

# Practica 12. Pentesting con Metasploit

Seguridad de Sistemas Informáticos

Carlos Pérez Fino `alu0101340333@ull.edu.es`

Cheuk Kelly Ng Pante `alu0101364544@ull.edu.es`

26 de diciembre de 2023

Índice general

1. Instalación de paquetes de Kali Linux en una máquina Debian	1
2. Capitulo 2	3
2.1. Seccion 2.1 . . . . .	3
3. Bibliografía	3

## 1. Instalación de paquetes de Kali Linux en una máquina Debian

Para instalar los paquetes básicos de Kali Linux en una máquina *Debian* hemos usado un script creado por un usuario en GitHub llamado *Katoolin3* [1]. Este script nos permite instalar los paquetes básicos de Kali Linux en una máquina Debian o Ubuntu y todo esto se ha instalado en una máquina *Debian* del *IaaS*. Para instalarlo, debemos tener instalado los siguientes requisitos:

- **apt como gestor de paquetes**
- **Privilegios de superusuario**
- **sh y bash**
- **Python >= 3.5:** `sudo apt install python3`
- **Git:** `sudo apt install git`
- **Python3-apt:** `sudo apt install python3-apt`

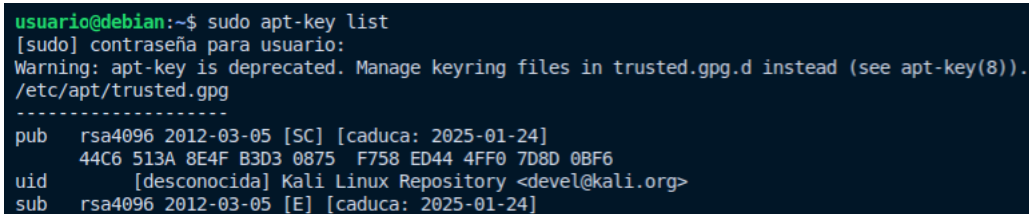
Una vez instalados los requisitos, procedemos a la instalación de *Katoolin3*:

```
git clone https://github.com/s-h-3-l-1/katoolin3;  
cd katoolin3;  
sudo chmod +x install.sh;
```

Ya instalado, entramos como root con *sudo su* y ejecutamos lo siguiente para poder descargar la clave pública desde la URL proporcionada y luego agregarla al sistema como una clave GPG válida y así poder descargar los paquetes de Kali Linux y verificar la autenticidad de los paquetes durante las operaciones de instalación:

```
wget -q -O - https://archive.kali.org/archive-key.asc | apt-key add;
```

Antes que nada, comprobamos con el comando `sudo apt-key list` que se ha añadido la clave de Kali Linux:



```
usuario@debian:~$ sudo apt-key list  
[sudo] contraseña para usuario:  
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).  
/etc/apt/trusted.gpg  
-----  
pub   rsa4096 2012-03-05 [SC] [caduca: 2025-01-24]  
      44C6 513A 8E4F B3D3 0875  F758 ED44 4FF0 7D8D 0BF6  
uid    [desconocida] Kali Linux Repository <devel@kali.org>  
sub    rsa4096 2012-03-05 [E] [caduca: 2025-01-24]
```

Figura 1.1: Imagen del comando `sudo apt-key list`

ya comprobada la clave, procedemos a comentar la línea 22 del script *install.sh* para que no de error como se muestra en la figura 1.2

```
install.sh M X
no hay elementos
1 #!/bin/bash
2
3 source "conf.sh";
4
5 PROGRAM_PREFIX="";
6
7 # If the installation directory is not in PATH issue a warning:
8 if ! echo $PATH | grep -q "$DIR";
9 then
10     echo "Warning: '$DIR' is not in your PATH.";
11     echo "    To use this program add '$DIR'";
12     echo "    to your PATH or manually copy";
13     echo "    katoolin3.py somewhere.";
14     echo;
15     PROGRAM_PREFIX="$DIR/";
16 fi
17
18 # Check if shebang from katoolin3.py can execute:
19 /usr/bin/env python3 -V >/dev/null || die "Please install 'python3'";
20
21 # Install all dependencies:
22 #apt-key adv --keyserver pool.sks-keyserver.net --recv-keys ED444FF07D80BF6
23 apt-get -qq -y -m install python3-apt || die;
24
25 install -T -g root -o root -m 555 ./katoolin3.py "$DIR/$PROGRAM" || die;
26
27 echo "Successfully installed."
28 echo "Run it with 'sudo $PROGRAM_PREFIX$PROGRAM'.";
29 exit 0;
30
```

Figura 1.2: Imagen del script *install.sh*

Una vez comentada la línea, ejecutamos el script de instalación: `sudo ./install.sh`

Una vez hecha la instalación procedemos a ejecutar el script *katoolin3.py* para poder instalar los paquetes de Kali Linux: `sudo python3 katoolin3.py`

Cuando ejecutemos el script nos aparecerá un menú como el de la figura 1.3a: Para instalar los paquetes básicos de Kali Linux, seleccionamos las opciones como aparece en la figura 1.3b:

```
KATOOLIN3
~~~~[ Author: s-h-3-l-l | Homepage: https://github.com/s-h-3-l-l ]~~~~

Obj:1 http://deb.debian.org/debian bookworm InRelease
Des:2 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Des:3 http://deb.debian.org/debian bookworm-updates InRelease [52,1 kB]
Des:4 http://kali.download/kali kali-rolling InRelease [41,2 kB]
Des:5 http://kali.download/kali kali-rolling/main amd64 Packages [19,4 MB]
Des:6 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45,8 MB]
Des:7 http://kali.download/kali kali-rolling/contrib amd64 Packages [122 kB]
Des:8 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [295 kB]
Des:9 http://kali.download/kali kali-rolling/non-free amd64 Packages [226 kB]
Des:10 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [919 kB]
Descargados 67,0 MB en 9s (7.255 kB/s)
Leyendo lista de paquetes...
W: http://http.kali.org/kali/dists/kali-rolling/InRelease: Key is stored in legacy trusted.gpg
keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.

DISCLAIMER:
Don't update your packages, upgrade your system or
modify your package cache in any other way while
katoolin3 is still running!

Main Menu
0) View Categories
1) Install All
2) Uninstall All
3) Search repository
4) List installed packages
5) List not installed packages
6) Install Kali Menu
7) Uninstall old katoolin
8) Help
9) Exit

kat> 1
```

(a) Menu principal

```
Main Menu
0) View Categories
1) Install All
2) Uninstall All
3) Search repository
4) List installed packages
5) List not installed packages
6) Install Kali Menu
7) Uninstall old katoolin
8) Help
9) Exit

kat> 0

Select a Category
0) Exploitation Tools
1) Forensics Tools
2) Hardware Hacking
3) Information Gathering
4) Maintaining Access
5) Password Attacks
6) Reporting Tools
7) Reverse Engineering
8) Sniffing & Spoofing
9) Stress Testing
10) Vulnerability Analysis
11) Web Applications
12) Wireless Attacks
13) HELP
14) BACK

kat> 0

Select a Package
0) armitage
1) Backdoor Factory
2) Beef Xes
3) Cisco Auditing Tool
4) Cisco Global Exploiter
5) Cisco Ocs
6) Cisco Torch
7) commix
8) crackle
9) exploitdb
10) Jboss Autopwn
11) Linux Exploit Suggester
12) Metasploit Framework
13) msfpoc
14) routersploit
15) set
16) shellnoob
17) sqlmap
18) The Ipv6
19) yersinia
20) ALL
21) HELP
22) BACK

kat> 20
```

(b) Menu de instalación

Figura 1.3: Ejecucion del script

## **2. Capitulo 2**

### **2.1. Seccion 2.1**

## **3. Bibliografía**

### **Bibliografía**

- [1] s-h-3-l-l. (2019). Katoolin3. Github. Recuperado de <https://github.com/s-h-3-l-l/katoolin3>