NetBus is a program that can be used as a RAT - Remote Administration Tool. It can be used for legitimate or malicious purposes and accesses ports similar to EAP / TCP NetBus consists of two parts, a server and a client program. The server program (patch.exe) must be running on the computer you wish to administrate (victim). The client program (netbus.exe) is used to connect by the hacker to another computer that has patch.exe running in the background.

**Use the Snipping Tool to capture the 9 steps and 1 question below and insert into a .ppt file. Add a cover sheet with the Course info, Assignment name, date and Student information - submit to the Submissions dropbox.**

Lab Setup

This lab requires the use of 2 VMware images. You will need to disable the Firewall on both systems to allow a hacked connection. *Login with the Administrator account on both VMs.*
Open the provided **Win7 VMware** image. This will be the **hacke**r computer.
Assign IP address **10.81.10.1/24** and set the Network Adapter to **Host-only** mode.
Open the provided **Win2008 server VMware** image. This will be the **victim** computer.
Assign IP address 10.81.10.2/24 and set the Network Adapters to **Host-only** mode.
Open a command prompt and ping the other VMware image to prove connectivity.

On the Win2008 **victim** VMware image create a folder with ***your FOLusername*** as the folder name. Use notepad to create a file with your full name as the content and save the file with ***your first name*** as the file name.

On the Win2008 **victim** VMware image find the **NetBus** folder in the **C:\Security** folder to install the NetBus server just double click on **patch.exe.**
***Note: you don't see patch.exe when it's running – it runs in the background.***
On the **Win7 hacker** VMware image navigate to the **c:\security\netbus** folder and right click on the **netbus.exe** program and run as an administrator.
In the NetBus client console enter the IP address of the victim computer and click connect. By default, the NetBus client connects to port **TCP 12345**
On the Win2008 image open **Task Manager** and select the **Processes tab** to verify that **patch.exe** is running.

1. ***Take a screen capture of Task Manager***

On the Win2008 image open a command prompt and enter the command **netstat –nao**

2. ***Take a screen capture of the netstat command***

By default, patch.exe installs itself into the Startup group so it starts automatically every time Windows starts.

On the Win2008 victim computer click **Start – Run**
Enter **msconfig** as the program to run
In the **System Configuration** Window, click on the **Startup** tab.
Note that **Patch**.exe is listed in the Startup group

3. ***Take a screen capture of the Startup tab***

**Perform the following actions on the NetBus control panel on the Win7 image and observe the results on the Win2008 sever target PC**

**1.** Select the Scan button. The subnet can be scanned to find computers running patch.exe Modify the entries to scan from 10.81.10.1 to 10.81.10.10 then perform a scan.

**2.** Listen for keystrokes on the victim computer.
Select the button labelled ***Listen*.**

Open **Wordpad or Notepad** on the Win2008 victim computer and enter some text.
All keystrokes are displayed in the hacker **Listen** window.
From the hacker computer enter text in the **Listen (and send)** window.
Enter a message to be sent to the victim computer. (***I am watching you***)

**3.** Select the **Key Manager** button and disable selected keys on the victim computer keyboard.

Test that the selected keys are not working on the victim.
Re-enable the keys

**4.** Select the **File manger** button. In the remote file manager window select show files and find the folder with your FOL username stored on the victim computer.

Files can be downloaded, deleted or uploaded. *(This process may take some time to complete. You can continue with the next step while this process is being performed.)*

***4. Take a screen capture of the file manager with your folder name***

**5.** Select the show image button. Any jpg or bmp extension file on the target computer can be made to be displayed on the monitor. Find any image file in the target computer and enter the path and file name in the image window of the client program to have the image displayed Try c:\security\plane.jpg
The plane jpg image will be displayed on the victim screen

**6.** Select the **Msg manager** button. In the Message manager window enter a message to be sent to the target computer. Select the button to identify the message type as Warning or Retry/Cancel

Send "Hello my name is <*your name*> "

***5. Take a screen capture of the message***

**7.** On the victim computer open Wordpad and enter your name. From the NetBus control panel on the hacker computer select the Screendump button to retrieve the current screen out from the victim computer.
The screen image can be saved as a jpeg file to be viewed later.

**8.** Select the **Start program** button. When the window opens enter the path to execute a program on the victim computer.

Try c:\windows\system32\calc.exe

The Windows calculator program will be displayed on the victim screen

**9.** Select the **Exit Windows** button to control the target computer. Control options are logoff, shutdown, reboot and power off.

**Netbus Options**

Several options can be set such as changing the listening port number, set a password and get an e-mail notification when the victim installs the patch.exe program

Set the listening port number

On the Win2008 victim computer use Task Manager to stop the patch.exe program Press the **ctlr alt insert** keys. And click the Start Task Manager button
In the Task Manager window Process tab click on **Patch.exe** and then click the **End Process** button and confirm.Open a command prompt and change to the **C:\security\netbus** directory
Enter the following command
C:\security\netbus> **Patch /port:20016** Patch will now listen on TCP port 20016 instead of the default 12345.
Restart the patch program and connect from the Win7Netbus console

Set a password

Set your FOL username as the password to gain access to patch program on the victim computer.

**Stop the patch program**

From the command prompt enter the command
C:security\netbus\> **Patch /pass:*yourFOLusername***
**Restart the patch program**

From the hacker computer start a connection to the victim computer
*Remember to change the port number to 20016*

6. ***Take a screen capture showing the new listening port to make the connection and the password prompt window***

7. ***Take a screen capture of the netstat –nao command showing the new listening port and the connection from the Win7 computer***

**The above options can be set in the NetBus Console**

Select the **Server Setup** button
In the Window set the port number to be **44177** and set a password of **Fan1** and click **Send setup .** Note the option to send an email notification to the hacker when patch is installed and running.

On the victim computer use Task Manager to stop patch.exe.
Restart patch and connect from the hacker computer
Note that the new port number and password are required to access the victim

8. ***Take a screen capture of the netstat –nao command showing the new listening port***

9. ***Take a screen capture showing the connection established using port 44177***

Remove patch.exe
C:\security\netbus\> **patch /remove -** removes patch from memory, startup group and registry. Verify by checking the **Task Manager** and **msconfig**

**10.** ***After completing all the actions, consider the options which you think could be the most useful to a hacker and explain why these are a security problem.***
***Enter your answer on Slide 10.***

Please submit your single .pptx answer file.

File name format = <*your_FOLID*>_LabA4_23W.docx