C3CM: Part 3 – ADHD: Active Defense Harbinger Distribution

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

Prerequisites

Linux OS –Ubuntu Desktop 12.04 LTS discussed herein

Parts 1 and 2 of our C3CM discussion covered the identify and interrupt phases of the process I've defined as an effort to *identify, interrupt, and counter the command, control, and communications capabilities of our digital assailants.* In Part 3 I'm going to cover…hey, a squirrel! ☺ In this, the final part of our series, I'll arm you for the interrupt phase with ADHD…no, not that; rather, it's the Active Defense Harbinger Distribution. You know how I know I have ADHD? My wife asked me for a glass of water and I made myself coffee instead. Wait, maybe that's just selfish…er, nevermind.

I hope you've enjoyed utilizing Nfsight with Nfdump, Nfsen, and fprobe for our *identification* phase and BroIDS (Bro), Logstash, and Kibana as part of our *interrupt* phase. But I have to say, I think the fun really kicks in here when we consider how to *counter* our ne'er-do-well denizens of digital destruction. We'll install the ADHD scripts on the C3CM Ubuntu system we've been building in Parts 1 and 2, but, much as you could have performed the interrupt phase using Doug Burk's Security Onion (SO), you could download the full ADHD distribution[1] and take advantage of it in its preconfigured splendor to conduct the *counter* phase. The truth of the matter is that running all the tools we've implemented during this C3CM campaign on one VM or physical machine, all at the same time, would be silly as you'd end up with port contention and resource limitations. Consider each of the three activities (identify, interrupt, and counter) as somewhat exclusive. Perhaps, clone three copies of the C3CM VM once we're all finished and conduct each phase uniquely or simply do one at a time. The ADHD distribution (absolutely download it and experiment in addition to this activity) is definitely convenient and highly effective, but again, I want you to continue developing your Linux foo, so carry on in our C3CM build out.

John Strand and Ethan Robish are the ADHD project leads, and Ethan kindly gave us direct insight into the project specific to the full distribution:

> "ADHD is an ongoing project that features many tools to counter an attacker's ability to exploit and pivot within a network. Tools such as Honey Badger, Pushpin, Web Bug Server, and Decloak provide a way of identifying an attacker's remote location, even if he has attempted to hide it. Artillery, Nova, and Weblabyrinth, along with a few shell scripts, provide honeypot-like functionality to confuse, disorient, and frustrate an attacker. And then there are the well-known tools that help the good guys turn the tables on the attacker: the Social Engineering Toolkit (SET), the Browser Exploitation Framework (BeEF), and the Metasploit Framework (MSF).
>
> "Future plans for the project include the typical updates along with the addition of new tools. Since the last release of ADHD, there has been some interesting research done by Chris John Riley on messing with web scanners. His preliminary work was included with ADHD 0.5.0, but his new work will be better integrated and documented with the next release of ADHD. We also plan to dive more into the detection of people that try to hide their identities behind proxies and other anonymizing measures. Further down the line you may see some big changes to the underlying distribution itself. We have started on a unified web control interface that will allow users of ADHD to control the various aspects of the system, as well as begun exploring how to streamline installation of both ADHD itself and the tools that are included. Our goal is to make it as simple as possible to install and configure ADHD to run on your own network."

Again, we're going to take, Artillery, Beartrap, Decloak, Honey Badger, Nova, Pushpin, Spidertrap, Web Bug Server, and Weblabyrinth and install them on our C3CM virtual machine as already in progress per Parts 1 and 2 of the series. In addition to all of Ethan's hard work on Spidertrap, Web Bug Server, and Weblabyrinth, it's with much joy that I'd like to point out that some of these devious offerings are devised by old friends of *toolsmith*. Artillery is brought to you by TrustedSec. TrustedSec is brought to you by Dave Kennedy (@dave_rel1k). Dave Kennedy brought us Social-Engineer Toolkit (SET) in February 2013 and March 2012 *toolsmiths*. Everyone loves Dave Kennedy.

Honey Badger and Pushpin are brought to you by @LaNMaSteR53. LaNMaSteR53 is Tim Tomes, who also works with Ethan and John at Black Hills Information Security. Tim Tomes brought us Recon-ng in May 2013's *toolsmith*. Tim Tomes deserves a hooah. Hooah! The information security

1 http://sourceforge.net/p/adhd/wiki/Home/.

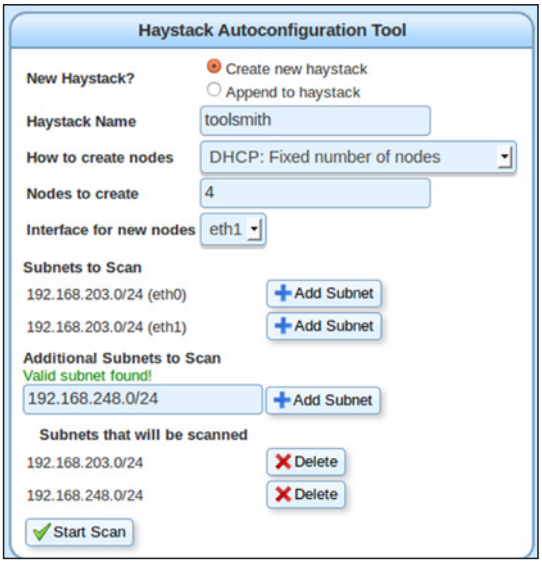

Figure 1 – Nova Haystack configuration

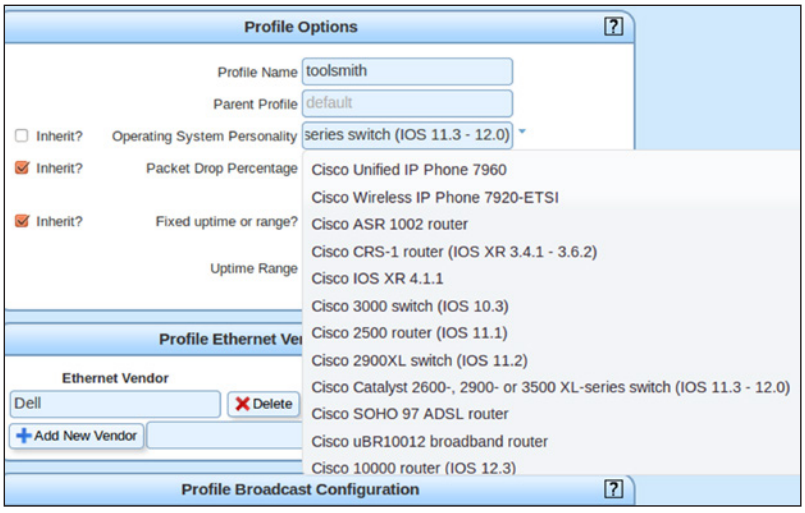

Figure 2 – Nova Profile configuration

community is a small world, people. Honor your friends, value your relationships, watch each other's backs, and praise the good work every chance you get. Let's counter, shall we?

ADHD installation tips

Be sure to install git on your VM via `sudo apt-get install git`, execute `mkdir ADHD`, then `cd ADHD`, followed by one big bundle of git cloning joy (copy and paste this big boy as a whole):

```
git clone https://github.com/trustedsec/
artillery/ artillery/&git clone https://github.
com/chrisbdaemon/BearTrap/ BearTrap/&git clone
https://bitbucket.org/ethanr/decloak decloak/&git
clone https://bitbucket.org/LaNMaSteR53/
honeybadger honeybadger/&git clone https://
bitbucket.org/LaNMaSteR53/pushpin pushpin/&git
clone https://bitbucket.org/ethanr/spidertrap
spidertrap/&git clone https://bitbucket.org/ethanr/
webbugserver webbugserver/&git clone https://
bitbucket.org/ethanr/weblabyrinth weblabyrinth/
```

Nova is installed as a separate process as it's a bigger app with a honeyd dependency. I'm hosting the installation steps on my website,[2] but to grab Nova and Honeyd issue the following commands from your ADHD directory:

```
git clone git://github.com/DataSoft/Honeyd.git
git clone git://github.com/DataSoft/Nova.git Nova
cd Nova
git submodule init
git submodule update
```

The ADHD SourceForge Wiki[3] includes individual pages for each script and details regarding their configuration and use. We'll cover highlights here but be sure to read each in full for yourself.

ADHD

I've chosen a select couple of ADHD apps to dive in to starting with Nova.

Nova is an open-source, anti-reconnaissance system designed to deny attackers access to real network data while providing false information regarding the number and types of systems connected to the network. Nova prevents and detects snooping by deploying realistic virtualized decoys while identifying attackers via suspicious communication and activity, thus providing sysadmins with better situational awareness. Nova does this in part with haystacks, as in find the needle in the.

Assuming you followed the Nova installation guidance provided above, simply run `quasar` at a command prompt then browse to https://127.0.0.1:8080. Login with username *nova* and password *toor*. You'll be prompted with the Quick Setup Wizard; do not use it.

From a command prompt execute `novacli start haystack debug` to ensure Haystack is running.

Click Haystacks under Configuration in the menu and define yourself a Haystack as seen in figure 1.

You can also add Profiles to emulate hosts that appear to attackers as very specific infrastructure such as a Cisco Catalyst 3500XL switch as seen in figure 2.

Assuming Packet Classifier and Haystack status show as online, you can click Packet Classifier from the menu and begin to see traffic as noted in figure 3.

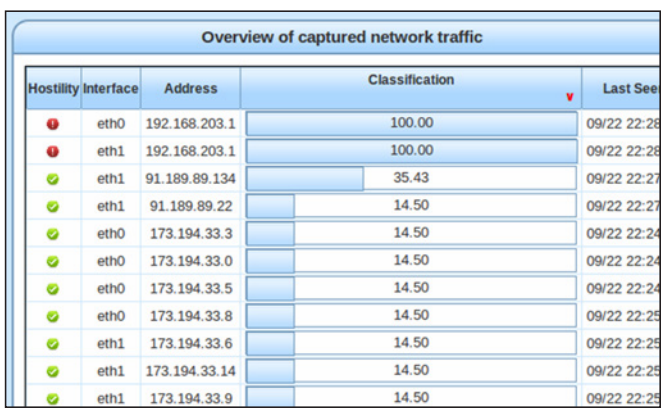

Figure 3 – Nova Packet Classifier (traffic overview)

2 http://holisticinfosec.org/toolsmith/files/adhd/NovaHoneydInstall.txt.

3 http://sourceforge.net/p/adhd/wiki/browse_pages/.

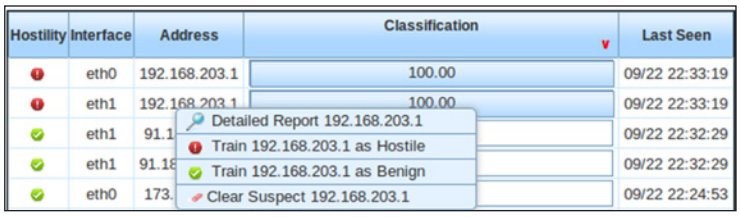

Figure 4 – Nova training capabilities

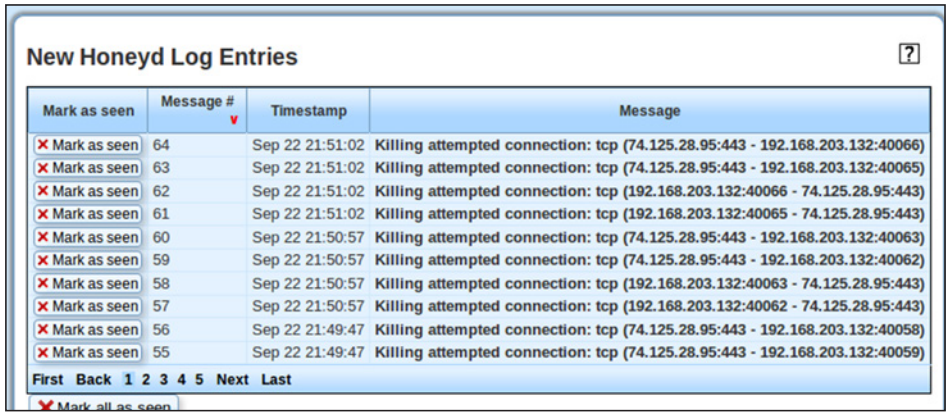

Figure 5 – Honeyd killing attempted connections

What's really cool here is that you can right-click on a suspect and train Nova to identify that particular host as malignant or benign per figure 4.

Over time training Nova will create a known good baseline for trusted hosts and big red flags for those that are evil. As you can see in figure 5, you'll begin to see Honeyd start killing attempted connections based on what it currently understands as block-worthy. Use the training feature to optimize and tune to your liking.

Nova's immediately interesting and beneficial; you'll discern useful results very quickly.

Spider Trap

The other ADHD app I find highly entertaining is Spider Trap. I come out on both sides of this argument. On one hand, until very recently I worked in the Microsoft organization that operates Bing. On the other hand, as website operator, I find crawler and spider traffic annoying and excessive (robots.txt is your friend assuming it's honored). Bugs you too and you want to get a little payback? Expose Spider Trap where you know crawlers will land, either externally for big commercial crawlers, or internally where your pentesting friends may lurk. It's just a wee Python script and you can run as simply as `python2 spidertrap.py`. I love Ethan's idea to provide Spider Trap with a list of links. He uses the big list from OWASP DirBuster like this, `python2 spidertrap.py DirBuster-Lists/directory-list-2.3-big.txt`, but that could just as easily be any text list. Crawlers and spiders will loop ad infinitum achieving nothing. Want to blow an attacker or pentester's mind? Use the list of usernames pulled from `/etc/passwd` I've uploaded[4] for you as `etcpasswd.txt`.

Download `etcpasswd.txt` to the Spider Trap directory, then add the following after line 66 of spidertrap.py:

```
#Attacker/pentester misdirect
self.wfile.write("<html><head><title>/etc/
passwd</title></head>")
```

Then run it like this: `python2 spidertrap.py etcpasswd.txt`.

The result will be something that will blow a scanner or manual reviewer's mind. They'll think they've struck pay dirt and have some weird awesome directory traversal bug at hand as seen in figure 6.

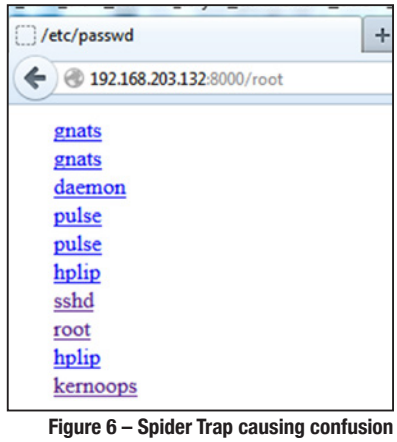

Figure 6 – Spider Trap causing confusion

Spider Trap runs by default on port 8000, but if you want to run it on 80 or something else just edit the script. Keep in mind if will fight with Apache if you try to use 80 and don't `service apache2 stop`.

You can have a lot of fun at someone else's expense with ADHD. Use it well, use it safely, but enjoy the prospect of countering your digital assailants in some manner.

In conclusion

In closing, for this three-part series I've defined C3CM as methods by which to identify, interrupt, and counter the command, control, and communications capabilities of our digital assailants.

ADHD, the counter phase of our C3CM concept, is not only downright fun but it becomes completely realistic to imagine taking active (legal) steps in defending your networks. ADHD gives me the energy to do anything and the focus to do nothing. Wait…never mind. Next month we'll discuss… um, I can't decide so you get to help!

For November which of the following three topics should toolsmith cover?

- Cuckoo Sandbox[5]
- Minion[6]
- OWASP Xenotix XSS Exploit Framework[7]

4 http://holisticinfosec.org/toolsmith/files/adhd/etcpasswd.txt.

5 http://www.cuckoosandbox.org/.

6 https://blog.mozilla.org/security/2013/07/30/introducing-minion/.

7 https://www.owasp.org/index.php/OWASP_Xenotix_XSS_Exploit_Framework.

Tweet your choice to me via @holisticinfosec, and email if you have questions regarding C3CM via russ at holisticinfosec dot org.

Cheers…until next month.

Acknowledgements

—John Strand and Ethan Robish, Black Hills Information Security

About the Author

Russ McRee manages the Security Analytics team (security incident management, penetration testing, monitoring) for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.