Security Onion

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

Prerequisites

Virtualization platform or dedicated hosts for Security Onion ISO installation

Introduction

We've discussed our share of Live CD/DVDs over the years for *toolsmith*, and for good reason. They often represent convenience, efficiency, and a discipline-specific focus (forensics, web application security, vulnerability assessment). It's been quite a while since we explored a network analysis distribution (HeX, February 2008) and we've got good reason to do so now. Doug Burks, president of the ISSA Augusta Chapter, recently released his latest version of Security Onion (SO).

The Security Onion LiveDVD is a bootable DVD useful for installing, configuring, and testing intrusion detection systems that are Xubuntu 10.04-based and includes Snort, Suricata,[1] Sguil, Squert, Xplico, metasploit, Armitage,[2] and a plethora of expected security tools. The Xubuntu choice is a good one as it uses the XFCE desktop environment and is designed for low-specification computers (great for sensors with limited horsepower) yet maintains all the benefits of the Ubuntu distribution.

Few Live CD/DVD distros have taken off as quickly as Security Onion, first launched in late 2009. Doug is passionate about this work, always strives to improve his craft and his offering, and has been lauded with high praise.

I recently asked Richard Bejtlich (*The Tao of Network Security Monitoring* and the TaoSecurity blog), now Chief Security Officer and Security Services Architect for Mandiant, how he uses Security Onion for his TCP/IP Weapons School.

"I'm using SO in class because I like Ubuntu on the desktop and I prefer students to use a public project rather than a custom setup, which is what I used to provide. Now I just recommend students to continue using SO outside the class so they can take advantage of updates. I add software that Doug doesn't include if necessary, but he keeps adding the sorts of apps I like as well."

If such feedback isn't impetus to make swift use of Security Onion, perhaps Doug's feedback will give due cause:

"I have many ideas for the future of Security Onion.[3] I have some other wild and crazy ideas in my head that I'm not yet willing to put in writing :) The next big project for Security Onion will be improving the package update process so that we can keep up with new releases of Snort, Suricata, and others. This will also allow us to more easily add new tools such as Ruminate IDS[4] and Project Razorback.[5] I've really been amazed at how Security Onion has taken off. The number of people using it around the world blows my mind. I'm glad that I can give back in such a small way to a security community that has given me so much."

Doug really understates his contribution (humble by nature); continued growth and attention for Security Onion is a benefit to all who take advantage of its focused feature set and convenient implementation.

Putting Security Onion to use

Doug is an excellent documentarian; his blog includes Security Onion related FAQ, presentations, issue tracking, and guidance. As such, we needn't reinvent the wheel or repeat what's been well-defined by Doug. The latest version of Security Onion (20110404) includes a setup script that literally turns the process of setting up a Sguil server and sensors a point and click prospect. Sguil[6] is *toolsmith* topic worthy by itself, but Security Onion does such a great job of Sguil, Snort/Suricata, and OSSEC integration that it's literally the quality instant coffee equivalent of SIEM. Imagine stable, performing correlation in minutes. "A little Security Onion in your cup!"

Figure 1 – Instant SIEM

I have a deep appreciation for all these tools, having discussed Snort, Suricata, and OSSEC at multiple times in the past. For this article I opted to use Security Onion with Advanced Setup for my primary server as follows:

Clicked *Setup*

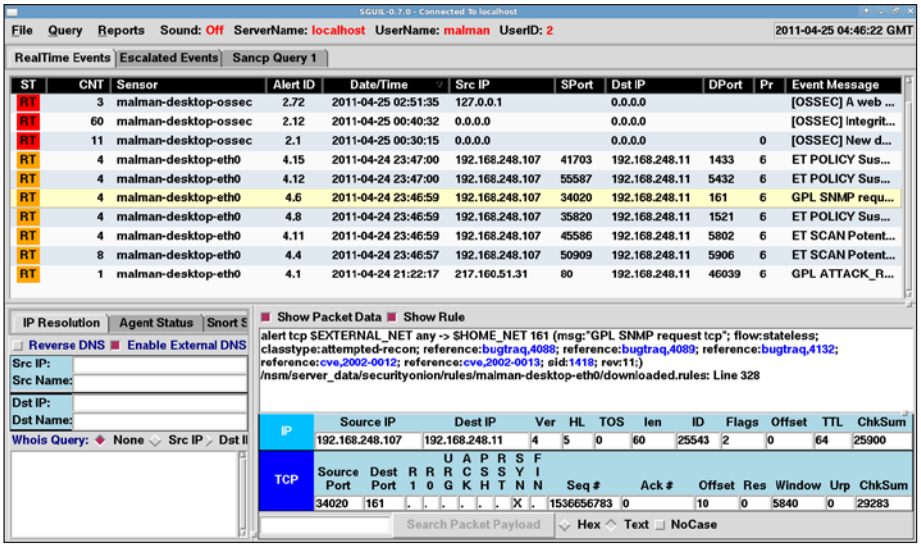
Chose *No, use Advanced Setup*

Chose *Both (configures server and sensor)*

Selected *Snort* (default IDS)

1 http://holisticinfosec.org/toolsmith/docs/august2010.html.
2 http://holisticinfosec.org/toolsmith/pdf/january2011.pdf.
3 http://code.google.com/p/security-onion/issues/list.
4 http://smusec.blogspot.com/2010/12/announcing-ruminate-ids.html.
5 http://labs.snort.org/razorback/.
6 http://sguil.sourceforge.net/.

Figure 2 – Sguil!



Set Snort to listen on eth0 (running only one interface on the VM, not ideal)

Selected *Snort VRT ruleset and Emerging Threats NoGPL ruleset* (need a Snort VRT oinkcode)

Entered oinkcode

Assigned Sguil client username and password

Selected *Yes, proceed with the changes!*

Security Onion uses PulledPork[7] to manage rules handling; as the server and sensor build after setup script execution, you'll note a rules update followed by an invitation to utilize Sguil or Squert[8] to view events. I must confess to having not spent as much time of late in the network security monitoring (NSM) discipline as I would like; it was refreshing to have a chance to use Squert a bit. Squert, while not a real-time event console, or a replacement for the Sguil client, is "a visual tool that attempts to provide additional context to events through the use of metadata, time series representations, and weighted and logically grouped result sets."

I'll circle back to Squert after generating some interesting event data.

You can use the Security Onion ISO to distribute multiple sensors, all of which can be managed via your primary server installation. You can also choose to add OSSEC agents to hosts you'd like to monitor and point them to your Security Onion server.

7 http://code.google.com/p/pulledpork/.

8 http://www.squertproject.org/.

To accept remote OSSEC agent connections, you'll need to allow traffic to UDP port 1514. Default allowed connections to Security Onion are to TCP port 22, 80, 7734, and 7736. The easiest way to allow UDP 1514 is with Uncomplicated Firewall (UFW).[9] Execute `sudo ufw allow 1514/udp` then `sudo ufw status numbered` to confirm.

Add an OSSEC agent to Windows or Linux hosts; October 2009's *toolsmith*[10] will give you all the information you need to do so.

I threw a few "attacks" at different targets including my VM hosts systems, the Security Onion guest, and a Windows XP guest VM. Figure 2 exhibits events as reported via Sguil.

If you don't already love Sguil, spending anytime with Security Onion will send you over the top; count on instant gratification. The thing to remember about Sguil is to right-click in columns of interest such as ST, CNT, and Alert ID. I right-clicked a three-count of events starting with Alert ID 2.72 and selected *View Correlated Events*. The event details (see Figure 3) confirmed a finding I'd spotted earlier and was overjoyed when Sguil reported it via OSSEC.

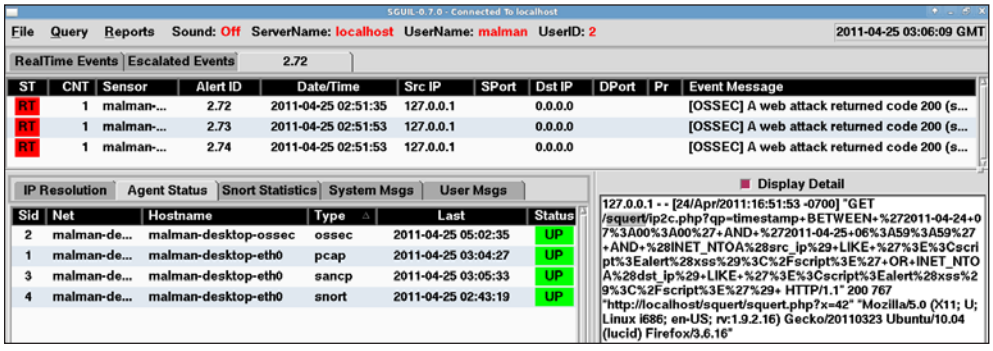


Figure 3 – Sguil reports a web attack against Squert

While experimenting with Squert I noticed cross-site scripting (XSS) flaws via manual testing while using the tool. Turns out the bug is already reported and publicly filed on the Squert site, but I was pretty impressed when a web application security flaw in one of the tools was reported by and to the same framework when exploited. Oh, the circle of life (in the matrix) ;-).

The Sguil suite leverages SANCP,[11] p0f,[12] PADS,[13] tcpdump, tcpflow, and Wireshark in addition to above-mentioned tools.

9 https://help.ubuntu.com/community/UFW.

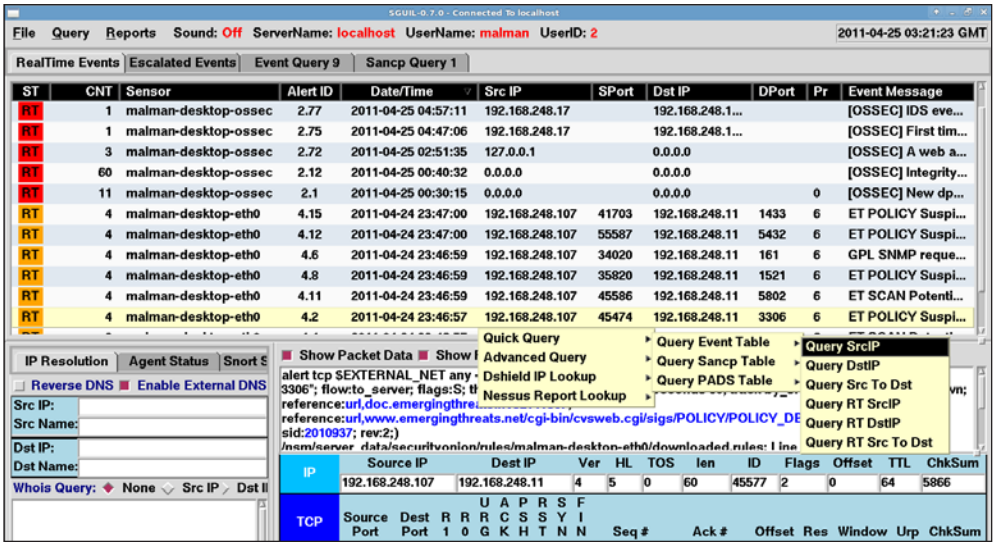
10 http://holisticinfosec.org/toolsmith/docs/october2009.html.

11 http://nsmwiki.org/SANCP.

12 http://nsmwiki.org/P0f.

13 http://nsmwiki.org/PADS.

Figure 4 – Sguil correlates attacker event data



PADS, the "passive asset detection tool that monitors a network interface and reports all systems and services it discovers," kicked out a malformed syslog message and was thus flagged by Sguil. Er, noise writing to your console? Right-click RT for the event row and choose *Expire Event as NA* (can do with comments as well). I had a similar noisy finding reported by the OSSEC agent on one of my non-virtual systems due to files written to Trash by root with everyone permissions. I simply cleared root's trash bin on the host and expired events as not applicable.

Event correlation (remember the instant SIEM comment above) is so key to successful network security monitoring. Using my main Linux server (192.168.248.107) as a scanning attacker, I probed my Security Onion server (192.168.248.11).

I right-clicked 192.168.248.107 under *SrcIP*, selected *Quick Query*, followed by *Query Event Table*, then *Query SrcIP*. 234 events later, I had all data specific to the attacking host.

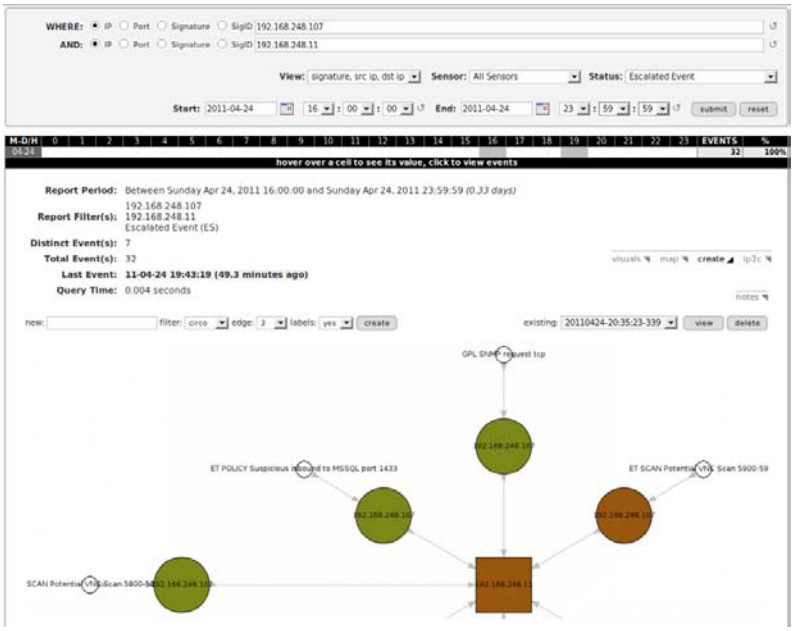


Figure 5 – Squert visualizes escalated event data

Right-clicking *RT* for an event also gives you the opportunity to escalate events with comments. Choose *Update Event Status* then *Escalate (F9)* or a specific *Incident Category*.

I promised you a look at Squert too, so I queried Squert for the same 192.168.248.107-related events as noted above via Sguil. Aside from Squert's advanced query capabilities, it also employs AfterGlow 1.6 and the graphviz libraries for visualization.[14] The joy keeps coming, right? Figure 5 shows Squert results based on the events I escalated above.

Should you be tracking routed traffic (non-RFC 1918), you can also build maps with Squert, as well as basic bar graph visuals.

In conclusion

I'll try to avoid flagrant gushing, but Security Onion employs a congregation of the most important tools available to security and network analysts that I've ever discussed. Attack and reconnaissance tools are important, but I am the ultimate blue-teamer at heart. I've said it before: "What you don't see can hurt you." You can see better with Security Onion and its well-implemented deployments of Snort/Suricata, SANCP, and Sguil/Squert. I will simply say that you can defend yourselves, and those you are charged with protecting, better with the likes of Security Onion.

Job well done, Doug. As an ISSA member I'm proud of your work and your contributions to our association and community. Readers, take advantage of this noteworthy effort.

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

Cheers…until next month.

Acknowledgements

—Doug Burks, project lead for Security Onion; president, ISSA Augusta Chapter

About the Author

Russ McRee, GCIH, GCFA, GPEN, CISSP, is team leader and senior security analyst for Microsoft's Online Services Security Incident Management team. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ at holisticinfosec dot org.

14 http://www.linux-magazine.com/Issues/2009/106/Security-Visualization-Tools.