

# “ATAQUES Y EVALUACIÓN DEVULNERABILIDADES (Parte IV)”

Trabajo Preparatorio N°5

Laboratorio de Seguridad en Redes

Melanny Dávila

*Ingeniería en Telecomunicaciones*  
*Facultad de Eléctrica y Electrónica*  
Quito, Ecuador  
melanny.davila@epn.edu.ec

Alejandra Silva

*Ingeniería en Telecomunicaciones*  
*Facultad de Eléctrica y Electrónica*  
Quito, Ecuador  
alejandra.silva@epn.edu.ec

**Abstract**—En el siguiente documento se presenta el sustento teórico acerca de diferentes ataques como los de fuerza bruta o de inanición DHCP mediante el uso de herramientas como Medusa la cual ataca servicios como HTTP, MySQL, SSH, entre otros.

**Index Terms**—Ataques, Kali, DHCP, Wireshark.

## I. INTRODUCCIÓN

Un ataque de fuerza bruta busca descifrar las credenciales de uno o varios usuarios, o descubrir la clave utilizada para cifrar mensajes. Consiste en aplicar el método de prueba y error esperando así dar con la combinación correcta. Si bien este método es un ataque antiguo, sigue siendo eficaz y muy popular entre las vulnerabilidades presentes.

Mientras que los ataques de inanición (starvation) es un problema relacionado con los sistemas multitarea, donde a un proceso se le deniega el acceso a un recurso compartido, este caso en particular se tratará a el caso de DHCP donde se terminará el suministro de direcciones IP.

## II. OBJETIVOS

- Explotar las vulnerabilidades de un equipo dentro de un entorno controlado.
- Realizar un ataque de fuerza bruta por diccionario a un RouterCisco.
- Realizar un ataque Starvation Attack a un servidor de DHCP.

## III. CUESTIONARIO

- Revisar el marco teórico para la realización de la práctica.
- Consulte sobre el funcionamiento y uso de la herramienta Yersiniade Kali Linux.(máximo una carilla)

Es una herramienta para realizar ataques de capa 2. Está diseñado para aprovechar algunas debilidades en diferentes protocolos de red [1]. Pretende ser un marco sólido para analizar y probar las redes y sistemas desplegados. Los ataques para los siguientes protocolos de red se implementan en esta versión en particular:

- Protocolo de árbol de expansión (STP)
- Protocolo de descubrimiento de Cisco (CDP)
- Protocolo de enlace dinámico (DTP)
- Protocolo de configuración dinámica de host (DHCP)
- Protocolo de enrutador Hot Standby (HSRP)
- 802.1q
- 802.1x
- Protocolo de enlace entre conmutadores (ISL)
- Protocolo de enlace troncal VLAN (VTP)

En el caso de DHCP se busca llenar al servidor con paquetes DHCP discover con direcciones MAC falsificadas. Entonces, el servidor DHCP otorga diferentes direcciones IP a todas las solicitudes y de esta manera cuando un nuevo cliente legítimo que solicite una dirección IP no la recibirá [1].

Las opciones presentes en esta herramienta son:

- “-h, -help” Pantalla de ayuda.
- “-V, -Version” Versión del programa.
- “-G ” Inicia una sesión GTK gráfica.
- “-I, -interactive” Inicia una sesión interactiva de ncurses.
- “-D, -daemon” Inicia la escucha de la red para el administrador remoto (emulación de la CLI de Cisco).
- “-d” Habilita los mensajes de depuración.
- “-l logfile” Guarda la sesión actual en el archivo de registro. Si existe un archivo de registro, los datos se agregarán al final.
- “-c” conf file Lee/escribe variables de configuración de/a conf file.
- “-M” Desactiva la suplantación de MAC [1].

- Consulte que es MAC Spoofing y cuando se utiliza.(máximo una carilla)

Mac Spoofing hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación, es decir, un atacante falsea el origen de los paquetes haciendo que la víctima piense que estos son de un host de confianza o autorizado para evitar la víctima lo detecte

[2]. En el spoofing entran en juego tres máquinas o hosts: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el atacante pueda conseguir su objetivo necesita por un lado establecer una comunicación falseada con su objetivo, y por otro evitar que el equipo suplantado interfiera en el ataque [2].

El sentido de MAC Spoofing son principalmente 5: [3]

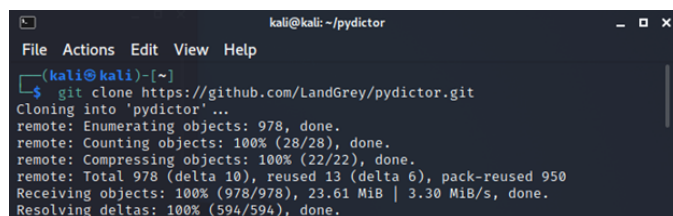
- Suplantación de identidad
- Acceso a servicios no contratados
- Evasión de filtros MAC
- Anonimato
- Envenenamiento ARP

El spoofing de dirección MAC está habilitado de forma predeterminada para todas las interfaces de red, por ejemplo: [4]

- Usando una propia computadora en una red pública sin autenticación, en este caso, el spoofing de la dirección MAC oculta el hecho de que la computadora está conectada a esta red.
- Usando una propia computadora en una red que utiliza con frecuencia, en este caso el spoofing de direcciones MAC oculta el hecho de que la computadora está conectada a esta red en un momento determinado.

*D. Clone el repositorio de pydictorgit clone <https://github.com/LandGrey/pydictorgit> con ayuda de este programa genere un diccionario de al menos 100 palabras en el que conste su nombre, cisco, admin.*

El primer paso es teclear el siguiente comando que se indica [5].



```
kali@kali: ~/pydictorg
File Actions Edit View Help
(kali@kali)-[~]
$ git clone https://github.com/LandGrey/pydictorgit.git
Cloning into 'pydictorgit'...
Remote: Enumerating objects: 978, done.
Remote: Counting objects: 100% (28/28), done.
Remote: Compressing objects: 100% (22/22), done.
Remote: Total 978 (delta 10), reused 13 (delta 6), pack-reused 950
Receiving objects: 100% (978/978), 23.61 MiB | 3.30 MiB/s, done.
Resolving deltas: 100% (594/594), done.
```

Fig. 1. Clonación.

Ahora, se debe cambiar de directorio al pydictorgit/ y se le debe dar permisos de ejecución(x) para que python pueda realizar la petición como se indica.



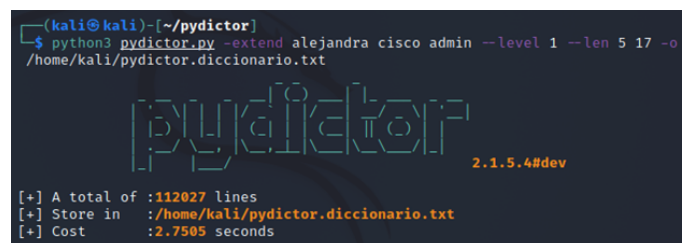
```
(kali@kali)-[~]
$ cd pydictorgit

(kali@kali)-[~/pydictorgit]
$ chmod +x pydictorgit.py

(kali@kali)-[~/pydictorgit]
$ python pydictorgit.py
```

Fig. 2. Comandos de ejecución.

Finalmente, se genera un diccionario de al menos 100 palabras en el que consta el nombre del estudiante, cisco, admin con el siguiente comando.

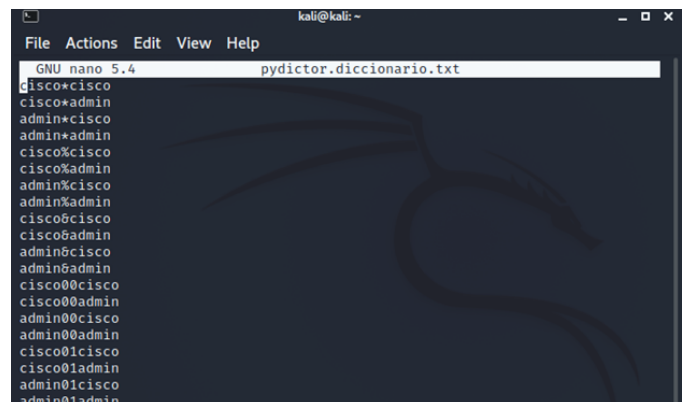


```
(kali@kali)-[~/pydictorgit]
$ python3 pydictorgit.py -extend alejandra cisco admin --level 1 --len 5 17 -o /home/kali/pydictorgit.diccionario.txt

[+] A total of :112027 Lines
[+] Store in :/home/kali/pydictorgit.diccionario.txt
[+] Cost :2.7505 seconds
```

Fig. 3. Creación del diccionario.

A continuación se indica el contenido del archivo creado.



```
File Actions Edit View Help
GNU nano 5.4 pydictorgit.diccionario.txt
cisco*cisco
cisco*admin
admin*cisco
admin*admin
cisco%cisco
cisco%admin
admin%cisco
admin%admin
cisco@cisco
cisco@admin
admin@cisco
admin@admin
cisco00cisco
cisco00admin
admin00cisco
admin00admin
cisco01cisco
cisco01admin
admin01cisco
admin01admin
```

Fig. 4. Contenido del diccionario.

## REFERENCES

- [1] R. Sankar, "Yersinia for Layer 2 - Vulnerability Analysis & DHCP Starvation Attack", Kali Linux Tutorials, jun. 25, 2018. <https://kalilinuxtutorials.com/yersinia/> (accedido jul. 07, 2021).
- [2] Garcia. C.(2010),"Hablemos de Spoofing".<https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/>.(accedido jul. 7, 2021).
- [3] "Spoofing de direcciones MAC". [https://tails.boum.org/doc/first\\_steps/welcome\\_screen/mac\\_spoofing/index.es.html#index2h1l](https://tails.boum.org/doc/first_steps/welcome_screen/mac_spoofing/index.es.html#index2h1l).(accedido jul. 7, 2021).

- [4] "Seguridad: Spoofing. Capítulo Segundo -¿ MAC Spoofing". <https://blog.theliel.es/2010/02/seguridad-spoofing-capitulo-segundo-mac-spoofing.html>. (accedido jul. 7, 2021).
- [5] "LandGrey/pydictor". <https://github.com/LandGrey/pydictor>. (accedido jul. 7, 2021).