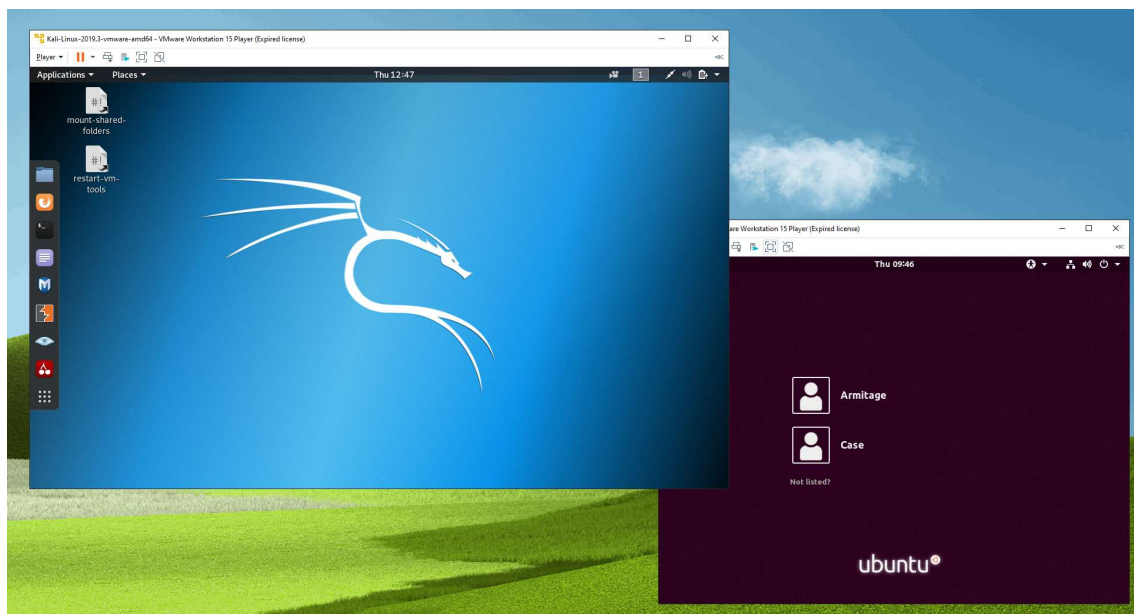


Escape room WGIBSON – Bandera 1

Introducción

Para comenzar, debemos lanzar las dos máquinas virtuales correspondientes, utilizando el programa VMware tal y como se explica en la guía de instalación del entorno para la resolución de la práctica.

De esta manera, deberíamos tener en nuestro ordenador una visión similar a esta:



En la ventana de la izquierda será donde realicemos nuestras acciones para acceder a la información de la máquina de la derecha.

Bandera 1

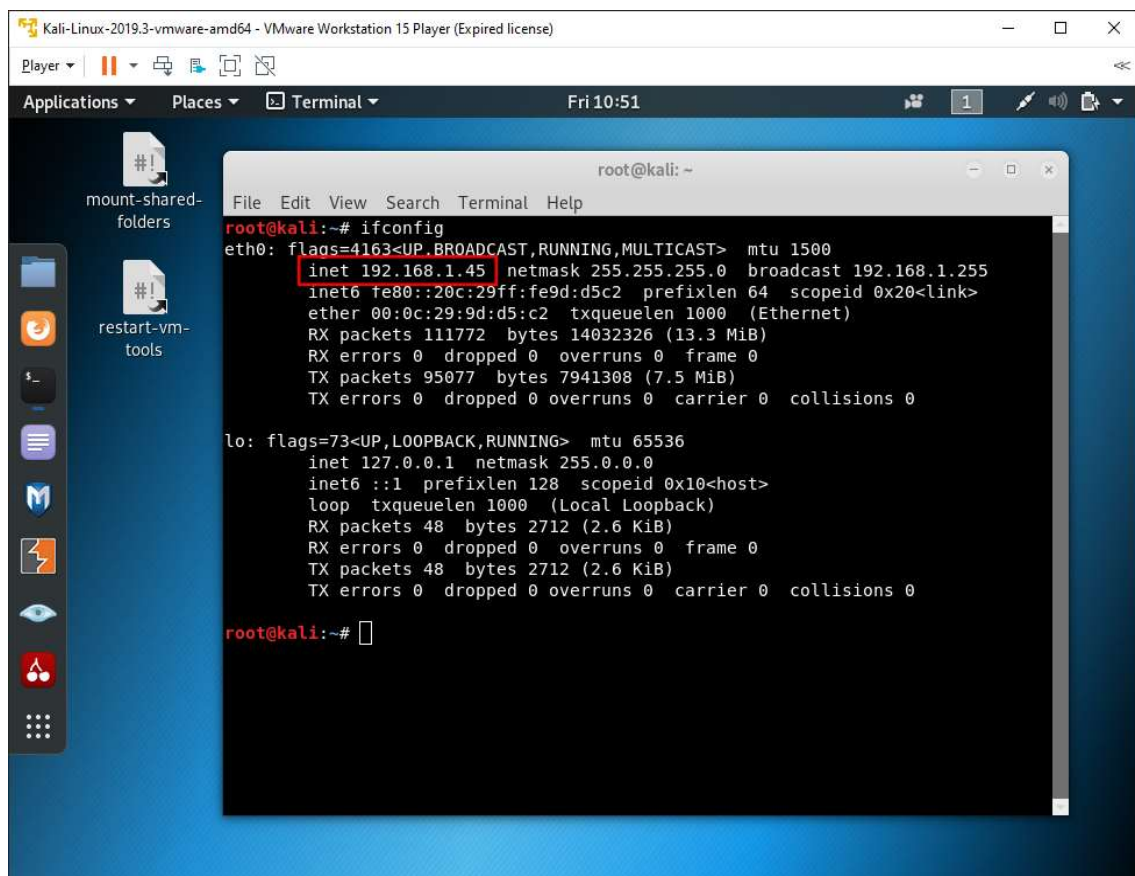
Lo primero que necesitamos saber es la dirección ip de nuestra máquina, para conocer en qué red nos estamos moviendo.

Para ello, abrimos una ventana de terminal y utilizamos el comando **ifconfig**, que nos proporciona información sobre la configuración de las interfaces de red.

Introducimos el comando

ifconfig

y pulsamos enter



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.45 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::20c:29ff:fe9d:d5c2 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:9d:d5:c2 txqueuelen 1000 (Ethernet)  
    RX packets 111772 bytes 14032326 (13.3 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 95077 bytes 7941308 (7.5 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 48 bytes 2712 (2.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 48 bytes 2712 (2.6 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@kali:~#
```

Podemos observar que, en nuestro caso, la dirección es: 192.168.1.45, pero cada alumno podría tener un valor diferente

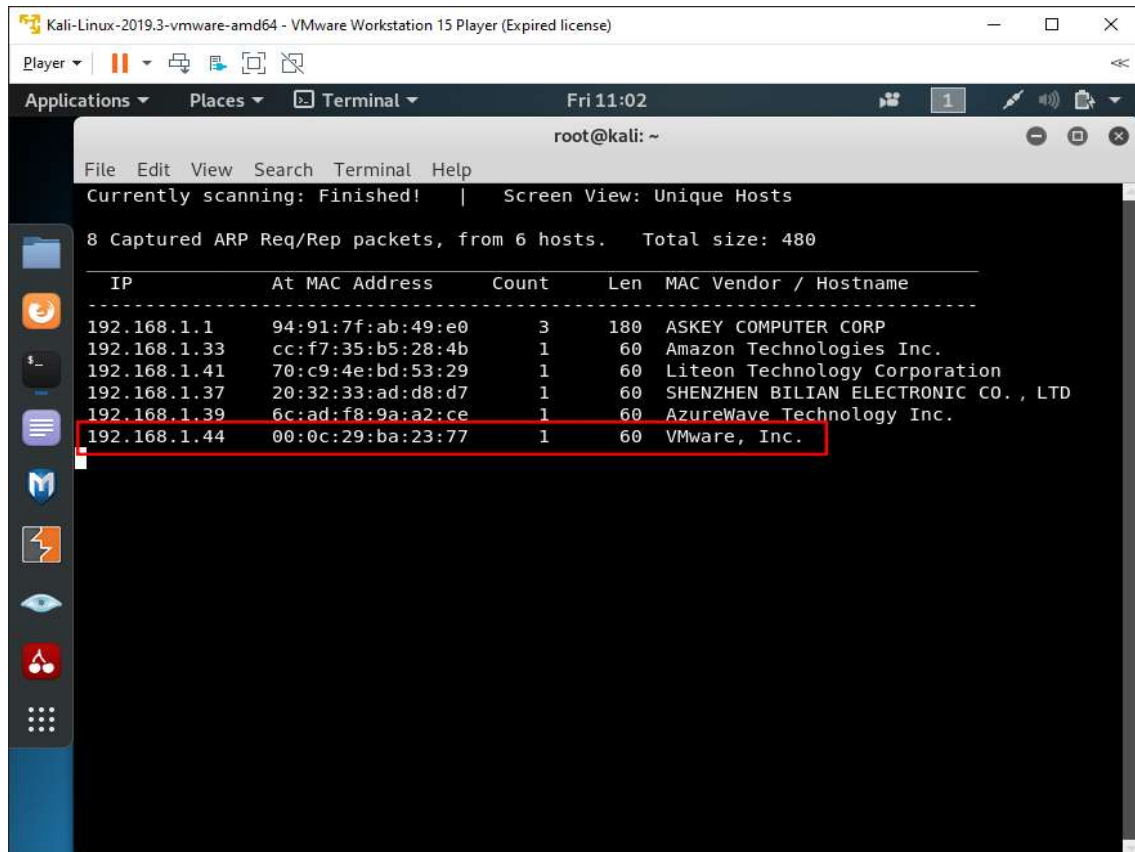
Para descubrir nuestro objetivo, buscaremos máquinas conectadas a nuestra misma red, utilizando el comando **netdiscover**, que realiza un barrido de paquetes ARP en la subred que se indica con el parámetro -r

En nuestro caso queremos analizar la subred 192.168.1.45/24, es decir, todas las direcciones que tengan la forma 192.168.1.xxx

Introducimos el comando

`sudo netdiscover -r [dirección ip]/24`

y pulsamos enter



```
root@kali: ~  
File Edit View Search Terminal Help  
Currently scanning: Finished! | Screen View: Unique Hosts  
8 Captured ARP Req/Rep packets, from 6 hosts. Total size: 480  
-----  
IP           At MAC Address    Count  Len  MAC Vendor / Hostname  
-----  
192.168.1.1   94:91:7f:ab:49:e0    3    180  ASKEY COMPUTER CORP  
192.168.1.33  cc:f7:35:b5:28:4b    1     60  Amazon Technologies Inc.  
192.168.1.41  70:c9:4e:bd:53:29    1     60  Liteon Technology Corporation  
192.168.1.37  20:32:33:ad:d8:d7    1     60  SHENZHEN BILIAN ELECTRONIC CO., LTD  
192.168.1.39  6c:ad:f8:9a:a2:ce    1     60  AzureWave Technology Inc.  
192.168.1.44  00:0c:29:ba:23:77    1     60  VMware, Inc.
```

La dirección IP de la máquina que queremos atacar será la que pertenezca a **VMware**, el resto son diferentes dispositivos que también se encuentran en la red en la que estemos trabajando.

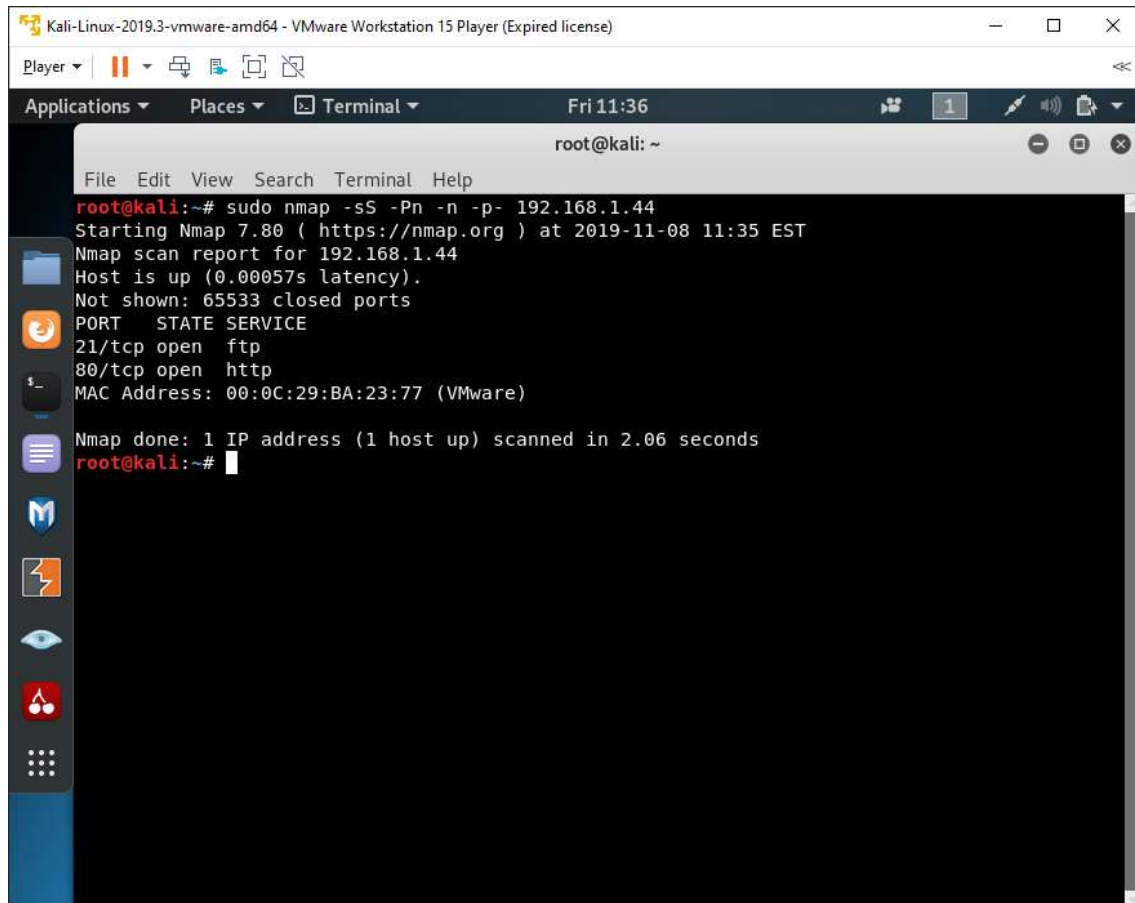
En nuestro caso la dirección sería 192.168.1.44, pero de nuevo, la dirección para cada alumno puede variar.

Una vez conseguido este dato, comenzaremos el análisis de puertos abiertos, que son los que aceptan conexiones TCP o paquetes UDP e indican los servicios disponibles para ser utilizados en una red.

Pulsamos Ctrl+C para dejar de ejecutar el comando anterior e introducimos el comando

```
sudo nmap -sS -Pn -n -p- [dirección ip]
```

y pulsamos enter



```
root@kali:~# sudo nmap -sS -Pn -n -p- 192.168.1.44
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-08 11:35 EST
Nmap scan report for 192.168.1.44
Host is up (0.00057s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
MAC Address: 00:0C:29:BA:23:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
root@kali:~#
```

Como se puede apreciar, en este caso los puertos abiertos son el **puerto 21 y 80**.

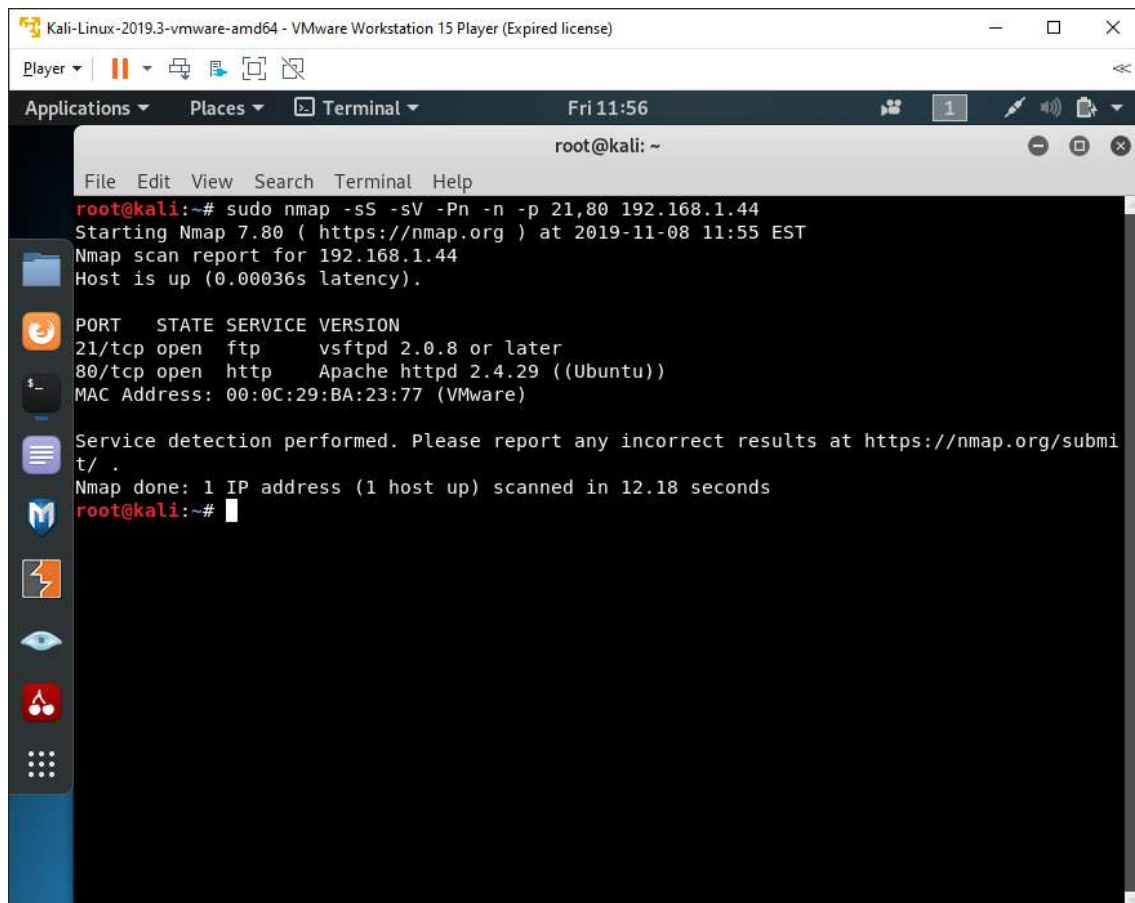
El siguiente paso es analizar los servicios que funcionan en los puertos abiertos que hemos descubierto y sus respectivas versiones.

Para esto utilizaremos el mismo comando **nmap** pero añadiendo el parámetro **-sV** y especificando los puertos a analizar mediante **-p 21,80**

Introducimos el comando

```
sudo nmap -sS -sV -Pn -n -p 21,80 [dirección ip]
```

y pulsamos enter



```
root@kali:~# sudo nmap -sS -sV -Pn -n -p 21,80 192.168.1.44
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-08 11:55 EST
Nmap scan report for 192.168.1.44
Host is up (0.00036s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 00:0C:29:BA:23:77 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 12.18 seconds
root@kali:~#
```

Se puede observar que en el puerto 21 funciona un servicio de FTP de vsftpd en la versión 2.0.8 y que en el puerto 80 funciona el servidor http Apache 2.4.29

Ahora evaluaremos las vulnerabilidades en estos servicios a través de los scripts de automatización de **nmap**, una de sus funciones más poderosas y flexibles.

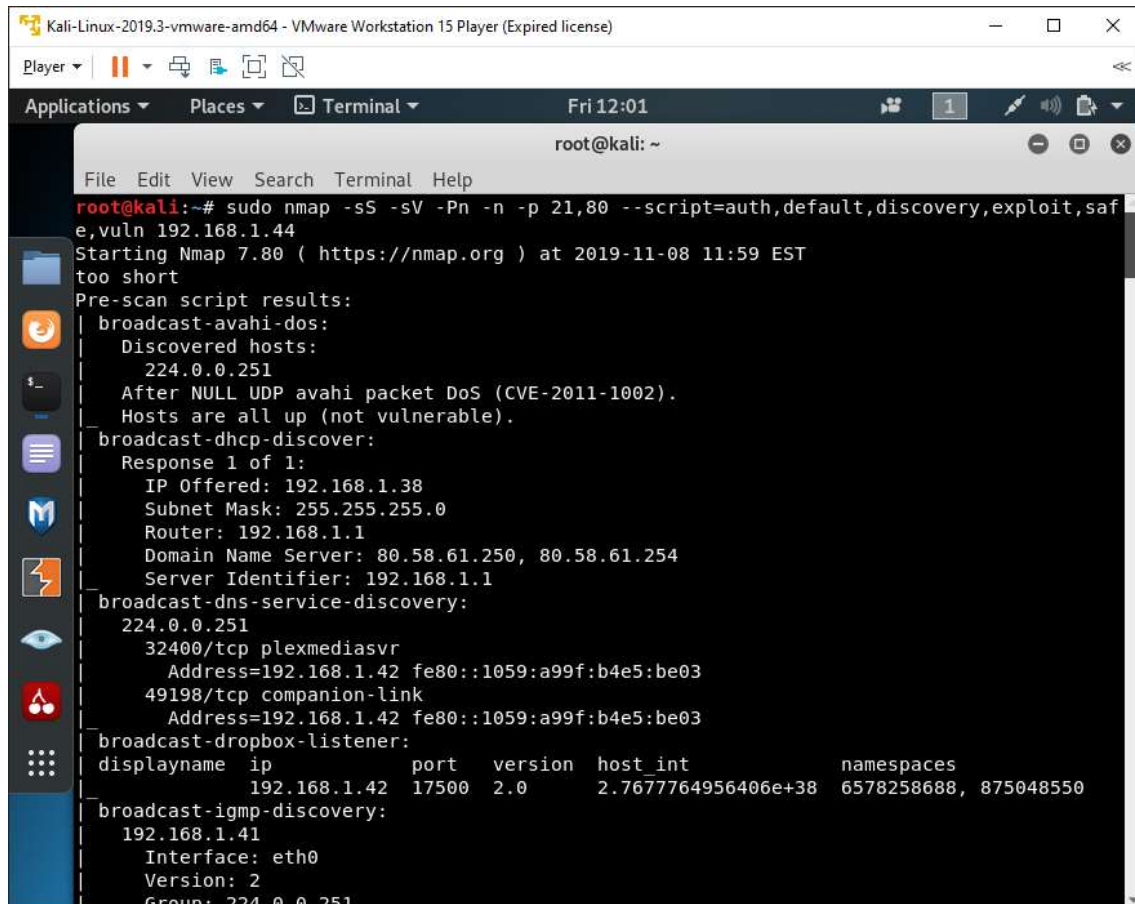
Utilizaremos de nuevo el comando **nmap** en los mismos puertos, añadiendo esta vez los parámetros de los scripts correspondientes. En este caso utilizaremos **default**, con un conjunto de scripts por defecto, **auth** para evaluar la autenticación, **discovery** para descubrir más sobre la red, **exploit** para descubrir vulnerabilidades de ese tipo, **safe** para obtener datos generales de la red y **vuln** para vulnerabilidades específicas.

Introducimos el comando

```
sudo nmap -sS -sV -Pn -n -p 21,80 --
script=auth,default,discovery,exploit,safe,vuln [dirección ip]
```

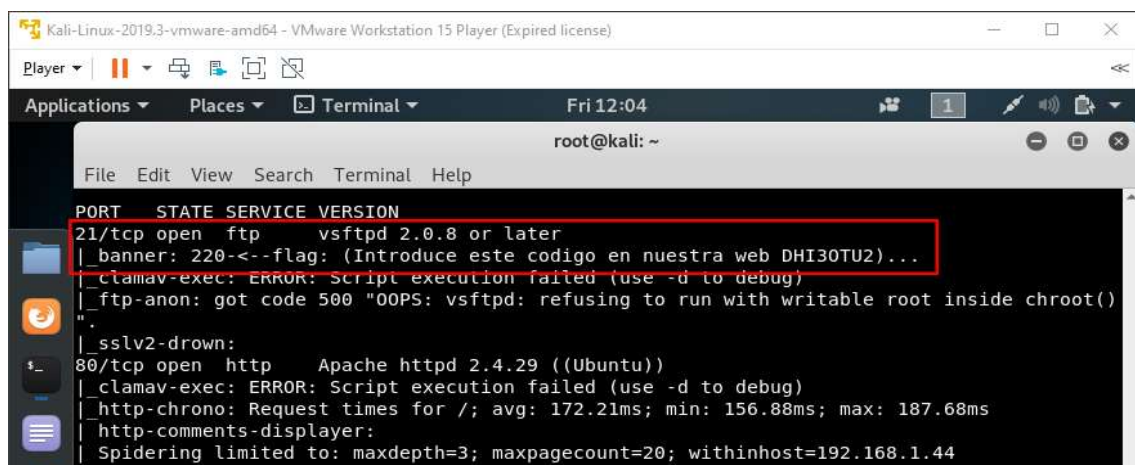
y pulsamos enter

Esperamos un tiempo hasta que se ejecuten todos los scripts y obtendremos una gran cantidad de información que tendremos que revisar.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sudo nmap -sS -sV -Pn -n -p 21,80 --script=auth,default,discovery,exploit,safe,vuln 192.168.1.44  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-08 11:59 EST  
too short  
Pre-scan script results:  
| broadcast-avahi-dos:  
|   Discovered hosts:  
|     224.0.0.251  
|   After NULL UDP avahi packet DoS (CVE-2011-1002).  
|   Hosts are all up (not vulnerable).  
| broadcast-dhcp-discover:  
|   Response 1 of 1:  
|     IP Offered: 192.168.1.38  
|     Subnet Mask: 255.255.255.0  
|     Router: 192.168.1.1  
|     Domain Name Server: 80.58.61.250, 80.58.61.254  
|     Server Identifier: 192.168.1.1  
| broadcast-dns-service-discovery:  
|   224.0.0.251  
|     32400/tcp plexmediasvr  
|       Address=192.168.1.42 fe80::1059:a99f:b4e5:be03  
|     49198/tcp companion-link  
|       Address=192.168.1.42 fe80::1059:a99f:b4e5:be03  
| broadcast-dropbox-listener:  
|   displayname ip port version host int namespaces  
|   192.168.1.42 17500 2.0 2.7677764956406e+38 6578258688, 875048550  
| broadcast-igmp-discovery:  
|   192.168.1.41  
|     Interface: eth0  
|     Version: 2  
|     Group: 224 0 0 251
```

Buscamos en la salida de los resultados de análisis de las vulnerabilidades la parte relativa al puerto TCP abierto para el protocolo FTP, que se utiliza para la transferencia de archivos.



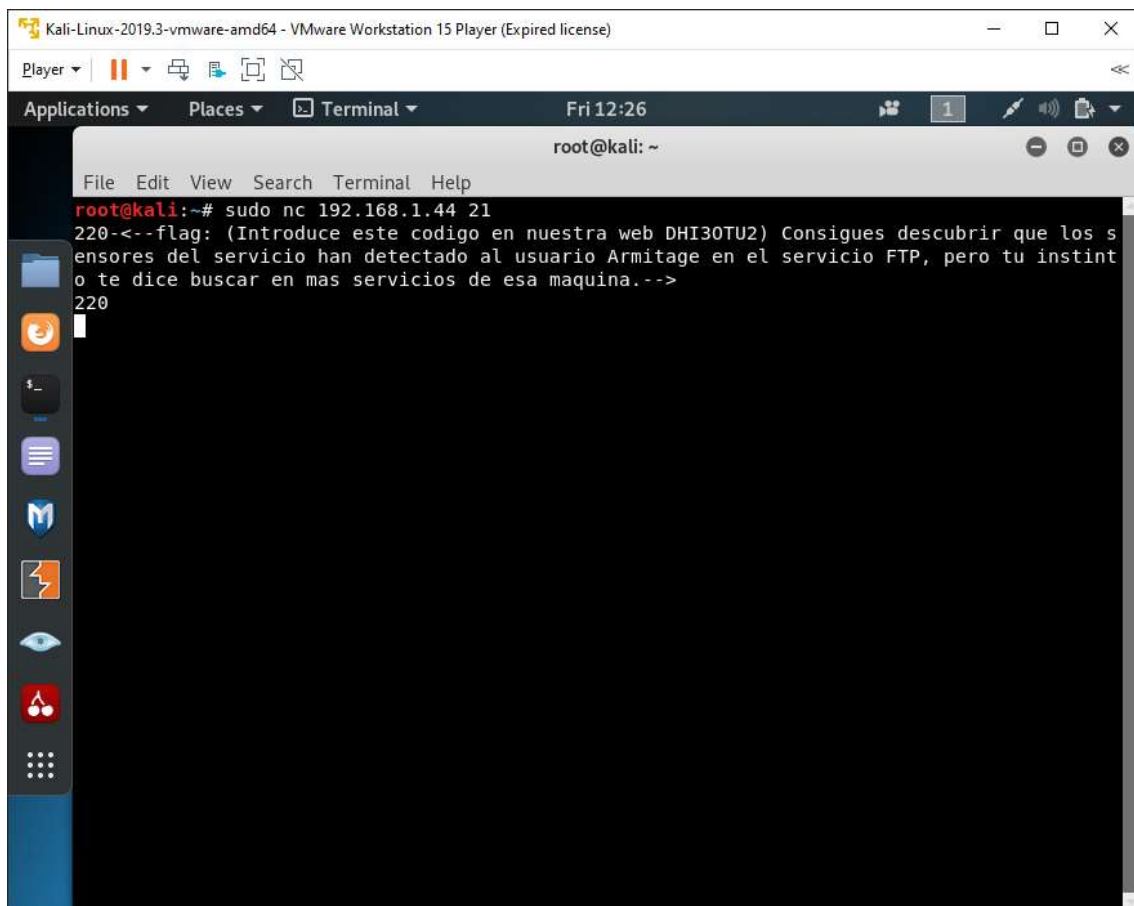
```
PORT STATE SERVICE VERSION  
21/tcp open  ftp      vsftpd 2.0.8 or later  
|_ banner: 220-<-flag: (Introduce este codigo en nuestra web DHI30TU2)...  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
|_ ftp-anon: got code 500 "OOPS: vsftpd: refusing to run with writable root inside chroot()"  
|_  
|_ sslv2-drown:  
80/tcp open  http      Apache httpd 2.4.29 ((Ubuntu))  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
|_ http-chrono: Request times for /; avg: 172.21ms; min: 156.88ms; max: 187.68ms  
|_ http-comments-displayer:  
|_ Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.44
```


Para poder conectarnos al puerto 21 del protocolo TCP, donde está funcionando el servicio FTP, utilizaremos la aplicación **netcat**, pasándole como parámetros la dirección IP y el número de puerto. De esta forma podremos ver el contenido completo de la bandera.

Introducimos el comando

```
sudo nc [direccion ip] 21
```

y pulsamos enter



```
Kali-Linux-2019.3-vmware-amd64 - VMware Workstation 15 Player (Expired license)
Player
Applications Places Terminal Fri 12:26
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo nc 192.168.1.44 21
220-<--flag: (Introduce este codigo en nuestra web DHI30TU2) Consigues descubrir que los s
ensores del servicio han detectado al usuario Armitage en el servicio FTP, pero tu instint
o te dice buscar en mas servicios de esa maquina.-->
220
```

CÓDIGO BANDERA 1: DHI30TU2

Utilizaremos la combinación de teclas **ctrl+c** para salir y cerrar la conexión por el momento, ya que aún no conocemos el usuario y contraseña correspondientes.