

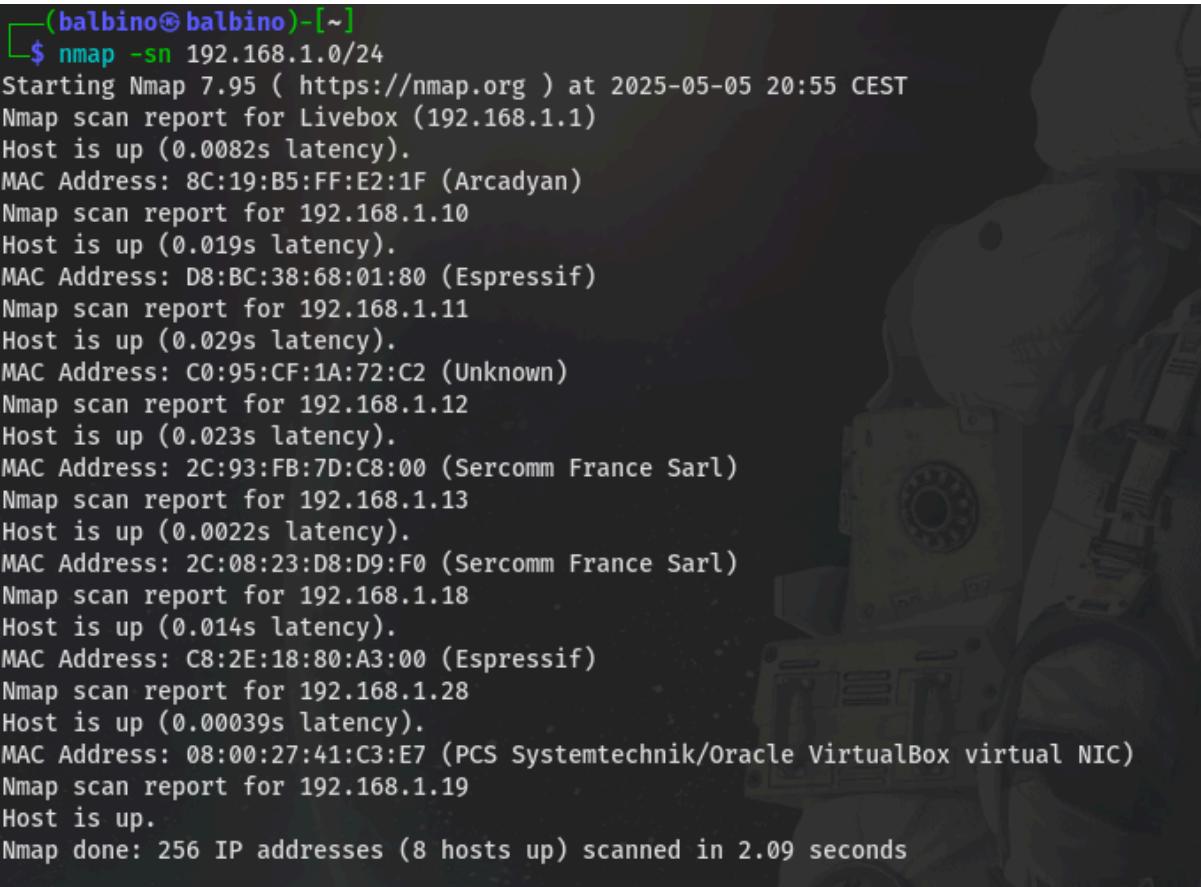
0. Introducción

El principal objetivo de esta práctica sería sacar información de un entorno preparado para ser atacado y saber que herramientas y cómo podemos explotar dicho entorno.

1. Reconocimiento

Primero de todo debemos averiguar la ip de nuestra máquina víctima, para poder atacar, en este caso para poder sacar la ip de la máquina, he usado el siguiente comando:

```
nmap -sn 192.168.1.0/24
```

A terminal window with a dark background and light-colored text. The prompt is '(balbino@balbino)-[~]'. The command '\$ nmap -sn 192.168.1.0/24' has been entered. The output shows the start of Nmap 7.95 at 2025-05-05 20:55 CEST. It then lists scan reports for several hosts: 192.168.1.1 (Livebox), 192.168.1.10, 192.168.1.11, 192.168.1.12, 192.168.1.13, 192.168.1.18, 192.168.1.28, and 192.168.1.19. Each report includes the host's MAC address and manufacturer. The scan concludes with 'Nmap done: 256 IP addresses (8 hosts up) scanned in 2.09 seconds'.

```
(balbino@balbino)-[~]  
$ nmap -sn 192.168.1.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 20:55 CEST  
Nmap scan report for Livebox (192.168.1.1)  
Host is up (0.0082s latency).  
MAC Address: 8C:19:B5:FF:E2:1F (Arcadyan)  
Nmap scan report for 192.168.1.10  
Host is up (0.019s latency).  
MAC Address: D8:BC:38:68:01:80 (Espressif)  
Nmap scan report for 192.168.1.11  
Host is up (0.029s latency).  
MAC Address: C0:95:CF:1A:72:C2 (Unknown)  
Nmap scan report for 192.168.1.12  
Host is up (0.023s latency).  
MAC Address: 2C:93:FB:7D:C8:00 (Sercomm France Sarl)  
Nmap scan report for 192.168.1.13  
Host is up (0.0022s latency).  
MAC Address: 2C:08:23:D8:D9:F0 (Sercomm France Sarl)  
Nmap scan report for 192.168.1.18  
Host is up (0.014s latency).  
MAC Address: C8:2E:18:80:A3:00 (Espressif)  
Nmap scan report for 192.168.1.28  
Host is up (0.00039s latency).  
MAC Address: 08:00:27:41:C3:E7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.1.19  
Host is up.  
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.09 seconds
```

2. Enumeración de puertos

Una vez hemos hecho el escaneo de la red, y hemos detectado la ip de la máquina que está actualmente corriendo empezamos a analizar qué puertos

activos tiene máquina:

[illegible]

como podemos ver en esta imagen, he usado el comando `nmap -sV -p-ip_maquina` pero perfectamente podría haber usado un formato grepeable con `-oG - | grep "open"` y vemos únicamente los puertos abiertos.

3. Preparación del entorno

Si queremos obtener más información como nos pide la práctica, usamos el siguiente comando:

```
nslookup ip_victima:
```

```
(balbino@balbino)-[~]  
$ sudo nano /etc/host  
[sudo] password for balbino:  
  
(balbino@balbino)-[~]  
$ nslookup maquina-bwap  
Server:          1.1.1.1  
Address:         1.1.1.1#53  
  
** server can't find maquina-bwap: NXDOMAIN
```

Antes yo he guardado la ip_victima en /etc/host para cada vez que yo haga referencia a la máquina con el nombre maquina_bwap kali entienda que me refiero a la ip de la máquina.

Siguiendo con la práctica usamos el comando whois para seguir recopilando más información de la máquina a la que vamos a atacar:

```
(balbino@balbino)-[~]
$ whois 192.168.1.28

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange:      192.168.0.0 - 192.168.255.255
CIDR:          192.168.0.0/16
NetName:       PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:     NET-192-168-0-0-1
Parent:        NET192 (NET-192-0-0-0-0)
NetType:       IANA Special Use
OriginAS:
Organization:  Internet Assigned Numbers Authority (IANA)
RegDate:       1994-03-15
Updated:       2024-05-24
Comment:       These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment:       These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http://www.iana.org/abuse/answers
Comment:
Comment:       These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:
Comment:       http://datatracker.ietf.org/doc/rfc1918
Ref:           https://rdap.arin.net/registry/ip/192.168.0.0

OrgName:       Internet Assigned Numbers Authority
OrgId:         IANA
Address:       12025 Waterfront Drive
Address:       Suite 300
City:          Los Angeles
StateProv:     CA
PostalCode:    90292
Country:       US
RegDate:
Updated:       2024-05-24
Ref:           https://rdap.arin.net/registry/entity/IANA
```

4. Detección de vulnerabilidades

Una vez ya tenemos toda la información que necesitamos de la máquina probamos a ver que vulnerabilidades tiene, para ellos usamos el comando: `nikto -h ip_victima:`

```
(balbino@balbino) [~] 4geeks.com/es/vulnmap/spain
$ nikto -h 192.168.1.28
- Nikto v2.5.0
-----
+ Target IP: 192.168.1.28
+ Target Hostname: 192.168.1.28
+ Target Port: 80
+ Start Time: 2025-05-06 13:12:15 (GMT2)
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
+ /: Server may leak inodes via ETags, header found with file /, inode: 838422, size: 588, mtime: Sun Nov 2 19:20:2014. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-nvites-cross-site.html
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.bak, index.html. See: http://www.wisec.it/sectou.php?id=468ebdc59d15, https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.2.4-2ubuntu5 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ OpenSSL/0.9.8g appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ mod_ssl/2.2.8 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow remote shell.
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /icons/: Directory indexing found.
+ /README: README file found.
+ /INSTALL.txt: Default file found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time: 2025-05-06 13:12:29 (GMT2) (14 seconds)
-----
+ 1 host(s) tested
```

Clasificando las vulnerabilidades que vemos son:

1.phpMyAdmin expuesto:esto quiere decir que se puede acceder desde internet y la base de datos es visible.

CVE:2018-126313

esto quiere decir que se pueden ver y ejecutar archivos dentro de phpmyadmin

CWE:287

esto quiere decir que no autentica el usuario cuando inicia sesión

CAPEC:137

Se puede inyectar una serie de parámetros es decir sentencias sql o XSS

CVSS:9.8 una nota crítica muy fácil de vulnerar

EPSS:0.976 alta probabilidad de explotación

Posible solución: restringir el acceso al servidor mediante un firewall o modificar el acceso para que solo sea disponible desde localhost, además de actualizar siempre a la última versión.

2.Cross-Site Scripting XSS:se puede inyectar código en formularios que sean vulnerables.

CVE: CVE-2019-8331

esto nos indica problemas con bootstrap el cual es vulnerable a inyección

CWE: CWE-79 (Improper Neutralization of Input During Web Page Generation)

Esto hace que el atacante pueda llegar a vulnerar la página enviando código javascript

CAPEC: CAPEC-63 (XSS)

CVSS: 6.1 una nota media

EPSS: 0.713 altas probabilidades.

Posible solución:usar un framework como podría ser angular,react,ionic,vue,y validar y sanitizar toda la entrada del usuario.

3.Buffer Overflow:cuando una aplicación se desarrolla mal,permite que un atacante pueda escribir fuera del buffer haciendo que pueda ejecutar código.

CVE: CVE-2019-19781 Posible ataque con vectores.

CWE: CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)

CAPEC: CAPEC-100 (Buffer Overflow via Environment Variables)

CVSS: 9.8 Una nota muy alta, quiere decir que está muy expuesto

EPSS: 0.978 Una vía muy fácil de entrar.

Posibles soluciones:usar lenguajes como java o python que tienen un buen manejo de la memoria, además de hacer validación de cada una de los campos.

4.ReverseShell:si un servidor tiene comandos mal filtrados un atacante puede llegar a usar una reverse shell y ejecutar comandos de manera interna.

CVE: CVE-2021-41773 (Apache RCE con path traversal) mediante un path traversal puede llegar a ver todo lo que está en el servidor

CWE: CWE-78 (Improper Neutralization of Special Elements used in an OS Command)

CAPEC: CAPEC-137 (Command Injection)

CVSS: 9.8 Nuevamente una nota muy alta lo que quiere decir que es muy probable atacar por esta vía

EPSS: 0.963 muy vulnerable.

Posible solución: Nunca concatenar entradas de usuario, usar funciones como `exec()` que son más seguras y otra práctica muy buena sería usar IDS/IPS para detectar conexiones sospechosas.

5. Fuerza Bruta y enumeración de archivos/directorios

Una vez sabemos esto, empezamos a probar diccionarios como el de SecList para hacer un ataque de fuerza bruta:

```
(balbino@balbino)~$ gobuster dir -u http://192.168.1.28 -w /home/balbino/SecLists/Discovery/Web-Content/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.1.28
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/balbino/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 374]
/.htpasswd (Status: 403) [Size: 379]
/.htaccess (Status: 403) [Size: 379]
/README (Status: 200) [Size: 2491]
/crossdomain.xml (Status: 200) [Size: 200]
/crossdomain (Status: 200) [Size: 200]
/drupal (Status: 301) [Size: 403] [--> http://192.168.1.28/drupal/]
/evil (Status: 301) [Size: 401] [--> http://192.168.1.28/evil/]
/index.html (Status: 200) [Size: 588]
/index (Status: 200) [Size: 45]
/phpmyadmin (Status: 301) [Size: 407] [--> http://192.168.1.28/phpmyadmin/]
/server-status (Status: 200) [Size: 4816]
/webdav (Status: 301) [Size: 403] [--> http://192.168.1.28/webdav/]
Progress: 4746 / 4747 (99.98%)
=====
Finished
=====
```

```
(balbino@balbino) [~]
$ dirb http://192.168.1.28 /home/balbino/SecLists/Discovery/Web-Content/common.txt

DIRB v2.22
By The Dark Raver

-----
Uso de nslookup:

START_TIME: Tue May 6 14:06:42 2025
URL_BASE: http://192.168.1.28/
WORDLIST_FILES: /home/balbino/SecLists/Discovery/Web-Content/common.txt

-----
Uso de whois:

1. whois <IP de BeeBox>

GENERATED WORDS: 4745

---- Scanning URL: http://192.168.1.28/ ----
+ http://192.168.1.28/README (CODE:200|SIZE:2491)
+ http://192.168.1.28/crossdomain (CODE:200|SIZE:200)
+ http://192.168.1.28/crossdomain.xml (CODE:200|SIZE:200)
=> DIRECTORY: http://192.168.1.28/drupal/
=> DIRECTORY: http://192.168.1.28/evil/
+ http://192.168.1.28/index (CODE:200|SIZE:45)
+ http://192.168.1.28/index.html (CODE:200|SIZE:588)
=> DIRECTORY: http://192.168.1.28/phpmyadmin/
+ http://192.168.1.28/server-status (CODE:200|SIZE:5685)
=> DIRECTORY: http://192.168.1.28/webdav/

-----
Uso de Gobuster:

---- Entering directory: http://192.168.1.28/drupal/ ----
+ http://192.168.1.28/drupal/README (CODE:200|SIZE:5382)
+ http://192.168.1.28/drupal/authorize (CODE:403|SIZE:3056)
+ http://192.168.1.28/drupal/cron (CODE:403|SIZE:7455)
=> DIRECTORY: http://192.168.1.28/drupal/includes/
+ http://192.168.1.28/drupal/index.php (CODE:200|SIZE:7779)
+ http://192.168.1.28/drupal/install (CODE:200|SIZE:3418)
=> DIRECTORY: http://192.168.1.28/drupal/misc/
=> DIRECTORY: http://192.168.1.28/drupal/modules/
=> DIRECTORY: http://192.168.1.28/drupal/profiles/
+ http://192.168.1.28/drupal/robots (CODE:200|SIZE:1550)
+ http://192.168.1.28/drupal/robots.txt (CODE:200|SIZE:1550)
=> DIRECTORY: http://192.168.1.28/drupal/scripts/
=> DIRECTORY: http://192.168.1.28/drupal/sites/
=> DIRECTORY: http://192.168.1.28/drupal/themes/
+ http://192.168.1.28/drupal/update (CODE:403|SIZE:4289)
+ http://192.168.1.28/drupal/web.config (CODE:200|SIZE:2178)
+ http://192.168.1.28/drupal/xmlrpc (CODE:200|SIZE:42)
+ http://192.168.1.28/drupal/xmlrpc.php (CODE:200|SIZE:42)

---- Entering directory: http://192.168.1.28/evil/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.28/phpmyadmin/ ----
+ http://192.168.1.28/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.1.28/phpmyadmin/index.php (CODE:200|SIZE:8122)
```

Con el primer comando que he usado, gobuster, lo que obtenemos son código(200,403), estos nos indican si el archivo es público, es decir un 200 o si el archivo está oculto o prohibido como un 403 o sino existe como sería un 404.

Y con el comando dirb, podemos sacar los directorios accesibles, como serían phpMyAdmin

.htaccess/ o incluso .htpasswd/ las cuales pueden contener alguna contraseña que ponga en jaque al sistema.

Con estos comandos hemos podido comprobar que hay una vulnerabilidad en cuanto a los directorios de tipo CWE-548 (posible exposición)

CAPEC(directory traversal) lo cual es una entrada muy común ya que con un simple “../..” pueden llegar a ver que archivos tiene el servidor.Además de un CWE-538(es posible ver el archivo .htpasswd).

Posible solución: negar el acceso a archivos ocultos del sistema,mover los archivos de directorio, y para el tema de directory traversal hacer que siempre exista un página de index.html o index.php

6. Herramientas utilizadas

Las herramientas que potencialmente hemos usado son:

-nmap:Nos ha servido tanto para averiguar cuál era la ip de nuestra máquina víctima como para sacar los puertos que tenía abiertos.

-whois,nslookup: ambos los hemos usado para saber y obtener más información de que era a lo que queremos atacar,su sistema operativo,su mac etc...

-nikto:con él hemos podido ver las posibles vulnerabilidades existentes en la máquina víctima.

-gobuster,dirb:ambos nos han servido para poder a qué ficheros o archivos podríamos llegar a acceder mediante fuerza bruta.

7. Conclusiones

Tenemos que tener muy claro el patrón a la hora de poder operar con una máquina ya que cualquier mínima duda puede hacer que te llegues a plantear dónde cometiste un fallo y a lo mejor volver a empezar por eso hay que si o si seguir los pasos muy poco a poco y entendiendo muy bien el porque lo estas haciendo y con qué finalidad,gracias a esta práctica he aprendido cual es la manera con la que tengo que actuar para poder llegar a sacar información y como puedo atacar a una máquina.