Final Project Setup and Exploitation Instructions

# Install Kali Linux VM

1. See WinCre3 Document already uploaded to the github repo

# Install Ubuntu 20.04 with Linux kernel 5.8.0

1. Navigate to <https://releases.ubuntu.com/20.04/?_ga=2.158895674.1041833567.1668977229-1417524537.1668977229> and download the desktop image (~20 min)
2. Setup a new virtual box with the iso above using all the default settings
3. Start the new virtual box, install only minimal installation, and when prompted to create a user, name the system ‘target’ and for continuity create a user with username ‘setup’ and password ‘setup’
4. Unless otherwise specified, always log into the virtual box you launch from Ubuntu using the Target::setup:setup credentials
5. With the virtual box configured to connect to the internet, download the following packages via apt:
   1. vim
   2. ssh
   3. net-tools
   4. gcc
6. Downgrade the kernel from 5.15 to 5.8.0 using Mainline Kernel Installer
   1. Add the repository with the command sudo add-apt-repository ppa:cappelikan/ppa
   2. Add the repository to your source lists sudo apt update
   3. Install Mainline Kernel Installer sudo apt install mainline
   4. Once installed, launch Mainline Kernel Installer and navigate to the 5.8.0 kernel and click ‘install’
   5. When the installation is finished close the window but don’t yet reboot.
   6. Edit the grub configuration to set the default kernel as the last one you boot into
      1. Edit the config file sudo vim \etc\default\grub and add the following lines:  
         GRUB\_SAVEDEFAULT=true  
         GRUB\_DEFAULT=saved
      2. Update grub sudo update-grub
   7. Reboot your machine using the command reboot
   8. On the splash screen for Virtual Box, press and hold the ‘Shift’ key to open the Grub Menu
   9. Select ‘Advanced Options’
   10. Find, select, and boot the 5.8.0 kernel
   11. Once your virtual box launches, confirm you are on the correct kernel by querying uname -a
   12. Reboot your virtual machine once more using the reboot command and verify it automatically boots into the 5.8.0 kernel using uname -a
7. Create a read-only user in the target VM
   1. Create a new user that does not have root privileges, for continuity use the username ‘readonly’ and password ‘readonly’, run the command sudo useradd readonly and follow the prompts to add the password and hit ‘Enter’ to bypass all other fields

# Ensure both VM’s are on the same local host-only network

1. With both VM’s closed (not currently launched) select one of the VM’s and then select settings in Virtual Box
2. Go to the ‘Network’ tab
3. Select ‘Host-Only’ from the drop down
4. Repeat for the second VM
5. Ensure the setup is correct and VM’s are appropriately linked
   1. Launch both VM’s
   2. Run the ifconfig command on both VM’s to ensure they are on the same subnet, for example both are on 192.168.XX.XXX
   3. Try pinging the other VM from each VM using ping <IP ADDR>
   4. If not successful, repeat above steps or consider using a ‘Bridged Adapter’ instead of ‘Host-Only’

# Performing the Exploit

1. Launch both VM’s
   1. Log into Kali with default credentials
   2. Log into Ubuntu target with setup credentials
2. Get the IP address from the target machine by running the command ifconfig in the target machine
3. SSH into the target machine from the Kali machine by using the command ssh readonly@<IPADDRESS>
4. Find a location that you want to and can write in from the ‘readonly’ account, I recommend ~/Documents/ and copy the exploits c file from the github repo to this location
5. NOTE: Take the time to understand what the exploit file is doing – it is going to replace the password hash for the root user with the corresponding hash for ‘SecurePassword’ in the cached /etc/passwd file, allowing the attacking machine to use that new password for root until the cache is cleared or the machine is rebooted
6. Compile the c file using the command gcc -lcrypt dirtypipe\_passwd.c -o dirtypipe\_passwd to create the executable
7. Run the command id from the ssh terminal in the Kali machine to verify the user and permissions for your current shell, you should see something like  
   Graphical user interface

   Description automatically generated with medium confidence
8. Execute the exploit ./dirtypipe\_passwd  
   Text

   Description automatically generated
9. You can verify the corresponding entry for the passwd file has been changed by running head -n 1 /etc/passwd from the ssh shell on the Kali machine  
   
10. Log into root from the ssh shell by running su - and when prompted for the password use the new password ‘SecurePassword’
11. You are now logged in as root, use the id command to verify you are now logged in as root  
    