**** Setting up Secure Shell ****

SSH IS THE SECURE SHELL. THIS IS HOW YOU REMOTELY CONTROL ANOTHER COMPUTER ACROSS A NETWORK. SSH IS INSTALLED ON MOST LINUX COMPUTERS AND CAN BE INSTALLED ON WINDOWS AND MAC AS WELL. THE SSH SERVER MUST BE RUNNING ON THE MACHINE YOU ARE TRYING TO ACCESS. FOR THIS WE WILL ONLY BE LOOKING AT DEBIAN BASED LINUX SYSTEMS (KALI, ZORIN, AND MINT ARE ALL BASED ON DEBIAN). TO ENSURE THAT THE SSH SERVER IS UP AND RUNNING ON THE MACHINE YOU WILL LOG INTO, THE 'SERVER' OR 'TARGET' MACHINE.

sudo systemctl status ssh

IF SSH IS PRESENT AND SAYS “ACTIVE” IN GREEN, STOP HERE.

IF SSH IS PRESENT BUT NOT RUNNING (DOES NOT SAY ACTIVE IN GREEN)

sudo systemctl enable –now ssh

IF SSH IS NOT PRESENT

STARTING SET UP SSH SERVER:

sudo apt update

sudo apt install openssh-server

CHECK FOR INSTALLATION AND SERVICE

sudo systemctl status ssh

TO ENABLE (IF DISABLED)

sudo systemctl enable –now ssh

Ensure that password authentication is enabled

From terminal:

sudo nano /etc/ssh/sshd_config

SCROLL DOWN TO CHANGE PASSWORDAUTHENTICATION TO YES (SIMPLY FIND WHERE IT SAYS NO, DELETE IT AND TYPE YES)

PRESS

CTRL+X Y [Enter]

RESTART THE SERVICE

sudo service sshd restart

ALTERNATIVELY, YOU CAN DO THIS FASTER USING THE SED COMMAND IN A 2 STEPS:

1.sudo sed -i 's/^#\?PasswordAuthentication .*/PasswordAuthentication yes/' /etc/ssh/sshd_config

2.sudo systemctl restart ssh