NETSEC

Ramblings of a NetSec addict

Linux Privilege Escalation Scripts

Peleus

In pen testing a huge focus is on scripting particular tasks to make our lives easier. As a result I need to call special attention to some fantastic privilege escalation scripts at pentest monkey and rebootuser which I'd highly recommend.

LinEnum

http://www.rebootuser.com/?p=1758

This tool is great at running through a heap of things you should check on a Linux system in the post exploit process. This include file permissions, cron jobs if visible, weak credentials etc. The first thing I run on a newly compromised system.

LinuxPrivChecker

http://www.securitysift.com/download/linuxprivchecker.py

This is a great tool for once again checking a lot of standard things like file permissions etc. The real gem of this script is the recommended privilege escalation exploits given at the conclusion of the script. This is a great starting point for escalation.

g0tmi1k's Blog

http://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

Not so much a script as a resource, g0tmi1k's blog post here has led to so many privilege escalations on Linux system's it's not funny. Would definitely recommend trying out everything on this post for enumerating systems.

Filed Under: Privilege Escalation

Tagged With: linux, privilege escalation