This lab will use Tini as a backdoor program and mFileBinder as a wrapper program to disguise Tini inside another program as a backdoor Trojan horse. Tini is a program that allows backdoor command line access to the victim computer across a telnet connection using TCP port 7777.
Windows2008 server will be the victim computer Win7 will be the hacker computer

Lab Preparation
Use VMware workstation to open the **Win2008** and **Win7** VMware images. The password is **Windows1.**

Assign IP addresses to both computers to be on the same subnet.
Assign IP address 10.81.10.1 to the **Win7 image**
Assign IP address 10.81.10.2 to the **Win2008 image**
Subnet mask 255.255.255.0 Leave the Default Gateway blank
Assign the network adapters for both images to **Host-only**

On the Win2008 image create a user account with your ***FOLusername*** and assign administrator privileges
Start - Control Panel - User Accounts – Manage Another Account – Create a new account Assign FOLusername - Select – Administrator – Create account

Enable Telnet Client on Win7 VMware Image
Select the following
Start – Control Panel – Programs
Under the **Programs and Features** option click on **Turn Windows features on or off**
Scroll down in the menu box and select **Telnet Client – OK** Close Control Panel

Exploit #1 – Backdoor access with Tini
On Win2008 **victim** computer login with the user account with your ***FOLusername*** Open the Task Manager.
Pressing the **Ctrl Alt & Insert** keys will open Task Manager in the VMware guest operating system.
Remember that your keyboard and mouse normally connect to the host computer operating system. To direct input to the VMware guest operating system press the Ctrl and G keys or click the mouse in the VMware window.
Verify with the **Task Manager** that no **cmd.exe** sessions are running in the Win2008 **victim** image
If a **cmd.exe** session is open, then stop the application with Task Manager
Logoff as administrator and logon as the user with your FOLusername

On drive C: find the **security** folder and the **Tini** folder
Have both **Task Manager** and the **Tini** folder shown on the desktop view
Select **tini.exe** and double click to execute the program
From the **Task Manager Process** tab note that a **Tini** session is now running and **cmd.exe** is now running. The cmd.exe program is running in the background and is not shown on the monitor screen.

1. ***Take a screen capture showing the Task Manager window Processes tab (Tini & cmd.exe)***

These processes are owned by the user that launched the programs. Since we logged on as your **FOLusername** cmd.exe lists the user as your name

The **netstat** command can be used to list all running process and the port that they are listening on for a connection. Tini listens on TCP port 7777 for a connection.
On the **Win2008** victim computer open a command prompt (Start – Run – enter **cmd** in the Run window)

At the prompt enter the following command

C:\> netstat –nao
This will display all of the listening process.

To just verify that Tini is running use the following command

C:\> netstat –nao | find "7777"

2. ***Take a screen capture of the netstat command make sure the process id (PID) is included***

On the **Win2008** image open notepad.exe and enter your full name as the text content and save a file in the C:\security\tini directory (folder) with your **first name** as the file name.

From the hacker computer use tini to establish a backdoor connection to the victim computer
On the **Win7 Hacker** computer open a command prompt and enter the following command **C:\> telnet 10.81.10.2 7777**
Press **enter twice** to complete the command
This command instructs the telnet program to use port 7777 for the connection rather than the default port 23 You will now have command line access in the directory that Tini resides on the Win2008 ***victim*** *computer* ***C:\security\tini***
From the command prompt ***C:\security\tini***> use the **dir** command and find the file **your First Name.txt** to verify this is the victim computer file system.

3. ***Take a screen capture of the directory listing***

On the **Win2008** computer verify that **Tini** is running and a connection has been established from the hacker computer use the following command

C:\> netstat –nao

Note that **10.81.10.2:7777** has a connection established from the ***foreign*** host 10.81.10.1

4. ***Take a screen capture of the netstat command make sure the process id (PID) is included***

Close the **cmd.exe** window on the **Win7 hacker** computer to terminate the session

Exploit #2 – Add tini.exe to startup menu of the users on the victim computer
To ensure that the hacker has access to the victim computer when different users logon tini.exe could be copied to the startup menu
Use the task manager to halt any running sessions of **tini.exe & cmd.exe** on **Win2008 image**

Logoff as the user with your FOLusername and logon as the administrator

Open a command prompt and change to this directory
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Copy the **tini.exe** program to the **C:\ProgramData\Microsoft\Windows\Start Menu\Programs \Startup**
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup> **copy c:\security\tini\tini.exe**
Use the dir command to verify tini.exe is now in the startup directory

On the **victim** computer restart and log back on as a user with **your FOLusername**

Use the **Task Manager** to verify that **tini.exe & cmd.exe** are both running on the victim PC.
Note the logon user is the owner of the process

5. ***Take a screen capture of Task Manager showing your name as the owner of tini.exe***

Note that Tini is now running with your username

Exploit #3– Create a Trojan Horse Program

On the Win7 computer use Task Manager to stop tini.exe and all cmd.exe sessions that are running

Find the program **felix.exe** in the Security folder (look for the paw print icon) Double click on **felix.exe** to run the program.
You will see a black and white cat moving around on the desktop.
This is the program which we will use to hide the Tini backdoor program to create a Trojan Horse program.
Use Task Manager to stop the **felix** program

From INFO6001 course content download the file **mFileBinder v1.0.rar** and copy into the Win7 **C:\security** folder
Right click on the **mFileBinder v1.0.rar** and extract the executable program
The executable file will be copied into **C:\security\mFileBinder** folder

Open a File Explorer window and copy the **felix.exe** and **tini.exe** files into the **mFileBinder** folder

Double click on the **mFileBinder.exe** program
When the **mFileBinder v1.0** program opens click on click ***here to Browse***
Select the **tini.exe** file - **Click Open** - Next click **Add File** Repeat the above steps for the **felix.exe** file.

Next click on the **Set Icon** button. Select the **8Ball** from the available icons and click **Open** Next click **Build/Bind Files**
For File name enter your initials as the filename
In the location bar at the top save the file to the **C:\security\mFileBinder** folder Click **OK** for message box **File Successfully Binded**
Notice that a file has been added to the folder with your ***initials*** and the **8Bal**l icon
This new program is actually a Trojan horse program that combines both Felix and the backdoor program Tini.

Double click on the newly created file. Felix the cat will appear on the screen and tini.exe and a command prompt will also be opened and be running in the background

Run netstat to verify that port 7777 is now listening

6. ***Take a screen capture that shows* the netstat –nao | find "7777" *and also shows felix on the desktop***