Privilege Escalation in Linux: Supplement

Exercises

1. Chapter 8 showed how to use Responder to attack Windows clients on a Windows domain. Do such attacks work against Linux clients joined to a Windows domain?
2. Exploit an Ubuntu 16.04 system. Try exploit/linux/local/netfilter\_priv\_esc\_ipv4
3. Exploit a CentOS 6.5 x64 system. Try /exploit/linux/local/libuser\_roothelper\_priv\_esc. How well does it function on other versions of CentOS?
4. Verify that Dirty COW fails when run against files that the attacker does not have read access.
5. Can a Dirty COW exploit be created that modifies cron rather than /etc/passwd?
6. Construct a Linux system and install NMap. Set it as SUID root. Use the Metasploit module exploit/unix/local/setuid\_nmap to escalate privileges.