

Índice:

Ejercicio 5	2
c).....	2

Ejercicio 5

c)

Solución:

- ¿Qué es un exploit?. Formas de protegerse.

Un exploit es un programa diseñado para **aprovechar vulnerabilidades** en sistemas o software con diversos propósitos, como obtener **privilegios** de administrador o **eludir** medidas de **seguridad**. Los exploits solo **explotan** la **vulnerabilidad**, y por sí solos pueden causar errores en el sistema. A menudo se utilizan **junto** con otras **aplicaciones** maliciosas, como **payloads** o **troyanos**, para realizar **infecciones más avanzadas** aprovechando las vulnerabilidades descubiertas.

Para protegerse

Es recomendable mantener nuestro Windows, y todos los programas instalados en él, totalmente actualizados para que todos los exploits que se descubran se parchen.

Utilizando software dedicado como Malwarebytes Anti-Exploit

Si junto a esto evitamos descargar archivos desde fuentes extrañas y de dudosa fiabilidad y abrir los archivos adjuntos que nos llegan a través de correos basura, estaremos bastante protegidos contra todas estas posibles amenazas potenciales.

- Tipos de exploits.

Los exploits se dividen en dos tipos principales: **conocidos** y **desconocidos (zero-day)**.

Los **exploits conocidos** son diseñados para aprovechar vulnerabilidades que ya se conocen y que han sido corregidas mediante actualizaciones. A menudo, persisten en sistemas no actualizados, y se pueden evitar instalando las actualizaciones correspondientes.

Por otro lado, los **exploits desconocidos** se desarrollan para aprovechar vulnerabilidades **zero-day**, que son fallas de seguridad no reveladas públicamente y para las cuales no existe un parche disponible. Estas vulnerabilidades son especialmente peligrosas en ataques dirigidos a empresas o gobiernos, ya que son difíciles de detectar y bloquear. Los exploits zero-day son altamente valorados en la comunidad de ciberdelincuentes y se utilizan para ataques graves.

- ¿Qué es Metasploit?

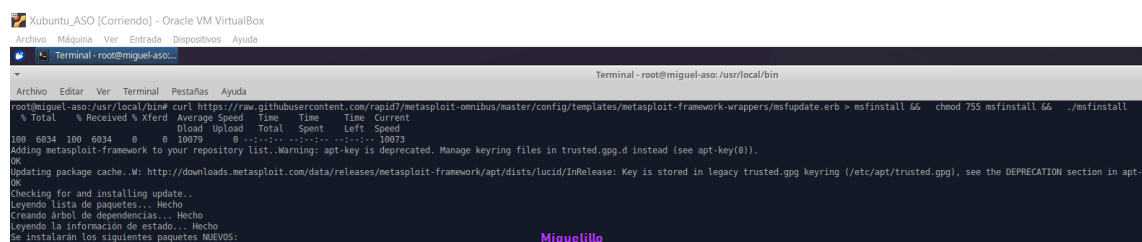
Es una **herramienta de código abierto utilizada** en el campo del **hacking ético**. Metasploit viene preinstalado en Kali Linux y es ampliamente reconocido en el mundo de la seguridad informática.

Ofrece más de 900 exploits que permiten probar vulnerabilidades en sistemas informáticos. Es multiplataforma y gratuito, aunque existe una versión de pago llamada Metasploit Pro que incluye exploits de día cero de forma anual.

Además, Metasploit ofrece otras herramientas como payloads (códigos maliciosos para la postexplotación de vulnerabilidades) y codificadores que encriptan malware para evadir sistemas de detección, entre otras funcionalidades.

Usa Metasploit

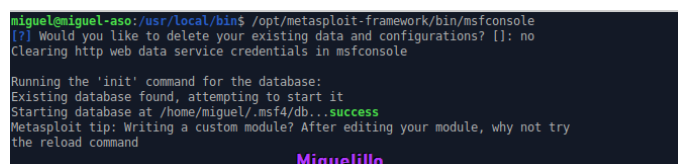
Instalo Metaexploit



```

root@miguel-aso: /usr/local/bin# curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall.rb
chmod 755 msfinstall.rb
./msfinstall.rb
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 6034 100 6034 0 0 10079 0 --:--:-- --:--:-- --:--:-- 10072
Adding metasploit-framework to your repository list. Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
Updating package cache..W: http://downloads.metasploit.com/data/releases/metasploit-framework/apt/dists/Lucid/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Checking for and installing update..
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  
```

Inicio metaexploit con mfsconsole

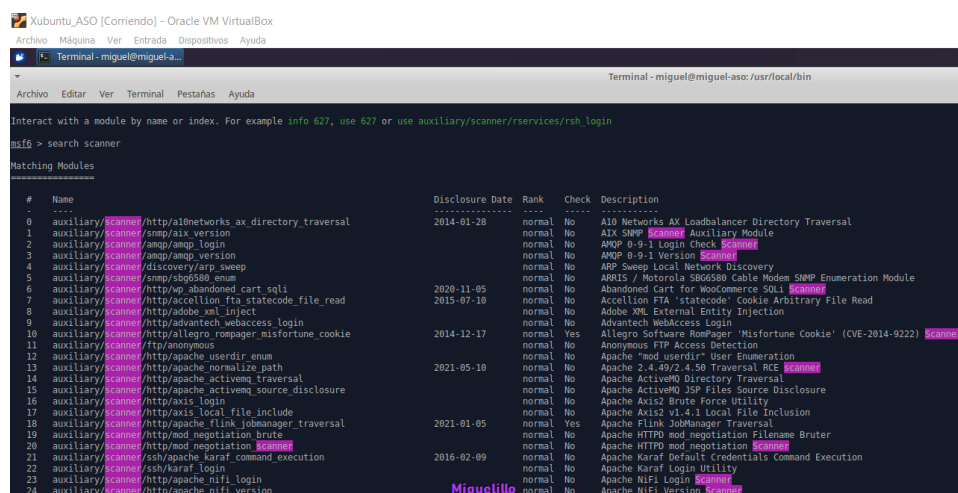


```

miguel@miguel-aso: /usr/local/bin$ /opt/metasploit-framework/bin/msfconsole
[?] Would you like to delete your existing data and configurations? [Y]: no
Clearing http web data service credentials in msfconsole

Running the 'init' command for the database:
Existing database found, attempting to start it
Starting database at /home/miguel/.msf4/db...success
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command
  
```

Escaneo la red con show scanner



```

Interact with a module by name or index. For example info 627, or use auxiliary/scanner/rservices/rsh_login

msf6 > search scanner

Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank  Check  Description
--  --
0  auxiliary/scanner/http/ai10networks_ax_directory_traversal          2014-01-28     normal No     A10 Networks AX Loadbalancer Directory Traversal
1  auxiliary/scanner/smb/smb_version                                    normal No     AIX SMB Scanner Auxiliary Module
2  auxiliary/scanner/amqp/amqp_login                                    normal No     AMQP 0-9-1 Login Check Scanner
3  auxiliary/scanner/amqp/amqp_version                                    normal No     AMQP 0-9-1 Version Scanner
4  auxiliary/scanner/discovery/arp_sweep                                normal No     ARP Sweep Local Network Discovery
5  auxiliary/scanner/smb/smbd500_enum                                    normal No     ARIS / Motorola SBD500 Cable Modem SNMP Enumeration Module
6  auxiliary/scanner/http/wp_abandoned_cart_sqli                      2020-11-05     normal No     Abandoned Cart for WooCommerce SQLi Scanner
7  auxiliary/scanner/http/accelion_fta_statecode_file_read             2015-07-10     normal No     Accellion FTA 'statecode' Cookie Arbitrary File Read
8  auxiliary/scanner/http/adobe_xml_inject                             normal No     Adobe XML External Entity Injection
9  auxiliary/scanner/http/advantech_webaccess_login                    normal No     Advantech WebAccess Login
10 auxiliary/scanner/http/allegro_rompager_misfortune_cookie            2014-12-17     normal Yes    Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
11 auxiliary/scanner/ftp/anonymous                                    normal No     Anonymous FTP Access Detection
12 auxiliary/scanner/http/apache_userdir_enum                          normal No     Apache 'mod_userdir' User Enumeration
13 auxiliary/scanner/http/apache_normalize_path                        2021-05-10     normal No     Apache 2.4.49/2.4.50 Traversal RCE Scanner
14 auxiliary/scanner/http/apache_activemq_traversal                    normal No     Apache ActiveMQ Directory Traversal
15 auxiliary/scanner/http/apache_activemq_source_disclosure             normal No     Apache ActiveMQ JSP Files Source Disclosure
16 auxiliary/scanner/http/axis_login                                    normal No     Apache Axis2 Brute Force Utility
17 auxiliary/scanner/http/axis_local_file_include                      normal No     Apache Axis2 v1.4.1 Local File Inclusion
18 auxiliary/scanner/http/apache_link_jobmanager_traversal             normal Yes    Apache Flink JobManager Traversal
19 auxiliary/scanner/http/mod_negotiation_brute                        normal No     Apache HTTPD mod_negotiation Filename Bruter
20 auxiliary/scanner/http/mod_negotiation_scanner                      normal No     Apache HTTPD mod_negotiation Scanner
21 auxiliary/scanner/ssh/apache_karaf_command_execution                2016-02-09     normal No     Apache Karaf Default Credentials Command Execution
22 auxiliary/scanner/ssh/apache_karaf_login                            normal No     Apache Karaf Login Utility
23 auxiliary/scanner/http/apache_nifi_login                            normal No     Apache NIFI Login Scanner
24 auxiliary/scanner/http/apache_nifi_version                          normal No     Apache NIFI Version Scanner
  
```