Cheat Sheet for Privilege Escalation Enumerations

- Linux Privilege Escalation Enumeration Cheat Sheet:
  - id = info on current user on linux
  - cat /etc/shadow = prints all usernames and password hashes
  - hostname = provides host name
  - cat /etc/issue
  - cat /etc/*-release
  - uname -a = kernel version and architecture
  - ps axu = prints running processes and users running them in user readable format
  - ip a = tcp/ip config of all interfaces and shows all information
  - /sbin/route or /sbin/routel = routing table
  - ss -anp = list all network connections and sessions
  - grep -Hs iptables /etc/* = looks for iptables commands
  - cat /etc/iptables-backup =prints these rules
  - /etc/cron.daily = daily tasks
  - /etc/cron.weekly = weekly tasks
  - cat /et/crontab = system admin added tasks with potentially insecure permissions
  - dpkg -l = list installed packages
  - yum list installed = list installed packages on redhat linux
  - find / -writable -type d 2>/dev/null = looks for world writable directories
  - mount = prints all drives mounted
  - cat /etc/fstab = all drives mounted at boot time
  - /bin/lsblk = partition information, try to mount them if unmounted
  - lsmod = list loaded modules
  - /sbin/modinfo modulename = more info about module
- Windows Privilege Escalation Enumeration Cheat Sheet:
  - net user = includes info on other users
  - hostname = provides host name
  - systeminfo
  - tasklist /SVC = prints running processes not by privileged users
  - ipconfig /all = displays full config of all adapters
  - route print = prints routing tables
  - netstat -ano = view all active tcp connections along with address/port number/process id
  - netsh advfirewall show currentprofile = view current firewall profile

    if profile is on:

    netsh advfirewall firewall show rule name=all = show all firewall rules

- schtasks /query /fo LIST /v = displays scheduled tasks and displays as a list with verbose output
- wmic product get name, version, vendor = enumerate installed applications and versions installed by windows installer
- wmic qfe get Caption, Description, HotFixID, InstalledOn = list system wide updates and when they were installed