CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 1, Número 1 / Julio – Diciembre 2021 pp. 50-55

Herramienta Medusa

Medusa tool

Jhonny Guilcapi [1]; Luis Aguas [2]

[1,2] Universidad Tecnológica Israel–Carrera de Sistemas de Información, 170516, Quito, Ecuador

Fecha de recepción: octubre 2021 **Fecha de aprobación:** diciembre 2021

RESUMEN

Medusa es reconocida como una de las grandes herramientas para la fuerza bruta, puesto que se caracteriza por ser un software que ataca a nivel de fuerza bruta basándose en diccionarios de palabras, además es muy estable, sencillo, rápido, y permite realizar el ataque a muchos servicios. Un ataque de fuerza bruta es la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

Palabras Clave: Medusa, Software, Ataque.

ABSTRACT

Medusa is recognized as one of the great tools for brute force, since it is characterized by being a software that attacks at the brute force level based on word dictionaries, it is also very stable, simple, fast, and allows the attack to be carried out on many services. A brute force attack is the way to recover a key by trying all the possible combinations until you find the one that allows access.

Key Words: Jellyfish, Software, Attack.

[1] Estudiante de Ingeniería en Sistemas, jhonnyguilcapi@gmail.com
[2] Magíster en Redes de Comunicaciones, aguaszoft@outlook.es

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 1, Número 1 / Julio – Diciembre 2021 pp. 50-55

1. INTRODUCCIÓN

El software Medusa es un forzador de datos bruto rápido, paralelo y modular. El objetivo es admitir tantos servicios que permitan la autenticación remota como sea posible. Por lo tanto, se considera los siguientes elementos como algunas de las características clave de esta aplicación [1];

Pruebas paralelas basadas en hilos: Las pruebas de fuerza bruta se pueden realizar contra múltiples hosts, usuarios o contraseñas al mismo tiempo.

Entrada flexible del usuario: La información de destino (host / usuario / contraseña) se puede especificar de varias maneras. Por ejemplo, cada elemento puede ser una sola entrada o un archivo que contiene varias entradas. Además, un formato de archivo combinado permite al usuario refinar su listado de destino.

El 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.

Múltiples protocolos compatibles: Actualmente se admiten muchos servicios (por ejemplo, SMB, HTTP, POP3, MS-SQL, SSHv2, entre otros).

Figura 1

2. DESARROLLO

2.1 Instalación de Medusa

```
apt-get install medusa
```

Figura 2

Revisamos los servicios a los que podemos realizar ataques de fuerza bruta con Medusa:

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 1, Número 1 / Julio – Diciembre 2021 pp. 50-55

```
medusa -d

Available modules in "/usr/lib/medusa/modules" :
+ afp.mod : Brute force module for AFP sessions : version 0.9.0
+ cvs.mod : Brute force module for CVS sessions : version 1.0.0
+ ftp.mod : Brute force module for FTP/FTPS sessions : version 1.3.0
+ http.mod : Brute force module for HTTP : version 1.3.0
+ imap.mod : Brute force module for IMAP sessions : version 1.2.0
+ mssql.mod : Brute force module for M$-SQL sessions : version 1.1.1
+ mysql.mod : Brute force module for MySQL sessions : version 1.2
+ ncp.mod : Brute force module for NCP sessions : version 1.0.0
+ nntp.mod : Brute force module for NNTP sessions : version 1.0.0
+ pcanywhere.mod : Brute force module for PcAnywhere sessions : version 1.0.2
+ pop3.mod : Brute force module for POP3 sessions : version 1.2
+ postgres.mod : Brute force module for PostgreSQL sessions : version 1.0.0
+ rexec.mod : Brute force module for REXEC sessions : version 1.1.1
+ rlogin.mod : Brute force module for RLOGIN sessions : version 1.0.2
+ rsh.mod : Brute force module for RSH sessions : version 1.0.1
+ smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions : version 1.5
+ smtp-vrfy.mod : Brute force module for enumerating accounts via SMTP VRFY : version 1.
0.0
+ smtp.mod : Brute force module for SMTP Authentication with TLS : version 1.0.0
+ snmp.mod : Brute force module for SNMP Community Strings : version 1.0.0
+ ssh.mod : Brute force module for SSH v2 sessions : version 1.0.2
+ svn.mod : Brute force module for Subversion sessions : version 1.0.0
+ telnet.mod : Brute force module for telnet sessions : version 1.2.2
+ vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 1.0.1
+ vnc.mod : Brute force module for VNC sessions : version 1.0.1
+ web-form.mod : Brute force module for web forms : version 1.0.0
+ wrapper.mod : Generic Wrapper Module : version 1.0.1
```

Figura 3

Crear los diccionarios de usuarios y password

Crear el fichero **usuarios.txt** con el siguiente contenido:

```
admin
Admin
Root
root
Administrdor
administrador
Administrator
administrator
```

Figura 4

Crear el fichero **password.txt**, con el siguiente contenido:

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 1, Número 1 / Julio – Diciembre 2021 pp. 50-55

Figura 5

2.1.1 Parámetros importantes de Medusa

-h: El host al cual le vamos a realizar el ataque

-H: Para especificar una lista de *hosts*

-u: Usuario al que le vamos a realizar el ataque

-U: Para especificar una lista de usuarios

-P: Para especificar una lista de contraseñas

-O: Crea un log

-e: Incluye la verificación con un *password* vacío y que el *password* sea el mismo nombre

-M: El modulo que deseamos emplear (sin la extension .mod)

-n: Para especificar el puerto del servicio (En caso de que no esté corriendo en el *default*)

-s: Habilita ssl

-f: Se detiene al encontrar la contraseña

-b: Suprime los *banners*

-v: Modo *verbose* (más información *level* de 0 a 6, siendo el 6 más alto)

Conociendo estos parámetros, procedemos a realizar un ataque de fuerza bruta a un equipo que tiene corriendo el servicio de ssh:

```
medusa -h IP_ORDENADOR -U usuarios.txt -P password.txt -M ssh -f -b -v 6 -e ns
```

Figura 6

En el caso que ya conociéramos el usuario, sería así:

```
medusa -h IP_ORDENADOR -u root -P password.txt -M ssh -f -b -v 6 -e ns
```

Figura 7

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 1, Número 1 / Julio – Diciembre 2021 pp. 50-55

Para encontrar que servicios y en que puertos se está ejecutando en determinado equipo debemos utilizar otras herramientas como Nmap.

Podemos ir armando nuestros propios diccionarios, también en Internet se pueden encontrar listado de diccionarios con claves y usuario comunes.

La mejor forma de defendernos de este tipo de programas es restringir el número de intentos de autentificación, y tener una compleja combinación de usuario/contraseña.

2.2 Herramienta genérica para hacer ataques de fuerza bruta

Una de las herramientas que tenemos disponibles en la distribución de Linux BackTrack es Medusa. Dicha herramienta permite hacer ataques de fuerza bruta contra un variado conjunto de protocolos [2], vamos a ver cómo funciona:

Si ejecutamos medusa con la opción -d podremos ver el conjunto de módulos disponibles:

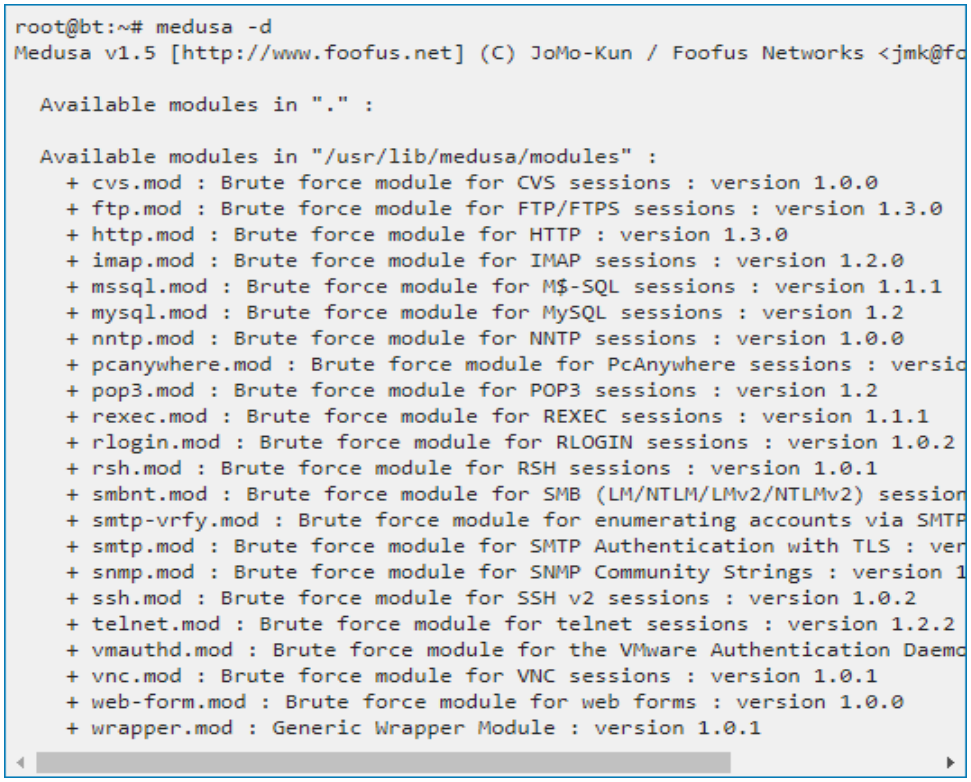

Figura 8

Las opciones interesantes para lanzar un ataque de fuerza bruta son:

- [-h host|-H file]: Mediante -h especificamos un determinado host, mientras que con -H indicamos un fichero dónde encontrar un listado de hosts a atacar
- [-u username|-U file]: Mediante -u indicamos un usuario y el complementario -U indicamos un diccionario con usuarios
- [-p password|-P file]: Mediante -p indicamos una contraseña a probar, mientras que con -P indicamos un diccionario de contraseñas

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 1, Número 1 / Julio – Diciembre 2021 pp. 50-55

Por ejemplo, para hacer un ataque de fuerza bruta al propio servidor con el usuario ejemplo y un diccionario de contraseñas llamado passfile:

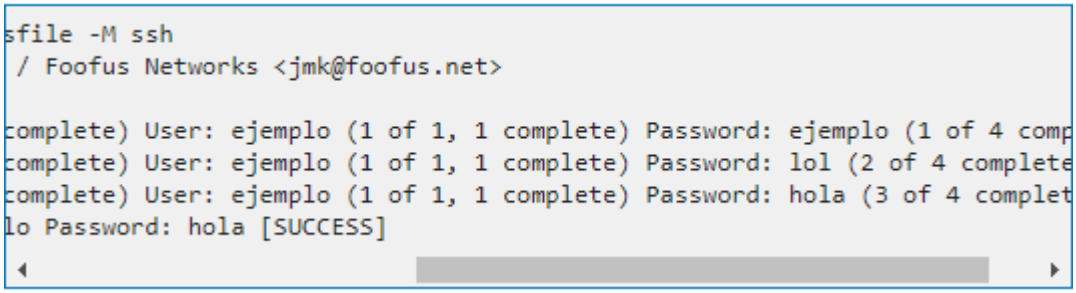

Figura 9

3. CONCLUSIONES

Medusa es un software para atacar a nivel de fuerza bruta basándonos en diccionarios de palabras, es muy estable, sencillo, rápido y nos permitirá realizar el ataque a muchos servicios. Con medusa podemos crackear por diccionario de una manera muy rápida [3]. Los parámetros más importantes a tener en cuenta de medusa son los siguientes:

- el host al cual le vamos a realizar el ataque
- usuario al que le vamos a realizar el ataque

REFERENCIAS

1. https://en.kali.tools/?p=200
2. http://systemadmin.es/2010/09/medusa-herramienta-generica-para-hacer-ataques-de-fuerza-bruta
3. https://mundo-hackers.weebly.com/medusa.html