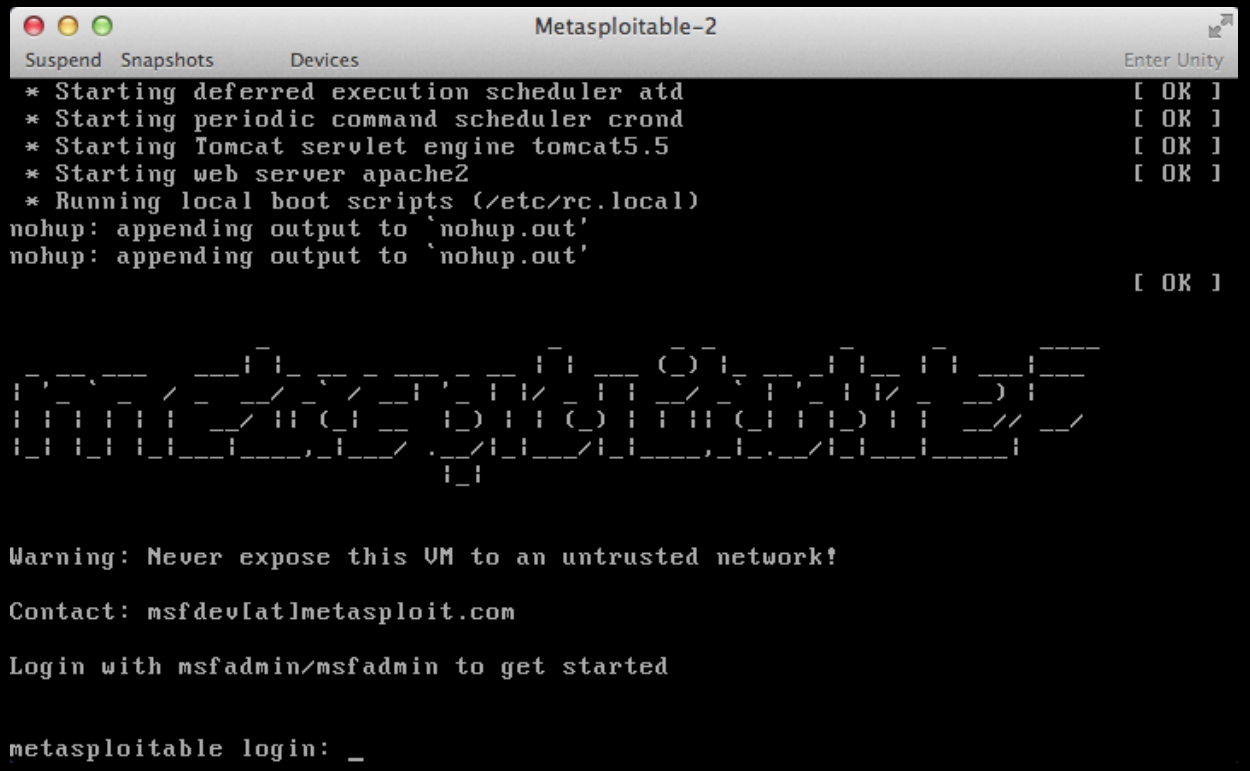
Modelo TCP/IP y OSI



HTTP


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
1
View:
Group by frame
Preserve log
Disable cache
Offline
Online
2
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
4
Name
3
what-is-http/
1cac8.css
adsbygoogle.js
df983.js
1fb96.js
Header-Logo.png
Header-Logo-Larger.png
HTTP-Request-and-Response-Over-Web-1...
Headers
Preview
Response
Cookies
Timing
1 <!DOCTYPE HTML><html lang="en-US" prefix="og: http://ogp.me/ns# fb: http://ogp.m
2 GET /home.html HTTP/1.1
3 Host: www.yoursite.com</textarea> <table
4 HTTP/1.1 200 OK
5 Date: Sun, 28 Jul 2013 15:37:37 GMT
6 Server: Apache
7 Last-Modified: Sun, 07 Jul 2013 06:13:43 GMT
8 Transfer-Encoding: chunked
9 Connection: Keep-Alive
10 Content-Type: text/html; charset=UTF-8
11 Webpage Content</textarea> <table class='
12 var form=d.getElementById('subscribe-blog-blog_subscription-2'),input=d.getEleme
13 return false;}};if(window.addEventListener){form.addEventListener('submit',hand
5

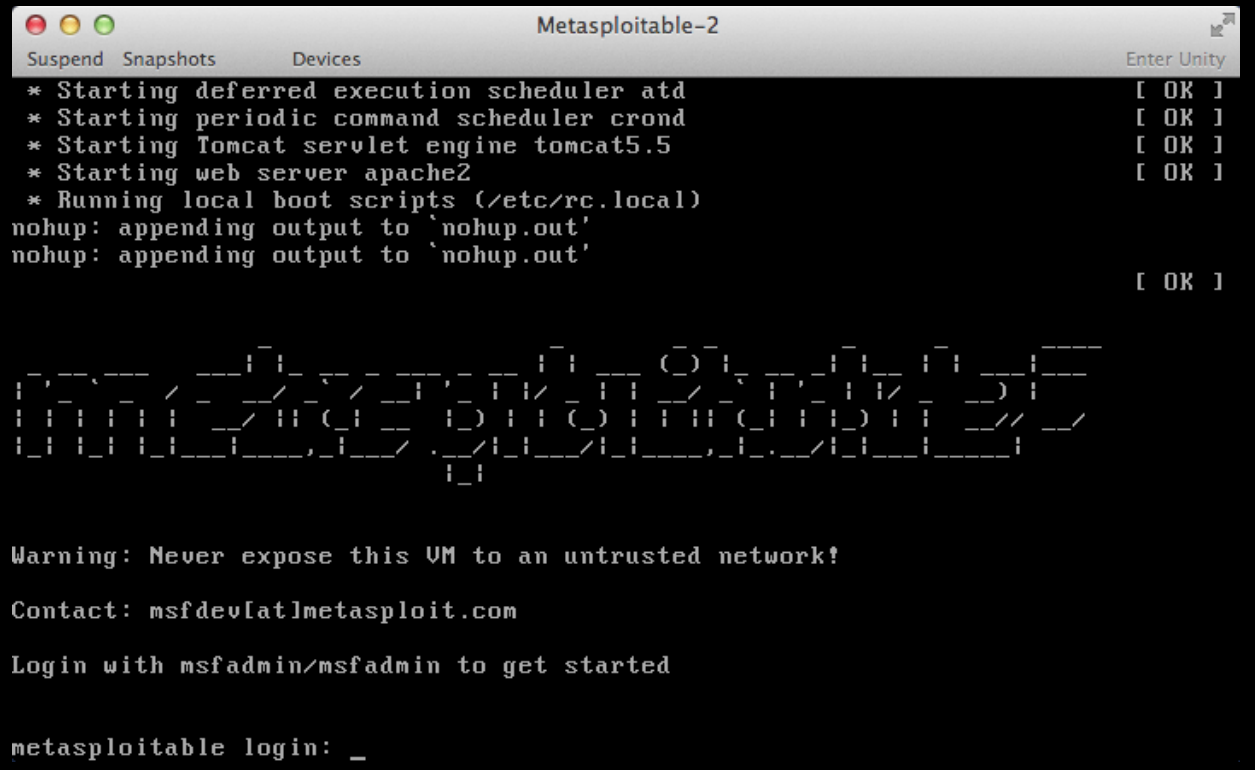
Entornos básicos de pruebas



Se recomienda trabajar en modo *host only*, es decir, aislar la máquina virtual de cualquier red externa.

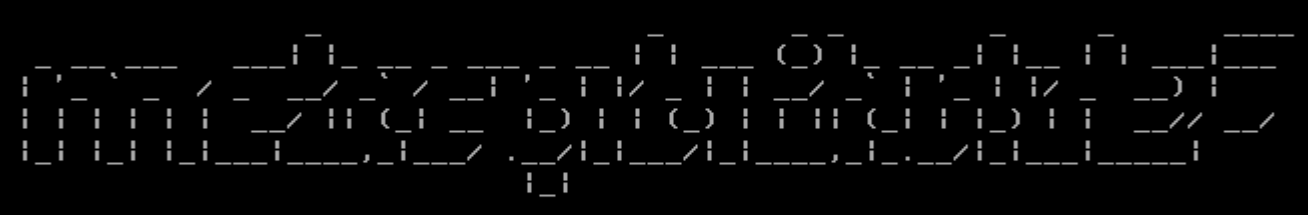
Workshop-1


KALI LINUX™
"the quieter you become, the more you are able to hear"


Metasploitable-2
Suspend Snapshots Devices Enter Unity
* Starting deferred execution scheduler atd [OK]
* Starting periodic command scheduler crond [OK]
* Starting Tomcat servlet engine tomcat5.5 [OK]
* Starting web server apache2 [OK]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
[OK]
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: _

Workshop-2

```
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ exit
logout
```



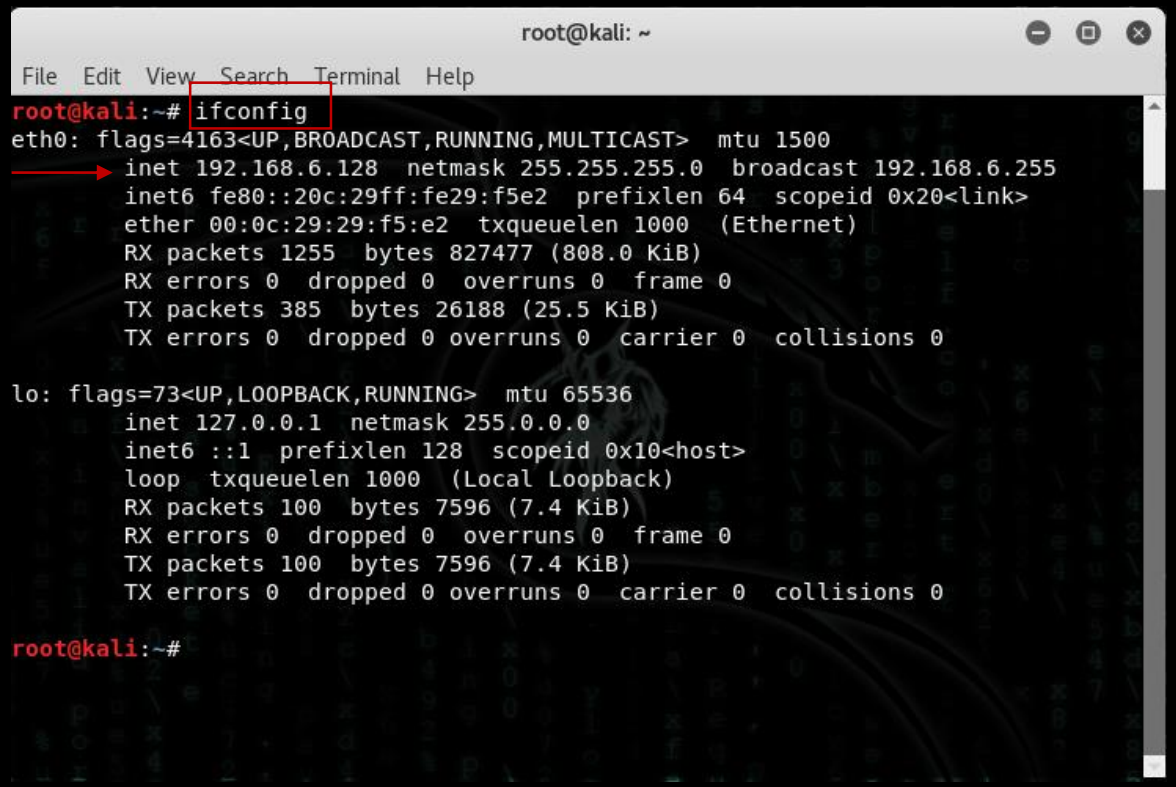
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin_
```

Usuario: msfadmin
Password: msfadmin

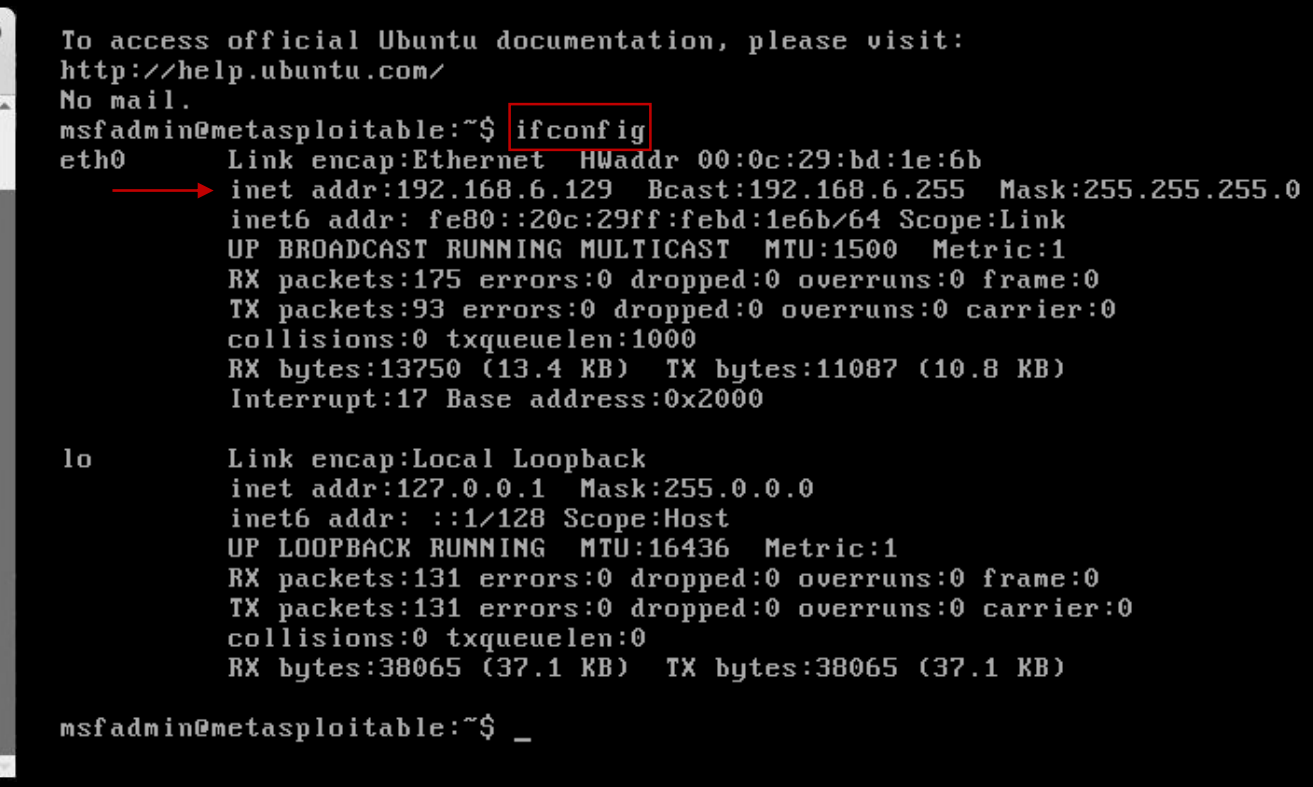
https://github.com/rapid7/metasploitable3/wiki

https://hackpuntes.com/metasploitable3-crea-una-maquina-vulnerable-para-probar-tus-ataques/

Workshop-2



Kali Linux



Metasploitable

Workshop-2

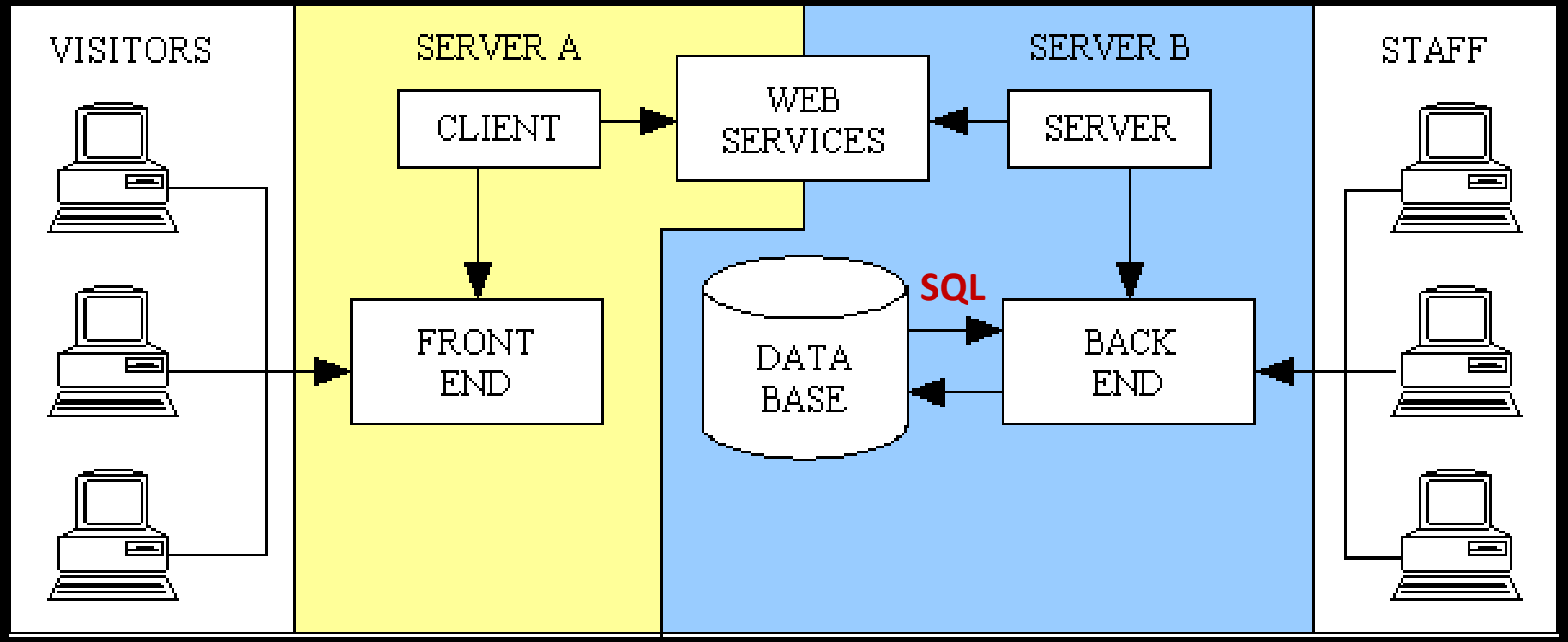

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV


DVWA
Username
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

Aplicación web

- **Frontend**
  - **Imágenes**
  - **Lenguaje de para estilos de la página CSS.**
  - **HTML.**
  - **Javascript, es un lenguaje que se ejecuta en el navegador web.**
- **Backend**
  - **La lógica del negocio, base de datos.**
  - **Lenguajes más especializados, por ejemplo, C#, Python y Java. Estos se ejecutan en el servidor.**

Aplicación web

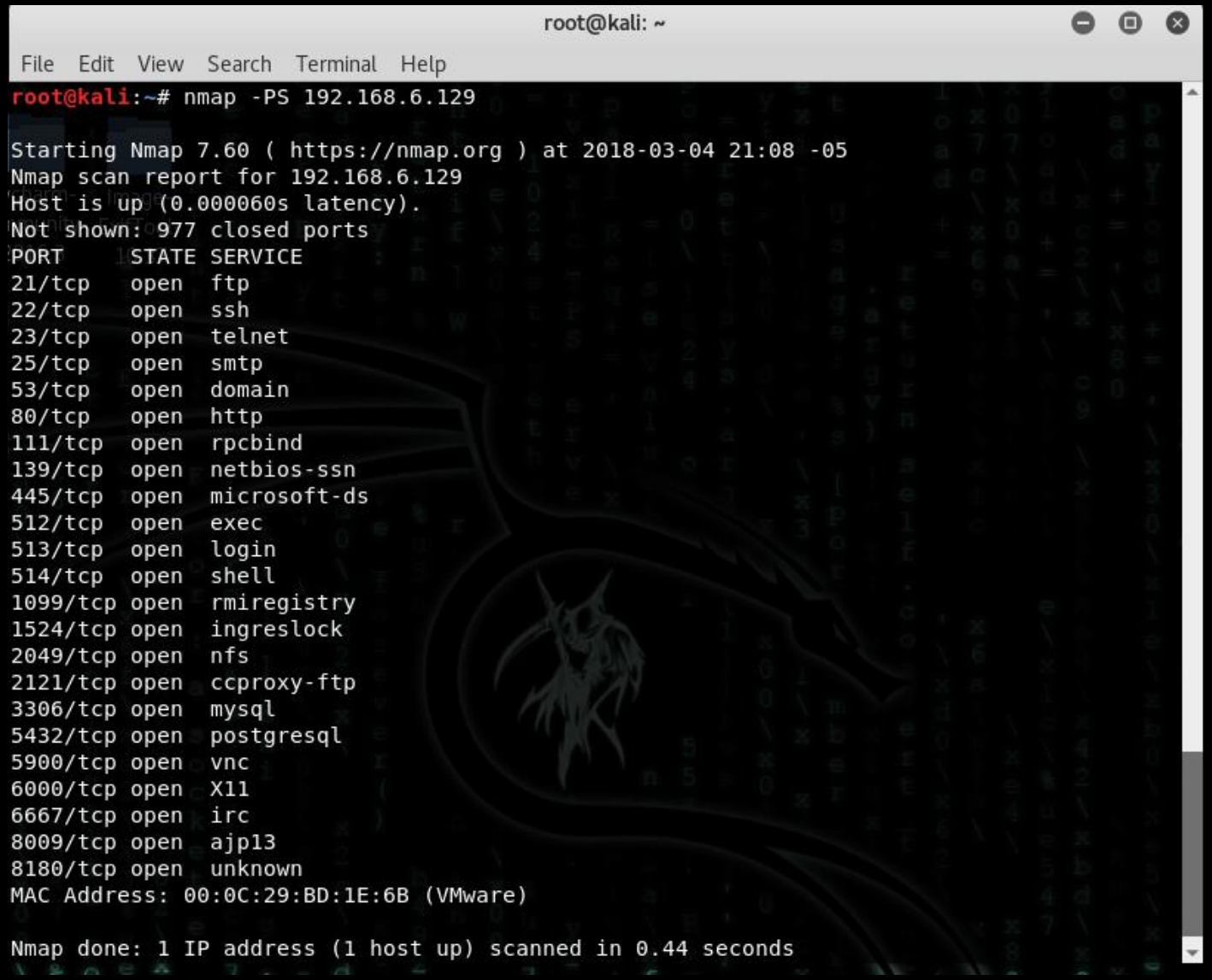


Nmap

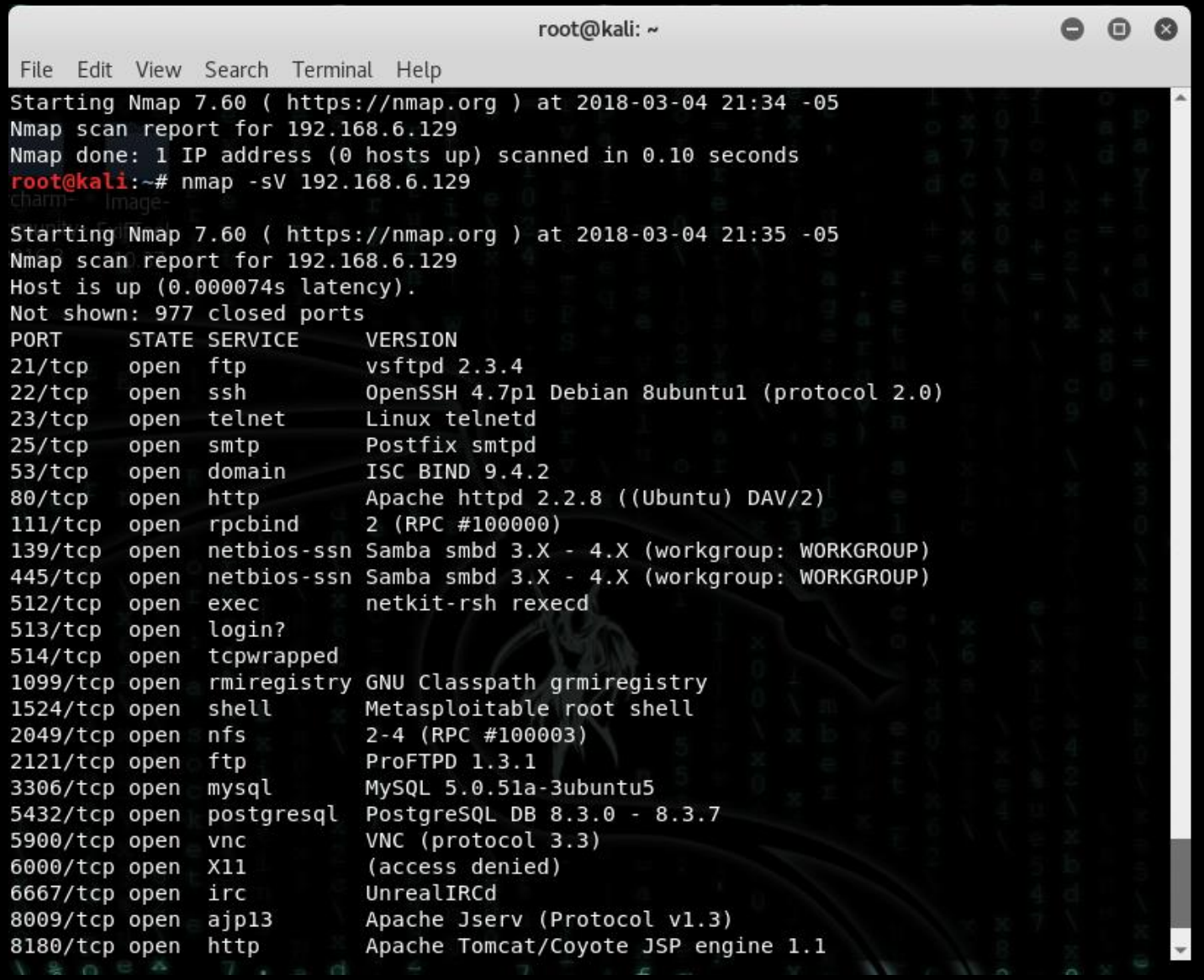
Es un programa de código abierto para el rastreo de equipos, puertos, servicios y sistemas operativos de una infraestructura de TI.

https://nmap.org/

Nmap


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -PS 192.168.6.129
Starting Nmap 7.60 (https://nmap.org) at 2018-03-04 21:08 -05
Nmap scan report for 192.168.6.129
Host is up (0.000060s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:BD:1E:6B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

Nmap


root@kali: ~
File Edit View Search Terminal Help
Starting Nmap 7.60 (https://nmap.org) at 2018-03-04 21:34 -05
Nmap scan report for 192.168.6.129
Nmap done: 1 IP address (0 hosts up) scanned in 0.10 seconds
root@kali:~# nmap -sV 192.168.6.129
Starting Nmap 7.60 (https://nmap.org) at 2018-03-04 21:35 -05
Nmap scan report for 192.168.6.129
Host is up (0.000074s latency).
Not shown: 977 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open tcpwrapped
1099/tcp open rmiregistry GNU Classpath grmiregistry
1524/tcp open shell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

Bibliografía

Ramos, Antonio., Barberto, C. Marugan, D., & Gonzáles I. Hacking y seguridad de páginas web

Seitz, J. (2014). Black Hat Python: Python Programming for Hackers and Pentesters. No Starch Press.

Imágenes

https://www.slideshare.net/arohan6/ethical-hacking-64018689

https://mobile.alphacoders.com/d_161/wallpaper/630507/Video-Game-Watch-Dogs-Wallpapers

https://docs.trafficserver.apache.org/en/5.3.x/admin/reverse-proxy-http-redirects.en.html

https://es.wikipedia.org/wiki/Modelo_OSI

https://www.webnots.com/what-is-http/

http://ciberseguridad.digital/sql-injection/

http://2.bp.blogspot.com/-FX00EIt6W2o/UwyrmFmcy0I/AAAAAAAABM4/H2AZ7SAAvvs/s1600/sql.jpg

https://snyk.io/blog/xss-attacks-the-next-wave/

http://www.mobileapplicationdevelopments.in/mobile-application-development/web-application/

https://www.tonymarston.net/php-mysql/an-end-to-end-ecommerce-solution-requires-more-than-a-fancy-website.html

Ubisoft – watch dogs 2.


THEIR CRIME IS CURIOSITY
HACKERS