Linux Privilege Escalation

1. What is the hostname of the target system?

```
Last login: Fri Jun 18 04:38:27 2021 from 10.0.2.15
Could not chdir to home directory /home/karen: No such file or directory
$ hostname
wade7363
$
```

2. What is the Linux kernel version of the target system?

```
$ cat /proc/version
Linux version 3.13.0-24-generic (buildd@panlong) (gcc version 4.8.2 (Ubuntu 4.8.
2-19ubuntu1) ) #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014
```

3. What Linux is this?

```
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)
```

4. What version of the Python language is installed on the system?

```
$ python
Python 2.7.6 (default, Mar 22 2014, 22:59:56)
```

5. What vulnerability seem to affect the kernel of the target system? (Enter a CVE number)

This module attempts to exploit two different CVEs related to overlayfs. CVE-2015-1328: Ubuntu specific -> 3.13.0-24 (14.04 default) < 3.13.0-55 3.16.0-25 (14.10 default) < 3.16.0-41 3.19.0-18 (15.04 default) < 3.19.0-21 CVE-2015-8660: Ubuntu: 3.19.0-18 < 3.19.0-43 4.2.0-18 < 4.2.0-23 (14.04.1, 15.10) Fedora: < 4.2.8 (vulnerable, un-tested) Red Hat: < 3.10.0-327 (rhel 6, vulnerable, un-tested)

Automated Enumeration Tools

LinPeas	https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS
LinEnum	https://github.com/rebootuser/LinEnum
LES (Linux Exploit Suggester)	https://github.com/mzet-/linux-exploit-suggester
Linux Smart Enumeration	https://github.com/diego-treitos/linux-smart-enumeration
Linux Priv Checker	https://github.com/linted/linuxprivchecker