# Open Source Cybersecurity Catalog

**Homeland Open Security Technology (HOST) Project
Department of Homeland Security – Science and Technology Directorate**

Homeland Open Security Technology (HOST) is a project within the Department of Homeland Security, Science and Technology Directorate (DHS S&T). HOST's focus is on open source security software. Its mission is:

- identifying new, emerging and undervalued open source solutions to cyber security challenges and sharing that information broadly
- making strategic investments in projects with high-impact potential
- encouraging innovation by enabling cross-industry collaboration

To enable users to easily find cybersecurity related open source software, the HOST program has compiled a catalog. This catalog is meant to be a starting point for evaluating different open source solutions. Due to the wide range of systems and requirements, some of these solutions maybe more appropriate than others. The catalog is simply meant to be a starting point and it is still important to examine whether a solution is appropriate before deploying it. This catalog will be made available through a HOST website, along with an automated method for open source project owners to update information about their software.

The list of software in the catalog is constantly being updated and improved. If you have suggestions for additional software to include, please send them to: host@hq.dhs.gov

| CATEGORY | APPLICATION(S) |
|---|---|
| **Administration** | CFengine, Expect, Process Hacker, Webmin |
| **Anti-spyware** | Nixory |
| **Antivirus** | ClamAV, ClamWin, Moon Secure Antivirus, Simple Machine Protect |
| **Application Languages & Development Environments** | BASH, Clang, Coccinelle, Cygwin, DDD, Eclipse, Emacs, GCC, GDB, Gedit, Java, phpHtmlLib, Python, Qlue, Ruby, Vi, VIM |
| **Browser Add On** | Password Maker, Web of Trust |
| **Business Continuity** | AMANDA, Areca Backup, Partimage |
| **Cloud Computing** | ABIQUO, Cloudstack, Eucalyptus, Juju, Nimbula, Open Nebula, OpenStack |
| **Configuration Management** | CFengine, Puppet, Salt |
| **Content Management** | Chef, Drupal, Joomla, Juju, Wordpress |
| **Data Backup & Archival** | Bacula, Open Nebula, PeaZip, Unison |
| **Database** | MariaDB, MySQL, NetDB, Percona, PostgreSQL, SQLite |
| **Data Removal** | BleachBit, Darik's Boot and Nuke, Eraser, Wipe |
| **Directory** | OpenLDAP |
| **Disk** | BleachBit, DBAN, Gparted, Midnight Commander, Parted, Partimage |
| **Email** | amavisd-new, ASSP, JAMES Mail, Mozilla Thunderbird, Postfix, Spam Assassin, SquirrelMail, VPOP Email, Zarafa, Zimbra |
| **Email Protection & Anti-Spam** | amavisd-new, ASSP, Postgrey, Spam Assassin |
| **Email Services** | JAMES Mail, Postfix, SquirrelMail, Zimbra |
| **Encryption** | AxCrypt, Crypt, Cryptacular, GNU Privacy Guard, John the Ripper, Mac GNU Privacy Guard, NeoCrypt, Network Security Services (NSS), OpenSSL, TrueCrypt |
| **Enterprise Applications** | Open Atrium, Open Source Corporate Management Information Systems (OSCMIS), WorldVistA |
| **File Transfer** | CyberDuck, FileZilla, Fugu, Samba, vsftpd, WinSCP |
| **Filtering** | DansGuardian, IP Tables, Java EE PDF uXSS Filter, Web Scarab |
| **Firewall** | Devil Linux, Endian Firewall Community, ferm, Firestarter, Firewall Builder, IP Cop, m0n0wall, ModSecurity, NetCop UTM, Open WAF, pfSense, Sentry Firewall, Shorewall, Smoothwall, Turtle Firewall, Untangle, Vuurmuur, Vyatta, Zentyal |
| **Forensics** | BackTrack, LibHTP, Maltego, Mobius Forensics Toolkit, mod_sslhaf, ODESSA, tcpdump, tcpindex, The Sleuth Kit/Autopsy Browser, WinDump, WinPcap, Wireshark |
| **Geographic Information Systems (GIS)** | Falcon View, Open Streetmap, Opticks, PGGIS |
| **Host Based IPS (HIPS)** | AFICK (Another File Integrity Checker), Open Source Tripwire, OSSEC |
| **ID Authentication Methods** | WiKID |
| **Information Technology Infrastructure** | Dradis, OpenCPI |
| **Intrusion Detection & Monitoring** | ackack, Kismet, Munin, Open Source Tripwire, OpenVAS, Process Hacker, Suricata, Thicknet, Zabbix |

| CATEGORY | APPLICATION(S) |
|---|---|
| **Intrusion Detection & Prevention Systems (IDS/IPS)** | Fail2Ban, IronBee, OSSEC, QuIDScor, Snort, Suricata |
| **Monitoring Systems** | Cacti, ICINGA, Nagios, NetDB, OpenNMS, PandoraFMS, Zabbix, Zenoss |
| **Network** | ackack, AFTR, BIND, BIND 10, Bird, BSD Router, ISC DHCP, Munin, Netcat, NetDB, Nmap, Quagga, Samba, Squid |
| **Network Communications Protection** | OpenSSH, OpenSSL, Squid |
| **Operating System (OS)** | Android, Arch Linux, BackTrack, CentOS, ClearOS, Cygwin, Debian Linux, Devil Linux, Endian Firewall Community, Fedora, FreeBSD, Gentoo, IP Cop, Knoppix, Kubuntu, Lightweight Portable Security (DoD Linux Distro), m0n0wall, Mandriva Linux, NetBSD, NetCop UTM, OpenBSD, openSUSE, Openwall GNU/Linux (OWL), Red Hat Enterprise Linux, Samuri WTF, Sentry Firewall, Slackware, Smoothwall, SUSE Enterprise, Ubuntu, Untangle, Zentyal |
| **OS Hardening** | AppArmor, Bastille Unix, Gentoo Hardened Profile, SE Linux |
| **Password Management** | KeePass Password Safe, KeePassX, Passkool, Password Maker, Password Safe |
| **Penetration Testing & Vulnerability Assessment** | Airoscript-NG, Angry IP Scanner, Auto Scan, BackTrack, batchyDNS, Cacti, Deblaze, Deface, Graudit, inSSIDer, JBoss Autopwn Script, JBroFuzz, JSP Tester, KisMAC, Kismet, Lynis, Metasploit, Nmap, Ophcrack, Peach Fuzzing Platform, QuIDScor, SQL Map, tcpindex, Vega, W3AF, Wireshark |
| **Problem Management** | BugZilla, Request Tracker |
| **Program Analysis** | AntiSamy, Apparat, Avalanche, BLAST: Berkeley Lazy Abstraction Software Verification Tool, Blind Elephant, Checkstyle, ClamWin, CppCheck, CQUAL, CSRF Guard, Dmalloc, DynInst, FindBugs, Flawfinder, Frama-C, Gendarme, JavaSnoop, Jchord, JSP Tester, LibHTP, Moon Secure Antivirus, Moose, Orizon, Pixy, PMD Copy/Paste Detector, ROSE, RTL-Check, Scrubbr, Simple Machine Protect, Smatch, Sonar, Soot, Sparse, Splint, Squale, Stanse, StyleCop, Valgrind, Yasca |
| **Remote Access Methods Clients** | NoMachine, OpenSSH, OpenSSL, PuTTY, PuTTY CAC, TightVNC |
| **Revision Control** | CVS, Fossil, git, Mercurial, Subversion |
| **Security Planning Tools** | Metasploit, spt (Simple Phishing Toolkit), WebGoat |
| **Storage Tools** | DRDB, OCFS 2, Openfiler, Orange FS, Sheepdog, Swift |
| **Virtualization** | Cygwin, KeepAlived, KVM, OpenStack Compute, OVM, Packetyzer, VirtualBox, Xen |
| **Visualization** | ParaView |
| **VPN** | Cacti, OpenVPN |
| **Vulnerability Patch Management** | Lynis, Nikto2, OpenVAS, Rogue Scanner |
| **Web Accessibility** | Chromium, Konqueror, Mozilla Firefox |
| **Web Server Software** | Apache, Apache Tomcat, Drupal, Enterprise Security API, Jboss Autopwn Script, JBoss Enterprise Application Platform, Lucene, mod_sslhaf, NGINX, Nikto2, Open Atrium, Plone, WebFSD, Zimbra, Zope |
| **Web Services** | AW Stats, Classic ASP Security Image Generator (CAPTCHA), Django, Joomla, MediaWiki, PIWIK, Plone |