Useful OSS Security Tools

1 – Alienvault – Open Source Security Information Management system – *good review in the latest (March 2010) Linux journal*

From the web site: The OSSIM platform consists of a Management Server, and Sensor or “Probe”. A professional version that includes SEM functionality is also available (please see below). The solution may be implemented as a single monolithic appliance or a set of appliances in which probes are separated from the management server, and distributed throughout the enterprise.

Probes capture network and system information in real time, and send it to the central Management Server where the data is analyzed to assess immediate threats and risk, filter out false positives, and locate false negatives that other security devices and software on the network cannot detect.

Probes not only capture data, but can be tasked as sophisticated attack detection components. They come with several attack detection systems, audit systems, and context learning systems (network profiles, inventory, availability), all of which are seamlessly integrated. When deployed in this fashion probes provide a very quick and safe way of continuously and transparently monitoring local and remote networks, providing provide full visibility of all security related aspects of the enterprise.

The information from the organization’s security systems, such as the firewall, antivirus, IPS, HIDS, etc, are all collected through these probes, and then analyzed through sophisticated intelligence technology. This technology correlates data from many sources to detect blended threats otherwise undetectable by individual systems; prioritize these threats; and make automated decisions with regard to the risk implied in each one.

2 -DEFT Linux – live Linux Distro for Forensics / Network Security / Analysis

DEFT Linux v5 is based on the new Xubuntu Kernel 2.6.31 (Linux side) and the DEFT Extra 2.0 (Computer Forensic GUI) with the best freeware Windows Computer Forensic tools ; it isn’t a customization of Xubuntu like the old version, it is a new concept of Computer Forensic live system that use LXDE as desktop environment and thunar file manager, mount manager as tool for device management, dhash2, guymager, dcfldd, ddrescue and linen as forensic imager tools, sleuthkit 3.01 andvautopsy 2.21 as landmark for the disk forensic, nessus 4 as security scanner and much more like:

an advanced file and directory researcher
foremost, scalpel and photorec carving tools
a complete support for the most used file systems
a complete support for logical volume manager

a complate support for afflib and ewflib support
a very powerful tools for network forensic as Xplico, wireshark,
kismet, ettercap and nmap
a very powerful tool for identify file type from their binary
signatures (TrID)
the last version of ophcrack, the password cracker based on rainbow
tables and john the ripper password cracker
chkrootkit, rkhunter and exploit scanner
clam 4.15 virus scanner
steganography detection software as outgess
tool for screenshot as take screen shot and video screen capture as
record my desktop
deft-mount script for mount device in read only

Can be booted from a thumbdrive or CD.

3 – Eraser for Windows Eraser is an advanced security tool for Windows which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns. Works with Windows 98, ME, NT, 2000, XP, Vista, Windows Server 2003 and Server 2008.

Sort of like a Windows-native Darik's Boot And Nuke

Taken from email to UC-CSC list by UCI colleague Harry Mangalam

---

Revision #1
Created Mon, Feb 15, 2010 7:04 AM by Franks, Mike
Updated Mon, Feb 15, 2010 7:05 AM by Franks, Mike