HoneyBOT User Guide

A Windows based honeypot solution

Visit our website at http://www.atomicsoftwaresolutions.com/

Table of Contents

What is a Honeypot?

A honeypot is a device placed on a computer network specifically designed to capture malicious network traffic. The logging capability of a honeypot is far greater than any other network security tool and captures raw packet level data even including the keystrokes and mistakes made by hackers. The captured information is highly valuable as it contains only malicious traffic with little to no false positives.

Honeypots are becoming one of the leading security tools used to monitor the latest tricks and exploits of hackers by recording their every move so that the security community can more quickly respond to new exploits.

How HoneyBOT Works

HoneyBOT works by opening over 1000 UDP and TCP listening sockets on your computer and these sockets are designed to mimic vulnerable services. When an attacker connects to these services they are fooled into thinking they are attacking a real server. The honeypot safely captures all communications with the attacker and logs these results for future analysis. Should an attacker attempt an exploit or upload a rootkit or trojan to the server the honeypot environment will safely store these files on your computer for analysis and submission to antivirus vendors. Our test servers have captured several thousand trojans and rootkits from these simulated services including:

Dabber
Devil
Kuang
MyDoom
Netbus
Sasser
LSASS
DCOM (msblast, etc)
Lithium
Sub7

Please note that HoneyBOT is still in development and at this time not all open ports are coded to mimic their associated service.

Secure the HoneyBOT Computer

Non-production Computer

A honeypot computer should have no real information resources required of it and should not be used for any other purpose other than for monitoring the network. Although HoneyBOT will work on a production system this is strongly discouraged and we recommend only installing HoneyBOT on a dedicated system.

Remember that we are attracting attackers to intrude into this system and you should be prepared in case of the unlikely event of a system compromise.

The other reason for installing HoneyBOT on a non-production machine is because in broad terms we can then consider that any traffic to or from the machine is malicious in nature. This makes identifying malicious traffic much easier when using additional monitoring tools such as Snort.

Patches

You should protect your computer from exploits by patching your system with service packs, updates and hot fixes available from Microsoft.

Antivirus

Use an up to date antivirus product on your HoneyBOT computer as an extra security precaution.

HoneyBOT has an option to 'Capture Binaries' and if this option is enabled your antivirus will alert you and quarantine any items captured by the system. We suggest that you either disable the 'Capture Binaries' option or create an exclusion in your antivirus product. You can exclude your antivirus from scanning the c:\honeybot\captures\ folder or alternatively exclude your antivirus from scanning files with a .txt extension. For details on how to create an exclusion refer to your antivirus documentation.

Firewalls

A firewall is designed to prevent unsolicited connections from reaching your computer and would therefore prevent HoneyBOT from being attacked so you will need to relax your firewall rules to some degree.

If your firewall hardware allows it you should allow all incoming connections to the honeypot whilst denying any outgoing connections from the honeypot computer.

A software based application level firewall can be used to allow only HoneyBOT to accept incoming connections whilst denying access to all other applications and windows services.

Change default configurations

If you are running any other software or network applications on the honeypot then consider changing their default installation parameters to assist in preventing a compromise. For example, if you were using a remote desktop application to monitor your honeypot then it would be wise to change the default listening port to a random high numbered port.

Configuring the Network

Internal Network Monitoring

Ensure that the computer that HoneyBOT is installed on has been allocated an IP address and has an operational network connection. In this scenario any attacks would indicate that another computer inside the network is already infected with a virus or worm, or even that a company employee is attempting to break into the computer.

An internal network honeypot acts as a great early warning system to alert you of attacks that have already made it past your perimeter network defences.

External Network Monitoring

Placing your honeypot in an Internet environment will usually capture and log malicious activity within a few minutes and is the most common deployment environment for a honeypot.

You can place the honeypot on the Internet by using a direct Internet connection. For example using a dial up adapter to connect your honeypot computer to your ISP. In this configuration your computer is allocated a public IP address and is the easiest setup for a research honeypot.

Alternatively you can place the honeypot in your network DMZ where all unsolicited Internet probes are forwarded to your honeypot computer. This is a good solution for an organisation who have production systems along side a honeypot system as it makes it difficult for an attacker to target the real production systems.

Network Baseline

You should take a baseline of your systems default listening ports before deploying HoneyBOT and take steps to stop all unnecessary services and listening ports in order to free up those ports for HoneyBot and also to increase security on your honeypot system.

A baseline can be taken using Microsoft Netstat.exe program using the –a parameter.

Foundstone offer an excellent tool called Fport.exe that not only lists listening ports but also displays the process name that is using the port.

It is possible to prevent Windows from opening all but port 135 UDP and TCP (RPC). On our test systems we have been able to disable port 445 UDP and TCP (SMB) however we should warn that doing this also breaks browsing and sharing files on the local network.

Installing HoneyBOT

HoneyBOT is compatible with and has been tested to work on Windows 2000 and Windows XP computers. At least 128MB of ram is recommended.

1. HoneyBOT can be downloaded from our web site at:
http://www.atomicsoftwaresolutions.com/honeybot.php

2. After clicking the download link save HoneyBOT_010.exe to a location on your hard drive.

3. Double click the HoneyBOT_010.exe installation file to begin the setup process.

4. Follow the prompts in the setup process. The default installation folder for setup is c:\honeybot\

5. Setup will create a shortcut in the Start Menu folder and an option is available to create a desktop icon.

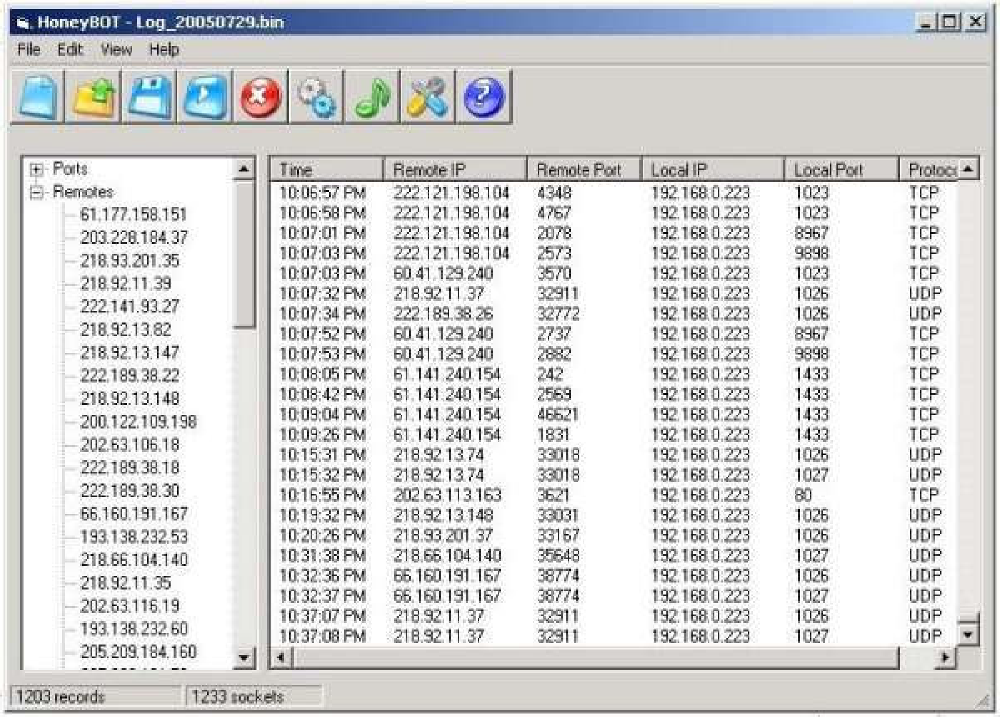
6. Now you can launch HoneyBOT using the programs shortcut icon.

HoneyBOT Application

Main Window

This is the main application window. In the left hand side is a tree view of all ports probed and remote machines responsible. You can expand the tree nodes by clicking the plus icon next to the item. On the right hand side is a list view of all hits logged by the system. The list view shows basic information about the hit including date, time, remote ip, local port, protocol, etc.

Click on one of the tree node items on the left hand side window to filter the list view to only display similar records. This can be useful to filter the list view to only hits from a specific source, or all hits on port 80 TCP (HTTP).



- Ports
- Remotes
  - 61.177.158.151
  - 203.228.184.37
  - 218.93.201.35
  - 218.92.11.39
  - 222.141.93.27
  - 218.92.13.82
  - 218.92.13.147
  - 222.189.38.22
  - 218.92.13.148
  - 200.122.109.198
  - 202.63.106.18
  - 222.189.38.18
  - 222.189.38.30
  - 66.160.191.167
  - 193.138.232.53
  - 218.66.104.140
  - 218.92.11.35
  - 202.63.116.19
  - 193.138.232.60
  - 205.209.184.160

Time	Remote IP	Remote Port	Local IP	Local Port	Protoc
10:06:57 PM	222.121.198.104	4348	192.168.0.223	1023	TCP
10:06:58 PM	222.121.198.104	4767	192.168.0.223	1023	TCP
10:07:01 PM	222.121.198.104	2078	192.168.0.223	8967	TCP
10:07:03 PM	222.121.198.104	2573	192.168.0.223	9898	TCP
10:07:03 PM	60.41.129.240	3570	192.168.0.223	1023	TCP
10:07:32 PM	218.92.11.37	32911	192.168.0.223	1026	UDP
10:07:34 PM	222.189.38.26	32772	192.168.0.223	1026	UDP
10:07:52 PM	60.41.129.240	2737	192.168.0.223	8967	TCP
10:07:53 PM	60.41.129.240	2882	192.168.0.223	9898	TCP
10:08:05 PM	61.141.240.154	242	192.168.0.223	1433	TCP
10:08:42 PM	61.141.240.154	2569	192.168.0.223	1433	TCP
10:09:04 PM	61.141.240.154	46621	192.168.0.223	1433	TCP
10:09:26 PM	61.141.240.154	1831	192.168.0.223	1433	TCP
10:15:31 PM	218.92.13.74	33018	192.168.0.223	1026	UDP
10:15:32 PM	218.92.13.74	33018	192.168.0.223	1027	UDP
10:16:55 PM	202.63.113.163	3621	192.168.0.223	80	TCP
10:19:32 PM	218.92.13.148	33031	192.168.0.223	1026	UDP
10:20:26 PM	218.93.201.37	33167	192.168.0.223	1026	UDP
10:31:38 PM	218.66.104.140	35648	192.168.0.223	1027	UDP
10:32:36 PM	66.160.191.167	38774	192.168.0.223	1026	UDP
10:32:37 PM	66.160.191.167	38774	192.168.0.223	1027	UDP
10:37:07 PM	218.92.11.37	32911	192.168.0.223	1026	UDP
10:37:08 PM	218.92.11.37	32911	192.168.0.223	1027	UDP

1203 records | 1233 sockets

Starting the Engine

Click on the blue play button to start the HoneyBOT listening engine. The status bar at the bottom of the window will increment as each port is successfully opened.

Stopping the Engine

Click on the red stop button to shut down all listening services and terminate and existing open sockets. The status bar at the bottom of the window will decrement as each port is closed.

Packet Log Viewer

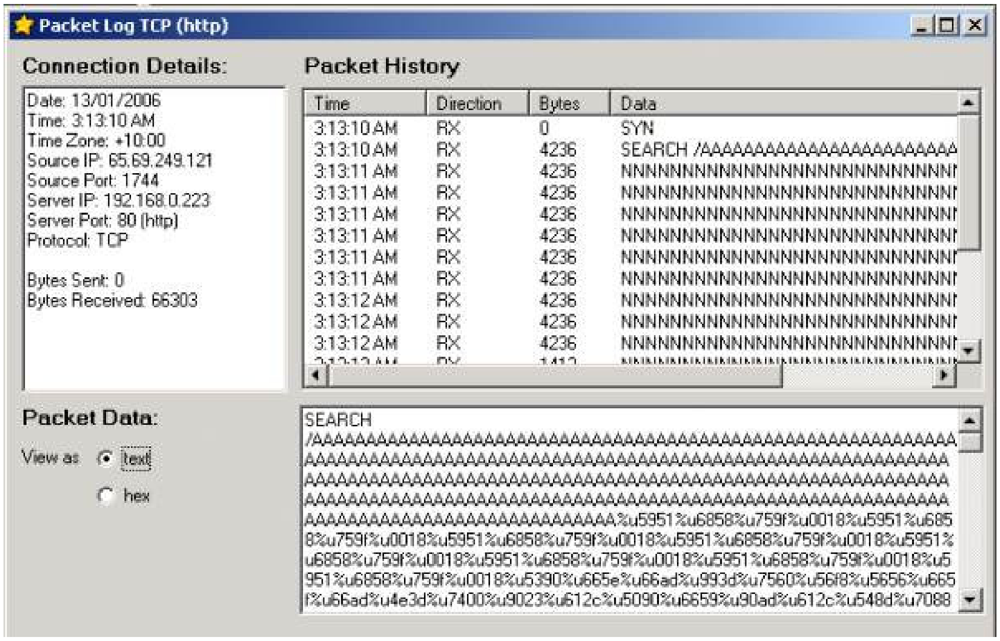
Double clicking a record in the list view of the main window will open the Packet Log viewer window.

On the upper left hand side of the window is the Connection Details which displays basic information about the selected hit including the total number of bytes sent and bytes received for that hit.

In the upper right hand side the application displays the Packet History list view of all transmitted and received IP packets associated with the hit. You can see information regarding the direction of the packet (TX or RX) and the number of bytes in each packet, and a small extract of the data within the packet.

By clicking on a record in the Packet History box you can view the complete Packet Data in the lower window. The user can select to have this Packet Data displayed in text format or hexadecimal format.

The example below shows the first data packet of an IIS Search Overflow attack.



Connection Details:

Date: 13/01/2006
Time: 3:13:10 AM
Time Zone: +10:00
Source IP: 65.69.249.121
Source Port: 1744
Server IP: 192.168.0.223
Server Port: 80 (http)
Protocol: TCP

Bytes Sent: 0
Bytes Received: 66303

Packet History

Time	Direction	Bytes	Data
3:13:10 AM	RX	0	SYN
3:13:10 AM	RX	4236	SEARCH /AAAAAAAAAAAAAAAAAAAAAAAA
3:13:11 AM	RX	4236	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
3:13:11 AM	RX	4236	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
3:13:11 AM	RX	4236	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
3:13:11 AM	RX	4236	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
3:13:11 AM	RX	4236	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
3:13:11 AM	RX	4236	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
3:13:12 AM	RX	4236	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
3:13:12 AM	RX	4236	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
3:13:12 AM	RX	4236	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
3:13:12 AM	RX	1412	NNNNNNNNNNNNNNNNNNNNNNNNNNNNN

Packet Data:

View as ● text ○ hex

```
SEARCH
/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA%u5951%u6858%u759f%u0018%u5951%u685
8%u759f%u0018%u5951%u6858%u759f%u0018%u5951%u6858%u759f%u0018%u5951%
u6858%u759f%u0018%u5951%u6858%u759f%u0018%u5951%u6858%u759f%u0018%u5
951%u6858%u759f%u0018%u5390%u665e%u66ad%u993d%u7560%u56f8%u5656%u665
f%u66ad%u4e3d%u7400%u9023%u612c%u5090%u6659%u90ad%u612c%u548d%u7088
```

Debug Log

A debug window is available by clicking Debug from the View menu. This window will display events and errors that occur during system operation.

Some events displayed will include:

- IP address that HoneyBOT is bound to
- Time zone determined from the operation system
- Engine Start and Stop commands
- Port opening errors (these are generally caused when another application is already using the port. See the section on Network Baseline to close these ports)
- Socket errors (generally caused when the TCP handshake does not complete successfully)
- Other Application errors

Options

Several options can be set by clicking Options from the View menu.

- Server Name – the fake name of the computer given to attackers
- Run as Service – currently disabled in this version of HoneyBOT
- Enable Sound Alert – plays a short sound each time the honeypot is hit
- Capture Binaries – saves trojans and other malware to a file in the captures directory

Bug Reporting and Feedback

You can submit a message to us by clicking Bug Report / Feedback on the Help menu. If you would like to report a problem with the application then please submit detailed information regarding the problem to assist us with bug testing. Please also include a copy of the Debug window and your computer specifications.

If you would like to give us your thoughts on the current version of HoneyBOT, make a suggestion for the next version, or thank the author for providing this software for free then please send us a message.

Check for Update

The user can check for updates to the application by clicking Check for Update on the Help menu. When clicking this button HoneyBOT will contact our web server to determine if a newer version of HoneyBOT is available.

If an update is available then click the Get Update button to download the new version of the application. After the update has completed downloading click the Install button to upgrade to the new version of HoneyBOT.

Please note this is a recent feature and has had little real world testing. If you encounter problems using the auto update feature then please download the complete installation package of the new version from our web site. Please submit a bug report if you encounter problems using this feature.

Log Files

All log files are saved by default to c:\honeybot\logs folder. Log files store information relating to the hits on the system and also store all data received and sent to the attacking computer. When a new log file is created the file name is defaulted to a unique name base on the system date.

It is recommended that a new log file be started each day where there are many records made by the system for faster system performance. In an internal network environment where hits are low this time can be increased.

Capture Files

If the 'Capture Binaries' option is selected then all captures will be saved to the c:\honeybot\captures folder. Binary captures are copies of executable malware so we urge caution when working with these files. When a new capture is saved it is allocated a unique name starting with the name of the trojan or backdoor used to upload the file, followed by the original filename, then a time and date stamp.

The capture files are saved with a txt extension to prevent accidental execution so be careful not to restore the original file extension and execute the file.

Capture files can be scanned with your antivirus software for easy identification.

If you are worried about saving binaries on your hard drive in any format or are even concerned that another user on your network may copy the captures and execute them then we suggest you disable the 'Capture Binaries' option.

Modifying Listening Ports

In some cases it may be required to edit the list of TCP and UDP ports opened by HoneyBOT. For example if the system is logging continuous hits on TCP 161 (SNMP) or TCP 162 (SNMPTRAP) with a source address of a network device within your network then you may want to disable listening on that port.

To disable a listening port open the service.ini file using notepad and remove the line relating to the port you want to disable. You can also add a new service by modifying this file.

The file format is:
Port (tab) Protocol (tab) Description

Where Protocol 0 = UDP and Protocol 1 = TCP

You will need to restart HoneyBOT for changes to the service.ini to take effect. The current version of HoneyBOT is limited to opening no more than 1500 concurrent ports.

Uninstalling HoneyBOT

Click the Uninstall HoneyBOT icon in the programs start menu to uninstall HoneyBOT and follow the prompts.

The uninstall process does not delete the log files or captures saved by HoneyBOT during its operation and these must be deleted manually using Windows Explorer.

Privacy Policy

Our HoneyBOT application is compiled with no advertising material, spyware, tracking functions, or any other third party applications.

Atomic Software Solutions does maintain a record of visits to our web site, the date and time of the visit to the site, the pages accessed and documents downloaded. We use these website log files to analyse trends and gather broad demographic information for aggregate use only.

If you should provide your email address when communicating with us we do not sell or provide your email address to any 3rd parties, and it will not be used for any purpose other than to relay information to you regarding your enquiry or support issue.