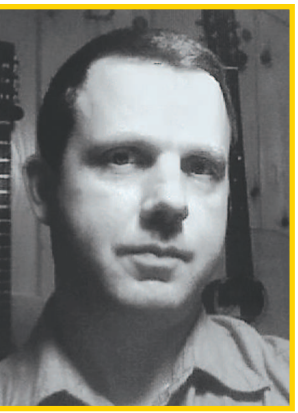

# OSSEC

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

## Prerequisites

Linux host for the OSSEC server/manager
OSSEC agents run on Linux, MacOS, Solaris, HP-UX, AIX and Windows

## Similar Projects

OSSEC is included in OSSIM[1]

This month's *toolsmith* is the first that comes to you as the result of a contest I put forth on my blog challenging you, dear reader, to propose a topic. The contest promised that the reader whose topic I choose for a given month will receive an information security book of my choosing. Doug Burks of Security Onion[2] proposed OSSEC. Congratulations, Doug, I'm long overdue to cover OSSEC HIDS and am pleased to finally be doing so.

OSSEC HIDS, from Third Brigade (a Trend Micro acquisition), is an open source host-based intrusion detection system (HIDS) that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting, and active response. OSSEC runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows. Learn everything you need to know about OSSEC at the website.[3]

I asked Doug to tell me about his experience using OSSEC and he provided some excellent examples.

One of his favorite uses for OSSEC is on a webserver running the LAMP stack. With OSSEC installed and *file integrity checking* and *rootkit detection* enabled, OSSEC will immediately monitor `/var/log`. If an attacker tries to brute force his SSH or FTP daemons, OSSEC alerts Doug. If an attacker attempts HTTP reconnaissance, OSSEC will see the excessive HTTP error codes and alert Doug. If an attacker is able to circumvent defenses and gain access to the server, any file modifications or rootkit installations will be detected by OSSEC and Doug will be alerted. This makes Doug happy, but he's not done yet. He also configures *iptables logging* for OSSEC.[4] If an attacker port-scans the server, OSSEC notes that iptables dropped a large number of packets from a single source IP and will alert. Doug further increases his detective capabilities by installing Snort and configuring it for plain-text logging. OSSEC can monitor the Snort log and alert anytime Snort does (see more on Snort monitoring below). Yet another useful option on Apache webservers is the ModSecurity module that acts as a Web Application Firewall (WAF), includes signatures for many web attacks, and is customizable. OSSEC can monitor and alert on the ModSecurity logs as well. For WordPress defenders (that best be all of you WordPress users ;-)), there's the new WPSyslog2,[5] a WordPress plugin that sends WordPress events to syslog, which in turn is monitored by OSSEC. Every layer of Doug's system architecture is instrumented and all logging is aggregated into OSSEC.

Doug also suggests that OSSEC users consider *Active Response*. If enabled, OSSEC will not only alert but also configure TCP Wrappers and iptables to block traffic from the attacker's IP address. This translates to OSSEC moving from HIDS to HIPS (host intrusion prevention system).

*NOTE: Like any use of intrusion prevention, proceed with caution. False positive detection with Active Response enable can lead to known good traffic being dropped. Yet, properly tuned, OSSEC running in Active Response mode can effectively protect your server from compromise.*

Finally, Doug's also used or suggests using OSSEC as follows:

- User Account Auditing
  - Install OSSEC agent on all Windows Active Directory Domain Controllers
- PCI[6]
- DMZ under strict Change Control
  - File integrity checking
- Splunk as a Web Interface[7]

I think I know why Doug called his namespace Security Onion. The man knows his layers, also best known as defense in depth. Well done, Doug.

## Install and configure OSSEC

There is an entire book[8] regarding OSSEC, and the installation chapter is freely available,[9] so I won't spend a great deal of time on what is already a well-established process.

1 http://www.alienvault.com/products.php?section=OpenSourceSIM.
2 http://securityonion.blogspot.com.
3 http://www.ossec.net/main/about.
4 http://www.ossec.net/wiki/index.php?title=Know_How:Iptables_Config.
5 http://www.ossec.net/wpsyslog2.
6 http://www.ossec.net/ossec-docs/ossec-PCI-Solution.pdf.
7 http://www.ossec.net/main/splunk-ossec-integration.
8 http://www.ossec.net/main/ossec-book.
9 http://www.ossec.net/main/manual/manual-installation.

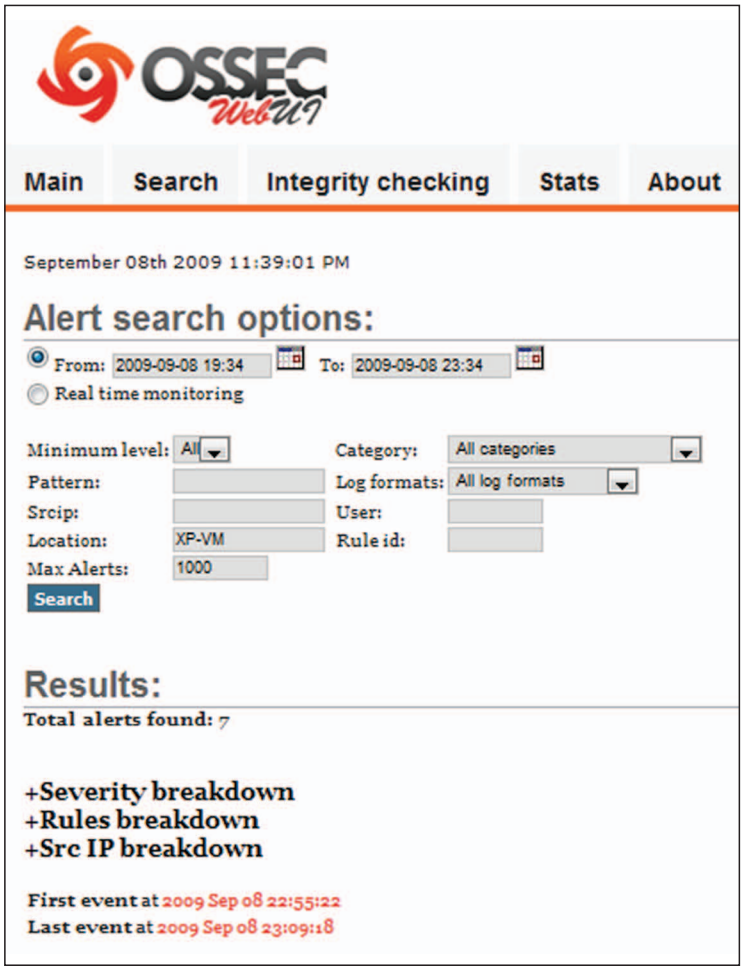


**Figure 1 – OSSEC Web**

On Ubuntu 9.04, setting up the server is as simple as downloading the latest OSSEC (version 2.2 is current as this is written) and executing the following:

1. `tar -zxvf ossec-hids-*.tar.gz`
2. `cd ossec-hids-*`
3. `sudo ./install.sh`

Be sure to allow port 1514 (UDP) if you're utilizing your server firewall so that agents can connect.

Execute `/var/ossec/bin/ossec-control start` to start OSSEC HIDS.

I followed all recommended conventions and installed the OSSEC server on my Ubuntu 9.04 servers. I further installed the OSSEC Windows agent of Windows XP and 2003 virtual machines.

Installing the agent is a point-and-click effort until you need to join the agent to the server. When prompted by the Windows agent, engage a terminal on the server and issue the following:

1. `sudo /var/ossec/bin/manage_agents`
2. Choose *A* to add an agent and provide the name, IP, and ID for the new agent.
3. Return to the menu and choose *E* to extract the key for the new agent, copy the key to a file or your clipboard, and make it available to the Windows host where you're installing the new agent.
4. On said Windows host, provide the OSSEC server IP and the agent key you extracted in step 3, save, and then start the agent.
5. You can confirm that the agent is running in the agent UI on the Windows host, and you can also choose *L* to lists agents on the server, from the manage_agents menu.

I also installed the OSSEC web interface (WI) on the server. As seen in Figure 1, the WI allows you to conveniently review and query events, modified files for all agents, and stats.

You certainly don't need the web UI, as you can configure email alerting to your preferences, and you can also grep or Splunk `/var/ossec/logs/alerts` for events of interest.

In `/var/ossec/etc/ossec.conf` on the server, and from *View => View Config* on the Windows OSSEC Agent Manager, you can tune the configurations to your liking. Decide what rules sets you'd like to make use of, what files and directories should be monitored for file integrity checks (think PCI compliance) as well as those you'd like ignored. You can also tune rootkit checks, log monitoring preferences, including syslog, Snort, and VMWare, as well as the active response option (again, set this carefully with lots of testing).

While I only tested OSSEC HIDS on Linux and Windows, it works quite capably on MacOS, Solaris, HP-UX, and AIX.

## OSSEC HIDS: Defense in depth

### OSSEC and Snort logs

I freaked myself out while writing this (neither uncommon nor difficult) when I fired OSSEC up for the first time on one of my stealth Ubuntu servers and the very first email alert it popped after the initial "ACK, I'm here" was as follows:

```
OSSEC HIDS Notification.
2009 Sep 10 10:55:08

Received From: flintstone01->/var/log/snort/alert
Rule: 20100 fired (level 8) -> "First time this
IDS alert is generated."
Portion of the log(s):

[**] [125:7:1] (ftp_telnet) FTP traffic encrypted
[**][Classification: Preprocessor] [Priority: 3]
92.243.8.139:21 -> none.of.your.business:37868

--END OF NOTIFICATION
```

Nice. Obviously I should have been watching `/var/log/snort`, and more obviously, had not been.

At first glance that alert looks really bad to someone who knows that there is absolutely no reason for an established

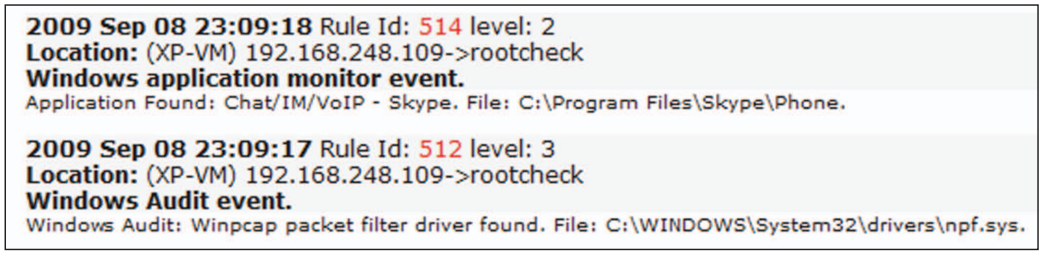


**Figure 2 – OSSEC spots Skype and Wireshark**

connection from the wild to his server, particularly traffic that has been interpreted as encrypted FTP traffic. "Breathe, son, breathe!" Either I've been rooted somehow (oh, the horror) or I'm running something weird and I've forgotten what the heck it…wait a minute, it's coming to me. Doh! I left Tor[10] running. A quick `netstat –ano` finds established connections to various hosts on 80, 9001, and 21, amongst others. Ok, color is returning to already uncommonly pale skin. I execute `sudo /etc/init.d/tor stop` and fire `netstat –ano` again. All established connections now show a time_wait state including the above mentioned 92.243.8.139. Thunk-thunk, thunk-thunk, my heartbeat returns to normal. Slap me for being stupid and careless, dear reader. OSSEC exhibits immediate value by helping keep my adult ADD in order.

## OSSEC and PCI

PCI DSS 11.5 states that organizations must "deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly."

**Note:** For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise."

Now imagine that your organization is a PCI-beholden SaaS provider who manages numerous virtual nodes via VMWare. As an example, might we assume unauthorized changes to DHCP leases to be an optimal candidate for integrity monitoring, specifically the *dhcpd.leases* file? Would the following alert be useful in said endeavor?

```
OSSEC HIDS Notification.
2009 Sep 11 09:32:51

Received From: flintstone01->syscheck
Rule: 550 fired (level 7) -> "Integrity checksum
changed."
Portion of the log(s):

Integrity checksum changed for: '/etc/vmware/
vmnet8/dhcpd/dhcpd.leases'
Size changed from '599' to '1327'
Old md5sum was:'bc3c25d3cdab17f4b3e167d95b4ca988'
New md5sum is:'4ce2129e1c328aae35475096b59ede7c'
Old sha1sum was:'22fcb668c13ed27b133b2b46192637e32f2611b4'
New sha1sum is:'a9abc0dcdff71c8650ac9cc0beebd163f810c6ff'

--END OF NOTIFICATION
```

I think we can assume the above to be rhetorical questions.

## OSSEC and application monitoring and audit events

Maybe you're working for one of those rare few organizations that actually does not let computer users do less than desirable things at work, such as use Skype or sniff network traffic. OSSEC can certainly help enforce those admirable tendencies as seen in Figure 2.

## OSSEC and malware behavioral analysis

I run a Windows XP victim virtual machine to conduct malware analysis. As I'd begun to write this article I was noting the expected events that OSSEC should see, particularly changes to known good directories, files, and registry entries. But what I also spotted, making me further happy, was the following as seen in Figure 3.


**Figure 3 – OSSEC wonders why my AV is disabled**

Spend any time playing with malware and you know that certain sample types will immediately disable any antivirus the victim host may be running. OSSEC alerted on that simple fact as well, lending credence to the fact that you should simply make use of OSSEC HIDS anywhere you can.

## In conclusion

I challenge you to give me one good reason why you can't use OSSEC HIDS somewhere in your environment. Even if organizational policy or standard requires a different HIDS solution, OSSEC will serve you in labs or non-production environments. Daniel Cid, the OSSEC HIDS lead developer and project founder, and his hard working team have created a framework that I believe you can consider indispensible.

Cheers…until next month.

## Acknowledgments

—Doug Burks, Security Onion

—Daniel Cid, OSSEC.net

## 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@holisticinfosec.org.*

10 http://www.torproject.org/torusers.html.en.