## EXPERIMENT 9

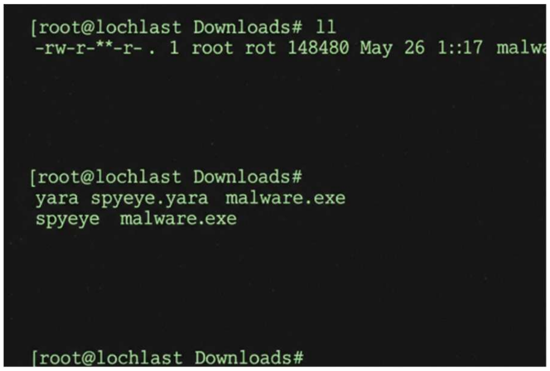
**Aim:**

To write a yara script to detect spyeye, a type of malware file.

**Yara Script:**

```
rule spyeye : banker

{

meta:

author = &quot;Ben&quot;

description = &quot;SpyEye X.Y memory&quot; date = &quot;2022-05-25&quot;

version = &quot;1.0&quot; filetype = &quot;memory&quot;

strings:

$g = &quot;bot_version&quot;

$h = &quot;bot_guid&quot;

condition:

any of ($g,$h) and filesize &gt;50000
```

**Output:**



```
[root@lochlast Downloads# ll
 -rw-r-**-r- . 1 root rot 148480 May 26 1::17 malwa



[root@lochlast Downloads#
 yara spyeye.yara  malware.exe
 spyeye  malware.exe



[root@lochlast Downloads#
```