# Linux Lab 5 - Apps and Services SysV

We will install a service that we will use later, SSH server. SSH is secure shell, and it allows us to connect to our VM via an encrypted terminal connection. We will practice starting and stopping it with the service command. Then we will create our own service, EvilHackerBackdoor, and see how it appears in the file system, ps, and Boot-Up Manager.

SSH needs two components to work properly. One computer must be listening for SSH connections using an SSH server or daemon (often abbreviated sshd, although Ubuntu calls it ssh.) A second computer uses an SSH client to initiate a connection to the SSH server.

# Practice with SSH server on your Ubuntu VM

If you were to Google “install ssh server on ubuntu desktop” you would find that the common SSH installation is called openssh-server. You can find it in the Ubuntu Software Center GUI, or, you can install it very quickly from the command line.  
 sudo apt-get install openssh-server

Once the SSH server is installed, you can check its status several ways. One is to use the SysV service command.  
 sudo service ssh status

Another is to use the ps command. There will be a lot of output, so you can save time by piping the output into grep  
 ps aux | grep ssh  
(Note that the file that is actually running is sshd, which is what other distributions call the SSH server service. I’m not sure why Ubuntu uses ssh--normally that refers to the client.)

Yet another way is to use the Boot-Up Manager. When you find the ssh service, you’ll see that it is running even though the “activate” box is not orange. This is because the service is being controlled by Upstart.

Stop and start the ssh service a few times, and check the result using the service command, ps, and Boot-Up Manager.

# Create an evil service using SysV

This is what a service script might look like.

#!/bin/bash  
# chkconfig: 2345 55 25  
# description: 0wn3d!  
echo “A truly evil attacker could do anything here.”

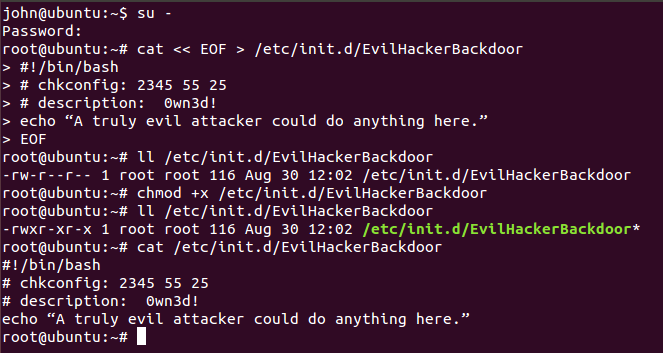
The first line tells Linux that the file should run in a BASH shell (we’ll cover this later in BASH scripting.) The second is a standard SysV line, although Ubuntu 14 does not support chkconfig. The meat of the script is the line without the comment (#) symbol, the last line. For now, we’re just writing a message to the display. In a real attack, this could be one or more lines of BASH commands that connect back to the attacker’s computer.

Create the file, /etc/init.d/EvilHackerBackdoor. You can use nano, gedit, or the attacker technique shown below.

Often, an attacker has a remote connection to the victim machine that gives command access but does not support text editors. In that case, the attacker can use a redirection technique called a “heredoc” to create the multi-line script. We will cover redirection in detail later, but here is the basic command:  
 cat << EOF > /etc/init.d/EvilHackerBackdoor

The “<< EOF” portion tells BASH to take input from the keyboard until it sees the characters “EOF” and then quit. The portion, > /etc/init.d/EvilHackerBackdoor, tells BASH to send the output to the file instead of sending it to the screen.

To make this screenshot, I pasted the “cat” line into root’s terminal. Then I pasted the script above and typed “EOF” to stop the script entry. Don’t forget to use chmod to make the script executable. Finally, I checked the file content using cat.



# Hand in

Show screenshots of the following actions:

1. A directory listing of /etc/init.d that shows you’ve created the evil script.
2. Start the service using root, or sudo service EvilHackerBackdoor start. What happens? Note: we didn’t put anything in the script other than an echo statement, so it will just execute and stop.
3. Use Boot-Up Manager to activate the evil script. If you use the advanced selection and the services tab, you should see S20 for the script in runlevels 2 - 5. (screenshot)
4. Make a screenshot of the results of ls -l /etc/rc5.d. Is there a suspicious service?
5. Completely remove the evil service. Show screenshots of your work.