Lab 2

Getting Ready for the Lab

(1) On the course VM, open the `D:\4630 Lab Start` folder and double click `lab2-start` to start the VMs for this lab: Windows 7 [217] and Win2003 [151].
(2) If you see an error message on Windows 2003, simply click "OK" to dismiss it and proceed:

(3) Enter `bcis4630` as the password to log on to Win2003.
(4) *In the Win2003 VM*, follow steps similar to those in previous labs and HOICs, change the third octet of its IP address to your assigned number.

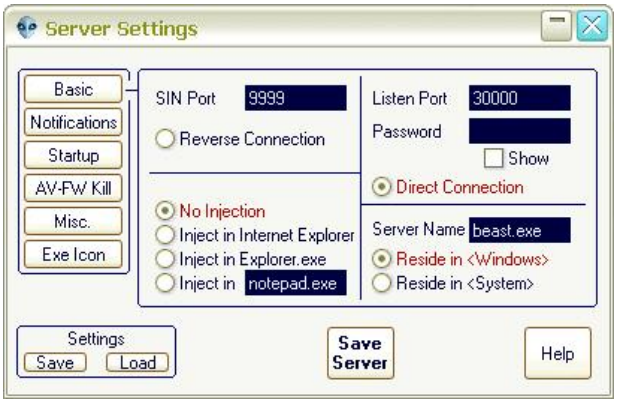
This lab is made up by two sections. In the first section, you'll configure the server component of Beast trojan. Then, in this lab environment, we emulate the task of getting the server onto the victim by simply mapping a network drive and copying the component over (for some methods of getting the victim to be infected with trojans, see my *Malware* slide deck). You then will remote-control the victim with the trojan, such as accessing the desktop of the victim, uploading files to it, etc. Feel free to explore the variety of "functionalities" in Beast even though they're not required by the lab. In the second section, you'll try to hide the existence of the trojan by using the Hacker Defender rootkit. When done correctly, the process, network ports, and files used by the trojan (and the rootkit itself too) will be hidden from view.

1. Beast Trojan

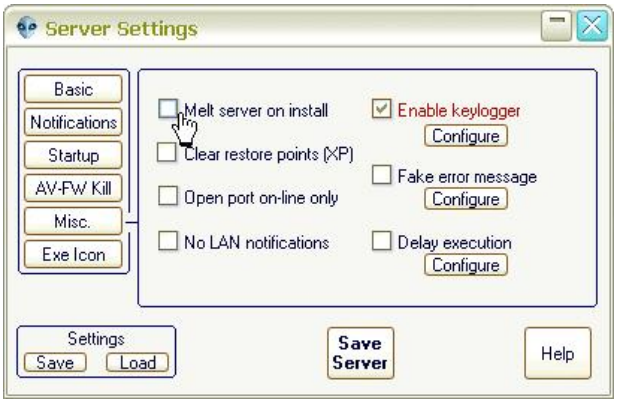
*Do the following in the **Windows 7** VM (`10.1.xx.217`):*

(1) Open `E:\Tools\Beast\207`.
(2) Double-click `Beast2.07.exe`. This opens the Beast window.
(3) Click "Build Server":

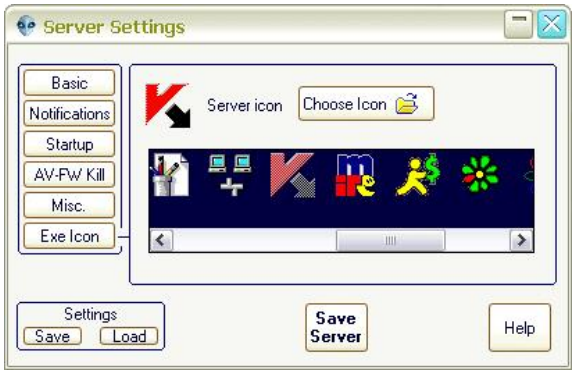
(4) In the "Server Settings," change the "Listen Port" to `30000`:



(5) Change "Server Name" to `beast.exe`.
(6) Click the "Misc." button on the left.
(7) Clear the checkbox for "Melt server on install":

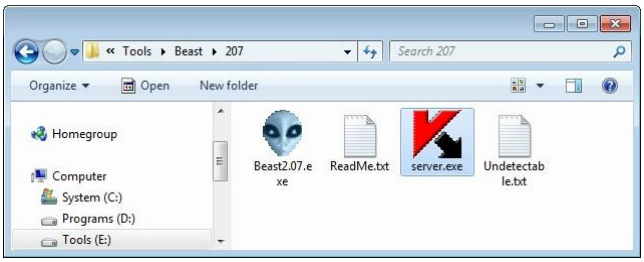


(8) Click "Exe Icon" on the left.
(9) In the right panel, scroll to the right and select the Kaspersky icon:

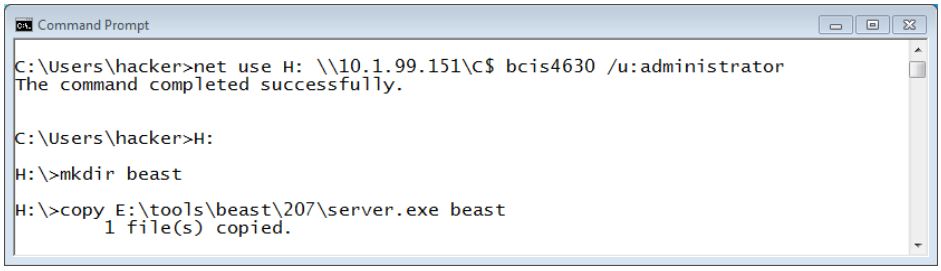


(10) Click the "Save Server" button.
(11) Click "OK". This creates the server component of the Trojan:

(12) Close the "Server Settings" window.
(13) Go to `E:\Tools\Beast\207` and make sure you see the new file `server.exe`:



(14) Open a command console.
(15) Run command: `net use H: \\10.1.xx.151\C$ bcis4630 /u:administrator` (change the `xx` to your assigned octet number).
(16) Change your working directory to the mapped drive by running: `H:`
(17) Create a new folder by running: `mkdir beast`
(18) Copy the server component to the target by running the command:
`copy E:\Tools\Beast\207\server.exe beast`
Now, we have copied the server component to the victim.



*Do the following in the **Victim 2003** VM (`10.1.xx.151`):*

(19) Start the task manager.
(20) Click the "Processes" tab.
(21) Click the "Image Name" column header so that the processes are sorted in alphabetic order.
(22) Take a screenshot of the Task Manager screen.
(23) Answer Question 2.1.1 in the worksheet.
(24) Open a command console.
(25) Run: `netstat -n`
(26) Scroll the output, if necessary, so that those lines starting with `TCP` and `10.1.xx.151` are visible. Take a screenshot of the command console.
(27) Answer Question 2.1.2 in the worksheet.
(28) Double-click `C:\beast\server.exe`.

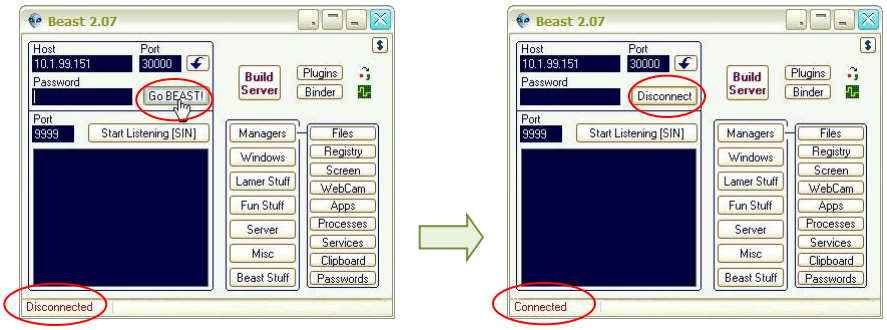
*Do the following in the **Windows 7** VM:*

(29) Go to the "Beast 2.07" window.

(30) In the "Host" textbox, enter `10.1.xx.151`.

(31) Change the port number in the "Port" box to `30000`.

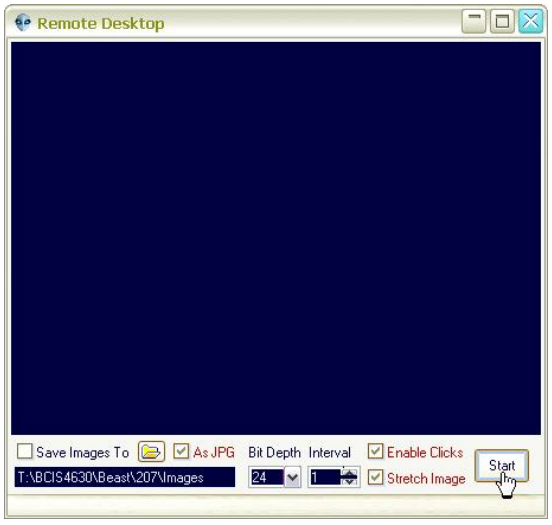
(32) Click the "Go BEAST!" button:



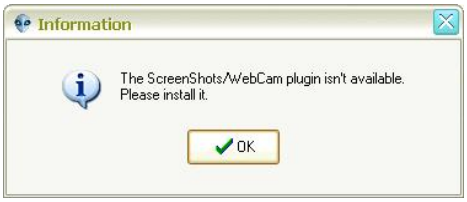
(33) Wait until the status in the bottom-left corner changes from `Disconnected` to `Connected`.

(34) In the right panel, make sure "Managers" is selected. Then click "Screen":

(35) Click "Start" in the "Remote Desktop" window:

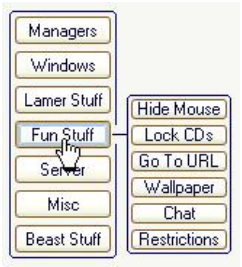


(36) *If* you see a dialog box about a plugin is not available, click "OK":

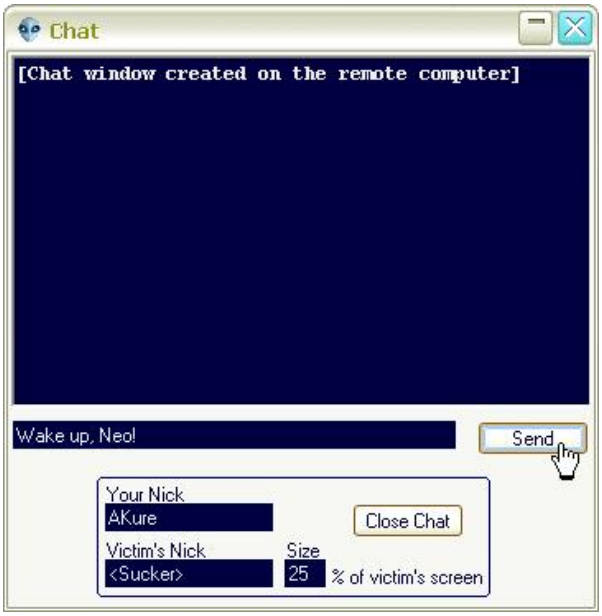


(37) In the "Plugins" dialog box, check "Screenshots/Webcam [50KB]" and click "Upload":

(38) Close the "Plugins" dialog box when the upload is done.
(39) In the "Remote Desktop" window, click "Start" again.
(40) The desktop of the victim should appear in the window. Clear the checkbox for "Stretch Image". Make some changes on the Windows 2003 VM desktop and observe how they are reflected in the "Remote Desktop" window on the attacker machine.
(41) Take a screenshot of the "Remote Desktop" window when the victim machine's desktop is visible in it.
(42) Answer Question 2.2.1 on the worksheet.
(43) Close the "Services Manager" window.
(44) In the "Beast 2.07" window, click "Fun Stuff" button. This will bring up a new set of sub-menus (buttons):

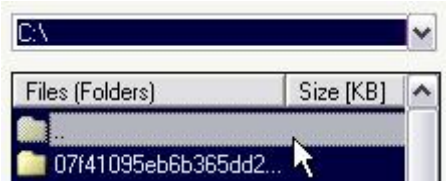


(45) Click the "Chat" button on the right.
(46) In the "Chat" window, enter `Hacker<YourTwoDigitNumber>` (in the screenshot below Andy Kure enters `AKure`) in the "Your Nick" textbox.
(47) Change the value in the "Size" box to 25.
(48) Click the "Open Chat" button.
(49) Enter `Wake up, Neo!` as the message to send.



(50) Click "Send". **Do not close the Chat window yet.**
(51) Go back to the "Beast 2.07" window and click the "Managers" button.
(52) Click "Files":

(53) In the "File Manager" window, click the "Find Drives" button.
(54) Take a screenshot of the "File Manager" window.
(55) Answer Question 2.2.2 in the worksheet.
(56) In the listing of the drive contents, click the root (folder icon followed by ..):



(57) Click the "Upload File" button on the right.
(58) In the "Upload" dialog box, click the folder icon and browse to `E:\Villain`.
(59) Select `Cartoon.jpg` and click "Open".
(60) Click "Upload".

*Do the following in the **Victim 2003** VM:*

(61) Open File Explorer and browse to `C:`.

(62) Find the file `C:\Cartoon.jpg`.

(63) With the entry for `C:\Cartoon.jpg` visible, take a screenshot of File Explorer.

(64) Answer Question 2.2.3 in the worksheet.

(65) Take a screenshot of the chat window created by Beast. It has a title of `Chat session started by Hacker<YourTwoDigitNumber>`.

(66) Answer Question 2.2.4 in the worksheet.

(67) Start Task Manager again if it was closed.

(68) Click the "Processes" tab.

(69) Make sure that the processes are listed alphabetically and make a screenshot.

(70) Answer Question 2.3.1 in the worksheet.

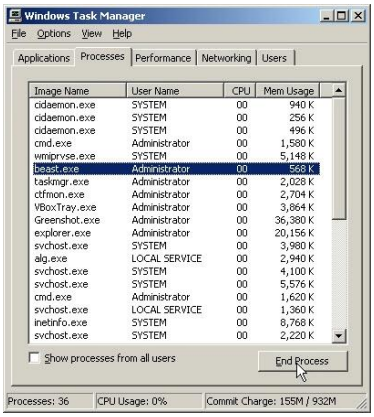
(71) Open a command console.

(72) Run: `netstat -n`

(73) Scroll the output, if necessary, so that those lines starting with `TCP` and `10.1.xx.151` are visible. Take a screenshot of the command console.

(74) Answer Question 2.3.2 in the worksheet.

(75) In Task Manager, click the process with the name `beast` and end the process:



(76) Close all the Task Manager and command console windows. Do not shutdown the VM.

*Do the following on the **Host VM**:*

(77) Open the `D:\4630 Lab Start` folder and double click `lab2-take-snapshot`.

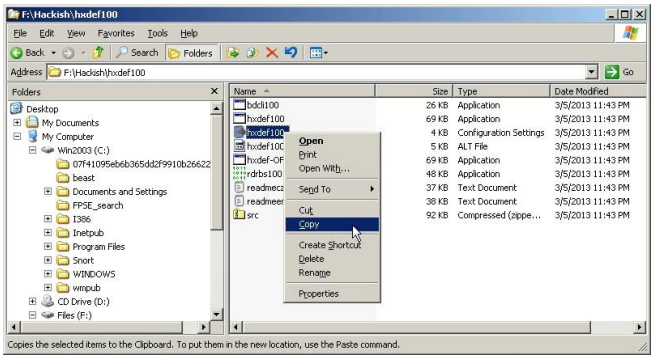
2. Rootkit – Hacker Defender

Among their many uses, rootkits can be used to hide the process, port, registry entries, and files related to the rootkits and other malware. One of the popular rootkits, HackerDefender (hxdef) does these by hooking multiple Windows APIs (in other words, replacing valid system calls or DLLs with malicious replacements). In this section, we will use it to hide the presence of Beast.

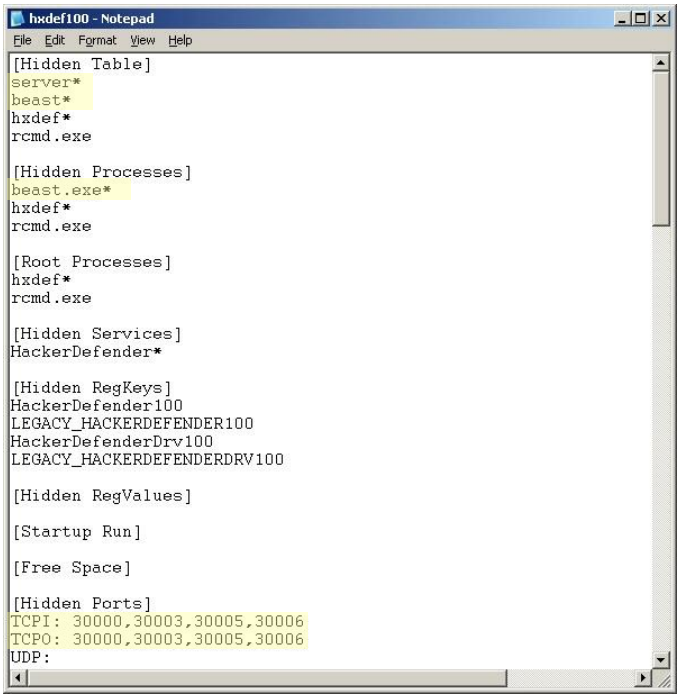
*Do the following in the **Victim 2003** VM:*

(1) Open `F:\Hackish\hxdef100`.

(2) Make a backup copy of `hxdef100.ini` by copying it and saving it as `hxdef100.bak`:



(3) Double click to edit `hxdef100.ini` with Notepad.
(4) In the `[Hidden Table]` section, enter `beast*` as a new line and `server*` as another.
(5) In the `[Hidden Processes]` section, enter a new line: `beast.exe*`
(6) In the `[Hidden Ports]` section, edit the `TCPO` line to be:
`TCPO: 30000,30003,30005,30006` (if your answer to Question 2.3.2 differs from these ports, modify this line to fit your output; for example, if you also saw `30001` in your answer to Question 2.3.2, then modify the line to read `TCPO: 30000,30001,30003,30005,30006`)
(7) Edit the `TCPI` line to be:
`TCPI: 30000,30003,30005,30006` (update the line to match your answer to Question 2.3.2 in the same manner as in the previous step).



(8) Save `hxdef100.ini` and close Notepad.
(9) Double click `C:\Beast\server.exe` to start the server component of the Beast Trojan.
(10) Close all File Explorer windows.

*Do the following in the **Windows 7** VM:*

(11) If your Beast window has been closed, double-click `E:\Tools\Beast\207\Beast2.07.exe` to start the Beast Trojan. If it's still running, skip to the next step.
(12) Make sure that "Host" is `10.1.xx.151` and "Port" is `30000`.
(13) Click "Go BEAST!".

*Do the following in the **Victim 2003** VM:*

(14) Start Task Manager again.
(15) Click the "Processes" tab.
(16) Answer Question 2.4.1 in the worksheet.
(17) Open a command console.
(18) Run: `netstat -n`
(19) Answer Question 2.4.2 in the worksheet.
(20) Open **another** command console.
(21) Change your working directory by running: `F:`
(22) Run: `cd hackish\hxdef100`
(23) Run: `hxdef100 -:refresh`
(24) Run: `hxdef100`

(25) Switch to the Task Manager window and take a screenshot of it.
(26) Answer Question 2.4.3 in the worksheet.
(27) Go back to the command console where you ran `netstat -n`. Run `netstat -n` again and then take a screenshot of it.
(28) Answer Question 2.4.4 in the worksheet.
(29) Open File Explorer.
(30) Open `C:`.
(31) Take a screenshot of File Explorer.
(32) Answer Question 2.4.5 in the worksheet.
(33) In File Explorer, go to `F:\Hackish`.
(34) Take a screenshot of File Explorer.
(35) Answer Question 2.4.6 in the worksheet.

*Do the following in the **Windows 7** VM:*

(36) Open a command console.
(37) Run: `netstat -n`.
(38) Scroll if necessary so that the `10.1.xx.151` address is visible in the third column, which lists remote machines and remote ports in connections.
(39) Take a screenshot of the command console.
(40) Answer Questions 2.4.7 and 2.4.8 in the worksheet.

*Do the following on the **Victim 2003** VM:*

(41) Go back to the command console for HackerDefender.

(42) Run: `net stop HackerDefender100.` It can take quite a while but wait until you see the result. If it reports that the service is not responding, repeat Steps (24) and (42) until it says that the service has been stopped successfully.

(43) Restart Task Manager if it has been closed.

(44) Locate the beast process and make sure it's visible. Take a screenshot.

(45) Answer Question 2.5.1 in the worksheet.

(46) Go back to the command console where you ran `netstat -n`. Run the command again.

(47) Take a screenshot of the command console with the trojan connections visible.

(48) Answer Question 2.5.2 in the worksheet.

(49) In File Explorer, browse to `C:`. If you're switching back to a File Explorer window with that location already open, refresh it. Take a screenshot with the `beast` folder visible.

(50) Answer Question 2.5.3 in the worksheet.

(51) In File Explorer, browse `F:\Hackish\hxdef100`.

(52) Answer Question 2.5.4 in the worksheet.

(53) Close all command consoles, File Explorer windows, and Task Manager windows.

Lab Submission

(1) Log in to Canvas.

(2) Open the link for Lab 2.

(3) Attach your Lab 2 worksheet.