Network Security Toolkit (NST): Packet Analysis Personified

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

Prerequisites

Virtualization software if you don't wish to run NST as a LiveCD or install to dedicated hardware.

As I write this I'm on the way back from SANS Network Security in Las Vegas where I'd spent two days deeply entrenched analyzing packet captures during the lab portion of the GSE exam. During preparation for this exam I'd used a variety of VM-based LiveCD distributions to study and practice, amongst them Security Onion. There are three distributions I run as VMs that are always on immediate standby in my toolkit. They are, in no particular order, Doug Burk's brilliant Security Onion, Kevin Johnson's SamuraiWTF, and Back Track 5 R3. Security Onion[1] and SamuraiWTF[2] have both been *toolsmith* topics for good reason; I've not covered Back Track only because it would seem so cliché. I will tell you that I am extremely fond of Security Onion and consider it indispensable. As such, I hesitated to cover the Network Security Toolkit (NST) when I first learned of it while preparing for the lab, feeling as if it might violate some code of loyalty I felt to Doug and Security Onion. Weird I know, and the truth is Doug would be one of the first to tell you that the more tools made available to defenders the better.

NST represents a number of core principles inherent to *toolsmith* and the likes of Security Onion. NST is comprehensive and convenient and allows the analyst almost immediate and useful results. NST is an **excellent** learning tool and allows beginners and experts much success in discovering more about their network environments. NST is also an inclusive, open project that grows with help from an interested and engaged community. The simple truth is Security Onion and NST represent different approaches to complex problems. We all have a community to serve and the same goals at heart, so I got over my hesitation and reached out to the NST project leads.

The Network Security Toolkit is the brainchild of Paul Blankenbaker and Ron Henderson and is a Linux distribution that includes a vast collection of best-of-breed, open-source. network-security applications useful to the network security professional. In the early days of NST, Paul and Ron found that they needed a common user interface and unified methodology for ease of access and efficiency in automating the configuration process. Ron's background in network computing and Paul's in software development lead to what is now referred to as the NST WUI (web user interface). Given the wide range of open source networking tools with corresponding command line interfaces that differ from one application to the next, this was no small feat. The NST WUI now provides a means to allow easy access and a common look-and-feel for many popular network security tools, giving the novice the ability to point and click while also providing advanced users (security analysts, ethical hackers) options to work directly with command line console output.

According to Ron, one of the most beneficial tool enhancements that NST has to offer for the network and security administrator is the Single-Tap and Multi-Tap Network Packet Capture interface. Essentially, adding a web-based front-end to Wireshark, Tcpdump, and Snort for packet capture analysis and decode has made it easy to perform these tasks using a web browser. With the new NST v2.16.0-4104 release, they took it a step forward and integrated CloudShark[3] technology into the NST WUI for collaborative packet capture analysis, sharing and management.

Ron is also fond of the Network Interface Bandwidth Monitor. This tool is an interactive, dynamic, SVG/AJAX-enabled application integrated into the NST WUI for monitoring network bandwidth usage on each configured network interface in pseudo real time. He designed this application with the controls of a standard digital oscilloscope in mind.

Ron is also proud of NST's ability to geolocate network entities. We'll further explore using NST's current repertoire of available network entities that can be geolocated with their associated application, as well as Ron's other favorites mentioned above.

Paul also shared something I enjoyed as acronyms are so common in our trade. He mentioned that the NST distribution can be used in many situations. One of his personal fa-

1 http://holisticinfosec.org/toolsmith/pdf/may2011.pdf.
2 http://holisticinfosec.org/toolsmith/pdf/december2010.pdf.
3 http://www.cloudshark.org.

vorites is related to the FIRST Robotics Competition (FRC) which occurs each year. FIRST for Paul is **F**or **I**nspiration and **R**ecognition of **S**cience and **T**echnology, where I am more accustomed to its use as **F**orum for **I**ncident **R**esponse and **S**ecurity **T**eams. Paul mentors FIRST team 868, the TechHounds at the Carmel high school in Indiana, where in FRC competitions teams have used NST (or could use) during a hectic FRC build season:

- Quickly identity which network components involved with operating the robot are "alive"
  - From the WUI menu: Security -> Active Scanners -> ARP Scan (arp-scan)
- Observe how much network traffic increases or decreases as we adjust the IP based robot camera settings
  - From the WUI menu: Network -> Monitors -> Network Interface Bandwidth Monitor
- Capture packets between the robot and the controlling computer
- Scan the area for WIFI traffic and use this information to pick frequencies for robot communications that are not heavily used
- Set up a Subversion and Trac server for managing source code through the build season.
  - From the WUI menu: System -> File System Management -> Subversion Manager
- Teach the benefits of scripting and automating tasks
- Provide an environment that can be expanded and customized

While Paul and team have used NST for robotics, it's quite clear how their use-case bullet list applies to the incident responder and network security analyst.

Installing NST

NST, as an ISO, can be run as LiveCD, installed to dedicated hardware, and also as a virtual machine. If you intend to take advantage of the Multi-Tap Network Packet Capture interface feature with your NST installation set up as a centralized, aggregating sensor, then you'll definitely want to utilize dedicated hardware with multiple network interfaces. As an example, figure 1 displays using NST to capture network and port address translation traffic across a firewall boundary.

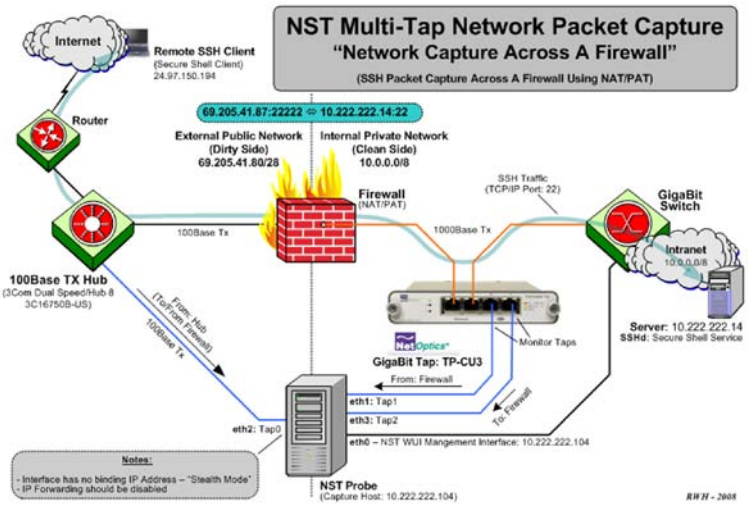

Figure 1 – Multi-Tap Network Packet Capture across a firewall - NAT/PAT Traffic

Once booted into NST you can navigate from *Applications* to *System Tools* to install NST to hard drive in order to execute a dedicated installation.

Keep in mind that when virtualizing you could enable multiple NICs to leverage multi-tap, but your performance will be limited as you'd likely do so on a host system with one NIC.

Using NST

NST use centers around the WUI; access it via Firefox on the NST installation at http://127.0.0.1/nstwui/main.cgi.

The first time you login, you'll be immediately reminded to change the default password (nst2003). After doing so, log back in and select *Tools -> Network Widgets -> IPv4 Address*. Once you know what the IP address is you can opt to use NST WUI from another browser. My session as an example: https://192.168.153.132/nstwui/index.cgi.

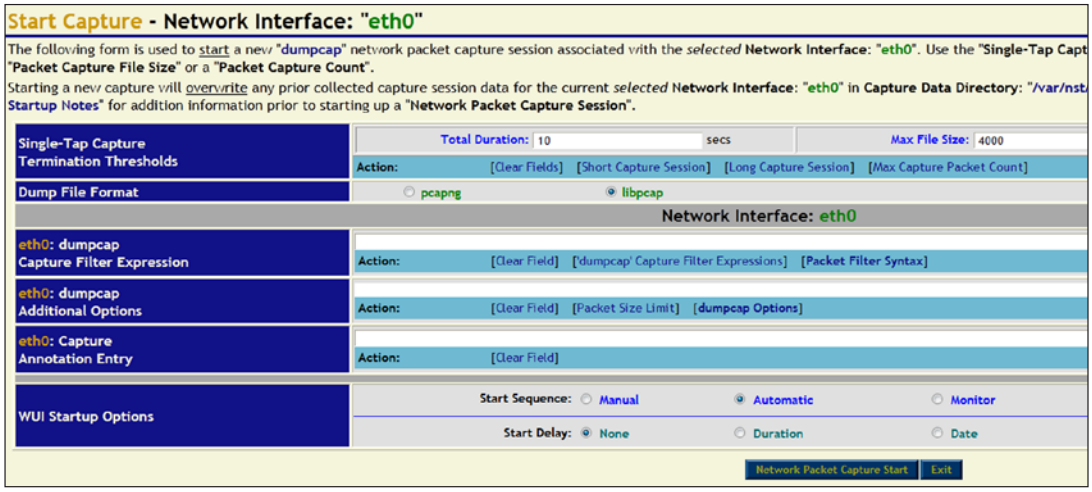

Figure 2 – Configure a Single-Tap capture with NST

Per Ron's above mentioned tool enhancements, let's explore Single-Tap Network Packet Capture (I'm running NST as a VM). Click *Network -> Protocol Analyzers -> Single-Tap Network Packet Capture* where you'll be presented with a number of options regarding how you'd like to configure the capture.

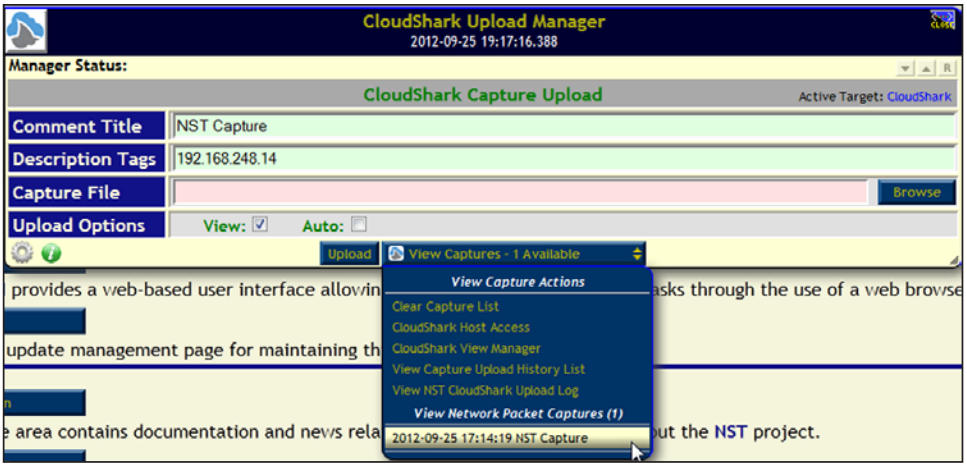

Figure 3 – CloudShark tightly integrated with NST

You can choose to define the likes of duration, file size, and packet count or select predefined short or long capture sessions as seen in figure 2.

If you accepted defaults for capture storage location, you can click *Browse* and find the results of your efforts in `/var/nst/wuiout/wireshark`. Now here's where the cool comes in. CloudShark (yep, Wireshark in the cloud) allows you to "secure, share, and analyze capture files anywhere, on any device" via either cloudshark.org or a CloudShark appliance. Please note that capture files uploaded to cloudshark.org are not secured by default and can be viewed by anyone who knows the correct URL. You'll need an appliance or CloudShark Enterprise to secure and manage captures. That aside the premise of CloudShark is appealing and NST integrates CloudShark directly. From the Tools menu select *Network Widgets* then *CloudShark Upload Manager*. I'd already upload `malicious.pcap` as seen in figure 3.

Users need only click on *View Network Packet Captures* in the upload manager and they'll be directed right to the CloudShark instance of their uploaded capture as seen in figure 4.

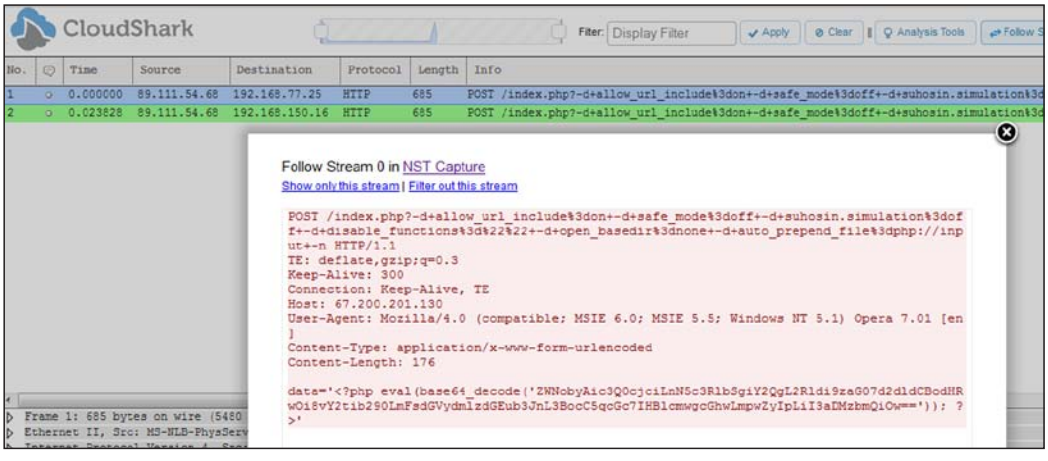

Figure 4 – Capture results displayed via CloudShark

Many of the features you'd expect from a local instance of Wireshark are available to the analyst, including graphs, conversations, protocol decodes, and follow stream.

NST also includes the Network Interface Bandwidth Monitor. *Select Network -> Monitors -> Network Interface Bandwidth Monitor.* A bandwidth monitor for any interface present on your NST instance will be available to you (eth0 and lo on my VM) as seen in figure 5.

You can see the +100 kbps spikes I generated against eth0 with a quick NMAP scan as an example.

NST's geolocation capabilities are many, but be sure to setup the

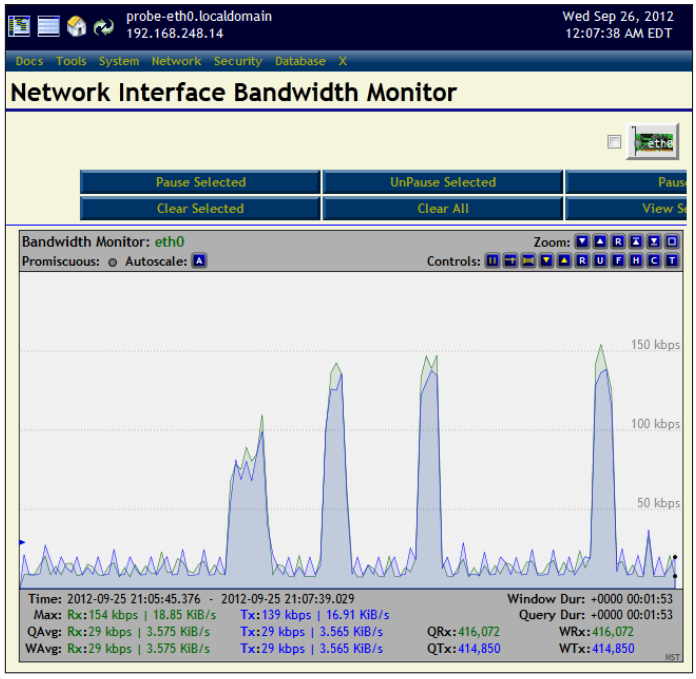

Figure 5 – NST's Network Interface Bandwidth Monitor

NST system to geolocate data first.[4] I uploaded a multiple host PCAP (P2P traffic) via Network Packet Capture Manager, clicked the A (attach) button under *Action* and was them redirected back to *Network -> Protocol Analyzers -> Single-Tap Network Packet Capture.* I then chose to use the Text-Based Protocol Analyzer Decode option as described on the NST Wiki[5] and clicked the

4 http://wiki.networksecuritytoolkit.org/nstwiki/index.php/HowTo_Setup_The_NST_System_To_Geolocate_Data.

5 http://wiki.networksecuritytoolkit.org/nstwiki/index.php/HowTo_Geolocate_Network_Packet_Capture_Data.

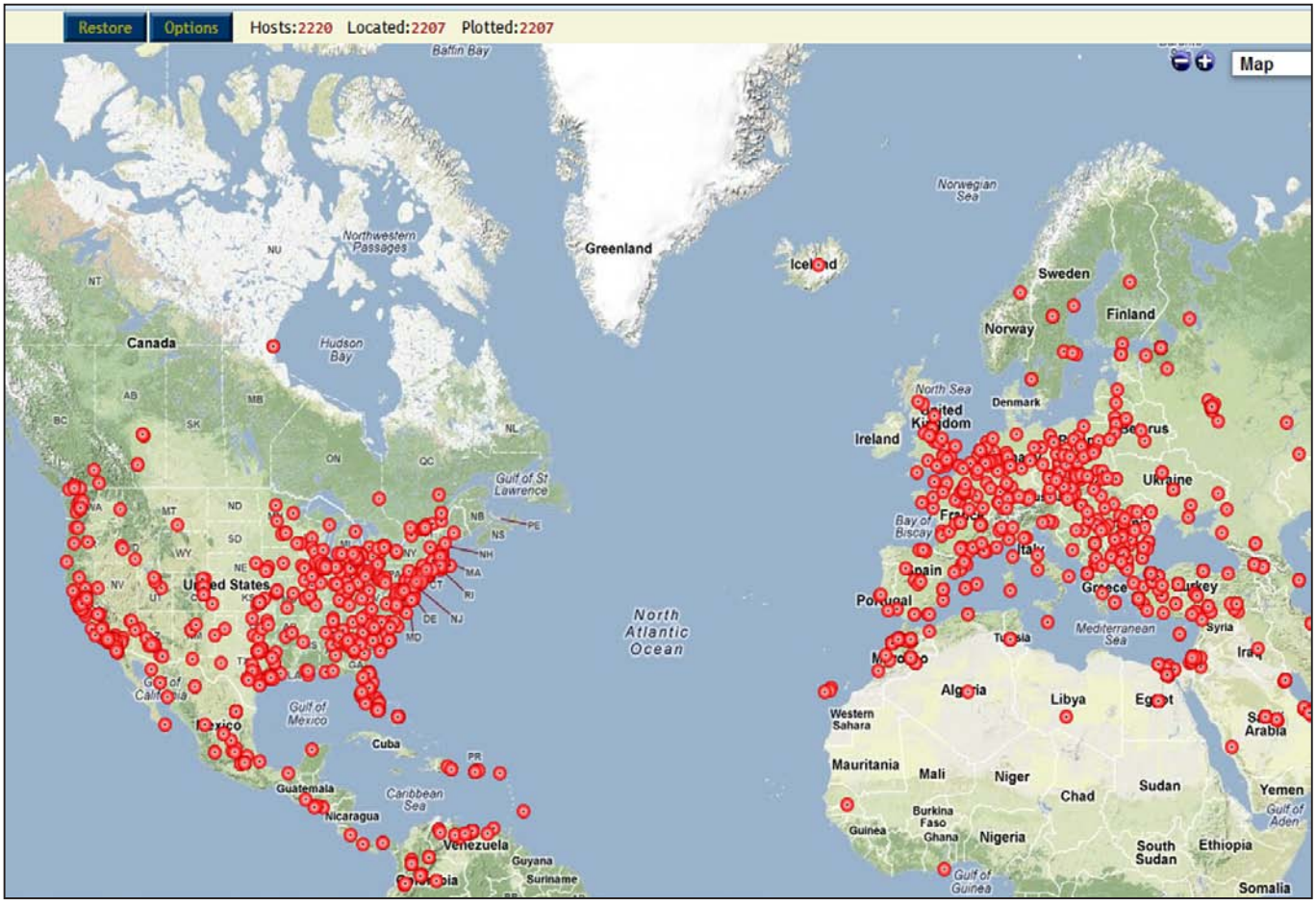

Figure 6 – P2P bot visually geolocated via NST

Hosts – Google Maps button. This particular capture gave NST a lot of work to do as it includes thousands of IPs, but the resulting geolocated visualization as seen in figure 6 is well worth it.

If we had page space available to show you the whole world you'd see that the entire globe is represented by this bot, but I'm only showing you North America and Europe.

As discussed in recent OSINT-related *toolsmiths*, there's even an NST OSINT feature called theHarvester, found under *Security -> Information Search -> theHarvester*. Information gathering with theHarvester includes email accounts, user names, hostnames, and domains from different public Internet sources.

So many features, so little time. Pick an item from the menu and drill in. There's a ton of documentation under the *Docs* menu, too, including the NST Wiki, so you have no excuses not to jump in head first.

In conclusion

NST is one of those offerings where the few pages dedicated to it in *toolsmith* don't do it justice. NST is incredibly feature rich, and literally invites the user to explore while the hours sneak by unnoticed. The NST WUI has created a learning environment I will be incorporating into my network security analysis teaching regimens. New to network security analysis or a salty old hand, NST is a worthy addition to your tool collection.

Ping me via email if you have questions (russ at holisticinfosec dot org).

Cheers…until next month.

Acknowledgements

—Paul Blankenbaker and Ron Henderson, NST project leads

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.