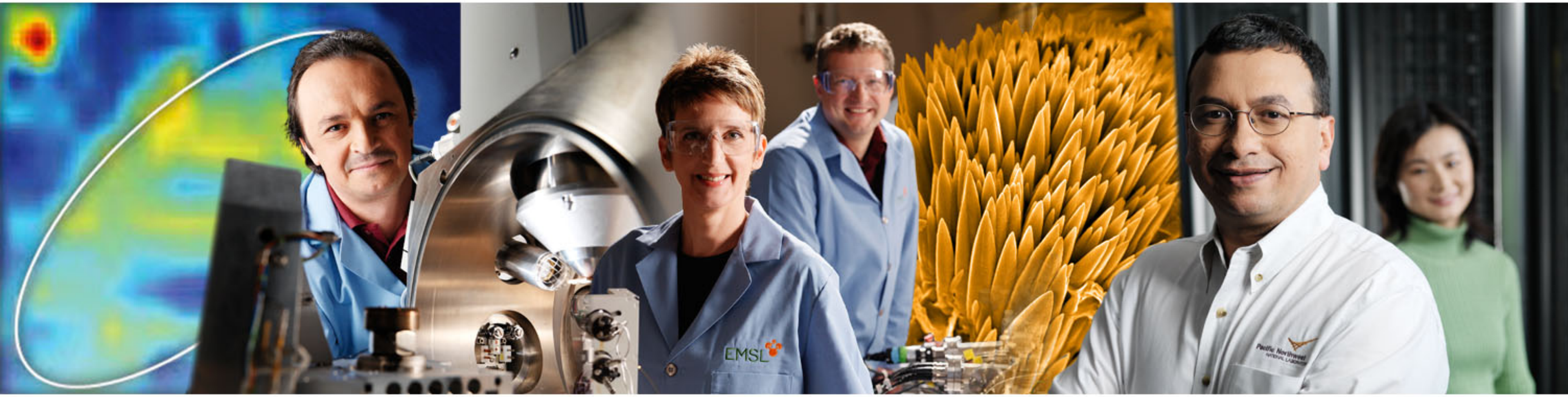
EMSL

Peeling Back the Layers of the Network Security with Security Onion

Gary Smith, Pacific Northwest National Laboratory



Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965
U.S. DEPARTMENT OF ENERGY

A Little Context

- The Five Golden Principles of Security
  - Know your system
  - Principle of Least Privilege
  - Defense in Depth
  - Protection is key but detection is a must.
  - Know your enemy.

What Is An IDS?

- An IDS (Intrusion Detection System)
  - Is usually passive in nature.
  - Detects and alarms on suspected intrusions using signature-based, statistical anomaly-based, or and/or stateful protocol analysis detection.
  - Has a reputation for false positives.

What If…

- Data breaches are occurring within the organization?
- A breached mobile device or infected personal laptop brings outside threats inside the network which goes undetected by most IDS?
- Any rogue or unauthorized device tries to access the network internally from behind the firewall?

Network Security Monitoring

- NSM (Network Security Monitoring)
  - Requires capture and storage of large amount of data.
  - Is concerned with the process of reconstructing a network event
    - Intrusion such as a hack or a penetration
    - Network or infrastructure outage
  - Is based on live IP data captures
    - A new way of looking at trace analysis
    - Continues from where traditional network troubleshooting ends
- Whether you’re tracking an adversary or trying to keep malware at bay, NSM provides context, intelligence and situational awareness of your network.

How do you get NSM?

- Many CIO's/CISO's believe NSM is a solution they can buy to fill a gap; purchase and deploy solution ABC from company XYZ and the problem is solved!
  - There are lots of companies that will sell you a "solution" but neglect the "M" in "NSM".
  - While Artificial Intelligence and fancy interfaces can assist in the process of sorting through false positives and malicious indicators, there is no replacement for human intelligence and awareness.
- Security Onion, create by Doug Burks, will provide visibility into your network traffic and context around alerts and anomalous events.
- It requires a commitment from you the administrator or analyst to review alerts, monitor the network activity.

Security Onion Components

- Security Onion seamlessly weaves together three core functions:
  - Full packet capture,
  - Network-based and host-based intrusion detection intrusion detection systems (NIDS and HIDS, respectively), and
  - Powerful analysis tools.

Full Packet Capture

- Full packet capture is like a video camera for your network, but better because
  - Not only can it tell us who came and went, but also
  - Exactly where they went and what they brought or took with them
    - Exploit payloads
    - Phishing emails
    - File exfiltration
- Full-packet capture is accomplished via netsniff-ng (http://netsniff-ng.org/), “the packet sniffing beast”.
- netsniff-ng captures all the traffic your Security Onion sensors see and stores as much of it as your storage solution will hold (Security Onion has a built-in mechanism to purge old data before your disks fill to capacity).

NIDS and HIDS

- Network-based and Host-based Intrusion Detection Systems (IDS) analyze network traffic or host systems, respectively, and provide log and alert data for detected events and activity.
- Security Onion provides multiple IDS options:
  - Rule-driven NIDS: For rule-driven network intrusion detection, Security Onion offers the choice of Snort (http://snort.org/) or Suricata (http://suricata-ids.org/).
  - Analysis-driven NIDS: For analysis-driven network intrusion detection, Security Onion offers The Bro Network Security Monitor, also known as Bro IDS (http://bro-ids.org/).
  - For host-based intrusion detection, Security Onion offers OSSEC (http://www.ossec.net/), a free, open source HIDS for Windows, Linux and Mac OS X.

Analysis Tools

EMSL

- With full packet capture, IDS logs and Bro data, there is a daunting amount of data available at the analyst's fingertips.
- Security Onion integrates the tools to make the task easier:
  - *Enterprise Log Search and Archive* (ELSA https://code.google.com/p/enterprise-log-search-and-archive/). ELSA is a powerhouse search tool that allows you to effortlessly comb through most all of the data collected by Security Onion as well as any additional syslog sources that you forward to it.
  - *Snorby* (https://snorby.org/), created by Dustin Webber (@Mephux), is a web application interface to view, search and classify Snort and Suricata alerts and generate various types of reports.

Analysis Tools – Cont.

- *Sguil* (http://sguil.sourceforge.net/), created by Bamm Visscher (@bammv), provides a single GUI (written in tcl/tk) in which to view Snort or Suricata alerts, OSSEC alerts, Bro HTTP events, and Passive Real-Time Asset Detection System (PRADS) alerts.
- *Squert* (http://www.squertproject.org/), created by Paul Halliday (@01110000), provides several visualization options for the data such as “time series representations, weighted and logically grouped result sets” and geo-IP mapping by interfacing to the Sguil database.
- *Snorby* (https://snorby.org/), created by Dustin Webber (@Mephux), is a web application interface to view, search and classify Snort and Suricata alerts and generate various types of reports, such as most active IDS signatures, most active sensors, and top source and destination IP addresses.

Security Onion Installation

- One would think that with so many packages as there in Security Onion, installation and configuration would be a nightmare.
- Such is NOT the case!
- In fact, installation and configuration of Security Onion is so easy, a Windows admin, with no knowledge of Linux, can have a working Network Security Monitoring system up in running in as little as 30 minutes.
- This includes:
  - Downloading and burning the ISO image to a CD.
  - Installing Security Onion to a PC with 2 NICS.
  - Running the installation wizard and answering a few simple questions.

Security Onion System Requirements

- 2 NICs
  - One for the management interface
  - One for packet capture
- Memory is highly dependent on several variables:
  - The services that you enable
  - The kinds of traffic you're monitoring
  - The actual amount of traffic you're monitoring
  - The amount of packet loss that is "acceptable" to your organization
- Storage
  - The more disk space you have, the more log retention you'll have for doing investigations after the fact.
  - Disks are dirt cheap! Cram all you can into the system.

Security Onion Deployment Scenarios

- There are the three Security Onion deployment scenarios:
  1. Standalone
  2. Sensor/Server
  3. Hybrid
- The Security Onion setup script allows you to easily configure the best installation scenario to suit your needs.

Conclusion

- With NSM, we have:
  - Full packet capture,
  - Snort or Suricata rule-driven intrusion detection,
  - Bro event-driven intrusion detection and
  - OSSEC host-based intrusion detection,
  - All running out of the box once you run Security Onion setup.
- These disparate systems with various dependencies and complexities all run seamlessly together and would otherwise take days, weeks or months to assemble and integrate on their own.
- What was once a seemingly impossible task is now as easy to install as Windows ;)

References

- Bro IDS (http://bro-ids.org/)
- Enterprise Log Search and Archive (ELSA https://code.google.com/p/enterprise-log-search-and-archive/)
- Netsniff-ng (http://netsniff-ng.org/)
- OSSEC (http://www.ossec.net/)
- Security Onions (http://blog.securityonion.net/)
- Sguil (http://sguil.sourceforge.net/)
- Snorby (https://snorby.org/)
- Snort (http://snort.org/)
- Squert (http://www.squertproject.org/)
- Suricata (http://suricata-ids.org/)

EMSL

Questions?

Gary Smith

Information System Security Officer, Molecular Science Computing, Pacific Northwest National Laboratory

Richland, WA

gary.smith@pnnl.gov