56:4E

Configuring and Using a Bait & Switch Honeypot Router

Version B-1

About The Bait & Switch Honeypot System: Violating Networks has produced a system that reacts to hostile intrusion attempts by redirecting all traffic from "bad" IPs to a honeypot that is partially mirroring your production server. Once switched, the would-be hacker is unknowingly attacking your honeypot instead of the real data while your clients and/or users are still safely accessing the real system. Life goes on, your data is safe, and as an added benefit you are learning about the bad guy. Currently the system is based on Snort, Linux's iproute2, netfilter, and custom code. We're planning on porting it to the BSDs as soon as possible.

About This Document: There are a number of components to running this system beyond the actual routing and switching mechanisms. You must be able to set up your honeypot, decide how similar to make your production system and your honeypot look, set up and configure Snort, etc. This document only covers setting up the routing and switching mechanisms. There are excellent existing sources of information that explain these things in far more detail then we can here. To help with this, we will soon be releasing a separate document or tool outlining Snort signatures that are useful in this environment and that will have the least potential for harm and abuse. Until then, you should know your pig!

Before Getting Started

Requirements: This system is designed to – for now – run on a standard Linux distribution. This means (to me) that it is modern enough to have iproute2 and iptables/netfilter. You will also need…

- The snort-1.9.0 sources. We use a custom snort plug-in to communicate with the IDS and need to patch some of the snort files before compilation.
- A PC with 3 network interfaces. Interface 1 is the gateway to your honeypot and production servers from the outside world. Interface 2 and 3 are the gateways from the production and honeypot servers respectively back out to the world. These interfaces can be any combination of real or VMware – whatever suits your network. Likewise, if you NAT back to your production/honeypot servers, the NATing shouldn't be affected.
- Obviously, you need the version of baitnswitch that's listed at the top of this document.
- UML? Honeyd? If anyone tests this with either of those I'd *love* to know about it.

What does the system *look* like: The diagram at the bottom of this document shows a fairly simple example network using VMware to represent both your production server and your honeypot. A flow chart will be included with this document at a later date.

Linux Configuration Notes: In order for the routing to work, I believe you need your internal gateway interfaces configured with /32 subnet masks. Do this before you continue with the configuration. (Or, don't, and let me know if it works.)

Configuring the System

Setting up snort, switchcore, and routing

1. Download the current baitnswitch package from either:

- http://baitnswitch.sourceforge.net or
- http://www.violating.us/projects/baitnswitch/

2. Download snort-1.9.0.tar.gz from http://www.snort.org

3. Extract B&S to the directory where you want it to stay (<bnsroot> from now on)

*tar -zxvf baitnswitch-**.tar.gz*
creates a bns directory in <bnsroot>

4. Extract snort to some directory. (We don't care which.) Do NOT configure or compile it at this point.

5. *cd <bnsroot>/bns/config*

6. Bring up the configuration menu by running the ./bns_conf.bash script. The first time you install B&S, choose option #1. This will simply echo the names of new routing tables to /etc/iproute2/rt_tables -- so don't select this option more than once per B&S router.

7. Back at the main menu, choose option #2 and answer the following questions:

- **External Interface:** This is the public facing interface that is either the gateway or the NATing device to your production & honeypot servers. I use eth0

- **External IP:** What is the IP of the external interface? Should *not* be on the same subnet as your honeypot/production server IP

- **Production Interface:** This is the internal device on your B&S box that is your production server's gateway to the rest of the world. I'm using vmnet1.

- **Production IP:** IP address on the Production GW Interface. Needs to be on the same subnet as your honeypot/production server IP

- **Honeypot Interface:** This is the internal device on your B&S box that is your honeypot's gateway to the rest of the world. I'm using vmnet2.

- **Honeypot's Gateway IP:** IP address on the Honeypot GW Interface. It needs to be on the same subnet as the production gw IP - which is the same subnet as your honeypot/production server IP: 192.168.2.2 is what I use.

- **IP of <both> Honeypot and Production Server:** Your honeypot and production server should be set up with the SAME IP address. In this case, mine have 192.168.2.10 as their address.

- **Length of Time (in minutes) that the mark time should be incremented:** Every time snort alerts on a sig, B&S increments the length of time that that source IP will be rerouted. How much should the time be incremented for each incident?

- **Length of Time DoS Protection - Max Alerts:** We don't want to have someone force a source to be rerouted forever, so we limit the number of marking increments per period of time that increment the rerouting time. Enter how many alerts per period of time is too many.

- **Length of Time DoS Protection**: Period ((in seconds) to look for too many marks from a single IP): this is the time period referenced in the previous step

- **IP DoS Protection:** How many IPs per a certain amount of time is too many? We don't want someone to spoof all our clients and quickly block them all, so we limit how many new source IPs per time period we'll reroute.

- **IP DoS Protection:** Within what length of time should a certain number of IPs be too many? This is the time period in seconds referenced in the previous instruction.

- **Fifo File Location:** This is the named pipe that snort uses to talk to baitnswitch. Where do you want it and what should it be called? /tmp/bns or something should work fine.

- **Log Location:** We log DoS alerts from B&S. Where should they go? I use /var/log/switchcore.log

- **Blacklist Location:** Certain IP's should always be rerouted, as they are known hostiles. Switchcore reads a list of IP's from a textfile. Where should this list be?

- **Path to snort:** What directory (full path to) did the snort tarball create? I use /root/dev/snort-1.9.0

You should now be brought back to the Config Menu. Choose 3 to patch snort to include the bns output plugin.

- Path to bns.dfff: Should be <bnsroot>/bns/snort/bns.diff
- 6 or so files should be patched.

You can choose e to exit here..

9. *cd <bnsroot>/bns/routing*

10. Run *./bnsroutes.bash* (chmod +x it if needed)

11. *cd <bnsroot>/bns/switching*

12. Compile switchcore.c with: *gcc -lpthread switchcore.c -o switchcore*

13. cd to your snort source directory and go ahead and configure/make/install it. (Out of this document's scope)

You are finished configuring the system, now to run it….

Running Bait and Switch:

How to use snort and switchcore Together

There really isn't much to running Bait & Switch, the difficult part is setting it up.

To run it, we first need to load switchcore. Switchcore handles the rerouting and normalizing of traffic and source IP's. To run it, simply type:

<bnsroot>/bns/switching/switchcore

This should daemonize to the background and you dont have to touch it anymore. In order for snort to interact with this, you have - as part of the installation procedure - compiled in an output plugin called bns_alert. There is an example of how to use this output plugin in <bnsroot>/bns/snort called:

rules.script

This is a simple conf file for snort that is only one, simple rule: redirect any source IP to the honeypot that is sending icmp data. To use the example, you can run:

snort -c <bnsroot>/bns/snort/rules.script

And then ping your production server IP (or the external if of the B&S router if you're using NAT). Everything beyond the first packet or two should go to the honeypot.

The only other feature that you need to worry about is the blacklist. If there are any source IP's that you absolutely know are bad, you can add them to the file you specified in the configuration section. Add one IP per line and that's all you have to do. Switchcore reads this file at startup and puts static rerouting rules in for each IP. You'll have to manually remove those rules if you want them gone.

How do I stop switchcore? Uhm, for now? *killall -9 switchcore* or something.

Example Diagram:

Setup referenced in the rest of the document.