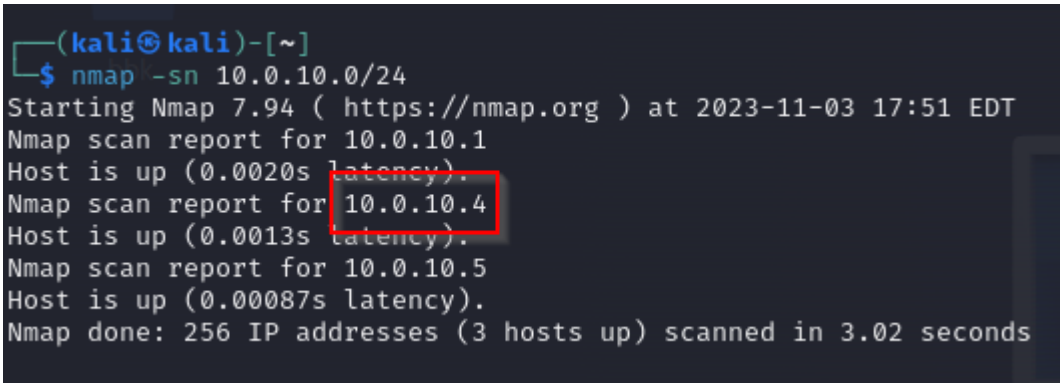
Ejercicios Nmap

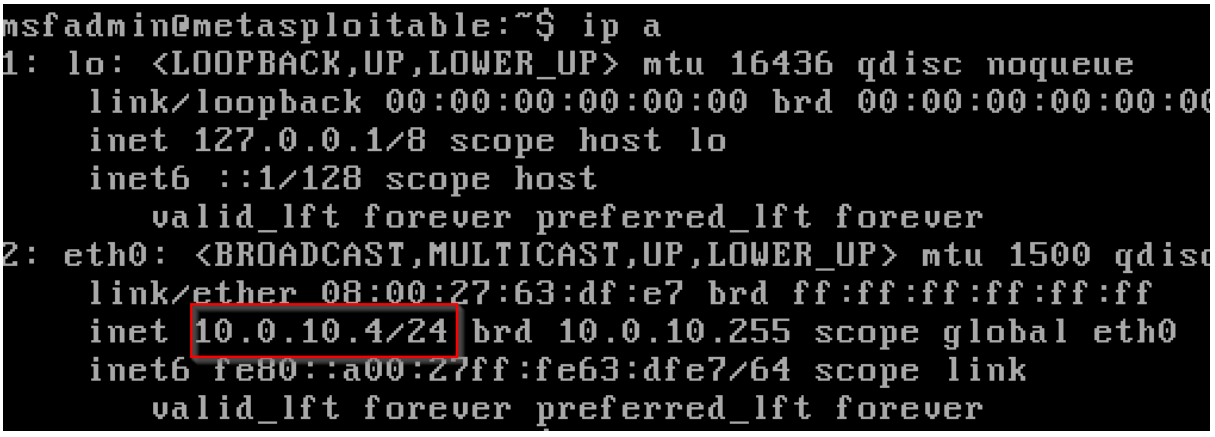
Ejercicio 1

Descubre los equipos conectados a la Red NAT 10.0.2.X-255 o 10.0.2.X/24
Comprueba que la IP de la máquina Metasploitable2 aparece

IPs en la red resaltando la de metasploitable:



Comprobación en la maquina metasploitable:



Ejercicio 2

Con los siguientes parámetros realizo un escaneo con nmap.

con -p- indico que se escaneen todos los puertos.

con -A que haga un descubrimiento de sistema operativo, detención de versión, escaneo con scripts de reconocimiento y traceroute.

con -T indico el tipo de timing template, hay diferentes niveles del 0 al 5 según el tipo de agresividad del escaneo.

```
nmap -A -T4 -p- 10.0.10.4
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 17:55 El
Nmap scan report for 10.0.10.4
Host is up (0.024s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.10.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (pr
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/or
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
```

```
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE
|_ssl-date: 2023-11-03T21:57:33+00:00; 0s from scanner time.
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      46875/tcp   mountd
|   100005  1,2,3      51887/udp   mountd
|   100021  1,3,4      39221/tcp   nlockmgr
|   100021  1,3,4      59182/udp   nlockmgr
|   100024  1          34006/tcp   status
|_  100024  1          37969/udp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: \
445/tcp   open  Detbios-�         Samba smbd 3.0.20-Debian (v
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
```

```
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, Support
|   Status: Autocommit
|_  Salt: K(&$~q?&>CwPh9&P?,\j
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/or
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-11-03T21:57:33+00:00; 0s from scanner time.
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:07:31
|   source ident: nmap
|   source host: AECBB81B.2B121274.7B559A54.IP
|_  error: Closing Link: ugglqkpdk[10.0.10.5] (Quit: ugglqkpd
6697/tcp  open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:07:32
```

```
|   source ident: nmap
|   source host: AECBB81B.2B121274.7B559A54.IP
|_  error: Closing Link: elmukjnmg[10.0.10.5] (Quit: elmukjnm
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr
34006/tcp open  status      1 (RPC #100024)
39221/tcp open  nlockmgr    1-4 (RPC #100021)
46875/tcp open  mountd      1-3 (RPC #100005)
49438/tcp open  java-rmi    GNU Classpath grmiregistry
Service Info: Hosts:  metasploitable.localdomain, irc.Metaspl

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-11-03T17:57:24-04:00
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknow

Service detection performed. Please report any incorrect resu
Nmap done: 1 IP address (1 host up) scanned in 141.90 seconds
```

Ejercicio 3 y 5

Puerto: 21

Estado: Abierto

Servicio: Ftp

Versión: vsftpd 2.3.4

Descripción:

El Protocolo de transferencia de archivos (FTP) es un protocolo de red estándar que se utiliza para la transferencia de archivos informáticos entre un cliente y un servidor en una red informática.

Para esta versión de ftp existe un exploit de ejecución de comandos:

https://www.exploit-db.com/exploits/49757

Puerto: 22

Estado: Abierto

Servicio: ssh

Versión: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

Descripción:

SSH es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

Para esta versión de ssh existe un exploit que realiza un ataque de fuerza bruta hasta obtener unas credenciales validas.

Puerto: 23

Estado: Abierto

Servicio: telnet

Versión: Linux telnetd

Descripción:

Telnet es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente.

Este protocolo se puede explotar a través de un modulo de metasploit realizando un ataque de fuerza bruta con un diccionario tanto para usuarios como contraseñas.

Puerto: 25

Estado: Abierto

Servicio: smtp

Versión: Postfix smtpd

Descripción:

El Protocolo Simple de Transferencia de Correo es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

Se pueden obtener nombres de usuarios validos a traves de la herramienta smpt-users-enum o utilizando un modulo de metasploit.

Puerto:53

Estado: Abierto

Servicio: Dominio

Versión: ISC BIND 9.4.2

Descripción:

Es utilizado para servicios DNS, este protocolo permite utilizar tanto TCP como UDP para la comunicación con los servidores DNS.

Existe un modulo en metasploit con el que poder explotar esta versión.

https://www.exploit-db.com/exploits/6122

Puerto: 80

Estado: Abierto

Servicio: http

Versión: Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Descripción:

Es el protocolo de comunicación que permite las transferencias de información a través de archivos en la World Wide Web.

Puerto: 111

Estado: Abierto

Servicio: rpcbind

Versión: 2 (RPC #100000)

Descripción:

Proporciona información entre sistemas basados en Unix. El puerto a menudo es sondeado, se puede utilizar para identificar el sistema operativo Nix y para obtener información sobre los servicios disponibles. Puerto utilizado con NFS, NIS o cualquier servicio basado en rpc.

Puerto: 139

Estado: Abierto

Servicio: netbios-ssn

Versión: Samba smbd 3.X - 4.X

Descripción:

Es un protocolo de aplicación para compartir recursos en red. Se encarga de establecer la sesión y mantener las conexiones.

Hay un modulo en metasploit que permite la ejecucion arbitraria de codigo sin autenticacion para esta versión de samba.

https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/

Puerto: 445

Estado: Abierto

Servicio: netbios-ssn

Versión: Samba smbd 3.0.20-Debian

Descripción:

Funciona igual que el puerto 139 y se utiliza para compartir archivos en una red.

Puerto: 512

Estado: Abierto

servicio: exec

Versión: netkit-rsh rexecd

Descripción: Este puerto segun el servicio y su version indica el acceso a una shell remota de la maquina metasploitable a traves de una herramienta de nuestro kali podemos acceder a esta shell indicando un usuario y la ip.

Puerto: 513

Estado: Abierto

servicio: login

Version: OpenBSD or Solaris rlogind

Descripcion:

Este servicio era utilizado principalmente en los viejos tiempos para la administración remota, pero ahora debido a problemas de seguridad, este servicio ha sido reemplazado por el slogin y el ssh.

Puerto: 514

Estado: Abierto

servicio: tcpwrapped

Version:

Descripcion:

es un sistema de red ACL que trabaja en terminales y que se usa para filtrar el acceso de red a servicios de protocolos de Internet

Puerto: 1099

Estado: Abierto

Servicio: java-rmi

Version: GNU Classpath grmiregistry

Descripción:

RMI es un mecanismo ofrecido por Java para invocar un método de manera remota. Forma parte del entorno estándar de ejecución de Java y proporciona un mecanismo simple para la comunicación de servidores en aplicaciones distribuidas basadas exclusivamente en Java.

Puerto: 1524

Estado: Abierto

Servicio: bindshell

Version: Metasploitable root shell

Descripcion: Este puerto y servicio que corre la maquina da acceso a una shell en la cual se puede ejecutar comandos del sistema.

Puerto: 2049

Estado: Abierto

Servicio: nfs

Version: 2-4 (RPC #100003)

Descripción:

Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.

Puerto: 2121

Estado: Abierto

Servicio: ftp

Version: ProFTPD 1.3.1

Descripcion:

El Protocolo de transferencia de archivos (FTP) es un protocolo de red estándar que se utiliza para la transferencia de archivos informáticos entre un cliente y un servidor en una red informática.

A través de metasploit se puede hacer un ataque de fuerza bruta al servicio para obtener credenciales validas de inicio de sesión.

Puerto: 3306

Estado: Abierto

Servicio: mysql

Versión: MySQL 5.0.51a-3ubuntu5

Descripción:

sistema de gestión de bases de datos relacional, se puede realizar un ataque de fuerza bruta con diccionario al login para obtener credenciales validas y acceder a la base de datos.

Puerto: 3632

Estado: Abierto

Servicio: distccd

Version: distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

Descripcion:

Distcc está diseñado para acelerar la compilación aprovechando la potencia de procesamiento no utilizada en otros equipos. Una máquina con distcc instalado puede enviar código para ser compilado a través de la red a una computadora que tenga el servicio distccd y un compilador compatible instalado.

Hay un modulo en metasploit que permite la ejecucion de comandos a traves de este servicio.

Puerto: 5432

Estado: Abierto

Servicio: postgresql

Versión: PostgreSQL DB 8.3.0 - 8.3.7

Descripción:

Es un sistema de gestión de bases de datos relacional orientado a objetos y de código abierto.

Se puede utilizar un modulo de metasploit para realizar un ataque de fuerza bruta y obtener credenciales, luego con estas credenciales se puede obtener una shell meterpreter.

Puerto: 5900

Estado: Abierto

Servicio: vnc

Version: VNC (protocol 3.3)

Descripcion:

VNC es un programa de software libre basado en una estructura cliente-servidor que permite observar las acciones del ordenador servidor remotamente a través de un ordenador cliente.

Puerto: 6000

Estado: Abierto

Servicio: X11

Descripción:

es un sistema de ventanas, común en sistemas operativos del tipo UNIX, Existe un modulo en metasploit con el que poder explotar este servicio.

Puerto: 6667 y 6697

Estado: Abierto

Servicio: irc

Versión: Unreal3.2.8.1.

Descripción:

IRC es un protocolo de comunicación en tiempo real, esta versión se puede explotar a traves de un modulo de metasploit.

Puerto: 8009

Estado: Abierto

Servicio: aip13

Versión: Apache Jserv (Protocol v1.3)

Descripción:

permite enviar solicitudes desde un servidor web a un servidor de aplicaciones que se encuentra detrás del servidor web.

Esta version permite la lectura de ficheros del sistema.

https://www.exploit-db.com/exploits/48143

Puerto: 8180

Estado: Abierto

Servicio: http

Version: Apache Tomcat/Coyote JSP engine 1.1

Descripción: Tomcat es un gestor de contenido web el cual se puede enumerar y explotar a través de diferentes módulos de metasploit.

Puerto: 8787

Estado: Abierto

Servicio: drb

Version: Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

Descripcion:

la abreviacion drb quiere decir Distributed Ruby Service, existe un modulo en metasploit con el que explotar este servicio.

Puerto: 34006

Estado: Abierto

Servicio: status

Version: 1 (RPC #100024)

Descripcion:

La version nos muestra un RPC que es un servicio que se asegura de que el cliente llegue al puerto correcto, lo cual significa que mapea las solicitudes RPC del cliente a los servicios correctos.

Puerto: 39221

Estado: Abierto

Servicio: nlockmgr

Version: 1-4 (RPC #100021)

Descripción:

nlockmgr es el gestor de bloqueo para los Sistemas de Archivos de Red (NFS).

Puerto: 46875

Estado: Abierto

Servicio: mountd

Version: 1-3 (RPC #100005)

Descripcion:

gestiona solicitudes de montaje de sistema de archivos desde sistemas remotos y proporciona control de acceso

Puerto: 49438

Estado: Abierto

Servicio: java-rmi

Versión: GNU Classpath grmiregistry

Descripción:

Es un mecanismo ofrecido por Java para invocar un método de manera remota.

Existe un modulo de metasploit para explotar la versiond de este servicio.

Ejercicio 4

```
sudo nmap -O 10.0.10.4
```

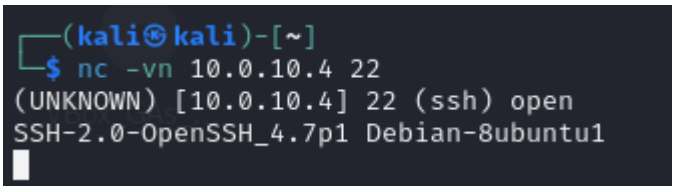
para obtener información a cerca del sistema operativo utilizo la flag -O.

```
8180/tcp open  unknown
MAC Address: 08:00:27:63:DF:E7 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

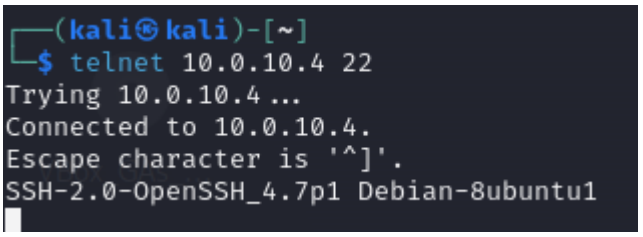
Ejercicio 5

Para obtener la versión de ssh que corre la maquina ejecuto el siguiente comando:

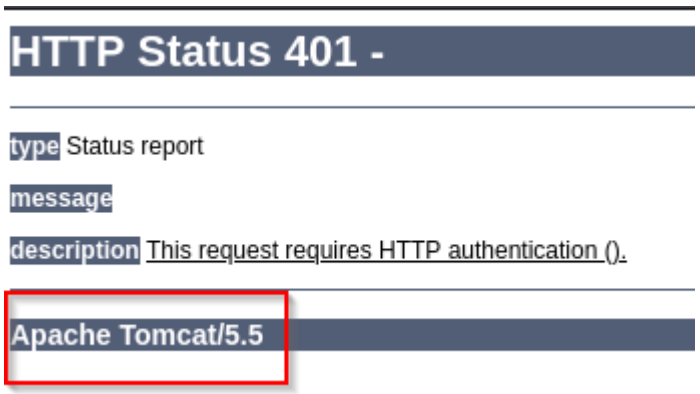
```
nc -vn 10.0.10.4 22
```

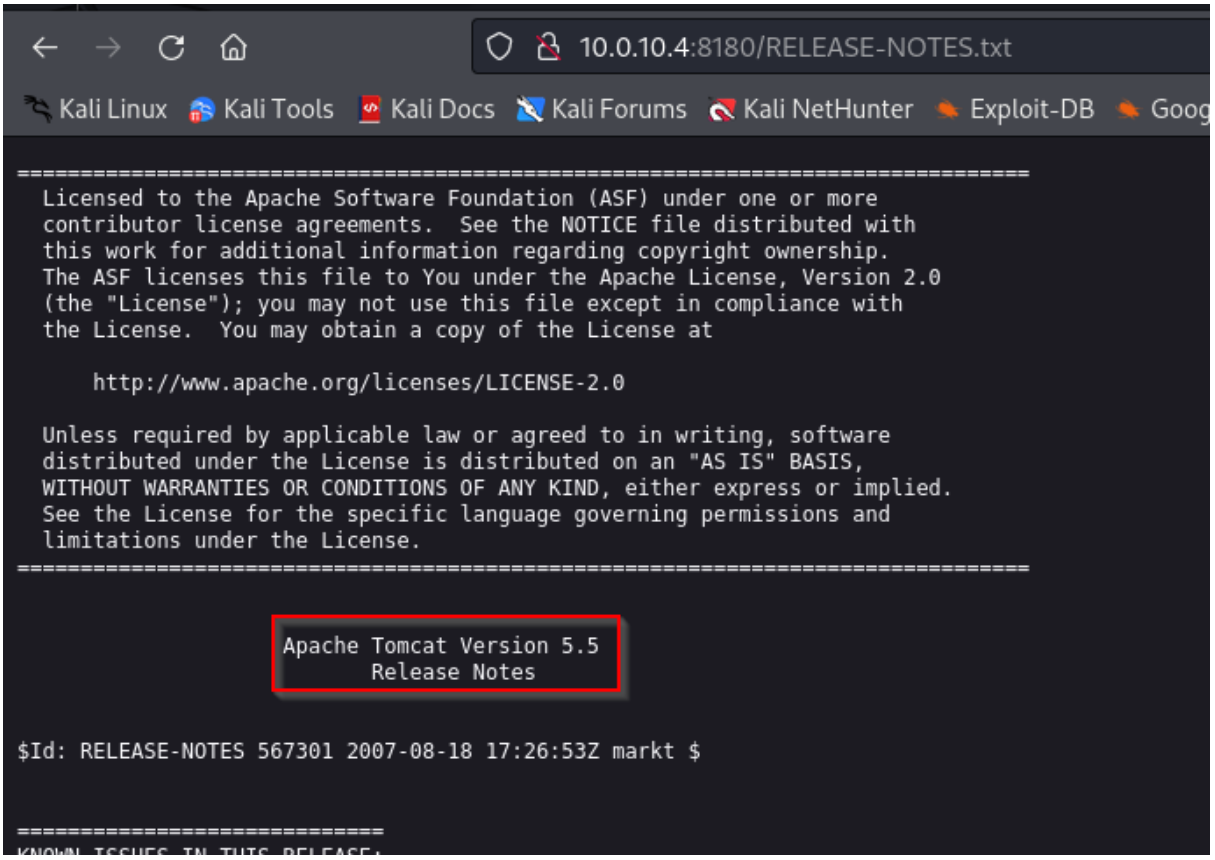


Con telnet



A través del navegador web si buscamos el puerto 8180 en el buscador aparece una pagina de apache tomcat, si provocamos un error nos aparece la versión de este o si clicamos en release-notes también nos aparecerá la versión.


HTTP Status 401 -
type Status report
message
description This request requires HTTP authentication ().
Apache Tomcat/5.5


10.0.10.4:8180/RELEASE-NOTES.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
Apache Tomcat Version 5.5
Release Notes
$Id: RELEASE-NOTES 567301 2007-08-18 17:26:53Z markt $