Open Source Network Security Tools for Beginners

www.alienvault.com

With so many open source tools available to help with network security, it can be tricky to figure out where to start, especially if you are an IT generalist who has been tasked with security. We all have to start somewhere.

The question is, where?

The sheer number of open source network security tools available can make it difficult to choose a place to start. This is complicated by the fact that most of the open source network security tools available have a very steep learning curve, and that many of these tools can be hazardous to run on a production network. Let’s take a look at a few of the tools available, which will not only provide some answers, but also help you learn more about the topic.

START SMALL

We have all heard the advice to “start small” when trying to learn something new. Well, it’s hard to get smaller than the packets themselves. Packet analysis is not only a good place to start on security, but it is also a good way to brush up on networking in general. This is a core skill set for any security professional.

While there are a number of tools out there for packet analysis, none of them compare to Wireshark. This utility is cross-platform, stable, and comes with a CLI peer application (Tshark) that uses all of the same filters and can be used to analyze from hosts without a UI. Wireshark also has a tremendous wealth of resources including Documentation, References, and even Sample Captures to download and review. This utility is, in my opinion, the king of its realm.

Alternatives TCPdump, nGREP, Cloudshark, LANGuardian

DISCOVER THE NETWORK AROUND YOU

I am, and always will be, a big fan of the phrase “you cannot manage what you cannot measure.” If you want to protect your network, it is critical to start by learning what is actually on it. A good network discovery tool should let you know not only what devices are on your network, but also what OS is running, what ports are listening, and as much detail on what services are listening on those ports as possible.

There are a number of tools available, but my preference is to use another solid contender in the market, Nmap. Nmap is a cross platform command line utility for network discovery and enumeration. This tool has an amazing amount of depth, with so many options available that they have literally written entire books on the switches available for this tool. The Nmap team also blazed the trail on enumeration, with built in flexibility for the type, depth, speed, and aggressiveness of scans.

Like Tshark, Nmap also has a partner cross-platform GUI, Zenmap, which provides a simpler to use UI, but also displays the filters used in the CLI as a learning aid. Documentation will also not be an issue with this utility as Nmap has a VERY thorough Documentation Section on their site.

Alternatives Skipfish, Ipscan, Umit (Umit used Nmap for its backend)

CATCHING THE SCENT

Although most often considered a reactive tool, the network IDS is still a valuable tool for preventing issues, as it can help you discover a variety of issues that other network security tools just do not see. There are a number of good open source tools available here, but these are actually one of the more difficult classes of tools to learn how to use effectively. The reason for this is that network IDS tools tend to walk the line on false positives, and the field of play is always changing. It's like playing baseball on a field where the bases are on tracks that slide along.

Bro IDS, Snort, and (my preference) Suricata are three capable Network IDS tools for analyzing network traffic to detect target activity. These tools are better run from a server or workstation, than on a mobile unit as they require configuring port mirroring on the network infrastructure.

A good choice for learning these is to install either a standalone server, or to install a SIEM, which includes a Network IDS such as OSSIM or Security Onion. You can then use the same server when you move on to learning about correlation. You can also install these as modules in some open source firewalls, such as pfSense. In this particular case, I will break from my preference and recommend Snort, as it has a much more robust selection of documentation available.

NO OPEN DOOR POLICY

While a good Patch Management Policy will alleviate the bulk of vulnerability issues on your network, it will never be able to close all holes, and any door left open is much easier to walk through. For this reason, vulnerability testing is an absolute necessity for any network. This brings up an important set of points on vulnerability scanners.

1 Version Analysis

While necessary, version analysis is not enough.
Some vulnerability scanners check the advertised version of a service or system and compare it to a list of known versions. While this IS important, it does not account for systems configured not to report version, or to deliberately misreport this information. Because of this fact, we need to scan for other factors.

2 Behavioral Analysis

Behavioral analysis should also be a component of any scanner. Keep in mind, however, that BA does not account for features that are not currently enabled, or for conditional faults (my favorite conditional fault is a previous IIS defect that is only exploitable if there is a folder with a 15 character or longer name starting with an a in the root of the public folder).

3 False positives may not be fun, but they are MUCH better than any false negative.

Vulnerability scanners work on the edge, testing for vulnerabilities that cannot be confirmed without causing damage to the system. As this is a rather large gray area to work in, even the best vulnerability scanner can be expected to generate some false positives.
This is, unfortunately, part of the game here.

4 A false positive could also be a conditionally false positive.

Never assume that a result is a false positive because it was last time. A number of vulnerabilities are highly conditional. A configuration change, an update to the Operating System, another application on the system, or a simple file or folder saved in the wrong place or with the wrong name can create a vulnerability that needs attention.

A very popular vulnerability scanning tool is OpenVAS, which is a fork of NESSUS that maintains a pretty impressive scanner. Documentation on the project is more than a little behind, but the theory of operation is documented very well with the now closed source NESSUS tool.

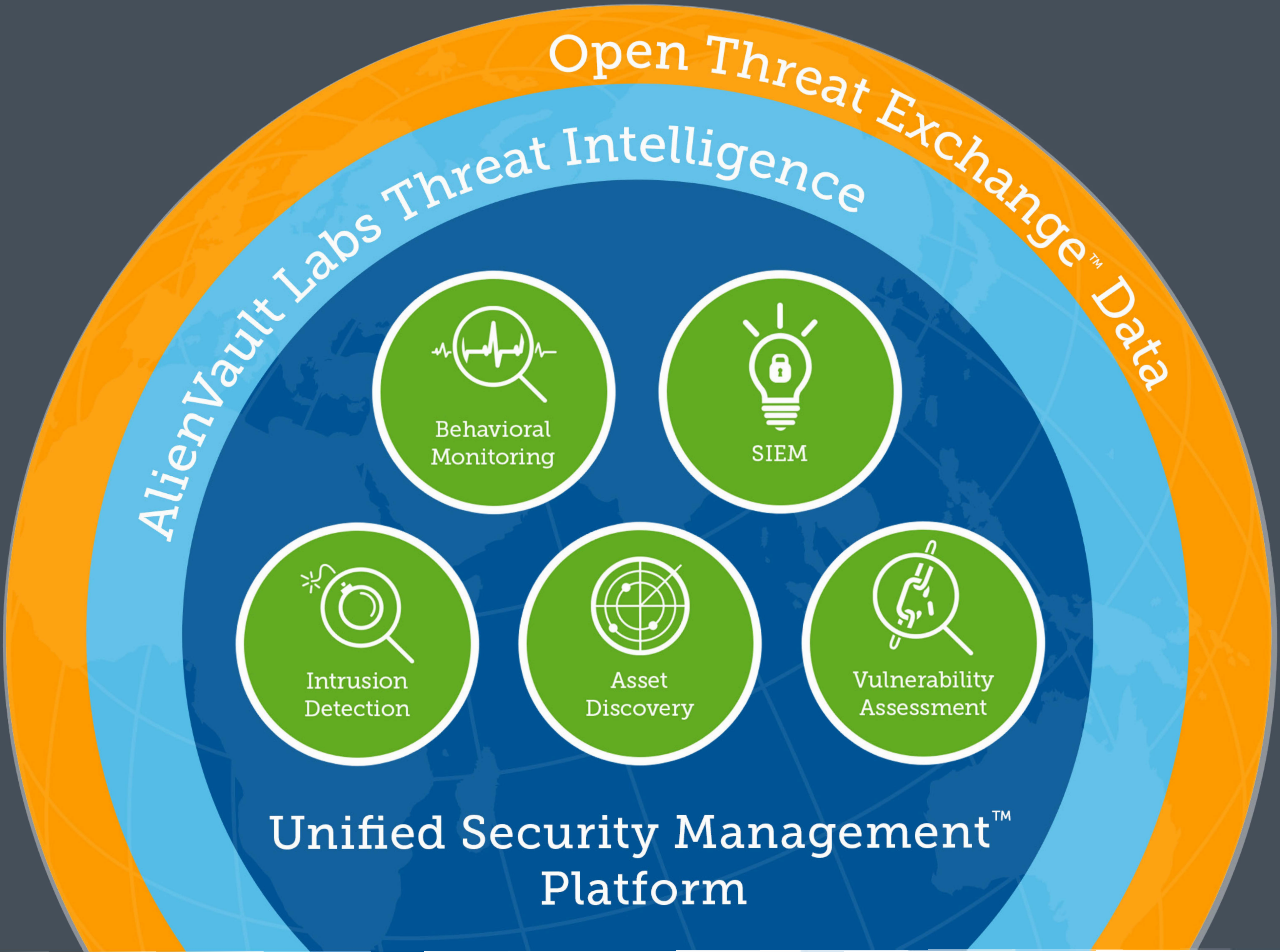
Like the IDS solutions described above, these tools are often best installed as part of a static server - it is difficult to configure, is VERY resource intensive, and tends to be very slow to scan. You could consider installing a SIEM that includes one or more of these tools. Conveniently, AlienVault® Unified Security Management® (USM) provides such a capability, with integrated Network IDS, Vulnerability Scanning and Management and Network Asset Discovery, with Host IDS as well, giving a very clear picture of what's going on in your network.

TAKING THE GAME TO THEM

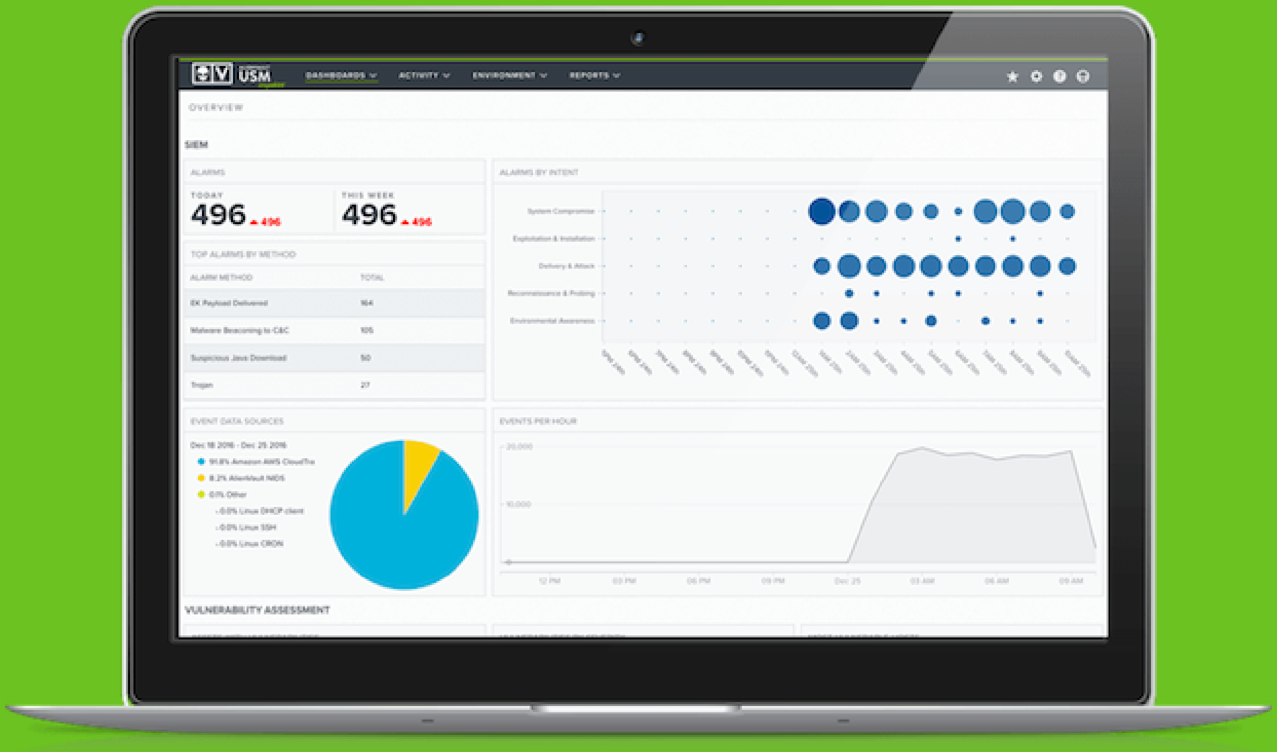
The next step after the tools above is to download and look at a penetration testing distribution. Pentesting is a way of pro-actively taking on security, as the best way to know if something can be exploited is to exploit it. Assuming you have WRITTEN permission to perform these tests, this allows you to probe the network carefully, using the same techniques that an infiltrator would use, and is the best method for discovering how security is practiced, and how it is compromised.

There are several pentesting distributions on the market (Pentoo, NodeZero, Kali, and BackBox are good examples) loaded with tools and utilities. Unfortunately, these offer so many tools, they don't help answer the question of where to start. In this particular case, I recommend downloading and trying each of them to find which you are most comfortable with.

Hopefully, this will get you started in the right direction as you explore open source network security tools. Once you start rolling, you will be able to start adding new tools to your toolset pretty regularly, and move right out of that "beginners" category.


Open Threat Exchange™ Data
AlienVault Labs Threat Intelligence
Behavioral Monitoring
SIEM
Intrusion Detection
Asset Discovery
Vulnerability Assessment
Unified Security Management™ Platform

Next Steps: Play, share, enjoy!



TOP ALARMS BY METHOD

ALARM METHOD	TOTAL
EK Payload Delivered	164
Malware Beaconing to C&C	105
Suspicious Java Download	50
Trojan	27

- Learn more about threat management with AlienVault USM
- Take a test drive of AlienVault USM
- Join the Open Threat Exchange® (OTX™)

www.alienvault.com

About the Author: **Kenneth Coe**

With over 20 years of practice in the field, Kenneth Coe's background includes experience in a wide cross-section of environments and industry technologies with focuses varying from console and terminal based mini-computer environments, through single PCs and small workgroups, to large corporate and government networks. Kenneth is currenlty a support engineer, forum moderator, and blog author at AlienVault.

ABOUT ALIENVAULT

AlienVault Unified Security Management (USM) and Open Threat Exchange (OTX) combines 5 key security capabilities – asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring and SIEM - with real-time threat intelligence from the Open Threat Exchange (OTX) and AlienVault Labs security research team to help customers identify threats.

AlienVault OTX, the world's first truly open threat intelligence community, enables collaborative defense with actionable, community-powered threat data to provide global insight into attack trends and bad actors. OTX pulses provide users with a summary of the threat, a view into the software targeted, and the related indicators of compromise (IoC) that they can use to detect the threats.

OTX pulses are integrated with USM so that threat detection capabilities stay up to date with the latest threats reported by the community, and vetted by the AlienVault Labs team.