

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	4
2.1. Seccion 2.1	4
3. Bibliografía	4

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. 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`

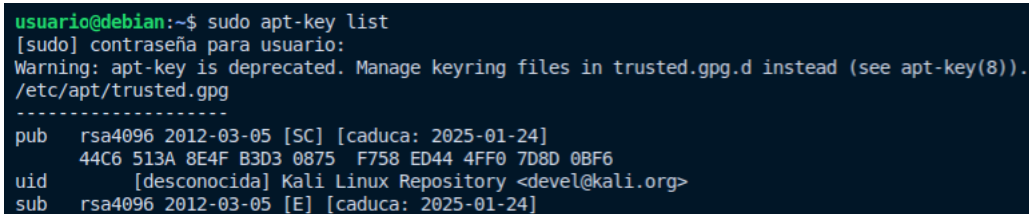
Una vez instalados los requisitos, procedemos a la instalación de *Katoolin3*:

```
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

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 1.3:

Para instalar los paquetes básicos de Kali Linux, seleccionamos la opción 0 y nos aparecerá un menú como el de la figura 1.4 y en el nuevo menú seleccionamos la opción 0 para instalar las herramientas de explotación y nos saldrá otro menú y seleccionamos la opción 20 para instalar todas las herramientas:

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

kat> 0

Select a Package
0) armitage                12) Metasploit Framework
1) Backdoor Factory       13) msfpoc
2) Beef Xss               14) routersploit
3) Cisco Auditing Tool    15) set
4) Cisco Global Exploiter 16) shellnoob
5) Cisco Ocs              17) sqlmap
6) Cisco Torch            18) The IPv6
7) commix                 19) yersinia
8) crackle                20) ALL
9) exploitable            21) HELP
10) Jboss Autopwn         22) BACK
11) Linux Exploit Suggester

kat> 20
```

Figura 1.3: Imagen del menú de *katoolin3.py*

2. Capítulo 2

2.1. Sección 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>