

RandomNet v0.1

*A tool for the random, realistic
generation of honeyd configuration files*

Andrew B. Smith

Purdue University - CERIAS

absmith@cerias.purdue.edu

Jason M. Fox

Purdue University - S3

jmfox@cs.purdue.edu

Introduction

RandomNet is a tool for generating random, realistic honeyd configuration files. It is designed for users who want to simulate large networks with honeyd, but who do not want to spend the time manually editing the complex honeyd configuration file.

RandomNet provides two interfaces for generating honeyd configuration files. RandomNet can be run off of the command line to generate honeyd config files quickly using a RandomNet configuration file. This configuration file contains necessary path information (such as the location of the honeyd directory) as well as optional arguments to fine-tune the random generation of the honeyd config file. As a second option, RandomNet can launch an easy to use GUI to help build a more descriptive RandomNet configuration file.

RandomNet was written entirely in Java for easy cross-platform use.

Installation Instructions

Since Java was used for this project, you need to have Java installed. This version of RandomNet was tested using Java 1.4.1. Assuming you have java installed, go to the directory where the RandomNet source code resides and type:

```
$ javac *.java
```

To run RandomNet, simply type:

```
$ java RandomNet
```

followed by the options of your choice. Options available are covered in the “Command Line Options” section. Appendix A gives an example of how to set up honeyd and use the created honeyd configuration file.

Command-Line Options

RandomNet supports a few command-line options. The options are the following:

- g Enable gui-mode (default is console mode)
- f [config] Loads the specified RandomNet configuration file (default is rn.conf)
- o [output] Gives the destination of the honeyd configuration file to be generated

For example, to run RandomNet in gui-mode using `rn.conf3` as an example RandomNet configuration file, type the following:

```
$ java RandomNet -f /home/absmith/Honeynet/honeyd-CVS/honeyd/rn.conf3 -g
```

Using the GUI

The easiest way to set/change options in the RandomNet configuration file is to use the optional Graphical User Interface. Using the GUI, you can select which nmap fingerprints to use, which “fake” services to run, as well as change the complexity level. The gui also supports advanced controls such as the number of routers or heirarchical layers to use in the simulated network.

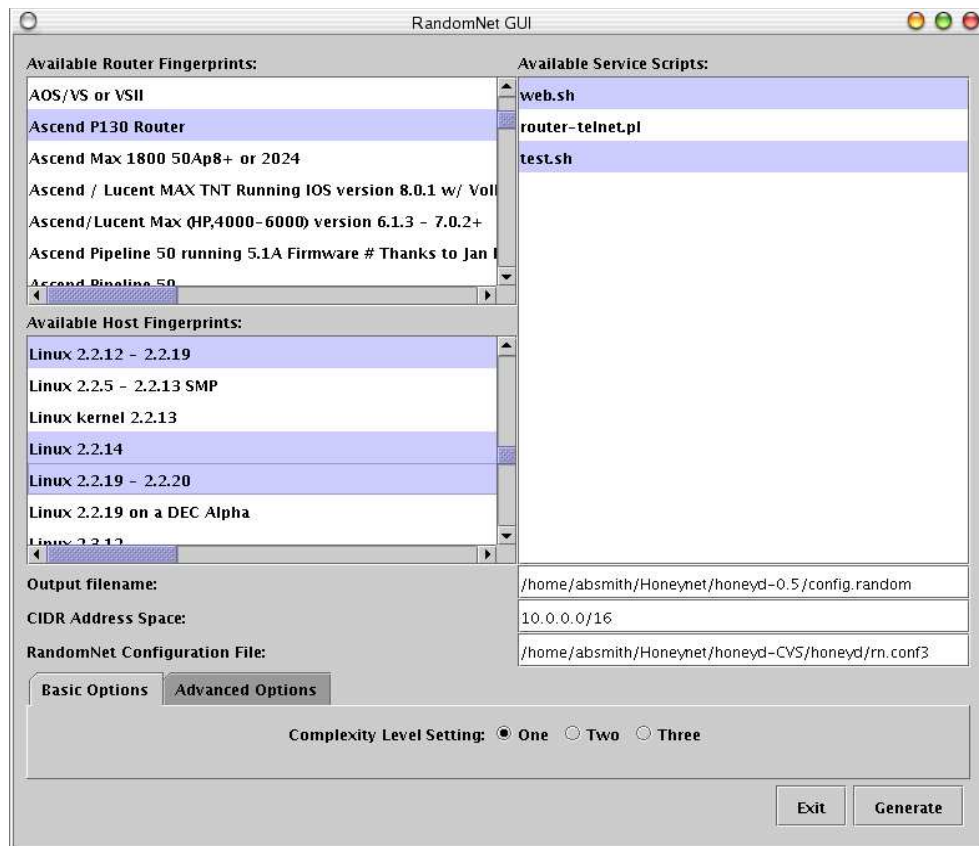


Figure 1: RandomNet GUI Screenshot

Figure 1 shows the RandomNet GUI in action. Basically, the user is presented with a number of options. Typical use of the gui would be as follows:

1. Select the fingerprints that you wish to use as router fingerprints in the Available Router Fingerprints menu. *You should only select routers from this list if you want your honeyd config file to work correctly.* You can select more than one router by holding the <CTRL> key while selecting a router.
2. Select the fingerprints that you wish to use as host fingerprints in the Available Host Fingerprints menu. You can select multiple hosts fingerprints by holding <CTRL> key

- while selecting.
3. Select the services you wish to use in your honeyd network. Similar to the fingerprints window, you can select more than one service to use by holding the <CTRL> key.
4. Type in the full-path name of the honeyd output file to use in the Output filename field.
5. Type in the CIDR address space to use for the randomly generated network in the CIDR Address Space field.
6. Type in the full-path name of the RandomNet configuration file that you are now creating/editing in the RandomNet Configuration File field. Note: When you press the Generate button, the RandomNet configuration file will be saved (and will possibly overwrite) in the location specified in this field.
7. Either use the Basic Options tab to set the complexity level of the network (the higher the complexity level, the more complex the network) or use the Advanced Options field to set the number of routers and number of layers to use.
8. Press the Generate button and let RandomNet take care of the rest!

It must be noted that for the RandomNet to run, a preliminary configuration file **MUST** be specified. This configuration file tells the RandomNet where to look for fingerprints and available services. An example configuration file is supplied with the RandomNet source code for the user to edit.

The RandomNet Configuration File

Figure 2 shows a typical RandomNet configuration file. This file can be edited directly or created/edited with the RandomNet GUI.

```
absmith@x1-6-00-c0-0c-b0-b0-84:~/Honeynet/honeyd-CVS/honeyd - Shell - Konsole
Session Edit View Bookmarks Settings Help

##### generated by RandomNetGui
##### Wed Mar 12 21:42:39 EST 2003

# Path Information
HONEYDDIR=/home/absmith/Honeynet/honeyd-0.5/
NMAPPDIR=/home/absmith/Honeynet/honeyd-0.5/nmap.dirs
HONEYDCONFIG=/home/absmith/Honeynet/honeyd-0.5/config.random

# Basic Configuration Information
complexity_level=1
cidr_address=10.0.0.0/16

# Router Fingerprint information
router_fingerprint=2 # 3COM OfficeConnect Remote 812 ADSL Router
router_fingerprint=56 # Ascend P130 Router
router_fingerprint=98 # Baystack Instant Internet 400 SoHo Router

# Host Fingerprint information
host_fingerprint=233 # FreeBSD 3.2-4.0
host_fingerprint=274 # IBM AIX v3.2.5 - 4
host_fingerprint=278 # IBM OS/2 V 2.1
host_fingerprint=324 # IRIX 6.5.14
host_fingerprint=352 # Linux 2.2.12 - 2.2.19

# Service information
use_service=web.sh
use_service=test.sh

~
~

1,1 All
```

Figure 2: An example RandomNet configuration file

The HONEYDDIR, NMAPPRINTS, and HONEYDCONFIG variables must be set in order for the RandomNet to work properly. Full-path names should be used. All variables and values should be separated by '=' and '#' can be used to comment the file.

The following table contains the different variables that can be set in the RandomNet Configuration file:

<i>Variable name</i>	<i>Description</i>
HONEYDDIR	Location of the honeyd source code (used to parse script information)
NMAPPRINTS	Location of the nmap.prints file to use for generating available fingerprints.
HONEYDCONFIG	File to output results of the random generation.
complexity_level	Basically, this sets how big the generated network is
num_routers	Specifies number of routers to use, only if complexity level is not used
num_layers	Specifies number of layers to use, only if complexity level is not used
router_fingerprint	Index into the nmap.prints file of what fingerprint to use for a router. For example, router_fingerprint=5 will use the fifth fingerprint parsed out of the nmap.prints
host_fingerprint	Index into the nmap.prints file of what fingerprint to use for a host.
use_service	Name of a service to make available on random hosts and routers. This service should reside in the scripts/ directory

Table 1: Variables available in the RandomNet configuration file

Future Work

The following features of RandomNet were not implemented due to time constraints:

- Ability to choose ports on which services are run. There needs to be some way to choose what ports the RandomNet should generate for each service script on the gui.
- The Advanced Options tab should include a number of parameter settings that control the different randomly generated options. For example, the user should be able to choose the approximate percentage of how many TCP ports should be open.

Acknowledgments

The authors would like to thank Ron Gula of Tenable Network Security for the preliminary idea of having a tool to randomly generate honeyd networks.

Appendix A

The following example shows how to set up honeyd, run using the new config file generated by RandomNet (parts of the actual file are shown in Appendix B), and a few simple test cases:

```
# su to root
$ su

# add entry in routing table for 10.0.0.0/8 to loopback interface
$ route -n add -net 10.0.0.0/8 lo

# verify that it exists
$ route

Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0      *              255.255.255.0   U        0      0        0 eth0
10.0.0.0         *              255.0.0.0       U        0      0        0 lo
127.0.0.0        *              255.0.0.0       U        0      0        0 lo
default          192.168.1.1    0.0.0.0         UG       0      0        0 eth0

# start honeyd with logging enabled and specifying the config.random file
$ ./honeyd -l honeyd.log -p nmap.prints -f config.random -i lo 10.0.0.0/8

# test ping
$ ping 10.170.170.129
PING 10.170.170.129 (10.170.170.129) from 192.168.1.101 : 56(84) bytes of data.
64 bytes from 10.170.170.129: icmp_seq=1 ttl=55 time=960 ms
64 bytes from 10.170.170.129: icmp_seq=2 ttl=55 time=959 ms
64 bytes from 10.170.170.129: icmp_seq=3 ttl=55 time=961 ms

# test traceroute
$ traceroute 10.170.170.129
traceroute to 10.170.170.129 (10.170.170.129), 30 hops max, 38 byte packets
 1  10.0.0.1 (10.0.0.1)  0.303 ms  0.184 ms  0.068 ms
 2  10.128.0.1 (10.128.0.1)  137.696 ms  141.075 ms  140.025 ms
 3  10.160.0.1 (10.160.0.1)  179.215 ms  172.677 ms  171.485 ms
 4  10.168.0.1 (10.168.0.1)  188.591 ms  195.396 ms  197.689 ms
 5  10.170.0.1 (10.170.0.1)  389.452 ms  395.394 ms  389.829 ms
 6  10.170.128.1 (10.170.128.1)  579.663 ms  571.629 ms  578.696 ms
 7  * 10.170.160.1 (10.170.160.1)  769.872 ms  770.883 ms
 8  10.170.168.1 (10.170.168.1)  860.199 ms  856.822 ms  859.027 ms
 9  10.170.170.1 (10.170.170.1)  859.443 ms  857.733 ms  859.911 ms
10  10.170.170.129 (10.170.170.129)  961.463 ms  957.167 ms  951.160 ms

# test nmap
$ nmap 10.64.0.118

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.64.0.118):
(The 1600 ports scanned but not shown below are in state: closed)
Port      State      Service
80/tcp    open      http

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

Appendix B

This contains part of a sample configuration file generated by RandomNet:

```
##### '/home/jmfox/honeyd-0.5/config.random' generated by RandomNet
##### Thu Mar 13 22:34:38 EST 2003

# Router/Routes Setup
route entry 10.0.0.1
route 10.0.0.1 link 10.64.0.0/10
route 10.0.0.1 add net 10.128.0.0/10 10.128.0.1 latency 68ms loss 0.2
route 10.128.0.1 link 10.144.0.0/12
route 10.128.0.1 add net 10.160.0.0/12 10.160.0.1 latency 17ms loss 0.2
route 10.160.0.1 link 10.164.0.0/14
route 10.160.0.1 add net 10.168.0.0/14 10.168.0.1 latency 9ms loss 0.1
route 10.168.0.1 link 10.169.0.0/16
route 10.168.0.1 add net 10.170.0.0/16 10.170.0.1 latency 99ms loss 0.1
route 10.170.0.1 link 10.170.64.0/18
route 10.170.0.1 add net 10.170.128.0/18 10.170.128.1 latency 92ms loss 0.2
route 10.170.128.1 link 10.170.144.0/20
route 10.170.128.1 add net 10.170.160.0/20 10.170.160.1 latency 98ms loss 0.2
route 10.170.160.1 link 10.170.164.0/22
route 10.170.160.1 add net 10.170.168.0/22 10.170.168.1 latency 43ms loss 0.2
route 10.170.168.1 link 10.170.169.0/24
route 10.170.168.1 add net 10.170.170.0/24 10.170.170.1 latency 2ms loss 0.1
route 10.170.170.1 link 10.170.170.64/26
route 10.170.170.1 add net 10.170.170.128/26 10.170.170.129 latency 47ms loss 0.2
route 10.170.170.129 link 10.170.170.144/28
route 10.170.170.129 add net 10.170.170.160/28 10.170.170.161 latency 34ms loss 0.1

annotate "Linux Kernel 2.4.3 SMP (RedHat)" fragment old
annotate "Linux 2.4.7 (X86)" no finscan
annotate "Linux 2.4.7 (X86)" fragment old
annotate "FreeBSD 4.4 for i386 (IA-32)" fragment drop
annotate "NetBSD 1.0 little endian arch" no finscan
annotate "NetBSD 1.2 - 1.2.1 big endian arch" fragment old
annotate "Windows 2000 Professional, Build 2128" no finscan
annotate "Windows 2000 Professional, Build 2128" fragment new
annotate "Win XP Pro or Windows 2000 Pro SP2+" fragment old
annotate "MS Windows2000 Professional RC1/W2K Advance Server Beta3" no finscan
annotate "MS Windows2000 Professional RC1/W2K Advance Server Beta3" fragment old
annotate "Cisco 766 non-IOS software 4.2(3.5)" finscan
annotate "Cisco 766 non-IOS software 4.2(3.5)" fragment new
annotate "Cisco 4500-M running IOS 11.3(6) IP Plus" finscan
annotate "Redback SMS 1000-2000 DSL Router" no finscan
annotate "Redback SMS 1000-2000 DSL Router" fragment new
annotate "Toshiba TR650 ISDN Router" no finscan
annotate "Toshiba TR650 ISDN Router" fragment new

# Router templates
create router_template0
set router_template0 personality "Cisco 4500-M running IOS 11.3(6) IP Plus"
add router_template0 tcp port 80 "web.sh"
add router_template0 tcp port 22 "test.sh"
set router_template0 uid 213

create router_template1
set router_template1 personality "Cisco 4500-M running IOS 11.3(6) IP Plus"
set router_template1 default udp action open
add router_template1 tcp port 23 "router-telnet.pl"
add router_template1 tcp port 22 "test.sh"
set router_template1 uptime 81816
set router_template1 droprate in 0.02

create router_template2
set router_template2 personality "Redback SMS 1000-2000 DSL Router"
set router_template2 default udp action open
add router_template2 tcp port 80 "web.sh"
add router_template2 tcp port 22 "test.sh"

create router_template3
set router_template3 personality "Cisco 766 non-IOS software 4.2(3.5)"
set router_template3 default tcp action block
set router_template3 default udp action open
set router_template3 default icmp action open
```

```

add router_template3 tcp port 22 "test.sh"
set router_template3 droprate in 0.28

create router_template4
set router_template4 personality "Redback SMS 1000-2000 DSL Router"
add router_template4 tcp port 80 "web.sh"
set router_template4 droprate in 0.76

create router_template5
set router_template5 personality "Cisco 4500-M running IOS 11.3(6) IP Plus"
set router_template5 default tcp action open
set router_template5 default udp action open
add router_template5 tcp port 23 "router-telnet.pl"
add router_template5 tcp port 22 "test.sh"

create router_template6
set router_template6 personality "Cisco 4500-M running IOS 11.3(6) IP Plus"
add router_template6 tcp port 80 "web.sh"
add router_template6 tcp port 23 "router-telnet.pl"

create router_template7
set router_template7 personality "Cisco Catalyst 1900 switch or Netopia DSL/ISDN router
or Bay 350-450"
set router_template7 default tcp action open
set router_template7 default udp action open
set router_template7 default icmp action open
add router_template7 tcp port 23 "router-telnet.pl"
add router_template7 tcp port 22 "test.sh"

create router_template8
set router_template8 personality "Toshiba TR650 ISDN Router"
set router_template8 default tcp action block
set router_template8 default udp action open
add router_template8 tcp port 23 "router-telnet.pl"
set router_template8 uid 198 gid 15

create router_template9
set router_template9 personality "Redback SMS 1000-2000 DSL Router"
set router_template9 default tcp action reset
set router_template9 default icmp action open
add router_template9 tcp port 80 "web.sh"
set router_template9 uptime 351644

create router_template10
set router_template10 personality "Cisco Catalyst 1900 switch or Netopia DSL/ISDN router
or Bay 350-450"
set router_template10 default tcp action open

create router_template11
set router_template11 personality "Toshiba TR650 ISDN Router"
add router_template11 tcp port 23 "router-telnet.pl"
set router_template11 droprate in 0.31

create router_template12
set router_template12 personality "Cisco 766 non-IOS software 4.2(3.5)"
set router_template12 default udp action open
set router_template12 default icmp action open
add router_template12 tcp port 22 "test.sh"

create router_template13
set router_template13 personality "Redback SMS 1000-2000 DSL Router"
set router_template13 default tcp action block
add router_template13 tcp port 80 "web.sh"
add router_template13 tcp port 22 "test.sh"

create router_template14
set router_template14 personality "Redback SMS 1000-2000 DSL Router"
set router_template14 default icmp action open

# Host templates
create default
set default personality "Linux Kernel 2.4.3 SMP (RedHat)"
set default default udp action open
set default uptime 456787
set default droprate in 0.68

create host_template0
set host_template0 personality "NetBSD 1.2 - 1.2.1 big endian arch"

```

```

set host_template0 default tcp action reset
set host_template0 default udp action open
set host_template0 default icmp action open
add host_template0 tcp port 80 "web.sh"
add host_template0 tcp port 23 "router-telnet.pl"

create host_template1
set host_template1 personality "Linux Kernel 2.4.3 SMP (RedHat)"
set host_template1 default tcp action block
set host_template1 default udp action open
set host_template1 droprate in 0.78

create host_template2
set host_template2 personality "Linux Kernel 2.4.3 SMP (RedHat)"
set host_template2 default tcp action reset
set host_template2 default udp action open
set host_template2 default icmp action open
set host_template2 droprate in 0.02

create host_template3
set host_template3 personality "NetBSD 1.2 - 1.2.1 big endian arch"
set host_template3 default tcp action open
set host_template3 default icmp action open
set host_template3 droprate in 0.23

create host_template4
set host_template4 personality "Windows 2000 Professional, Build 2128"
set host_template4 default icmp action open

create host_template5
set host_template5 personality "Windows 2000 Professional, Build 2128"
add host_template5 tcp port 80 "web.sh"
add host_template5 tcp port 23 "router-telnet.pl"

create host_template6
set host_template6 personality "Win XP Pro or Windows 2000 Pro SP2+"
set host_template6 default udp action open
add host_template6 tcp port 80 "web.sh"
add host_template6 tcp port 22 "test.sh"

create host_template7
set host_template7 personality "FreeBSD 4.4 for i386 (IA-32)"
set host_template7 default udp action open
set host_template7 uptime 249211

create host_template8
set host_template8 personality "NetBSD 1.2 - 1.2.1 big endian arch"
set host_template8 default udp action open
set host_template8 default icmp action open
add host_template8 tcp port 23 "router-telnet.pl"

create host_template9
set host_template9 personality "Win XP Pro or Windows 2000 Pro SP2+"
set host_template9 default udp action open
set host_template9 default icmp action open
add host_template9 tcp port 80 "web.sh"
set host_template9 uid 254 gid 46

create host_template10
set host_template10 personality "NetBSD 1.0 little endian arch"

create host_template11
set host_template11 personality "MS Windows2000 Professional RC1/W2K Advance Server Beta3"
set host_template11 default tcp action reset
add host_template11 tcp port 80 "web.sh"
add host_template11 tcp port 22 "test.sh"

create host_template12
set host_template12 personality "MS Windows2000 Professional RC1/W2K Advance Server Beta3"
set host_template12 default tcp action reset
add host_template12 tcp port 80 "web.sh"

create host_template13
set host_template13 personality "FreeBSD 4.4 for i386 (IA-32)"
set host_template13 default udp action open
add host_template13 tcp port 80 "web.sh"
add host_template13 tcp port 22 "test.sh"

```



```

create host_template14
set host_template14 personality "NetBSD 1.2 - 1.2.1 big endian arch"
set host_template14 default tcp action open
set host_template14 default icmp action open
add host_template14 tcp port 23 "router-telnet.pl"

create host_template15
set host_template15 personality "NetBSD 1.2 - 1.2.1 big endian arch"
set host_template15 default icmp action open

create host_template16
set host_template16 personality "Windows 2000 Professional, Build 2128"
add host_template16 tcp port 80 "web.sh"
add host_template16 tcp port 23 "router-telnet.pl"

create host_template17
set host_template17 personality "Windows 2000 Professional, Build 2128"
set host_template17 default icmp action open
add host_template17 tcp port 80 "web.sh"
add host_template17 tcp port 23 "router-telnet.pl"
set host_template17 droprate in 0.78

create host_template18
set host_template18 personality "Linux Kernel 2.4.3 SMP (RedHat)"
set host_template18 default udp action open
set host_template18 default icmp action open
add host_template18 tcp port 22 "test.sh"

create host_template19
set host_template19 personality "Windows 2000 Professional, Build 2128"
add host_template19 tcp port 80 "web.sh"
set host_template19 droprate in 0.49

create host_template20
set host_template20 personality "NetBSD 1.0 little endian arch"
set host_template20 default tcp action open
add host_template20 tcp port 80 "web.sh"

create host_template21
set host_template21 personality "Windows 2000 Professional, Build 2128"
set host_template21 default tcp action block
set host_template21 default icmp action open

create host_template22
set host_template22 personality "Linux 2.4.7 (X86)"
set host_template22 default udp action open
add host_template22 tcp port 80 "web.sh"
add host_template22 tcp port 22 "test.sh"
set host_template22 uptime 406112

create host_template23
set host_template23 personality "Linux Kernel 2.4.3 SMP (RedHat)"
set host_template23 default udp action open
set host_template23 default icmp action open

create host_template24
set host_template24 personality "Windows 2000 Professional, Build 2128"
set host_template24 default udp action open
add host_template24 tcp port 80 "web.sh"
add host_template24 tcp port 23 "router-telnet.pl"
add host_template24 tcp port 22 "test.sh"
set host_template24 uid 262

create host_template25
set host_template25 personality "NetBSD 1.0 little endian arch"
set host_template25 default icmp action open
add host_template25 tcp port 80 "web.sh"
add host_template25 tcp port 23 "router-telnet.pl"

create host_template26
set host_template26 personality "FreeBSD 4.4 for i386 (IA-32)"
set host_template26 default tcp action reset
set host_template26 default udp action open
set host_template26 default icmp action open
add host_template26 tcp port 80 "web.sh"
add host_template26 tcp port 23 "router-telnet.pl"
set host_template26 uptime 271921

```

```

create host_template27
set host_template27 personality "FreeBSD 4.4 for i386 (IA-32)"
set host_template27 default tcp action reset
set host_template27 default udp action open
add host_template27 tcp port 80 "web.sh"
add host_template27 tcp port 23 "router-telnet.pl"
set host_template27 uptime 452135

create host_template28
set host_template28 personality "Linux Kernel 2.4.3 SMP (RedHat)"
set host_template28 default icmp action open
add host_template28 tcp port 23 "router-telnet.pl"

create host_template29
set host_template29 personality "Linux 2.4.7 (X86)"
set host_template29 default udp action open
add host_template29 tcp port 80 "web.sh"
add host_template29 tcp port 23 "router-telnet.pl"
add host_template29 tcp port 22 "test.sh"
set host_template29 uptime 241746
set host_template29 droprate in 0.30

create host_template30
set host_template30 personality "MS Windows2000 Professional RC1/W2K Advance Server Beta3"
set host_template30 default icmp action open
add host_template30 tcp port 80 "web.sh"
add host_template30 tcp port 23 "router-telnet.pl"

create host_template31
set host_template31 personality "FreeBSD 4.4 for i386 (IA-32)"
set host_template31 default tcp action reset
set host_template31 default icmp action open
add host_template31 tcp port 80 "web.sh"

create host_template32
set host_template32 personality "FreeBSD 4.4 for i386 (IA-32)"
set host_template32 default icmp action open
add host_template32 tcp port 80 "web.sh"
add host_template32 tcp port 23 "router-telnet.pl"
add host_template32 tcp port 22 "test.sh"
set host_template32 uptime 446478

create host_template33
set host_template33 personality "Win XP Pro or Windows 2000 Pro SP2+"
set host_template33 default udp action open
set host_template33 default icmp action open
add host_template33 tcp port 23 "router-telnet.pl"
add host_template33 tcp port 22 "test.sh"
set host_template33 droprate in 0.31

create host_template34
set host_template34 personality "FreeBSD 4.4 for i386 (IA-32)"
set host_template34 default udp action open
set host_template34 default icmp action open
add host_template34 tcp port 80 "web.sh"
add host_template34 tcp port 22 "test.sh"

create host_template35
set host_template35 personality "Linux Kernel 2.4.3 SMP (RedHat)"
set host_template35 default udp action open
add host_template35 tcp port 80 "web.sh"
add host_template35 tcp port 22 "test.sh"
set host_template35 droprate in 0.94

create host_template36
set host_template36 personality "NetBSD 1.0 little endian arch"
set host_template36 default tcp action open
set host_template36 default udp action open
set host_template36 default icmp action open
add host_template36 tcp port 22 "test.sh"
set host_template36 droprate in 0.61

create host_template37
set host_template37 personality "Win XP Pro or Windows 2000 Pro SP2+"
set host_template37 default tcp action block

create host_template38
set host_template38 personality "NetBSD 1.2 - 1.2.1 big endian arch"

```

```

set host_template38 default tcp action block
set host_template38 default icmp action open
add host_template38 tcp port 80 "web.sh"
set host_template38 droprate in 0.28
set host_template38 uid 122

create host_template39
set host_template39 personality "Linux Kernel 2.4.3 SMP (RedHat)"
set host_template39 default tcp action block
add host_template39 tcp port 22 "test.sh"
set host_template39 droprate in 0.53

create host_template40
set host_template40 personality "Linux 2.4.7 (X86)"
set host_template40 default udp action open
add host_template40 tcp port 80 "web.sh"
add host_template40 tcp port 23 "router-telnet.pl"
set host_template40 uid 288 gid 68

create host_template41
set host_template41 personality "NetBSD 1.0 little endian arch"
add host_template41 tcp port 22 "test.sh"

create host_template42
set host_template42 personality "FreeBSD 4.4 for i386 (IA-32)"
set host_template42 default tcp action reset
set host_template42 default icmp action open
add host_template42 tcp port 80 "web.sh"
add host_template42 tcp port 22 "test.sh"

create host_template43
set host_template43 personality "Linux 2.4.7 (X86)"
set host_template43 default udp action open
add host_template43 tcp port 23 "router-telnet.pl"
set host_template43 uptime 467926

create host_template44
set host_template44 personality "Win XP Pro or Windows 2000 Pro SP2+"
set host_template44 default icmp action open
set host_template44 uptime 18997
set host_template44 droprate in 0.78

# Router bindings
bind 10.0.0.1 router_template13
bind 10.128.0.1 router_template14
bind 10.160.0.1 router_template2
bind 10.168.0.1 router_template2
bind 10.170.0.1 router_template1
bind 10.170.128.1 router_template0
bind 10.170.160.1 router_template1
bind 10.170.168.1 router_template2
bind 10.170.170.1 router_template0
bind 10.170.170.129 router_template6

# Host bindings
bind 10.64.0.35 host_template1
bind 10.64.0.53 host_template9
bind 10.64.0.70 host_template44
bind 10.64.0.117 host_template5
bind 10.64.0.118 host_template31
bind 10.64.0.120 host_template40
bind 10.64.0.140 host_template26
bind 10.64.0.148 host_template38
bind 10.64.0.195 host_template31
bind 10.144.0.25 host_template33
bind 10.144.0.50 host_template17
bind 10.144.0.94 host_template29
bind 10.144.0.141 host_template2
bind 10.144.0.147 host_template25
bind 10.144.0.168 host_template20
bind 10.164.0.29 host_template18
bind 10.164.0.32 host_template39
bind 10.164.0.71 host_template34
bind 10.164.0.77 host_template23
bind 10.164.0.85 host_template25
bind 10.164.0.86 host_template25
bind 10.164.0.109 host_template18
bind 10.164.0.133 host_template39

```

```
bind 10.169.0.42 host_template11
bind 10.169.0.83 host_template34
bind 10.169.0.84 host_template43
bind 10.169.0.106 host_template40
bind 10.169.0.145 host_template38
bind 10.169.0.188 host_template6
bind 10.169.0.228 host_template8
bind 10.169.0.231 host_template34
bind 10.169.0.248 host_template24
bind 10.169.1.15 host_template34
bind 10.170.64.14 host_template40
bind 10.170.64.42 host_template21
bind 10.170.64.76 host_template42
bind 10.170.64.119 host_template18
bind 10.170.64.125 host_template34
bind 10.170.64.144 host_template23
bind 10.170.64.180 host_template16
bind 10.170.64.194 host_template2
bind 10.170.64.240 host_template18
bind 10.170.65.24 host_template40
bind 10.170.65.58 host_template12
bind 10.170.65.93 host_template27
bind 10.170.65.104 host_template26
bind 10.170.144.39 host_template6
bind 10.170.144.40 host_template42
bind 10.170.144.61 host_template23
bind 10.170.144.62 host_template24
bind 10.170.144.111 host_template9
bind 10.170.144.146 host_template44
bind 10.170.144.150 host_template12
bind 10.170.144.153 host_template18
bind 10.170.144.202 host_template23
bind 10.170.144.230 host_template40
bind 10.170.164.48 host_template33
bind 10.170.164.61 host_template1
bind 10.170.164.76 host_template11
bind 10.170.164.110 host_template11
bind 10.170.164.135 host_template32
bind 10.170.169.36 host_template38
bind 10.170.169.67 host_template8
bind 10.170.169.104 host_template4
bind 10.170.169.114 host_template23
bind 10.170.169.127 host_template7
bind 10.170.170.89 host_template18
```

Appendix C

This is the RandomNet config file used to generate the previous honeyd config file:

```
##### generated by RandomNetGui
##### Thu Mar 13 22:34:38 EST 2003

# Path Information
HONEYDDIR=/home/jmfox/honeyd-0.5/
NMAPPRINTS=/home/jmfox/honeyd-0.5/nmap.prints
HONEYDCONFIG=/home/jmfox/honeyd-0.5/config.random

# Basic Configuration Information
complexity_level=3
cidr_address=10.0.0.0/8

# Router Fingerprint information
router_fingerprint=127 # Cisco 766 non-IOS software 4.2(3.5)
router_fingerprint=131 # Cisco 4500-M running IOS 11.3(6) IP Plus
router_fingerprint=132 # Cisco Catalyst 1900 switch or Netopia DSL/ISDN router or Bay
350-450
router_fingerprint=488 # Redback SMS 1000-2000 DSL Router
router_fingerprint=541 # Toshiba TR650 ISDN Router

# Host Fingerprint information
host_fingerprint=364 # Linux Kernel 2.4.3 SMP (RedHat)
host_fingerprint=365 # Linux 2.4.7 (X86)
host_fingerprint=377 # FreeBSD 4.4 for i386 (IA-32)
host_fingerprint=408 # NetBSD 1.0 little endian arch
host_fingerprint=411 # NetBSD 1.2 - 1.2.1 big endian arch
host_fingerprint=564 # Windows 2000 Professional, Build 2128
host_fingerprint=565 # Win XP Pro or Windows 2000 Pro SP2+
host_fingerprint=569 # MS Windows2000 Professional RC1/W2K Advance Server Beta3

# Service information
use_service=web.sh
use_service=router-telnet.pl
use_service=test.sh
```