PRIORITY

- □ Open README
- □ Solve Forensics
- □ enable/disable ssh (depending on read me)(install openssh-service to enable/ “systemctl stop ssh” then “systemctl disable ssh” to disable)
- □ Check for daily updates in Software and Updates (Ubuntu specific)
- □ Remove/Change user accounts/admin privileges
- □ Fix permissions
- □ Delete hacking tools (like wireshark)
- □ Set password requirements. (check below for detail)
- □ Install and Enable gufw (Terminal> “sudo apt install gufw”> type “gufw” and make status=ON and Incoming=Reject)
- □ Update software (Terminal> “sudo apt-update” > “sudo apt-upgrade”)

Security tools to install (“sudo apt install [PROGRAM NAME]”)

- Clamav (open it with “clamscan” after install)(virus removal tool)
- Gufw(firewall)
- Openssh-server(ssh service)
- libpam-cracklib(creates better password policies)
- Bum (Boot Up Manager) (Use “sudo bum” to run)

Looking for media files

- Use “ls -la” to also view hidden files
- To search for files use “locate *[filetype]”
    - .mp3
    - .mp4
    - .jpg (careful with these as some may be important)
    - .avi
    - .wav
    - .midi
    - .bmp
    - .gif
    - .jpeg
- “rm [PathToFile]”

For solving forensics

- Custom script wip

For password requirements

<u>Pam.d</u>

1. **MAKE SURE libpam-cracklib IS INSTALLED!!!!**

2. Through terminal (“cd etc/pam.d/”)
3. “Sudo nano common-password”
4. Find the line that says “pam_unix.so” and add “remember=5”
5. Find the line that says “pam_cracklib.so” and add “ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1” (Enforces password complexity)

1. Through terminal (“gedit /etc/pam.d/common-auth”)
2. At the end of the file add “auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800” (Sets the allowed failed login attempts to 5)

<u>Login.defs</u>

1. Go to terminal (“gedit /etc/login.defs”)
2. Set “PASS_MAX_DAYS” to “90”
3. Set “PASS_MIN_DAYS” to “10”
4. Set “PASS_WARN_AGE” to “7”

Disable guest accounts

1. Go to terminal (“sudo nano /etc/lightdm/lightdm.conf”)(might be “users.conf”)
2. Add the line “allow-guest=false” at the bottom of the file