1. Security onion
2. OSSEC
3. OpenWips-ng
4. Suricata
5. Bro IDS

1.Security Onion:

Security Onion is an Ubuntu-based Linux distribution for network monitoring and intrusion detection.

The image can be distributed as sensors within the network to monitor multiple VLANs and subnets, and works well in VMware and virtual environments.

This configuration can be used as an IDS only. It isn’t currently supported to be run as an IPS.

There is the option to run this both as a network and host intrusion-detection deployment, and to utilize services such as Squil, Bro IDS and OSSEC to perform the IDS functions of the service.

As great as Security Onion is, however, it still needs more assistance with development, which will most likely happen in time.

2.OSSEC:

OSSEC is an open source host intrusion-detection system (HIDS) that does more than detect intrusions.

Like most open source IDS offerings, there are multiple additional modules that can be used with the core functionality of IDS.

In addition to network intrusion-detection, the OSSEC client has the ability to perform file integrity monitoring and root kit detection with real-time alerts, all of which are centrally managed with the ability to create different policies, depending on a company’s needs.

The OSSEC client runs locally on most operating systems, including Linux versions, Mac OSX and Windows.

It also offers commercial support via Trend Micro’s Global Support Team. This is a very mature offering.

3.OpenWIPS-NG:

OpenWIPS-NG is a free wireless IDS/IPS that relies on a server, sensors and interfaces.

It runs on commodity hardware. Created by the author of Aircrack-NG, this system uses many of the functions and services already built into Aircrack-NG for scanning, detection and intrusion prevention.

OpenWIPS-NG is modular and allows an administrator to download plug-ins for additional features.

The documentation isn’t as detailed as some systems’, but it allows for companies to perform WIPS on a tight budget.

4.Suricata:

Out of all the IDS/IPS systems that are currently available, Suricata competes most directly with Snort.

This system has an architecture that is similar to Snort’s, relies on signatures like Snort.

If Snort isn’t an option in your organization, this is the closest free tool available to run on an enterprise network.

5.Bro IDS:

Bro IDS is similar to Security Onion in that it uses more than IDS rules to determine where attacks are coming from.

Bro IDS uses a combination of tools.

At one point it used Snort-based signatures converted into Bro signatures.

This is no longer the case, and it is now possible to write custom signatures for the Bro IDS.

This system is highly documented and has been around for over 15 years.

Related posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security

5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intoduction to intrusion
9. Categories of security assessments
10. Intrusion terminology
11. Cryptography attacks
12. Cryptography
13. SSH
14. MD5
15. Message digest functions
16. Digital signature
17. Authentication Functions
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer