HoneyBOT

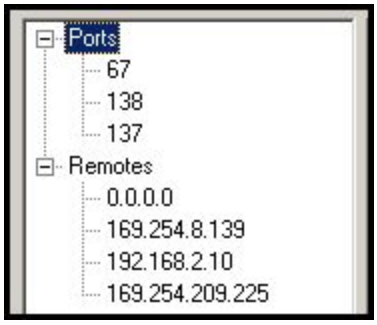
HoneyBOT is a piece of honeypot software. A honeypot is used to entice attackers by appearing to be a legitimate host with vulnerabilities, and honeypots are designed with the intent that they will be attacked. When an attacker compromises the honeypot, his/her actions are recorded and the honeypot can alert the system administrators that an attack is in progress.

A. Introduction to HoneyBOT

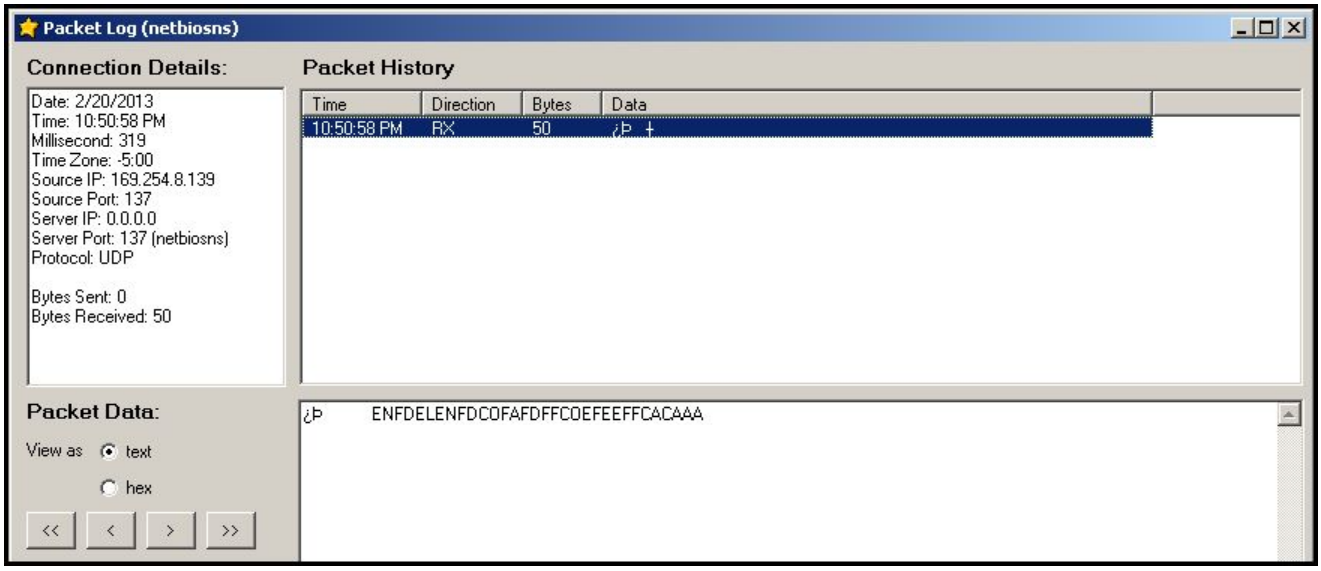
1. To open HoneyBOT, click **Start**, then type **`honey`** into the search box. Click on **HoneyBOT** to open the program.
2. You may see a **Bindings** window appear. Click OK to close the window.
3. Click on the red **Stop** button below the menu bar to temporarily stop the engine so that you can view the honeypot's settings.
4. To see what services are currently enabled on the honeypot, click on the **Services** button below the menu bar.

5. The Services window lists all of the port numbers and their respective services. If a service is marked **True** under the **Enabled** category, it means that the **port is open** (susceptible for attack). Look through the various services, then click Close.
6. To turn on the honeypot engine, click the Start button below the menu bar.

7. In the tree on the left, click the **+** sign to expand the trees for Ports and Remotes. Ports will list the various port numbers that traffic is being detected on, while Remotes will list the IP addresses of the devices that there is interaction with.



8. You should see entries begin to appear in the log. To view the contents of a recorded packet, double click on its entry to view the **Packet Log**. Under **Connection Details**, you can see the time that the packet was logged, as well as the source IP address and port (where the traffic originated from). Depending on the type of packet, the **Packet History** portion may contain detailed data showcasing an attacker's exact actions. Honeypots are even capable of recording an attacker's keystrokes. To close the Packet Log, click the **X** in the top right corner of the window.



9. You may stop recording packets by clicking the **Stop** button.

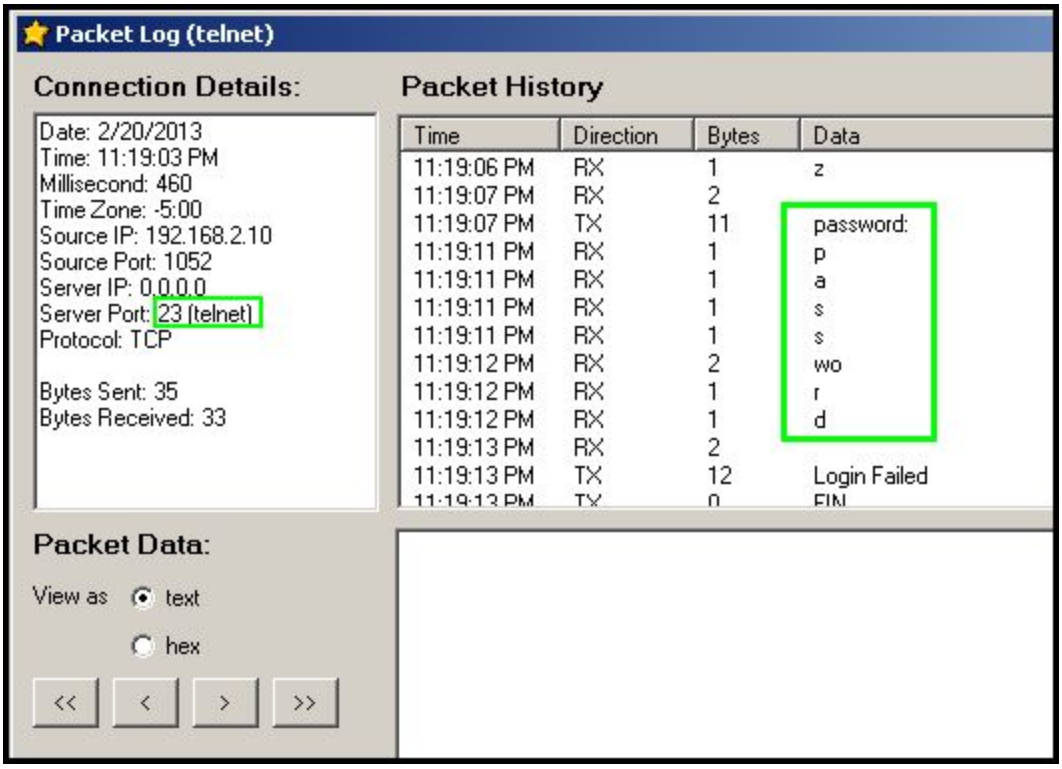
B. Launching and Analyzing an Attack

1. Open the **Command Prompt**, then type **`telnet localhost`** and press Enter. This will attempt to launch a Telnet connection into your computer. However, you should receive a message that the connection failed.
2. Type **`netstat -t 1`** and press Enter. The **netstat** command will list the active connections on your computer, and the **-t 1** means that netstat will check the active

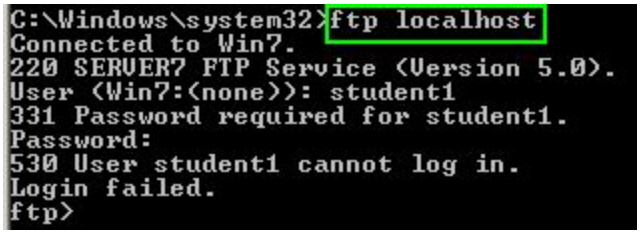
connections every 1 second. Notice that the **Telnet** service is not currently running, otherwise it would be listed here. So, Telnet is not activated on your computer.

3. Leave netstat running, and in **HoneyBOT**, click **File**, then **New** and ensure that the engine is started.
4. Open a **second Command Prompt window**, type **`telnet localhost`** and press **Enter**. This time, because of the HoneyBOT software, Telnet will proceed.
5. When the Telnet session attempts to connect to your computer, try pressing keys on the keyboard. Notice, back in the HoneyBOT window, there is a new log entry, and its byte size increases the more you type in the Telnet window. This is because HoneyBOT is documenting every keystroke you make.
6. While it is attempting to connect, press **Enter** to reach the **Password** prompt. Try typing in something for the password, then press **Enter** again.
7. In the **first Command Prompt window**, press **Ctrl + C** keys to stop the netstat command, but leave the window open. Look through the active connections. You should see a Telnet connection recorded. Remember, Telnet was not running on your computer previously, so HoneyBOT was able to create a fake Telnet connection that looked real to lure in attackers. This is the main objective of the software.

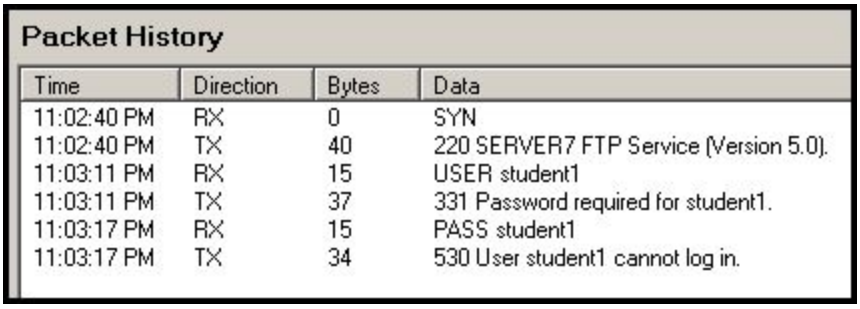
8. Back in the HoneyBOT window, you may click the **Stop** button. To analyze the log for the traffic you created, expand the **Ports** section and click on **23** (23 is the port number for Telnet). Double click on the log entry to see more details.
9. Under **Packet History**, you can see what keys you pressed when you were attempting to connect to the honeypot through Telnet. Can you see the keystrokes for the password you entered?



10. Next, you will try to capture keystrokes in **FTP** packets. In HoneyBOT, open a new log and start the engine.
11. In the Command Prompt, type **`ftp localhost`**. You will then be prompted for an FTP username and password. Type in something for each and press Enter. The connection will fail, but HoneyBOT will have recorded your actions.



12. In HoneyBOT, look under **Port 21 (FTP)**. Double click on the log entry for FTP and view its contents. You will then see the username and password that the attacker attempted to use.



Packet History

Time	Direction	Bytes	Data
11:02:40 PM	RX	0	SYN
11:02:40 PM	TX	40	220 SERVER7 FTP Service (Version 5.0).
11:03:11 PM	RX	15	USER student1
11:03:11 PM	TX	37	331 Password required for student1.
11:03:17 PM	RX	15	PASS student1
11:03:17 PM	TX	34	530 User student1 cannot log in.