BEGINNER'S GUIDE to

Open Source Intrusion Detection Tools

www.alienvault.com

IDS Basics

If you aren't already running network IDS, you should be. There are two types of Network IDS:

Signature Detection & Anomaly Detection

In a signature-based IDS, there are rules or patterns of known malicious traffic that it is looking for. Once a match to a signature is found it generates an alert. These alerts can turn up issues such as malware, scanning activity, attacks against servers and much more.

With anomaly-based IDS, the payload of the traffic is far less important than the activity that generated it. An anomaly-based IDS tool relies on baselines rather than signatures. It will look for unusual activity that deviates from statistical averages of previous activities or activity that has been previously unseen. Perhaps a server is sending out more HTTP activity than usual or a new host has been seen inside your DMZ.

Both are typically deployed in the same manner, though one could make the case you could easily (and people have) create an anomaly-based IDS on externally-collected netflow data or similar traffic information.

Looking for attacks isn't the only use case for IDS, you can also use it to find violations of network policy. IDS will tell you an employee was using Gtalk, uploading to Box, or spending all their time watching Hulu instead of working.

Whether you need to monitor hosts or the networks connecting them to identify the latest threats, there are some great open source intrusion detection (IDS) tools available to you.

Snort

Ah, the venerable piggy that loves packets. I'm sure everyone remembers 1998 as the year a version of Windows came out but it was also the year that Martin Roesch first released Snort. Though then it really wasn't a true IDS, its destiny had been written. Since then it has become the de-facto standard for IDS and eventually IPS (thanks to community effort!). It's important to note that Snort has no real GUI or easy to use administrative console. Lots of other open source tools have been created to help out, notably Snorby and others like Base and Squil. Some of the advantages of Snort:

- Long product life with no signs of going away
- Great community support
- Plenty of administrative front-ends
- Thoroughly proven and tested

You can find Snort inside AlienVault Unified Security Management™ (USM), not just used as a tool but fully integrated from signature updates to packet match display.

Suricata

What's the only reason for not running Snort? If you're using Suricata instead. Though Suricata's architecture is different than Snort, it behaves the same way as Snort and can use the same signatures. What's great about Suricata is what else it's capable of over Snort. Let's run down a few examples:

- **Multi-Threaded -** Snort runs with a single thread meaning it can only use one CPU(core) at a time. Suricata can run many threads so it can take advantage of all the CPU/cores you have available. There has been much contention on whether this is advantageous, Snort says No and a few benchmarks say Yes.
- **Built in Hardware Acceleration -** Did you know you can use graphic cards to inspect network traffic?
- **File Extraction -** Someone downloading malware? You can capture it right from Suricata and study it.
- **LuaJIT -** It's a lot of letters yes, but it's also a scripting engine that can be used with information from the packets inspected by Suricata. This makes complex matching even easier and you can even gain efficiency by combining multiple rules into one script.
- **Logging more than packets -** Suricata can grab and log things like TLS/SSL certs, HTTP requests, DNS requests
- **So much more...**

With so many features and capabilities it's no wonder it's the default network IDS inside AlienVault USM now.

Bro

Bro, or sometimes referred to as Bro-IDS is a bit different than Snort and Suricata. In a way, Bro is both a signature and anomaly-based IDS. Its analysis engine will convert traffic captured into a series of events. An event could be a user logon to FTP, a connection to a website or practically anything. The power of the system is what comes after the event engine and that's the Policy Script Interpreter. This policy engine has it's own language (Bro-Script) and it can do some very powerful and versatile tasks.

If you're an analyst and you've wondered "How can I automate some of my work?" then this is the tool you've been looking for. Want to download files seen on the wire, submit them for malware analysis, notify you if a problem is found then blacklist the source and shutdown the user's computer who downloaded it? Want to track the usage patterns of a user after they've contacted an IP from a reputation database?

If you're not an analyst than this tool will have a challenging learning curve. Since it was developed as a research tool it didn't initially focus on things like GUIs, usability, and ease of installation. While it does many cool things out of the box many of those things aren't immediately actionable and may be difficult to interpret. Summary:

- Complicated to set up
- Can detect patterns of activity other IDS systems can not
- Very extensible architecture
- Starting to gain a larger community following

Kismet

Just as Snort became the standard for network intrusion, Kismet is the baseline for wireless IDS. Wireless IDS deals less with the packet payload but more with strange things happening inside the wireless protocols (mostly 802.11) and functions. WIDS will find unauthorized Access Points (**Rogue AP Detection**), perhaps one created by an employee accidentally (yes, I've seen that) that opens a network up. Perhaps someone has stood up an AP with the same name as your corporate network to perform MITM attacks? Kismet will find all of these. Kismet runs on a variety of platforms, even Android. Besides IDS, Kismet can also be used for more utilitarian things like wireless site surveys or fun activities like WarDriving.

Host IDS

Host-based IDS systems, or HIDS, work by monitoring activity that is occurring internally on a host.

HIDS look for unusual or nefarious activity by examining logs created by the operating system, looking for changes made to key system files, tracking installed software, and sometimes examining the network connections a host makes. The first HIDS systems were rather rudimentary, usually just creating md5 hashes of files on a recurring basis and looking for discrepancies (**File Integrity Monitoring**). Since then HIDS have grown far more complex and perform a variety of useful security functions. Also, if you need to become compliant to one of the many standards (PCI, ISO, etc..) then HIDS is compulsory.

OSSEC

In the realm of full featured Open Source HIDS tools, there is OSSEC and not much else. Go ahead and google away, I'll wait. The great news is OSSEC is very good at what it does and it is rather extensible. OSSEC will run on almost any major operating system and uses a Client/Server based architecture which is very important in a HIDS system. Since a HIDS could be potentially compromised at the same time the OS is, it's very important that security and forensic information leave the host and be stored elsewhere as soon as possible to avoid any kind of tampering or obfuscation that would prevent detection.

OSSEC's architecture design incorporates this strategy by delivering alerts and logs to a centralized server where analysis and notification can occur even if the host system is taken offline or compromised. Another advantage of this architecture is the ability to centrally manage agents from a single server. Since deployments can range from one to thousands of installations, the ability to make changes en masse via a central server is critical for an administrator's sanity.

When discussing OSSEC and other HIDS, there is often trepidation in installing an agent or software on to critical servers. It should be noted that the installation of OSSEC is extremely light, the installer is under 1MB, and that the majority of analysis actually occurs on the server which means very little CPU is consumed by OSSEC on the host. OSSEC also has the ability to send OS logs to the server for analysis and storage, which is particularly helpful on Windows machines that have no native and cross-platform logging mechanisms. Summary:

- Agents for almost every OS
- Compiled Agent for Windows
- Lots of functionality other than just FIM
- Rigid but simple installation process

AlienVault USM features a complete integration of OSSEC. Whether you need to install agents on servers, modify policies, or even instigate OSSEC's active response features, it can all be done within USM. Logs from OSSEC clients are also pre-integrated into USM's SIEM and Correlation engines.

Samhain Labs

In comparison to OSSEC, Samhain is the best competition. But it's very much the case of **same but different** when making the comparison. Samhain has the same client/server architecture but it's not beholden to it like OSSEC is. The agent itself has a variety of output methods, one being a central server but others like Syslog, Email, and RDBMS which are greatly appreciated.

Another important difference is where the analysis occurs. Unlike OSSEC the processing occurs on the client itself. While this does give an advantage in terms of processing speed it could have potential impact on your servers. However, it does put those CPU cycles to good use as it has a much stronger emphasis on FIM.

Summary:

- Harder to install
- Windows clients require Cygwin
- Great FIM functionality
- More flexible client

Open DLP

OpenDLP isn't really a HIDS system but it's functionality makes it worth a mention here. This tool has one goal and that's DLP or Data Loss Prevention. It will scan data while it's "at-rest" looking for pieces of data like credit cards or SSNs and can be extended with regular expressions to find data that is sensitive to your organization. OpenDLP will look for this data on file systems or even inside databases on both Windows and Linux. It can also perform these scans via an installable agent or without any software installation.

- Not a FIM or HIDS technically, but interesting
- Very Windows friendly
- Looks for DLP only

Rounding out your toolset

FIM ONLY

There are quite a few FIM tools that get categorized with HIDS. Some are actively developed and others haven't been updated in years. Since these tools only perform one function I won't elaborate much more. A few of these are AIDE, OS Tripwire and AFick.

SECURITY ONION

If you're interested in trying out some or all of the open source IDS tools from this post you could save some time and check out Security Onion. It's a distribution of Ubuntu with everything pre-installed.

AlienVault USM
BRINGS IT ALL TOGETHER

SECURITY INTELLIGENCE
SIEM Event Correlation
Incident Response

ASSET DISCOVERY
Active Network Scanning
Passive Network Scanning
Asset Inventory
Host-based Software Inventory

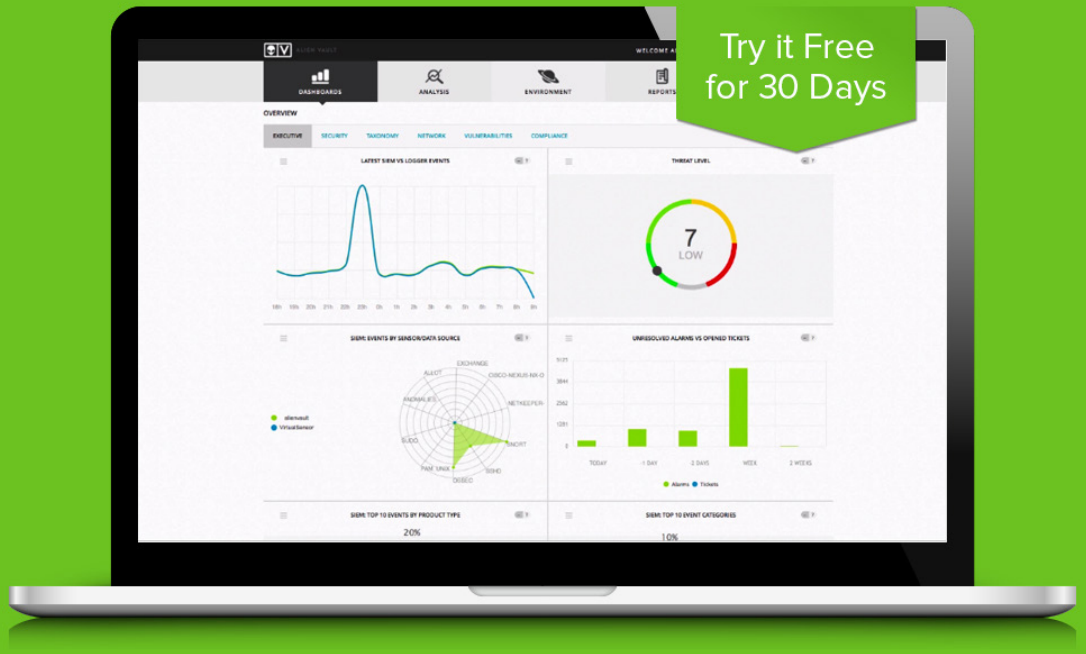
powered by
AV Labs Threat Intelligence

BEHAVIORAL MONITORING
Log Collection
Netflow Analysis
Service Availability Monitoring

THREAT DETECTION
Network, Host & Wireless IDS
File Integrity Monitoring

VULNERABILITY ASSESSMENT
Continuous Vulnerability Monitoring
Authenticated / Unauthenticated Active Scanning

Next Steps: Play, share, enjoy!



- Learn more about the IDS capabilities of AlienVault USM
- Watch our 3-minute overview video
- Play in our product sandbox
- Start detecting threats today with a free 30-day trial
- Join the Open Threat Exchange

www.alienvault.com

About the Author

Joe Schreiber, Director of Solutions Architecture at AlienVault

Joe has been working in hands-on roles in IT security since the days of dial-up. In fact, he has deployed and managed virtually every commercial and open source IDS tool out there. His ardor for packets landed him a job analyzing network traffic for Fortune 50 companies with AT&T Managed Security Services. In this role, Joe built one of the world's largest SIEM systems, bringing thousands of devices under real-time security management and monitoring more than 2 petabytes of network traffic daily.