Actividad práctica número 3:

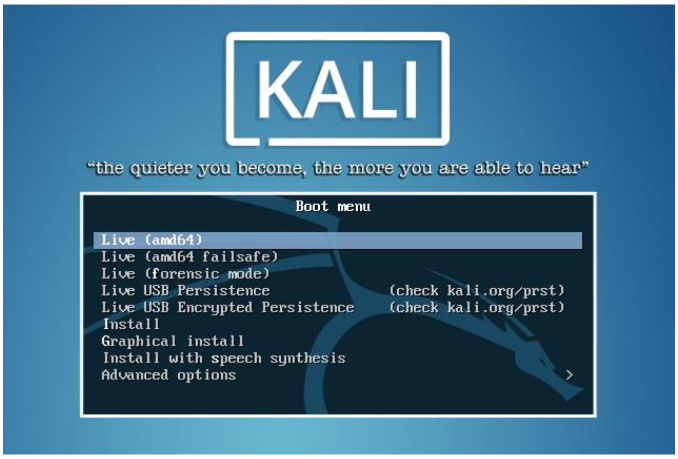
Formato: Individual.

Asignatura: Seguridad de Sistemas

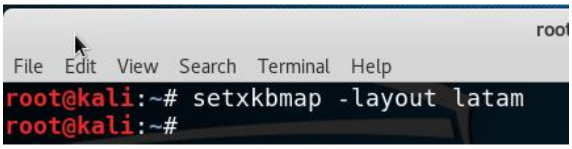
Título: Reconocimiento Activo

A.- Reconocimiento con Kali

1.- Levante la máquina virtual Kali, con la interfaz de red en modo Red NAT


KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options ›

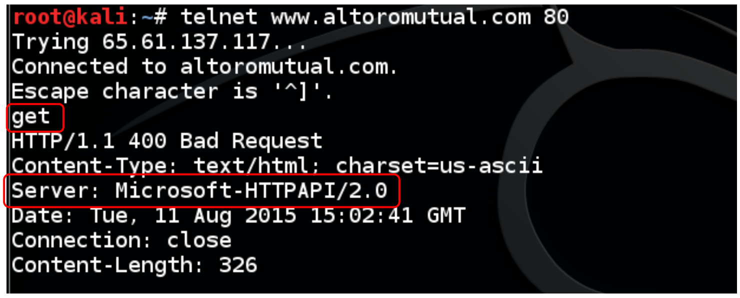
2.- Configure el teclado en español (Latinoamericano), con el siguiente comando:



```
root@kali:~# setxkbmap -layout latam
root@kali:~#
```

3.- Abra una interfaz de comandos y ejecute lo siguiente:

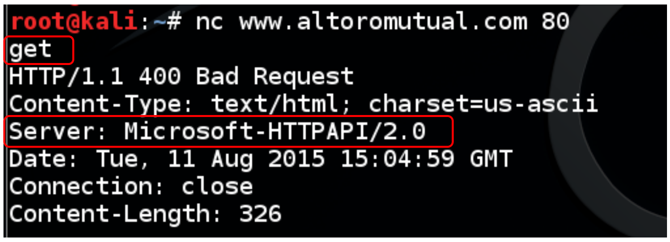
telnet www.altoromutual.com 80



```
root@kali:~# telnet www.altoromutual.com 80
Trying 65.61.137.117...
Connected to altoromutual.com.
Escape character is '^]'.
get
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 11 Aug 2015 15:02:41 GMT
Connection: close
Content-Length: 326
```

4.- Repita el mismo ejercicio utilizando la aplicación netcat

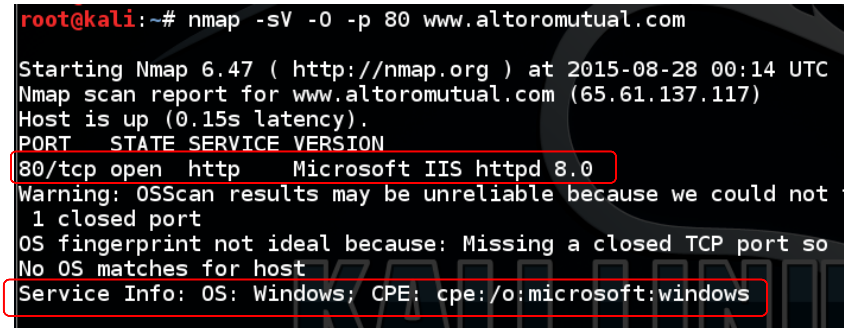
nc www.altoromutual.com 80



```
root@kali:~# nc www.altoromutual.com 80
get
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 11 Aug 2015 15:04:59 GMT
Connection: close
Content-Length: 326
```

5.- Repita el mismo ejercicio con la aplicación nmap

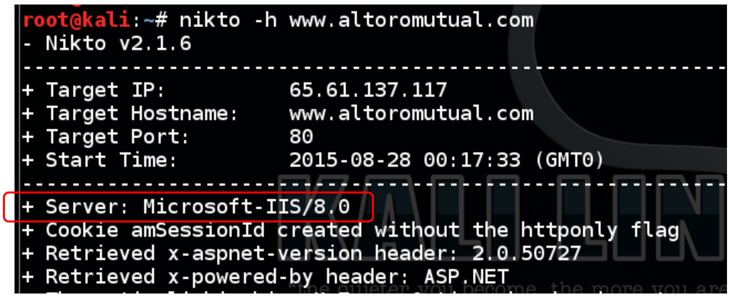
nmap –sV –O –p 80 www.altoromutual.com



```
root@kali:~# nmap -sV -O -p 80 www.altoromutual.com

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-28 00:14 UTC
Nmap scan report for www.altoromutual.com (65.61.137.117)
Host is up (0.15s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 8.0
Warning: OSScan results may be unreliable because we could not
 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so
No OS matches for host
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

6.- Repita el mismo ejercicio con la aplicación nikto

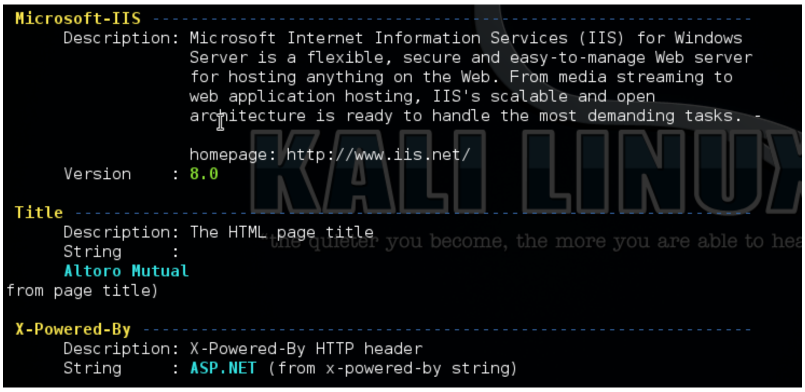
nikto –h www.altoromutual.com



```
root@kali:~# nikto -h www.altoromutual.com
- Nikto v2.1.6
---------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    www.altoromutual.com
+ Target Port:        80
+ Start Time:         2015-08-28 00:17:33 (GMT0)
---------------------------------------------------------------
+ Server: Microsoft-IIS/8.0
+ Cookie amSessionId created without the httponly flag
+ Retrieved x-aspnet-version header: 2.0.50727
+ Retrieved x-powered-by header: ASP.NET
```

7.- Repita el ejercicio con la aplicación whatweb

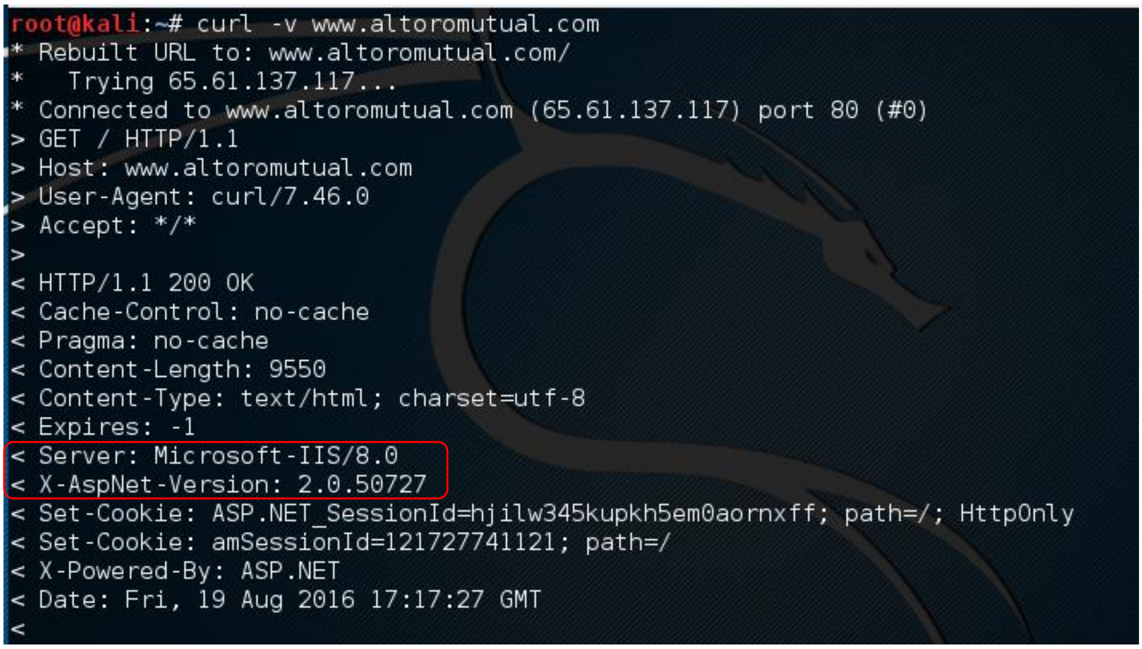
# whatweb –v www.altoromutual.com



```
 Microsoft-IIS ---------------------------------------------------------------
      Description: Microsoft Internet Information Services (IIS) for Windows
                   Server is a flexible, secure and easy-to-manage Web server
                   for hosting anything on the Web. From media streaming to
                   web application hosting, IIS's scalable and open
                   architecture is ready to handle the most demanding tasks. -

                   homepage: http://www.iis.net/
      Version    : 8.0

 Title ----------------------------------------------------------------------
      Description: The HTML page title
      String     :
      Altoro Mutual
from page title)

 X-Powered-By ---------------------------------------------------------------
      Description: X-Powered-By HTTP header
      String     : ASP.NET (from x-powered-by string)
```

8.- Realice nuevamente la operación con la aplicación CURL

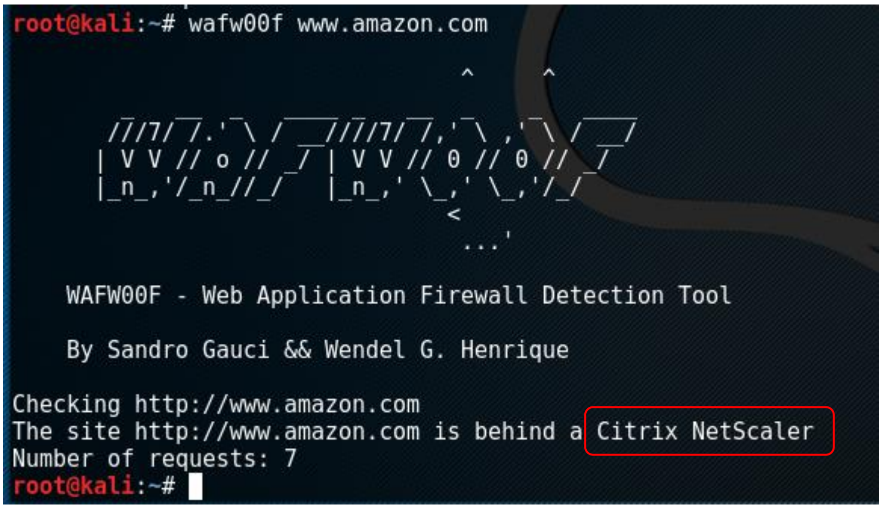
curl –v www.altoromutual.com



```
root@kali:~# curl -v www.altoromutual.com
* Rebuilt URL to: www.altoromutual.com/
*   Trying 65.61.137.117...
* Connected to www.altoromutual.com (65.61.137.117) port 80 (#0)
> GET / HTTP/1.1
> Host: www.altoromutual.com
> User-Agent: curl/7.46.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Cache-Control: no-cache
< Pragma: no-cache
< Content-Length: 9550
< Content-Type: text/html; charset=utf-8
< Expires: -1
< Server: Microsoft-IIS/8.0
< X-AspNet-Version: 2.0.50727
< Set-Cookie: ASP.NET_SessionId=hjilw345kupkh5em0aornxff; path=/; HttpOnly
< Set-Cookie: amSessionId=121727741121; path=/
< X-Powered-By: ASP.NET
< Date: Fri, 19 Aug 2016 17:17:27 GMT
<
```

9.- Aplique el siguiente comando para descubrir si el sitio está protegido con algún “Web Application Firewall”

#wafw00f *URL*

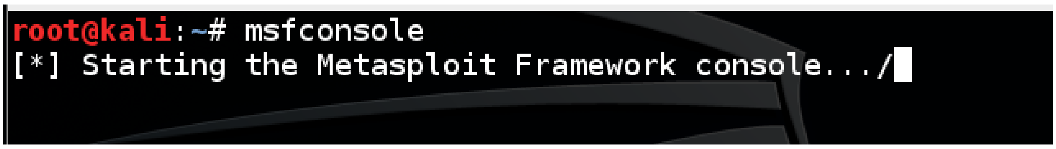


```
root@kali:~# wafw00f www.amazon.com

                                 ^     ^
        _   __  _   ____ _   __  _    _   ____
       ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
      | V V // o // _/ | V V // 0 // 0 // _/
      |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://www.amazon.com
The site http://www.amazon.com is behind a Citrix NetScaler
Number of requests: 7
root@kali:~#
```

<u>Metasploit:</u>

1.- Inicie la aplicación metasploit en su máquina Kali con el siguiente comando:

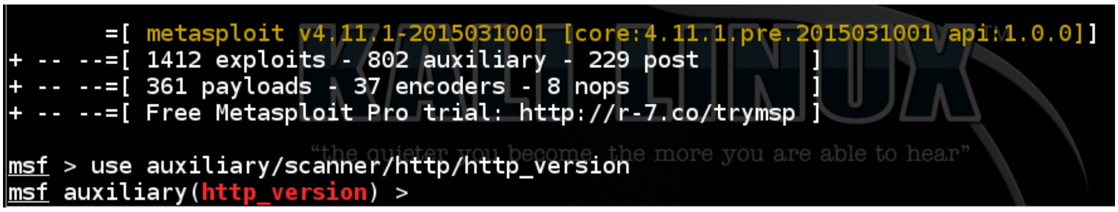
msfconsole



```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console.../
```

2.- Cargue el módulo auxiliar con el siguiente comando:

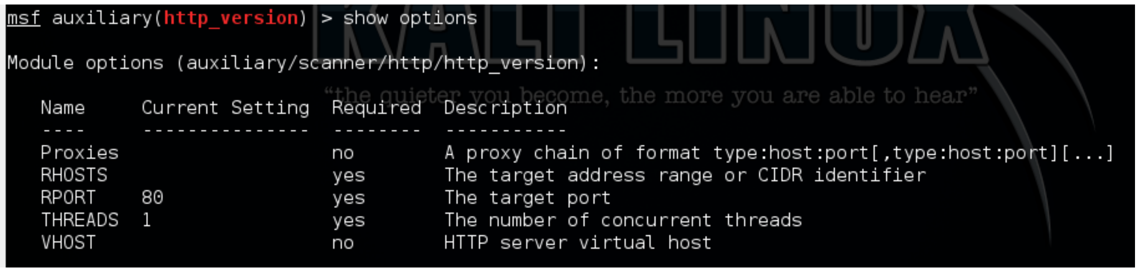
msf> use auxiliary/scanner/http/http_version



```
       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/http/http_version
msf auxiliary(http_version) >
```

3.- Ejecute el comando para visualizar los parámetros de configuración

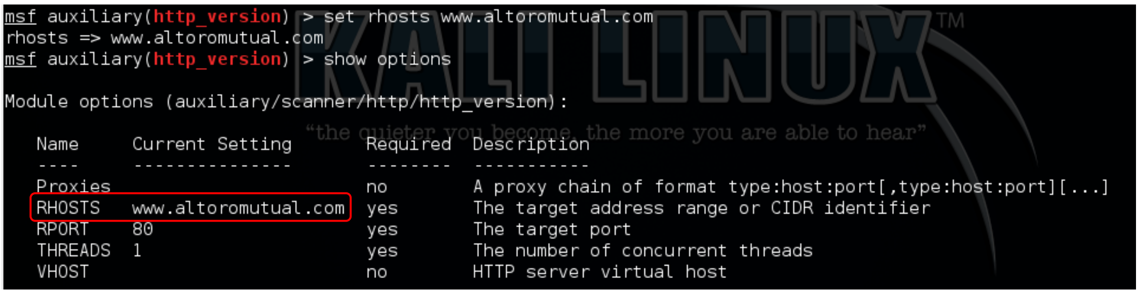
msf auxiliary(http_version) > show options



```
msf auxiliary(http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    80               yes       The target port
   THREADS  1                yes       The number of concurrent threads
   VHOST                     no        HTTP server virtual host
```

4.- Configure el host a revisar con el siguiente comando:

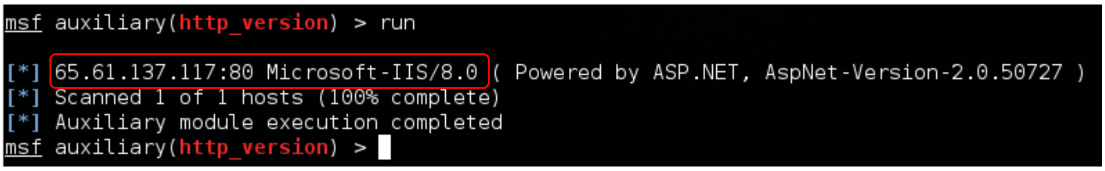
msf auxiliary(http_version) > set rhosts www.altoromutual.com



```
msf auxiliary(http_version) > set rhosts www.altoromutual.com
rhosts => www.altoromutual.com
msf auxiliary(http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting       Required  Description
   ----     ---------------       --------  -----------
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   www.altoromutual.com  yes       The target address range or CIDR identifier
   RPORT    80                    yes       The target port
   THREADS  1                     yes       The number of concurrent threads
   VHOST                          no        HTTP server virtual host
```

5.- Ejecute el módulo auxiliar con el comando:

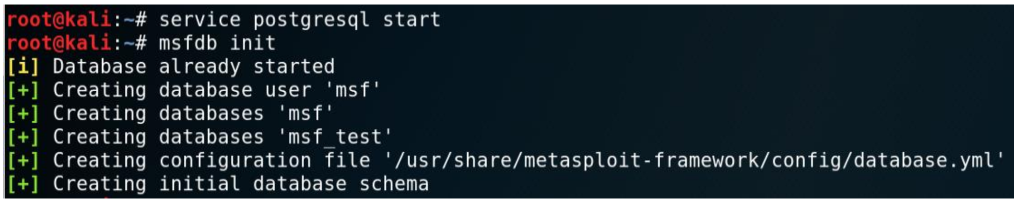
msf auxiliary(http_version) > run



```
msf auxiliary(http_version) > run

[*] 65.61.137.117:80 Microsoft-IIS/8.0 ( Powered by ASP.NET, AspNet-Version-2.0.50727 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) >
```

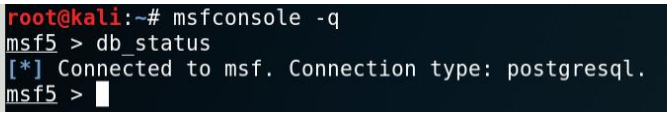
B.- Reconocimiento usando workspace

1.- Inicie la base de datos para trabajo con “workspace”



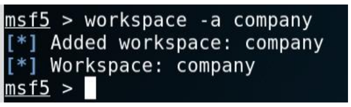
```
root@kali:~# service postgresql start
root@kali:~# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

2.- Inicie Metasploit y confirme la conexión con la base de datos



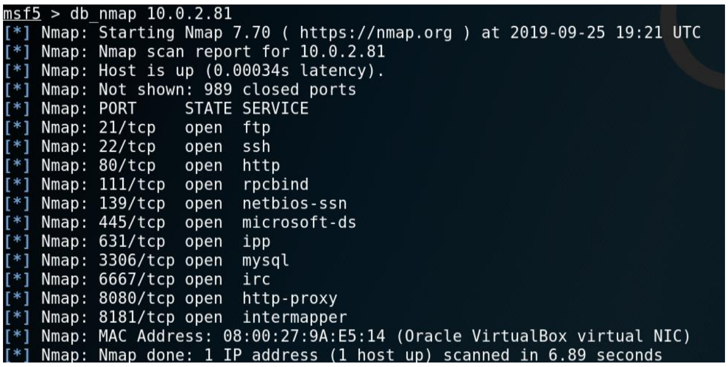
```
root@kali:~# msfconsole -q
msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 >
```

3.- Cree un workspace



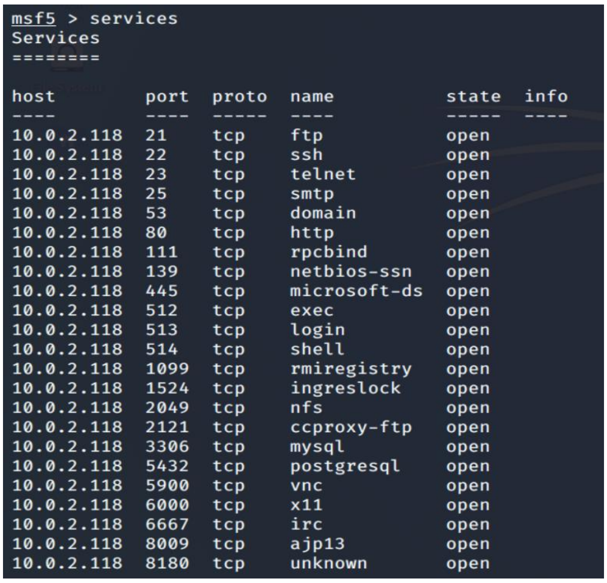
```
msf5 > workspace -a company
[*] Added workspace: company
[*] Workspace: company
msf5 >
```

4.- Realice un scan de pruebas a un servidor



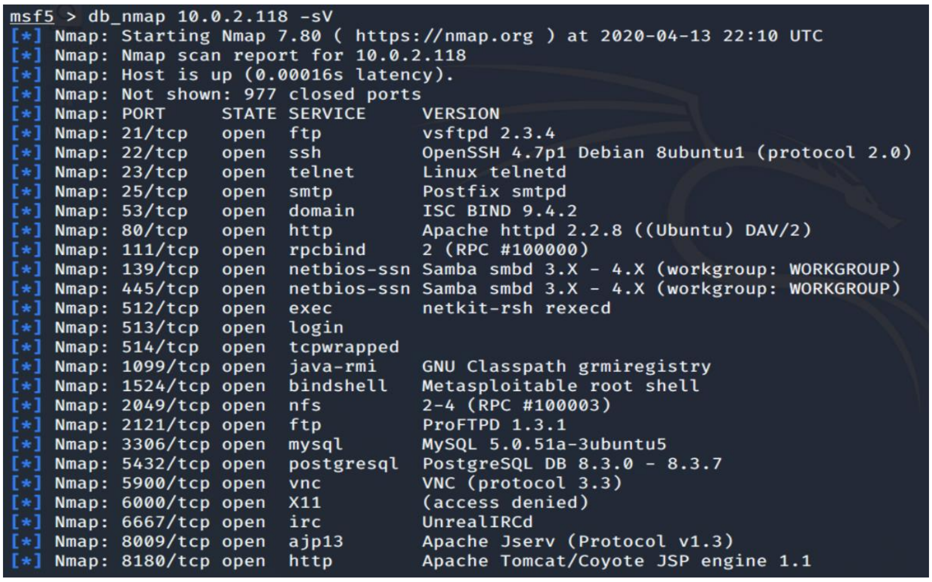
```
msf5 > db_nmap 10.0.2.81
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-25 19:21 UTC
[*] Nmap: Nmap scan report for 10.0.2.81
[*] Nmap: Host is up (0.00034s latency).
[*] Nmap: Not shown: 989 closed ports
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 21/tcp   open  ftp
[*] Nmap: 22/tcp   open  ssh
[*] Nmap: 80/tcp   open  http
[*] Nmap: 111/tcp  open  rpcbind
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 631/tcp  open  ipp
[*] Nmap: 3306/tcp open  mysql
[*] Nmap: 6667/tcp open  irc
[*] Nmap: 8080/tcp open  http-proxy
[*] Nmap: 8181/tcp open  intermapper
[*] Nmap: MAC Address: 08:00:27:9A:E5:14 (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 6.89 seconds
```

5.- Revisamos el listado de servicios



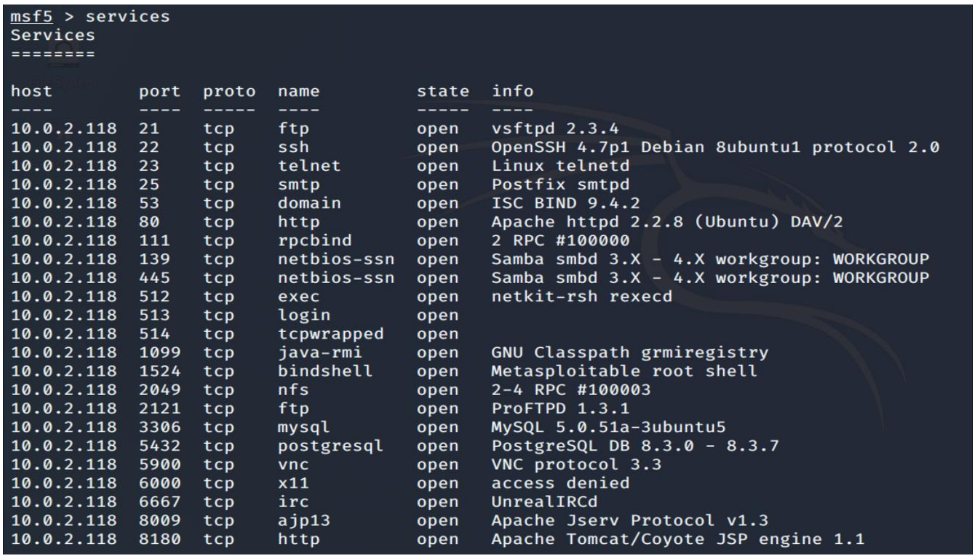
```
msf5 > services
Services
========

host        port  proto  name          state  info
----        ----  -----  ----          -----  ----
10.0.2.118  21    tcp    ftp           open
10.0.2.118  22    tcp    ssh           open
10.0.2.118  23    tcp    telnet        open
10.0.2.118  25    tcp    smtp          open
10.0.2.118  53    tcp    domain        open
10.0.2.118  80    tcp    http          open
10.0.2.118  111   tcp    rpcbind       open
10.0.2.118  139   tcp    netbios-ssn   open
10.0.2.118  445   tcp    microsoft-ds  open
10.0.2.118  512   tcp    exec          open
10.0.2.118  513   tcp    login         open
10.0.2.118  514   tcp    shell         open
10.0.2.118  1099  tcp    rmiregistry   open
10.0.2.118  1524  tcp    ingreslock    open
10.0.2.118  2049  tcp    nfs           open
10.0.2.118  2121  tcp    ccproxy-ftp   open
10.0.2.118  3306  tcp    mysql         open
10.0.2.118  5432  tcp    postgresql    open
10.0.2.118  5900  tcp    vnc           open
10.0.2.118  6000  tcp    x11           open
10.0.2.118  6667  tcp    irc           open
10.0.2.118  8009  tcp    ajp13         open
10.0.2.118  8180  tcp    unknown       open
```

6.- Realizamos la revisión de servicios con el detalle de las aplicaciones



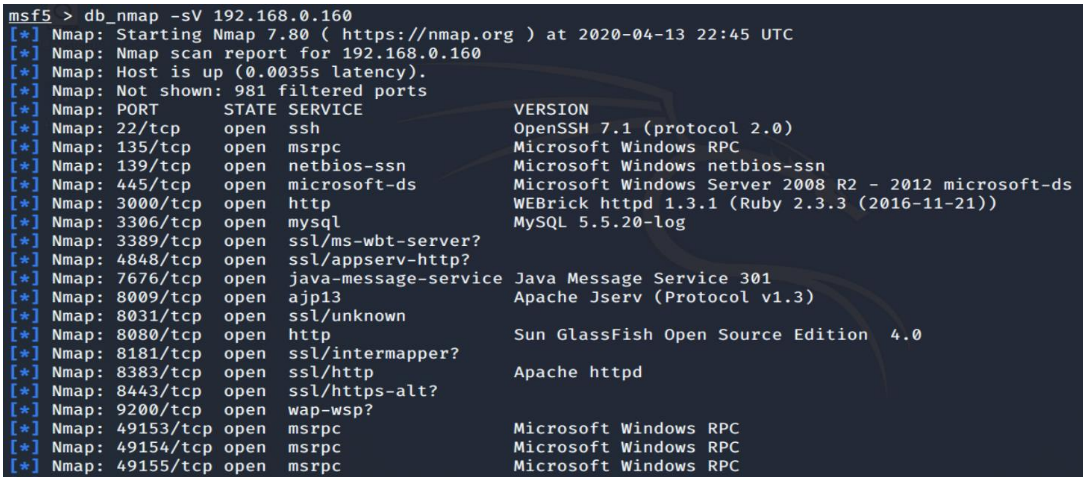
```
msf5 > db_nmap 10.0.2.118 -sV
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-13 22:10 UTC
[*] Nmap: Nmap scan report for 10.0.2.118
[*] Nmap: Host is up (0.00016s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: 53/tcp   open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp  open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp  open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp  open  login
[*] Nmap: 514/tcp  open  tcpwrapped
[*] Nmap: 1099/tcp open  java-rmi    GNU Classpath grmiregistry
[*] Nmap: 1524/tcp open  bindshell   Metasploitable root shell
[*] Nmap: 2049/tcp open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp open  X11         (access denied)
[*] Nmap: 6667/tcp open  irc         UnrealIRCd
[*] Nmap: 8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

7.- Si listamos los servicios



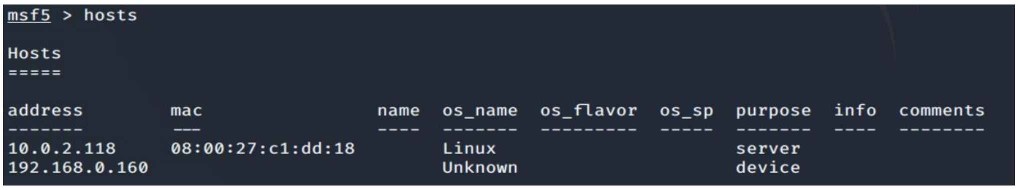
```
msf5 > services
Services
========

host        port  proto  name         state  info
----        ----  -----  ----         -----  ----
10.0.2.118  21    tcp    ftp          open   vsftpd 2.3.4
10.0.2.118  22    tcp    ssh          open   OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
10.0.2.118  23    tcp    telnet       open   Linux telnetd
10.0.2.118  25    tcp    smtp         open   Postfix smtpd
10.0.2.118  53    tcp    domain       open   ISC BIND 9.4.2
10.0.2.118  80    tcp    http         open   Apache httpd 2.2.8 (Ubuntu) DAV/2
10.0.2.118  111   tcp    rpcbind      open   2 RPC #100000
10.0.2.118  139   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.118  445   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.118  512   tcp    exec         open   netkit-rsh rexecd
10.0.2.118  513   tcp    login        open
10.0.2.118  514   tcp    tcpwrapped   open
10.0.2.118  1099  tcp    java-rmi     open   GNU Classpath grmiregistry
10.0.2.118  1524  tcp    bindshell    open   Metasploitable root shell
10.0.2.118  2049  tcp    nfs          open   2-4 RPC #100003
10.0.2.118  2121  tcp    ftp          open   ProFTPD 1.3.1
10.0.2.118  3306  tcp    mysql        open   MySQL 5.0.51a-3ubuntu5
10.0.2.118  5432  tcp    postgresql   open   PostgreSQL DB 8.3.0 - 8.3.7
10.0.2.118  5900  tcp    vnc          open   VNC protocol 3.3
10.0.2.118  6000  tcp    x11          open   access denied
10.0.2.118  6667  tcp    irc          open   UnrealIRCd
10.0.2.118  8009  tcp    ajp13        open   Apache Jserv Protocol v1.3
10.0.2.118  8180  tcp    http         open   Apache Tomcat/Coyote JSP engine 1.1
```

8.- Revisamos los servicios de otro servidor



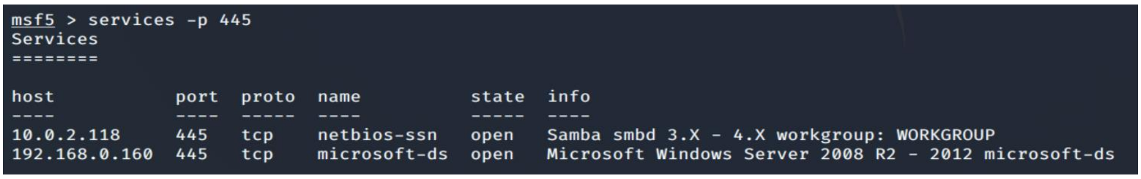
```
msf5 > db_nmap -sV 192.168.0.160
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-13 22:45 UTC
[*] Nmap: Nmap scan report for 192.168.0.160
[*] Nmap: Host is up (0.0035s latency).
[*] Nmap: Not shown: 981 filtered ports
[*] Nmap: PORT      STATE SERVICE              VERSION
[*] Nmap: 22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
[*] Nmap: 135/tcp   open  msrpc                Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
[*] Nmap: 3000/tcp  open  http                 WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
[*] Nmap: 3306/tcp  open  mysql                MySQL 5.5.20-log
[*] Nmap: 3389/tcp  open  ssl/ms-wbt-server?
[*] Nmap: 4848/tcp  open  ssl/appserv-http?
[*] Nmap: 7676/tcp  open  java-message-service Java Message Service 301
[*] Nmap: 8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
[*] Nmap: 8031/tcp  open  ssl/unknown
[*] Nmap: 8080/tcp  open  http                 Sun GlassFish Open Source Edition  4.0
[*] Nmap: 8181/tcp  open  ssl/intermapper?
[*] Nmap: 8383/tcp  open  ssl/http             Apache httpd
[*] Nmap: 8443/tcp  open  ssl/https-alt?
[*] Nmap: 9200/tcp  open  wap-wsp?
[*] Nmap: 49153/tcp open  msrpc                Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc                Microsoft Windows RPC
[*] Nmap: 49155/tcp open  msrpc                Microsoft Windows RPC
```

9.- Revisamos el listado de los servidores revisados



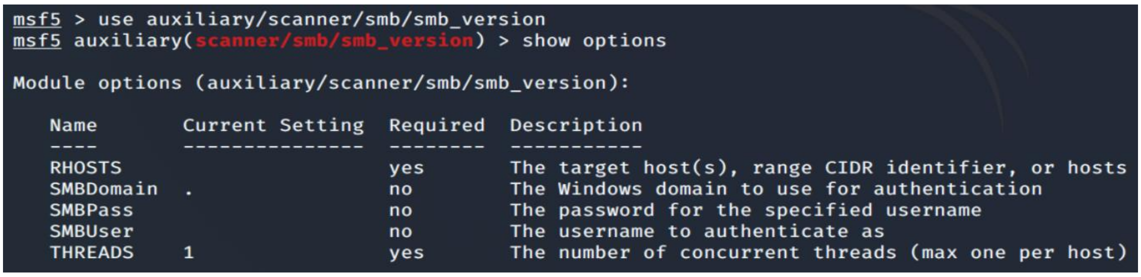
```
msf5 > hosts

Hosts
=====

address        mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------        ---                ----  -------  ---------  -----  -------  ----  --------
10.0.2.118     08:00:27:c1:dd:18        Linux                      server
192.168.0.160                           Unknown                    device
```

10.- Revisamos los servicios en el puerto 445



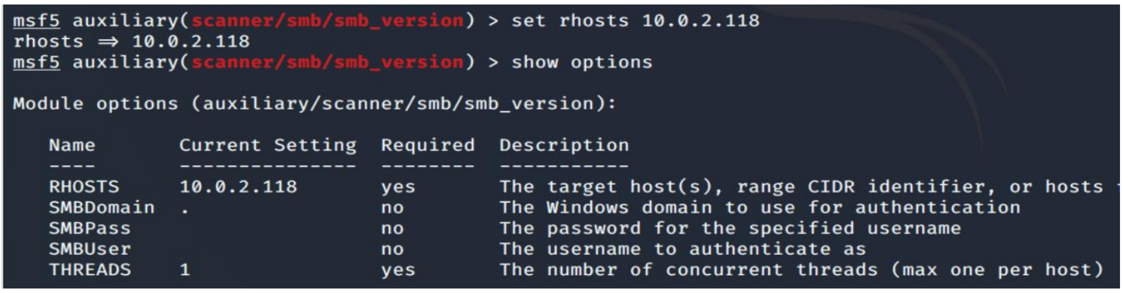
```
msf5 > services -p 445
Services
========

host           port  proto  name          state  info
----           ----  -----  ----          -----  ----
10.0.2.118     445   tcp    netbios-ssn   open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.0.160  445   tcp    microsoft-ds  open   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
```

11.- Actualizamos la información con un auxiliar de Metasploit



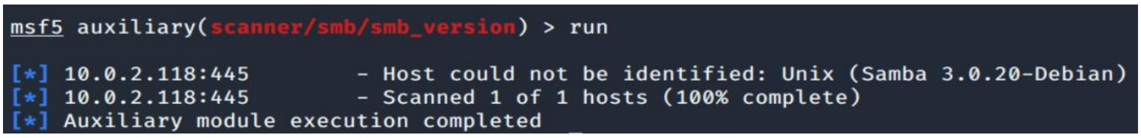
```
msf5 > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)
```

12.- Configuramos el auxiliar



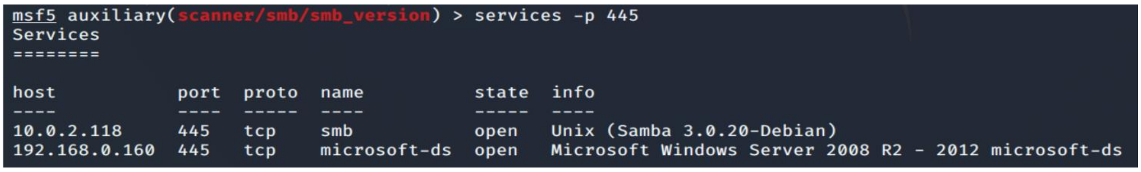
```
msf5 auxiliary(scanner/smb/smb_version) > set rhosts 10.0.2.118
rhosts ⇒ 10.0.2.118
msf5 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     10.0.2.118       yes       The target host(s), range CIDR identifier, or hosts
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)
```

13.- Lo ejecutamos y vemos que nos entrega la versión del servicio SMB



```
msf5 auxiliary(scanner/smb/smb_version) > run

[*] 10.0.2.118:445        - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.0.2.118:445        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

14.- Y observamos que se actualiza en la Base de Datos



```
msf5 auxiliary(scanner/smb/smb_version) > services -p 445
Services
========

host           port  proto  name          state  info
----           ----  -----  ----          -----  ----
10.0.2.118     445   tcp    smb           open   Unix (Samba 3.0.20-Debian)
192.168.0.160  445   tcp    microsoft-ds  open   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
```

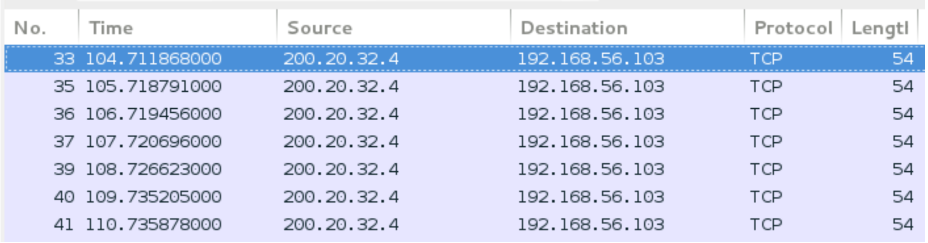
C.- HPING

1.- Abra una ventana de comando en su máquina Kali y ejecute el siguiente comando

# hping3 -a *ip_falsa* *ip_victima*

donde: *ip_victima*, es la dirección IP de su servidor Windows 2008

2.- Observe lo capturado en su aplicación Wireshark



No.	Time	Source	Destination	Protocol	Lengtl
33	104.711868000	200.20.32.4	192.168.56.103	TCP	54
35	105.718791000	200.20.32.4	192.168.56.103	TCP	54
36	106.719456000	200.20.32.4	192.168.56.103	TCP	54
37	107.720696000	200.20.32.4	192.168.56.103	TCP	54
39	108.726623000	200.20.32.4	192.168.56.103	TCP	54
40	109.735205000	200.20.32.4	192.168.56.103	TCP	54
41	110.735878000	200.20.32.4	192.168.56.103	TCP	54

3.- Ejecute el mismo comando nuevamente, cambiando el parámetro *ip_falsa* y observe lo que sucede

4.- A continuación, ejecute el siguiente comando y observe lo que sucede:

# hping3 -1 *ip_victima*

Efecto:____

5.- A continuación, ejecute el siguiente comando y observe lo que sucede

# hping3 -1 --rand-source *ip_victima*

Efecto:___________________________________

6.- A continuación, ejecute el siguiente comando y observe lo que sucede:

# hping3 -1 -d 80 *ip_victima*

Efecto:____________________________________

7.- Investigue como realizar los siguientes paquetes IP con el comando hping3

a) IP origen aleatoria, IP destino servidor Windows, puerto destino 80

b) IP origen host local, IP destino servidor Windows, tamaño de paquete 100 bytes, servicio UDP, puerto destino 53