Global Information Assurance Certification Paper

Integrating Wired and Wireless IDS Data

GIAC (GCIA) Gold Certification

Author: Michael D. Stanton, corenor@gmail.com
Advisor: Rich Graves

Accepted: January 30th 2014

Abstract

The types of attacks that target wired networks and those that target wireless networks are very different. Wireless attacks may span the protocol spectrum from physical denial of service to upper layer attacks against many of the authentication protocols. Wired networks have exposures at the physical layer as well but the biggest risks are from threats that operate at the network layer and above. The solution described in this paper will provide a foundation for further research by exploring open source tools that can be used to discover indications of attack in both the wired and wireless networks. In addition, we will begin to correlate these cross platform attacks using a security incident and event management framework.

1. Integrating Wired and Wireless Data

According to Gartner, smart phones and other mobile computing devices are rapidly replacing personal computers.

> "The second quarter of 2013 saw another quarter of shipment declines with worldwide volumes dropping to 2009 levels. Volumes declined by 11% year over year but only 3% sequentially during 1Q13 (Gartner 2013)."

They also note that this was the fifth consecutive quarter showing declines. Regarding smart phones, the trend is in the opposite direction. The number of devices sold surpassed traditional phones in 2011 and outpaced global PC sales the next year (IDC, Gartner, Morgan Stanley Research). A necessary feature of all mobile devices is that they connect wirelessly in order to operate. Often these mobile devices share the same wireless spectrum and logical networks as their PC counterparts. Therefore, the wireless domain must be considered a major exposure point for any enterprise.

Wireless communication operates at the lower layers of the OSI or TCP/IP model. The physical medium is RF transmission utilizing unguided electromagnetic waves. In wireless networks the data link layer commonly implements the 802.11 protocol suite. Because this lower layer information is encapsulated or stripped by routers and other devices, there is very little information contained within the data stream to trace an attacker back to their wireless origin without additional log capture and correlation. While wireless logs are often collected for troubleshooting purposes and to detect common threats, it is difficult to find monitoring solutions that will detect attacks by correlating events originating from wireless networks with logs originating from the traditional wired log sources.

Our goal is to demonstrate a working model for capturing and analyzing wired and wireless event logs collectively. This paper will describe a basic framework that includes the following components:

- Wired and wireless sensors for collecting network traffic

Michael Stanton, corenor@gmail.com

- Signature or other types of intrusion analysis engines for processing the sensor data
- A centralized event and incident management platform for additional analysis and correlation between the two data sources.

2. Component Selection

The minimal set of components necessary to begin examining and accurately correlating and alerting on wired and wireless log sources is relatively complex. Commercial versions of each component may cost thousands of dollars. We will highlight the basic building blocks of an integrated solution using a set of tools that can be acquired easily. An open source set of tools offers a more approachable environment for learning about each area, wired intrusion detection and prevention, wireless intrusion detection and prevention, and security incident and event management.

Further, the chosen components are not restricted by non-disclosure or other contract elements. Furthermore, these solutions have documentation readily available and often there is an active community of contributors and users willing to provide support at no cost. Finally, the chosen solutions have the potential to be tailored to suit specific hardware and other architecture needs. For example, they can be implemented in virtual environments for proof of concept or to repurpose surplus hardware.

3. Component Overview

It is no great leap to say that a robust monitoring program should include many diverse log sources. Having a large diversity of log sources will add context to the logs from the security specific solutions described below. For example, a security specific log or alert may indicate that an attack was attempted against a critical server. The additional context logs may help determine the attacker's next moves. These logs may also help to more accurately classify the events. Some examples of these additional log sources may include switches, routers and other network infrastructure components, operating systems, critical applications, as well as authentication systems like RADIUS, LDAP or Active

Directory. While these additional log sources are essential for a robust monitoring environment they will not be discussed for this framework in order to focus on the three primary components previously discussed.

Because our goal is to track activity crossing between wired and wireless network zones it is also important that the monitoring solutions for each zone are instrumented to see traffic or collect logs from points that where this traffic traverses between these two areas. If there are no overlapping network segments between the wired and wireless zones that are monitored, it is much less likely that the data can be correlated effectively.

3.1 The First Component: Security Incident and Event Management (SIEM)

Like wireless intrusion detection, choices for open source SIEM are also quite limited. The search is even more difficult when looking for something that includes support for wireless IDS logs. In the introduction to David Miller's 2001 book "Security Information and Event Management (SIEM) Implementation" he provides the following definition for SIEM:

"The SIEM system is a complex collection of technologies designed to provide vision and clarity to the corporate IT system as a whole, benefitting security analysts and IT administrators as well."

What this "collection of technologies" does, generally speaking, is analyze data with the goal of discovering security incidents based on rules that correlate a variety of relevant event logs.

For this framework we demonstrate an open source solution developed by AlienVault called "OSSIM" (AlienVault 2013). OSSIM parses a large number of log sources including wireless alerts produced by Kismet. In addition, OSSIM maintains a list of wireless clients and servers similar to the running display from the Kismet client.

3.2 The Second Component: Wired IDS

Of the three component areas that are described, a wired intrusion detection system or IDS represents the most mature technology. There are many

choices for wired IDS. Some examples of successful and active open source projects include Bro, Suricata, and Snort. Snort will provide the wired monitoring capability for this demonstration. Snort benefits from all of the features described for other open source solutions; easy access to documentation, an open framework and the ability to customize.

3.3 The Third Component: Wireless IDS

Open source options for wireless IDS are rare. Quite a few projects have been started in this area but they don't enjoy robust support or wide distribution. Some examples include air-snort, widz, openwips-ng, beholder, and whiff. The consensus I have seen from surveying various projects and research papers is that Kismet is the most readily available and robust platform at this time although openwips-ng may expand to eclipse Kismet. Kimset was chosen because it is readily integrated with OSSIM.

4. Build Details

All of the components for this demonstration environment were built as virtual machines (VMs). When working with virtual computing there are some key terms to consider. The "Host" operating system is the operating system that has the virtual computing software installed. This is the native operating system for the hardware. For the framework described hardware is an Apple Macbook Pro with 2.4 Ghz i7 processor and 8GB of physical RAM. The host operating system is Apple Mac OS X 10.8.5 "Mountain Lion". The virtualization software installed is VMware Fusion 4.1.4.

Additionally, there are three virtual guest operating systems supporting the remaining components of the framework; the OSSIM console, a virtual guest acting as a wired IDS and a virtual guest acting as a wireless IDS. The wired and wireless sensors have the Linux Mint 13 "Maya" OS installed. Each IDS virtual machine has one virtual processor and 1GB of RAM. In addition to the virtual "wired" adapter, the wireless IDS has a second USB wireless network adapter that performs traffic capture. The USB card is the "awus051nh" from Alfa.

Configuring static IP addresses using NAT mode for each guest simplifies the configuration of the various components and makes it possible to copy the guest instances to various physical server machines without significant changes.

Figure 1. Located in Section 5.2 provides a logical diagram of the monitoring framework.

OSSIM was also installed as a virtual machine guest using the ISO provided from the Alien Vault website. As with the Mint distributions, OSSIM was configured with a static IP and NAT networking mode. The OSSIM server was configured with one processor and 3GB of RAM.

Alien Vault provides some helpful configuration guides for setting up both the OSSIM platform and also the integration with Kismet (OSSIM 2009). The website for Kismet describes the application as:

> .. an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins which allow sniffing other media such as DECT.
>
> Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic (Kismet 2013).

The guides provided by contributors to the OSSIM project are quite detailed and helpful for configuring each of the elements described.

5. Build Steps

5.1 Build Steps for Wireless Integration

Ash Wilson (2012) provides an excellent guide for integrating wireless IDS using Kismet. I've provided a high level summary below.

High Level Build Process for Wireless IDS:

1	Configure 'OpenVPN'(OSSIM 2010) connectivity between the wireless guest and the OSSIM console. This is recommended to protect sensitive log information as it traverses the network.
2	Configure an SSH key pair for use by the OSSIM console to retrieve log files from the sensor.
3	On the Console: Configure Kismet for automatic startup, security alerting, and remote logging to OSSIM
5	Configure the OSSIM console to receive logs from Kismet.

5.1 Build Steps for Wired Integration

Configuring a remote wired IDS log source is simpler than the wireless configuration. OSSIM can receive snort logs as syslog. As with the wireless configuration, a VPN connection is recommended.

High Level Build Process for Wired IDS:

1	Configure 'OpenVPN'(OSSIM 2010) connectivity between the wired sensor guest and the OSSIM console. This is recommended to protect sensitive log information as it traverses the network.
2	On the sensor: Configure Snort and enabled the 'alert_syslog' output plugin.
3	On the sensor: Configure syslog to send Snort alerts to the OSSIM console.
4	On the console: Insure that the "snort_syslog" detector type is enabled. This is defined in "ossim_setup.conf".
5	On the console: Edit snort_syslog.cfg and check that the "location" setting is defined properly for incoming wired alerts. By default "/var/log/daemon.log"

5.2 Infrastructure Overview

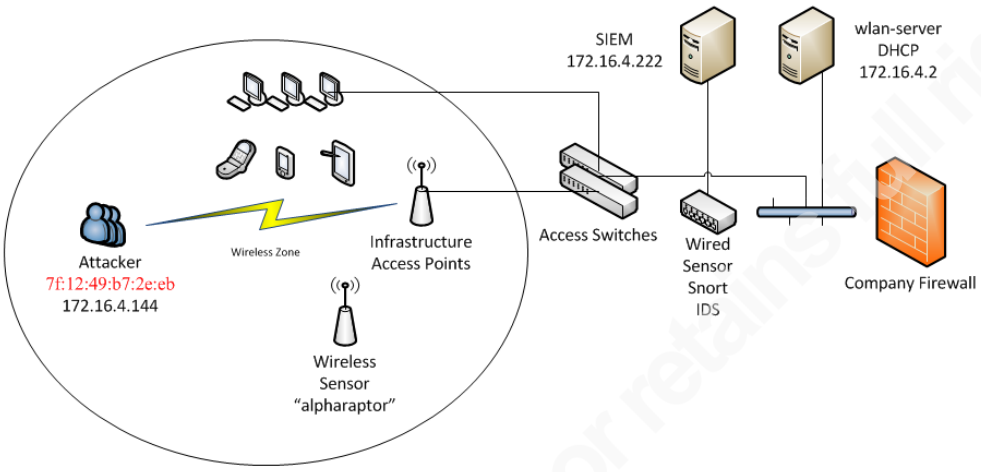


Figure 1. Shows a simple network logical diagram. In this scenario attackers may bypass firewalls or other wired intrusion detection or prevention solutions depending on the network architecture. Wireless sensors should be placed to cover spectrum that is accepting infrastructure wireless connections.

6. Logs

To better demonstrate how log sources can be correlated, MAC address fields are colored in blue and IP address fields in red.

6.1 Logs from Kismet

Below are sample alert type logs issued by Kismet in response to crafted attack packets using the 'WIDSTT.PY' Python script (Blasco 2010). These are seen as syslog on the collector and are forwarded using the "rsyslog" application to the OSSIM console.

Nov 15 10:37:57 alpharaptor kismet: ALERT Sun Sep 15 14:40:57 2013 Unknown disassociation reason code 0x1F4 from 7F:12:49:B7:2E:EB

Nov 15 10:38:24 alpharaptor kismet: ALERT Sun Sep 15 12:27:24 2013 Illegal SSID length (100 > 32) from 7F:12:49:B7:2E:EB

Nov 15 10:38:56 alpharaptor kismet: ALERT Sun Sep 15 14:40:56 2013 Suspicious client FF:FF:FF:FF:FF:FF - probing networks but never participating.

Nov 15 14:40:57 alpharaptor kismet: ALERT Sun Sep 15 14:40:57 2013 Unknown deauthentication reason code 0x1F4 from 7F:12:49:B7:2E:EB

While all of these events are suspicious, the log entry highlighted in red might be seen as a precursor to an attack against a WPA/WPA2 pre shared secret. Note the MAC address at the end of the log entry. For WPA2-PSK it is desirable to capture the 4-way handshake so that the information can be used to crack the pass phrase off line (SANS 2011). One way to force clients to authenticate is to attempt to deauthenticate their session. The client will then automatically reauthenticate with the access point.

6.2 Additional Logs as Seen by OSSIM

2013-11-12 10:40:03 Kismet: Found new network 0 Kismet alienvault N/A N/A

2013-11-12 10:40:03 Kismet: Illegal SSID length 0 Kismet alienvault N/A N/A

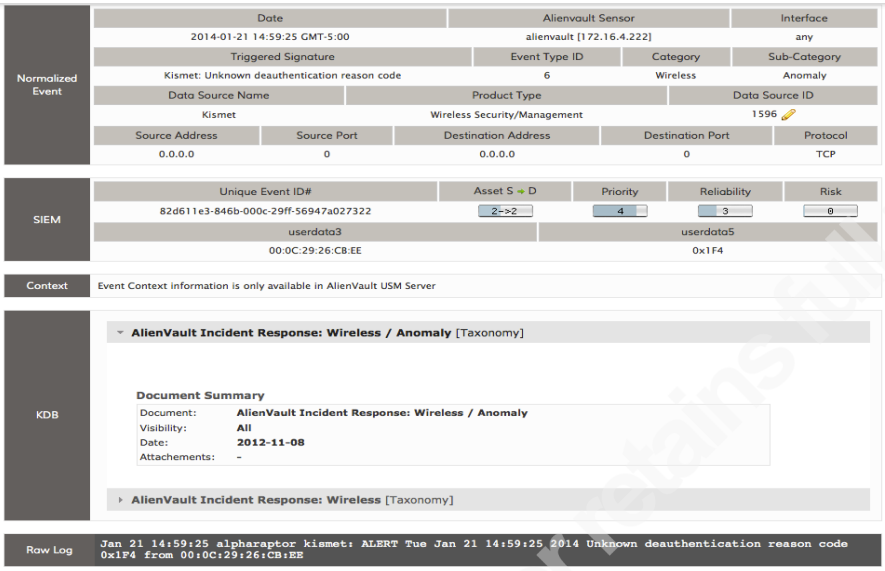
2013-11-12 10:40:03 Kismet: Unknown disassociation reason code 0 Kismet alienvault N/A N/A

2013-11-12 10:40:03 Kismet: Found new network 0 Kismet alienvault N/A N/A

2013-11-12 10:40:03 Kismet: Unknown deauthentication reason code 0 Kismet alienvault N/A N/A

OSSIM captures the entire alert from Kismet but the above short display is provided for easy review. It is possible to click on an individual event to see more detail and the original log.

View of alert within OSSIM incident detail:



6.3 Raw Packets

Below are sample raw packets captured on the wireless sensor host from similar suspicious events. Source MAC address is highlighted.

297 1.773794 7f:12:49:b7:2e:eb -> c3:c5:8d:28:a8:07 802.11 26 Deauthentication, SN=0, FN=0, Flags=.....

0000 c0 00 00 00 c3 c5 8d 28 a8 07 7f 12 49 b7 2e eb .....(...CL...

0010 f1 43 4c 07 c9 ce 00 00 09 00 .CL.....

298 1.774315 7f:12:49:b7:2e:eb -> c3:c5:8d:28:a8:07 802.11 26 Deauthentication, SN=0, FN=0, Flags=.....

0000 c0 00 00 00 c3 c5 8d 28 a8 07 7f 12 49 b7 2e eb .....(...CL...

0010 f1 43 4c 07 c9 ce 00 00 09 00 .CL.....

6.4 Infrastructure Logs

Systems and protocols that translate between layer 2 and layer 3 are key to linking together wireless and wired attacks. If an attack is originating from a wireless network we should first see indicators of attack on the wireless network. Next there should be some event that shows that an IP address is assigned or associated with a wireless client. Finally the suspicious host will begin

originating scans or other attack related activity from the assigned IP address. As with the Kismet logs and raw packets, the original MAC address is highlighted in red and the new identifying source IP address is highlighted in blue.

Nov 11 10:41:22 wlan-server dhcpd: DHCPREQUEST for 172.16.4.144 from 7f:12:49:b7:2e:eb via wlan0

Nov 11 10:41:22 wlan-server dhcpd: DHCPACK on 172.16.4.144 to 7f:12:49:b7:2e:eb via wlan0

6.5 Wired IDS Logs

Nov 11 10:45:33 alpharaptor snort: [1:1390:5] SHELLCODE x86 inc ebx NOOP [Classification: Executable code was detected] [Priority: 1] {UDP} 172.16.4.144:47246 -> 172.16.4.222:30538

Nov 11 10:45:37 alpharaptor snort: [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 172.16.4.144:53763 -> 172.16.4.222:443

Nov 11 10:45:40 alpharaptor snort: [1:1421:11] SNMP AgentX/tcp request [Classification: Attempted Information Leak] [Priority: 2] {TCP} 172.16.4.144:53307 -> 172.16.4.222:705

The wired logs will generally include the traditional source and destination IP addresses and port numbers. If the log source were from a switch then it would also include MAC address. Wireless access points and associated enterprise authentication systems like RADIUS or DHCP servers will also link and correlate specific source MAC addresses.

7. Security Incident and Event Management

7.1 Methods for Identifying Mobile Attackers

At the network layer an IP address is commonly used to identify a host. Wireless networking starts at layer 2 of the TCP/IP Model. For this reason, attacks generally begin prior to obtaining an IP address. A MAC address identifies a wireless client and is the next logical choice for correlating attacks. While a MAC address is not ideal there is one good argument for using this to identify an attacker; while an attacker may change their MAC address arbitrarily,

they must keep the same value in order to carry on any bidirectional communication. A randomly changing MAC address may be used for performing denial of service attacks, but it won't suffice for data exfiltration or as a launching point for further exploitation. Additionally, in most cases the attacker probably will not go to the effort of changing their MAC address. If the MAC address is unaltered then the vendor string may also provide clues about the manufacturer of the card or device.

Within the OSSIM framework, first level alerts are called 'SIEM events'. These are events that match a signature of some kind. Once an event is recorded it can be linked or combined with other incident to generate an alert. SIEM events are combined using correlation rules or directives. Below is a sample directive for OSSIM designed to link wired and wireless events as a single alert.

```
<?xml version="1.0" encoding="UTF-8"?>

<directive id="500001" name="Precursor Wireless Deauth Attack" priority="3">
        <rule type="detector" name="Event from Wireless Sensor"
from="ANY" to="ANY" port_from="ANY" port_to="ANY" reliability="1"
occurrence="1" product="30" plugin_sid="ANY" sensor="dd5b6bf2-3598-c938-
6e70-78f14a5b43bf">
          <rules>
            <rule type="detector" name="DHCP Lease" from="ANY"
to="ANY" port_from="ANY" port_to="ANY" reliability="+3" occurrence="1"
time_out="30" product="6" category="13" subcategory="220"
userdata1="1:userdata3">
              <rules>
                <rule type="detector" name="Event from Wired IDS"
from="2:SRC_IP" to="ANY" port_from="ANY" port_to="ANY"
reliability="+5" occurrence="5" time_out="60" product="13"
plugin_sid="ANY"/>
              </rules>
```

```
        </rule>
      </rules>
    </rule>
  </directive>
```

The above example is a three-tier rule. The first tier looks for any wireless event from our defined sensor. The second tier looks for a DHCP lease event. The final tier looks for any IDS event within 60 seconds and is linked to the tier 2 source IP addresses. The snort alerts do not include a MAC address; however, the DHCP lease events would include both MAC and IP address and link those two values. Another source of MAC address and IP address could be switch logs.

Beyond MAC address there are quite a few research projects focusing on other methods for identifying wireless devices. Two examples are, "Specification-Based Intrusion Detection in WLANs" (Gill 2006) and "Passive Techniques for Detecting Session Hijacking Attacks in IEEE 802.11 Wireless Networks" (Gill 2005). This is similar to fingerprinting research for "Internet" based attackers such as is described in the paper "Attack modeling for information security and survivability." In this paper, the author(s) describe some methods for wireless including detecting the timing and latency characteristics of gateway or router components close to the attacker sources (Moore 2001). For wireless, some of the research is looking at algorithms that combine signal to noise ratio, signal strength, triangulation of signal location, as well as radio characteristics to better identify attack sources (Hall 2005).

The advantage of having a flexible and extensible monitoring framework that is able to collect diverse log sources is that these newer identification mechanisms can be incorporated to improve the overall solution.

8. Conclusion

While there is no perfect solution for combining, normalizing and correlating all log sources that could link the attacks that affect both wired and wireless networks, there are some simple tools available that can be combined to act as the foundation of a robust monitoring solution. Each of the components

discussed here can be expanded and tuned to suit more complex and demanding enterprise environments. Hopefully as newer methods for identifying wireless and wired attackers are discovered these can also be incorporated.

9. References

AlShourbaji, I., & AlAmeer, R. (2013). Wireless Intrusion Detection Systems (WIDS). arXiv preprint arXiv:1302.6274.

Blasco, J,. (2010). WIDSTT.PY: Wireless Attack Testing Tool. Available from http://www.alienvault.com/open-threat-exchange/blog/attacks-wireless-intrusion-detection-systems-testing-tool.

Chuvakin, Schmidt, Phillips, Logging and Log Management, 2013

Deraison, R., (2013). Nessus: Vulnerability Scanner (Version 3.2.4) [software]. Retrieved from http://www.tenable.com

Gill, R. S., Smith, J., Looi, M. H., & Clark, A. J. (2005). Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks.

Gill, R., Smith, J., & Clark, A. (2006, December). Specification-based intrusion detection in WLANs. In Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual (pp. 141-152). IEEE.

Hall, J., Barbeau, M., & Kranakis, E. (2005). Radio frequency fingerprinting for intrusion detection in wireless networks. IEEE Transactions on Defendable and Secure Computing.

Karg, D., Casal, J., (2012). OSSIM: [Open Source Security Incident and Event Management Software [software]. Available from http://www.alienvault.com

Kershaw, M., (2008). Kismet: Network Detector, Packet Sniffer, and Intrusion Detection System for 802.11 Wireless LANs (Version 2008.05.R1) [software]. Available from http://www.kismetwireless.net

Lyon, G., (2013) NMAP: Network Scanning and Vulnerability Detection Tool (Version 6.4) [software]. Available from http://nmap.org

Miller, Harris, Allen et. al, Security Information and Event Management (SIEM) Implementation. 2011

Moore, A. P., Ellison, R. J., & Linger, R. C. (2001). *Attack modeling for information security and survivability* (No. CMU-SEI-2001-TN-001).

CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

OSSIM, Installation Guide, 2010. Retrieved from http://www.alienvault.com/docs/Installation_Guide.pdf

Rapid 7. (2013). Metasploit Community (Version 4.8) Penetration Testing Software [software]. Available from http://www.rapid7.com/products/metasploit/download.jsp

Roesch, M. (2013). Snort: Intrusion Detection Software. [software]. Maryland: Columbia.

SANS Institute. 2011. Courseware: Security 617 Wireless Ethical Hacking, Penetration Testing, and Defenses. Wireless Security Exposed Part 2. version V2011_0711

Wilson, A., (2012). WIDS How To, How to set up WIDS on AlienVault USM V3, Retrieved from https://alienvault.bloomfire.com/posts/525219-wids-howto/public