MALDIVES OPEN SOURCE SOCIETY

YOUR MONTHLY FLOSS MAGAZINE | APRIL 2010

DOWNLOAD FREE FROM MOSS.ORG.MV

SECURING UBUNTU

YUSUF ABDULLA SHUNAN

MANAGE YOUR PHOTOS LIKE A PRO

MOHAMED MALIK

KDE EDUCATIONAL APPS: PERFECT SOLUTION FOR SCHOOLS

MOHAMED MALIK

ENABLING PROJECTS

INASH ZUBAIR

CAN YOUR SYSTEM BE A BOT-NET?

YUSUF ABDULLA SHUNAN

WE MAKE FREE MAGAZINES LOOK GOOD!

MOSS Magazine is not only about the Free Software movement, it is also about finding real world solutions to simple and basic needs. Of course all with Free Libre Open Source Software (FLOSS).

With this edition of MOSS: Your Monthly FLOSS Magazine, we wish to redesign and give a face lift to this magazine: we make free magazines LOOK GOOD!

Real world solutions require multi-discipline that combines a range of different competencies, including those brought by brilliant coders, designers and all kinds of computer geeks who's imagination and intellect has made FLOSS a beautiful thing.

With the development of free knowledge sharing societies, the software that we use are not only created, but they form a bond that glue us together as humans.

The need for Software will remain for a long time to come; in this age of information societies never rest with what they have today. We always want more, FLOSS promises a constant supply of innovations in a shared development model today and tomorrow.

MOSS: Your Monthly FLOSS Magazine is freely available at moss.org.mv. For any questions or comments about MOSS magazine, we can be contacted at **magazine@moss.org.mv**

contents

04. SECURING UBUNTU

13. ﷺ ﷺ ﷺ ﷺ ﷺ ﷺ ﷺ ﷺ

14. DIGIKAM

16. CAN YOUR SYSTEM BE A BOT-NET?

17. KDE EDUCATIONAL APPLICATIONS

20. ENABLING PROJECTS

23. HOW TO ADD DHIVEHI FONTS ON UBUNTU

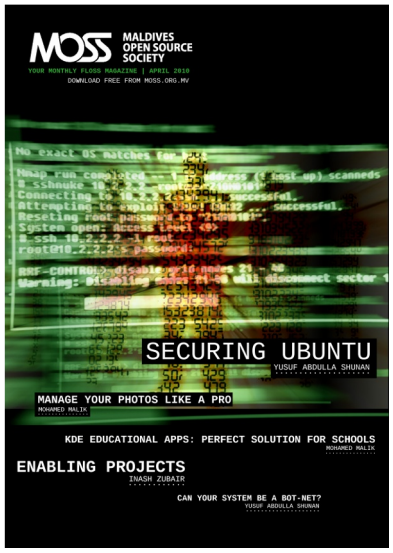
contact us

Maldives Open Source Society Website
http://moss.org.mv

Sending Your Voice
magazine@moss.org.mv

Maldives Linux User Group/MOSS Mailing List
http://groups.google.com/group/mlugmv

Launch Pad Dhivehi Translators Mailing List
http://groups.google.com/group/divtranslators



COVER April 2010, ISSUE #04
designer: Yusuf Abdulla SHUNAN

Maldives Open Source Society

STEERING COMMITTEE

President
INASH Zubair

Vice President
SOFWATHULLA Mohamed

Secretary
Mohamed VISHAH

Public Relations
Ibrahim SOBAH

Program Coordinator
Yusuf Abdulla SHUNAN

Treasurer
HUSSAIN Sharaah

Magazine Editors
SIMON Shareef
Mohamed MALIK
Ahmed SHUJAAU Mohamed
IHSAN Sadiq
SOUL

THE READERS' VOICE

Readers' opinions regarding our magazine and/or previous articles.

MOSS is all about Software Freedom. If you think you could be part of MOSS or you know someone who could, please let us know, we want our magazine to be interactive. We want to progress with you. The common use of free software is not as far off as you think, so let's open our minds to the world and the future. Let's make it happen!

If you have any good ideas or constructive opinions regarding MOSS magazine's contents, this is the place to express yourself.

Please email use at magazine@moss.org.mv

SECURING UBUNTU

The following article is about computer security and hacking, under the right of free and independent expression, the author is free to write and you are free to continue reading or to stop there. Therefore, if you feel offended by the themes treated and/or the way information is presented, immediately stop reading. Continuing on reading, you take any kind of responsibility for the use you make of the information in this MOSS Magazine article.

Yusuf Abdulla SHUNAN > shunan@gmail.com

This article is about securing your Ubuntu box, the topic is vast and it would be impossible to cover all topics in step by step details. So take this article more of like pointers for you to consider in securing your box. Linux is known to be made secure but whether it is Windows or Linux no computer can ever be 100% safe, especially when connected to the Internet. In another sense the purpose of connecting to a network is about sharing information with one another, so logically access to a computer is an intended outcome. However as humans, we at times want/need to limit the access others have to the information on our computers. In reality once you are connected to a network it is rather impossible for you to stop a skilled frivolous cracker. At the same time once you are connected to the Internet you are at the mercy of Viruses, Worms, Trojans, Spyware, Rootkits, Crackers, Phishing, Pharming and Social Engineering. When you think of it, it is rather easy to get afraid and paranoid, but there is a better way to handle that, be eggheaded. As there are ways in which you can make it harder or ways to know when such things are in action.

> Due to the open nature of FLOSS it is rather easier and you can reliably secure your Linux box.

Due to the open nature of FLOSS it is rather easier and you can reliably secure your Linux box. In fact even in Linux Kernel there are many low-level and networking protective services, which can be enabled and disabled at will. I will specifically take Ubuntu as the Linux box here, but most of the ideas will work well in other distributions too.

Before jumping into the how-to's let me clarify few of the terms used in the world of security. In the good old days, the term **hacker** is a person who have enough knowledge to use information technology in creative and unique ways, mostly to learn and see weaknesses in a network. However, today a **hacker** is used to refer to both forms of security experts to abusers, commonly referred to as white-hat and black-hat **hackers** respectively. The proper term to use on someone who exploit a network for abuse is cracker. So in this article I will stick to the old meanings of these terms.

Coming back to the topic, types of attacks may be categorized by a hacker into many different and creative ways, however to simplify things let us break it down to two. One the local attacks and the other foreign attacks. Local attacks are when someone on the same network try to attack your computer. Most probably someone who want to harm you or spy on you, who is living side by side. The foreign attacks are from those who are outside your network, almost always, via the Internet.

We have a need to prevent both type of attacks, but the foreign attacks, given the shear number of people and possibilities are rather more demanding and dangerous. Though this is the case, it would be near insanity to think of this as people are waiting to get into your network as soon as you connect to the Internet. In most cases a cracker will need to know a good amount of knowledge and information to break into any network. In the world of Microsoft Windows, which is more forgiving when it comes to Viruses, Trojans and Worms, are a result of automated scripts that make use of well known vulnerabilities that only very few knows that exist, a result of very few talented crackers attacking many. The issue is further escalated by the fact that Microsoft is late in producing effective security patches. As of the local attacks, this is more like a trusted friend or a staff stealing from you, this is more of an ethical issue than technological. Anyways, we can look into some well known best practices that can make all types of attacks to a minimal.

First of all know the programs and services that you are using or need along with a sound knowledge of access distributions. In an office environment when sharing folders, services or privileges, make sure to document it. If you have a server, lock it down as much as you can, including physical access. Remove or do not install any unnecessary/unwanted services or programs. Patch all known vulnerabilities on a regular basis, and keep yourself updated on the security issues.

In an office environment it is always good practice to create security policies based on the worst that can happen, so you are prepared for the worst that you can imagine. The best security policy is to customize your box, notably your firewall to your own needs. Installing a firewall does not necessarily make your network secure, but a customized firewall will be harder for a cracker to learn. With FLOSS, ways in which customizations can be done is limitless. So let us drill down on someways on how we can do it.

Update Your System

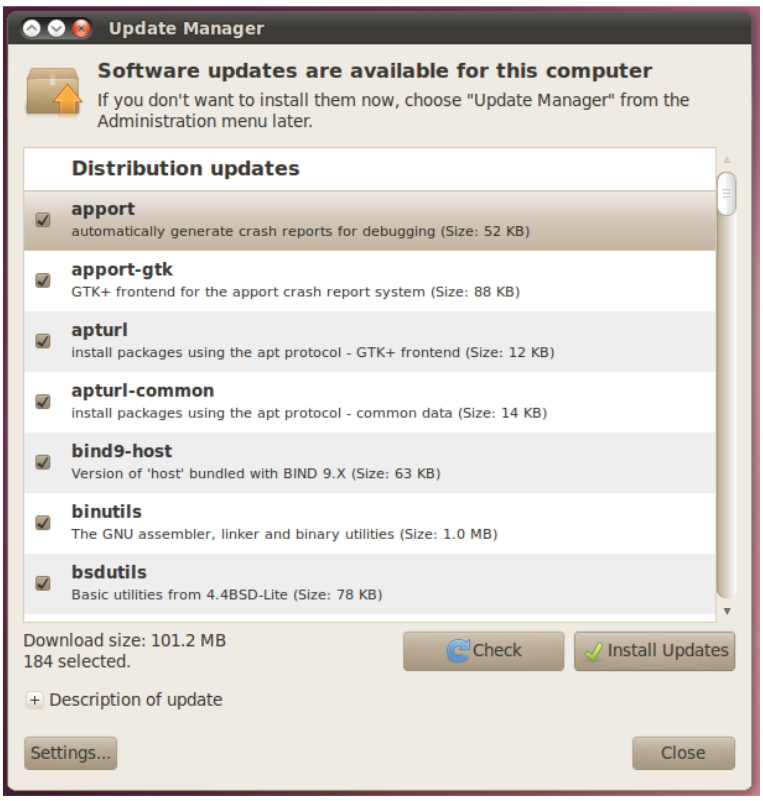
First of all update your system on a regular basis, as vulnerabilities and bugs are found and fixed on a daily basis, you need to patch your system as soon as these updates are available. On an Ubuntu terminal just issue the command

sudo apt-get update && sudo apt-get upgrade

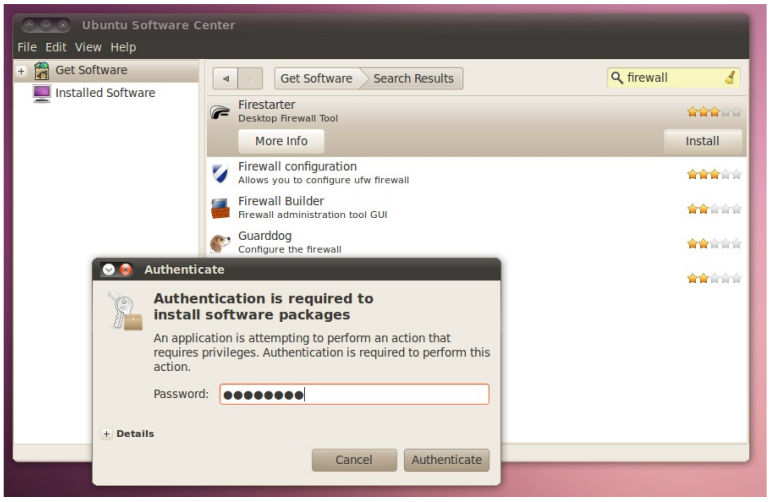
this will update your repository data and at the same time download and install any updates that are found. You will be asked to type your sudo password and it will prompt before downloading additional software. If you want to update the system via GUI select

System -> Administration -> Update Manager

just click on Check and after the system has checked for updates select and/or deselect which ever package you want and click on Install updates. While you are there you can make sure to automate your security updates, click on the settings, and make sure your automatic updates is set to daily (which is by default).



Install Firestarter



Second install Firestarter, a GUI based firewall configuration tool that uses netfilter system built into the Linux Kernel. Firestarter has a graphical interface to configure inbound and outbound network connections based on rules and settings. In addition Firestarter can be used to view real-time network traffic events and active connections. Last it can be used to configure port-forwarding, Internet connection sharing and DHCP services. Firestarter is in the Ubuntu Repository so you can install it using Ubuntu Software Center or by issuing

sudo apt-get install firestarter

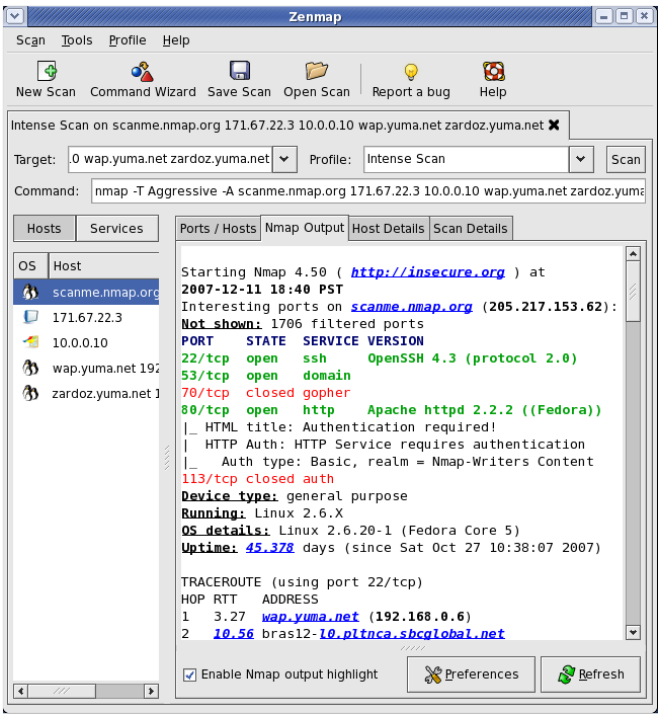
in the terminal, while connected to the Internet. After installing, launch it by going to

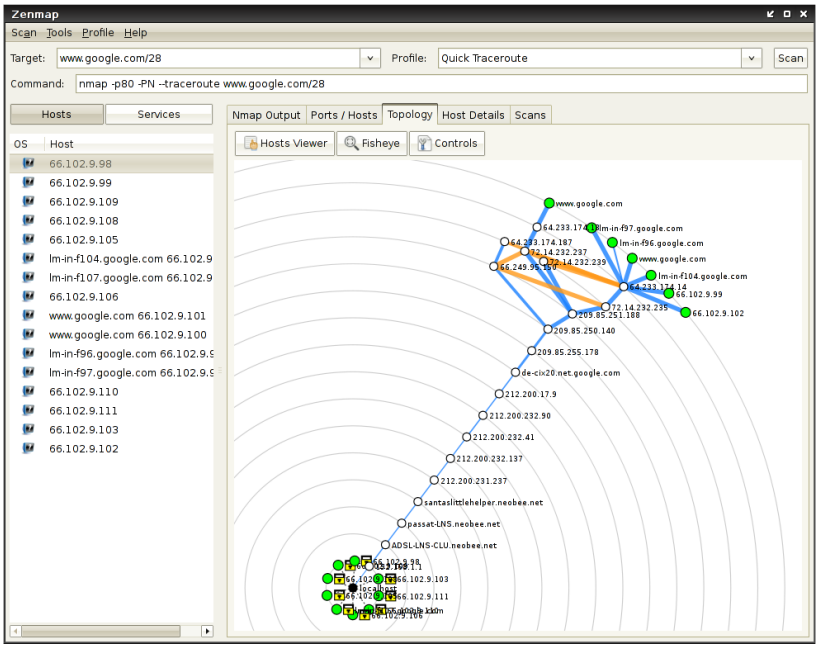
Applications -> Internet -> Firestarter

For more information visit:
http://www.fs-security.com/docs/tutorial.php

Nmap

Once the firewall is in place, access distributions are documented, physical access localized and security policies up in the place, it is time to hack, scan the network or computer for vulnerabilities and spot them. I will recommend you look into three products: Nessus, SARA and Nmap. Nessus is powerful but report a lot of false alarms, so can make a novice user lost. SARA is good too, but it's development is discontinued. So I will recommend that you go with Nmap. Nmap is in the Ubuntu repository, so you can install directly from Ubuntu Software Center. In addition Nmap do have a GUI interface nmapfe or zenmap which you can use if you are not too comfortable with the terminal. After installing, just open a terminal and shoot the command **"sudo nmapfe"** or **"sudo zenmap"**.





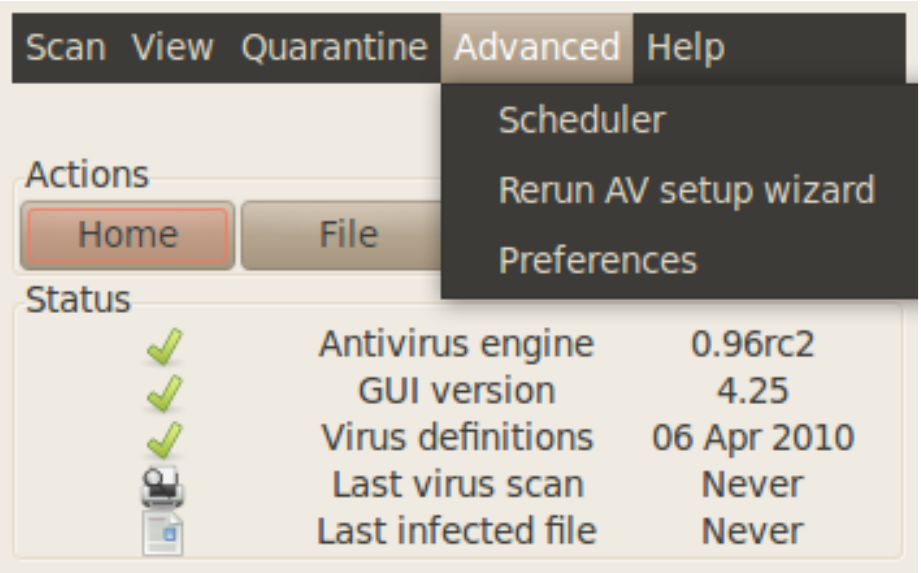
Make sure you run the scan on SYN Stealth Scan, with OS Detection and Version Probe. The scan result will show open ports with the service name, along with version numbers. In general the fewer services and ports are open on your systems, it is more secure.

For more information visit: http://nmap.org/

Virus Scanner

Next when all you have is those services that you only want/need and all unwanted ports blocked install a virus scanner. If you prefer a commercial Anti-Virus you can go for NOD32, F-prot or Kespersky, but if you don't want to buy a virus scanner you can give a try with AVG, Avast or Avira AntiVir. Last there is the FLOSS favorite virus scanner ClamAV which is again in the Ubuntu Repository so you can use Ubuntu Software Center to install it, just search for Virus Scanner or you can use the terminal

sudo apt-get install clamav



After installing you will need to update the Virus Signature, just issue the command

sudo freshclam

or open the Virus Scanner via

Applications -> Accessories -> Virus Scanner

and select

Help -> Check for updates

While you are there you can schedule a daily virus scan and signature update by selecting

Advanced -> Scheduler

choose the Hour and Minutes and clicking 'Add' for each.

For servers and/or automated use install

sudo apt-get install clamav-deamon

To make sure clamav deamon is running, issue in the terminal

ps ax | grep [c]lamd

If you want you can stop or start the deamon using

sudo /etc/init.d/clamav-deamon stop
or
sudo /etc/init.d/clamav-deamon start

Hack to Learn

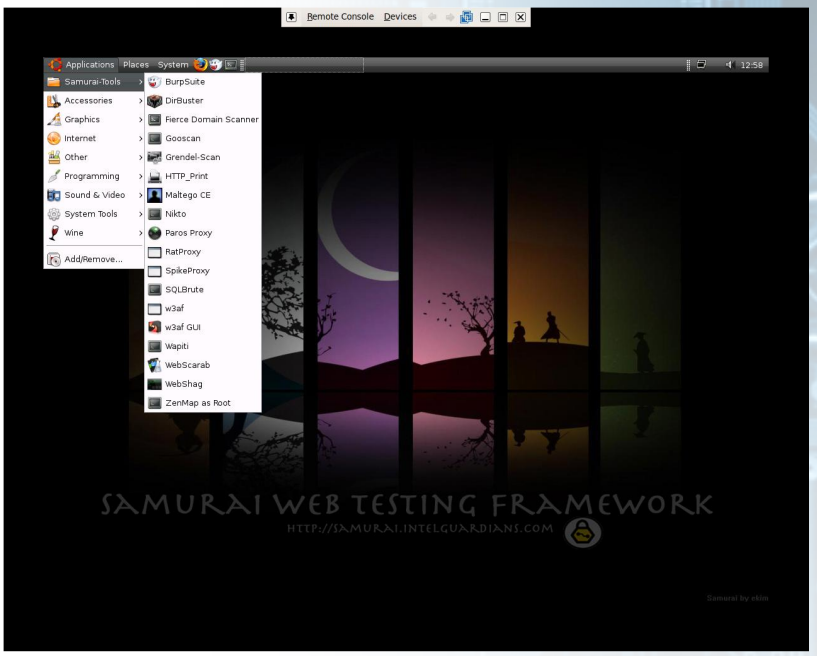
If you are serious about security you need to hack to learn. You might want to have a look at Linux based security distros. The most famous and well equipped Linux distributions for hacking is BackTrack

http://www.backtrack-linux.org

Samurai

http://samurai.inguardians.com

Samurai is specialized for web testing while backtrack has more than 300 hacking tools packaged with the distribution, free to download and ready to use.



Hacking Tools

Using hacking tools at times can be considered as a script kiddie, but you got to start somewhere. So below find few of the hacking tools that can make you occupied for months, if not for years (in no particular order).

SpiderLabs Tools
https://www.trustwave.com/spiderLabs-tools.php
SpiderLabs has developed dozens of tools over the years. Most of them end up as internal-only tools since they eventually make their way into one of Trustwave's product offerings. Recently, they have decided to showcase some of these tools and provide them as Open Source to the information security community.

iScanner
http://iscanner.isecur1ty.org/
iScanner is free open source tool lets you detect and remove malicious codes and web pages viruses from your Linux/Unix server easily and automatically.

BeFF
http://www.bindshell.net/tools/beef/
BeEF is a browser exploitation framework. This tool will demonstrate the collecting of zombie browsers and browser vulnerabilities in real-time. It provides a command and control interface which facilitates the targeting of individual or groups of zombie browsers.

Burp Proxy
http://www.portswigger.net/proxy/
Burp Proxy is an interactive HTTP/S proxy server for attacking and testing web applications. It operates as a man-in-the-middle between the end browser and the target web server, and allows the user to intercept, inspect and modify the raw traffic passing in both directions.

W3af
http://w3af.sourceforge.net/
w3af is a Web Application Attack and Audit Framework. The project's goal is to create a framework to find and exploit web application vulnerabilities that is easy to use and extend

ratproxy
http://code.google.com/p/ratproxy/
A semi-automated, largely passive web application security audit tool, optimized for an accurate and sensitive detection, and automatic annotation, of potential problems and security-relevant design patterns based on the observation of existing, user-initiated traffic in complex web 2.0 environments.

WebScarab
http://dawes.za.net/rogan/webscarab/
WebScarab is a Web Application Review tool. It sprang from the designs of the people inhabiting the WebAppSec list run from SourceForge, for a powerful, free, open tool for reviewing web applications for security vulnerabilities.

Maltego
http://www.paterva.com/web4/index.php/maltego
Maltego is an open source intelligence and forensics application. It will offer you timous mining and gathering of information as well as the representation of this information in a easy to understand format.

Fierce Domain Scan
http://ha.ckers.org/fierce/
Fierce is a reconnaissance tool. Fierce is a Perl script that quickly scans domains (usually in just a few minutes, assuming no network lag) using several tactics.

DMitry
http://www.mor-pah.net/index.php?file=projects/dmitry
DMitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.

dnstracer
http://www.mavetju.org/unix/dnstracer.php
dnstracer determines where a given Domain Name Server (DNS) gets its information from, and follows the chain of DNS servers back to the servers which know the data.

Fport 2.0 (Windows Binary)
http://www.foundstone.com/us/resources/proddesc/fport.htm
fport reports all open TCP/IP and UDP ports and maps them to the owning application. This is the same information you would see using the 'netstat -an' command, but it also maps those ports to running processes with the PID, process name and path. Fport can be used to quickly identify unknown open ports and their associated applications.

Mbenum 1.5.0 (Windows Binary)
http://www.cqure.net/wp/mbenum/
MBEnum queries the master browser for whatever information it has registered. Windows servers/workstations store information about what services they run in the MB.

PStoreView 1.0 (Windows Binary)
http://www.ntsecurity.nu/toolbox/pstoreview/
PStoreView lists the contents of the Protected Storage. It usually contains things like Internet Explorer username and password autocomplete, and Outlook account names and passwords.

Relay Scanner
http://www.cirt.dk/tools/
This program is used to test SMTP servers for Relaying problems that could lead to an spammer using your mailserver to send SPAM.

Hping3
http://gd.tuwien.ac.at/www.hping.org/hping3.html
hping3 is fully scriptable using the TCL language, and packets can be received and sent via a binary or string rappresentation describing the packets. In pratice this means that a few lines of code can perform things that usually take many lines of C code. Examples are automated security tests with pretty printed report generation, TCP/IP test suites, many kind of attacks, NAT-ting, prototypes of firewalls, implementation of routing protocols, and so on.

IKEProbe
http://www.securityfocus.com/infocus/1821
http://www.ernw.de/download/ikeprobe.zip
IKEProbe can be used to determine vulnerabilities in the PSK implementation of the VPN server. It tries out various combinations of ciphers, hashes and Diffie-Helman groups and attempts to force the remote server into aggressive mode.

Netcat
http://netcat.sourceforge.net/
Netcat is a featured networking utility which reads and writes data across network connections, using the TCP/IP protocol.

Netdiscover
http://nixgeneration.com/~jaime/netdiscover/
Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks.

Nmap
http://www.insecure.org/nmap
Nmap ("Network Mapper") is a free and open source (license) utility for network exploration or security auditing

aircrack-ng /Aircrack
http://www.aircrack-ng.org/
http://www.grape-info.com/doc/linux/config/aircrack-ng-0.6.html
Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured.

UnicornScan
http://www.unicornscan.org/
Unicornscan is a new information gathering and correlation engine built for and by members of the security research and testing communities. It was designed to provide an engine that is Scalable, Accurate, Flexible, and Efficient.

Absinthe
http://www.0x90.org/releases/absinthe/docs/basicusage.php
Absinthe does not discover injections, so it requires the user to enter all relevant information about the target host.

Checkpwd
http://www.red-database-security.com/software/checkpwd.html
Checkpwd is one of the fastest dictionary based password checker for Oracle databases. This is a useful tool for DBA's to identify Oracle accounts with weak or default passwords.

Cisco OCS Mass Scanner
http://www.hacklab.tk/
Vulnerability scanner for Cisco routers. For now head the telnet password and enable mode by default.

Fuzzer
http://www.securiteam.com/tools/5TP012AHFU.html
"Fuzzing" is an automated software testing technique that generates and submits random or sequential data to various areas of an application in an attempt to uncover security vulnerabilities.

GFI LanGuard
http://www.gfi.com/lannetscan/
GFI LANguard scans your network and ports to detect, assess and correct security vulnerabilities with minimal administrative effort.

NTA Monitor
http://www.nta-monitor.com/tools/ike-scan/
IPsec VPN scanning, fingerprinting and testing tool.

Mezcal HTTP/S
http://0x90.org/releases/mezcal/
Mezcal is an HTTP/HTTPS bruteforcing tool allowing the crafting of requests and insertion of dynamic variables on-the-fly.

Nikto
http://www.cirt.net/code/nikto.shtml
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6100 potentially dangerous files/CGIs, checks for outdated versions of over 950 servers, and version specific problems on over 260 servers.

Peach
http://peachfuzz.sourceforge.net/
Peach is a SmartFuzzer that is capable of performing both generation and mutation based fuzzing.

SQLbrute
http://www.justinclarke.com/archives/2006/03/sqlbrute.html
SQLBrute is a tool for brute forcing data out of databases using blind SQL injection vulnerabilities. It supports time based and error based exploit types on Microsoft SQL Server, and error based exploit on Oracle.

Snmpcheck
http://www.nothink.org/perl/snmpcheck/
snmpcheck is a free open source utility to get information via SNMP protocols.

Spike
http://www.immunitysec.com/resources-freesoftware.shtml
When you need to analyze a new network protocol for buffer overflows or similar weaknesses, the SPIKE is the tool of choice for professionals.

Taof
http://sourceforge.net/projects/taof
Taof is a GUI cross-platform Python generic network protocol fuzzer. It has been designed for minimizing set-up time during fuzzing sessions and it is especially useful for fast testing of proprietary or undocumented protocols.

Wapiti
http://wapiti.sourceforge.net/
Wapiti allows you to audit the security of your web applications.

Yersinia
http://www.yersinia.net/
Yersinia is a network tool designed to take advantage of some weakeness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

sqldict /sqldumplogins
http://www.vulnerabilityassessment.co.uk/sqlat.htm
SQLat is a nice suite of tools which come in handy when trying to carry out a vulnerability assessment/penetration test against a MS SQL Server.

Framework3-MsfC
http://en.wikibooks.org/wiki/Metasploit/Contents
http://www.metasploit.com/
Metasploit provides useful information and tools for penetration testers, security researchers, and IDS signature developers.

Milw0rm Archive
http://www.milw0rm.com/
Milw0rm is a site for obtaining Proof of concept exploit code.

Pirana
http://www.guay-leroux.com/projects/SMTP%20content%20filters.pdf
http://www.guay-leroux.com/projects.html
PIRANA is an exploitation framework that tests the security of a email content filter.

Driftnet
http://www.ex-parrot.com/~chris/driftnet/
Driftnet is a program which listens to network traffic and picks out images from TCP streams it observes.

Dsniff
http://monkey.org/~dugsong/dsniff/
dsniff is a collection of tools for network auditing and penetration testing

Etherape
http://etherape.sourceforge.net/
EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, ip and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display.

EtterCap
http://ettercap.sourceforge.net/
Ettercap is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks.

File2Cable
http://phenoelit-us.org/irpas/docu.html#file2cable
This tool is perfect to find new vulnerabilities and test concepts.

Hydra
http://www.thc.org/
http://freeworld.thc.org/thc-hydra/
A very fast network logon cracker which support many different services

John
http://www.openwall.com/john/
John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS.

Medusa
http://www.darknet.org.uk/2006/05/medusa-password-cracker-version-11-now-available-for-download/
Medusa is a speedy, massively parallel, modular, login brute-forcer for network services created by the geeks at Foofus.net.

PHoss
http://phenoelit-us.org/phoss/docu.html
PHoss is a sniffer.

PackETH
http://packeth.sourceforge.net/
packETH is a Linux GUI packet generator tool for ethernet.

> Hacking Tools[3]

Rcrack
http://project-rainbowcrack.com/
RainbowCrack is a general propose implementation of Philippe Oechslin's faster time-memory trade-off technique. It cracks hashes with rainbow tables.

VNCrack
http://phenoelit-us.org/vncrack/docu.html
VNCrack is a VNC remote control tool cracker; the tool tries to brute force the username/password authentication scheme by trying every possible combination.

Wireshark
http://wireshark.org/
Wireshark is the world's foremost network protocol analyzer, and is the de facto (and often de jure) standard across many industries and educational institutions.

chntpw
http://pwet.fr/man/linux/administration_systeme/chntpw
http://home.eunet.no/~pnordahl/ntpasswd/
A utility to overwrite Windows NT/2000 SAM passwords.

Matahari
http://matahari.sourceforge.net/
matahari is a python script designed to provide a basic non-interactive shell on remote systems behind firewalls. It is intended for use by system administrators who may need some emergency backdoor to access a firewalled machine.

ICMPTX
http://thomer.com/icmptx/
ICMPTX is a program that allows a user with root privledges to create a virtual network link between two computers, encapsulating data inside of ICMP packets.

ProxyTunnel
http://proxytunnel.sourceforge.net/
ProxyTunnel is a program that connects stdin and stdout to a server somewhere on the network, through a standard HTTPS proxy.

ASLeap
http://asleap.sourceforge.net/
Exploit CISCO leap.

Airpwn
http://airpwn.sourceforge.net/
Airpwn is a framework for 802.11 (wireless) packet injection.

AirSnarf
http://airsnarf.shmoo.com/
Airsnarf is a simple rogue wireless access point setup utility designed to demonstrate how a rogue AP can steal usernames and passwords from public wireless hotspots.

CowPatty
http://www.churchofwifi.org/default.asp?PageLink=Project_Display.asp?PID=95
http://www.renderlab.net/projects/WPA-tables/
A program to pre-hash WPA-PSK password lists for quick lookup tables, thus applying the time-space trade off of rainbow tables to WPA-PSK cracking.

FakeAP
http://www.blackalchemy.to/project/fakeap/
Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points.

Karma
http://theta44.org/karma/index.html
http://www.offensive-security.com/madwifi-r3406-hdm-032608.tar.gz
KARMA is a set of tools for assessing the security of wireless clients at multiple layers.

Kismet
http://www.kismetwireless.net/
Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.

MDK3
http://homepages.tu-darmstadt.de/~p_larbig/wlan/
A tool to bruteforce MAC Filters, bruteforce hidden SSIDs, probe networks to check if they can hear you, intelligent Authentication-DoS to freeze APs, FakeAP - Beacon Flooding with channel hopping, Disconnect everything with Deauthentication and Disassociation packets, WPA TKIP Denial-of-Service & WDS Confusion - Shuts down large scale multi-AP installations.

MacChanger
http://alobbs.com/macchanger/
A GNU/Linux utility for viewing/manipulating the MAC address of network interfaces.

Wicrawl
http://midnightresearch.com/projects/wicrawl
Wicrawl is a simple wi-fi (802.11x) Access Point auditor with a simple and flexible plugin architecture.

BTcrack
http://www.nruns.com/_en/security_tools_btcrack.php
BTCrack is the worlds first Bluetooth Pass phrase (PIN) bruteforce tool, BTCrack will bruteforce the Passkey and the Link key from captured Pairing exchanges.

Blueprint
http://trifinite.org/trifinite_stuff_blueprinting.html
Blueprinting is a method to remotely find out details about bluetooth-enabled devices.

Bluesmash
http://sourceforge.net/projects/bluesmash/
Blue|Smash is a python based tool for pentesting bluetooth enabled devices.

Sleuthkit
http://www.sleuthkit.org/sleuthkit/
The Sleuth Kit (TSK) is a library and collection of command line tools that allow you to investigate volume and file system data.

Autopsy
http://www.sleuthkit.org/autopsy/index.php
The Autopsy Forensic Browser is a graphical interface to the command line digital investigation tools in The Sleuth Kit.

DD_Rescue
http://freshmeat.net/projects/ddrescue/
dd_rescue copies data from one file or block device to another. It is intended for error recovery, so, by default, it doesn't abort on errors, and doesn't truncate the output file.

Foremost
http://foremost.sourceforge.net/
Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving.

Magicrescue
http://jbj.rapanden.dk/magicrescue/
Magic Rescue scans a block device for file types it knows how to recover and calls an external program to extract them.

Rootkithunter
http://directory.fsf.org/RootkitHunter.html

Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.

GDB GNU Debugger
http://sourceware.org/gdb/documentation/
The purpose of a debugger such as gdb is to allow you to see what is going on “inside” another program while it executes—or what another program was doing at the moment it crashed.

GNU DDD
http://www.gnu.org/manual/ddd/
The purpose of a debugger such as DDD is to allow you to see what is going on "inside" another program while it executes--or what another program was doing at the moment it crashed.

SNORT
http://www.snort.org/
Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire.

USE RESPONSIBLY

All material contained in this MOSS Magazine article is for security and educational purposes only. The author or MOSS will not be considered responsible in any way for damages perpetrated to persons or property caused by code, programs, information and techniques contained within this MOSS Magazine article.

all information are correct at the time of creation.

ކޮޕީރައިޓް ޤާނޫނާ ޚިލާފު ދިވެހިން
ހުށަހެޅުއްވި ސުވާލަކަށް ޖަވާބު؟

ދިވެހިރާއްޖޭގެ ސިޔާސީ މުޝްތަރަކު ބެލެހެއްޓުމަށް

ދިވެހިރާއްޖޭގައި ކޮޕީރައިޓް އުސޫލު

މުސްތަޤްބަލުގައި އަމަލުކުރާނެ ގޮތް ބަލަމާ.

ދުރުމިންނަށް ވިސްނާލާއިރު، 2011 ބެލެހެއްޓުމާ

ވަރަށް ދިގު ތަރިކާއެއްގައި ކޮޕީރައިޓްއާ ގުޅޭ

ކަންކަން ބަލަން ބޭނުންވެއްޖެ. ހަމަގައިމު މިހާރު

އަޅުގަނޑު ހުށަހަޅާ ސުވާލަކީ ވެސް ކޮބައިތޯ؟ އަދި

މިކަމަށް ޙައްލު ހުށަހަޅާ ކޮމްޕިއުޓަރ ލައިސަންސް

ބޭނުންކުރާ ވެރިންނަށް ކިހިނެއް ދެކެނީ؟

ކޮޕީރައިޓް ޤާނޫނު ކަށަވަރު ކުރުމަށް ބޭނުންވާ

ސޮފްޓްވެއަރ އާއި، ލައިސަންސް ހަދާ އަދި

މިނިވަން ޚިޔާލުގެ އަހަރު ތަކެއް ގޮސް ބާކީ

ކުރަމުން ބޭނުންކުރާ. މީގެ ތަފާތު ހިތް ވާނުވާ

ކޮބާ އަދި ޢާއްމު ކަމަކަށް ވިސްނާލުމަށް.

ހައްލުވާ މިފަދަ ކަންކަމެއް ވަކިން ކުރިޔަށް

ދިވެހިން މިހާރު ކޮމްޕިއުޓަރ ކަމަށް މިހެން

ކަމެއް.

އެންމެ ގިނައިން ގަނޑުގައި ބޭނުންކުރާ ކަމާ

ކޮންމެ އަހަރަކު ސަރުކާރުން ދޫކުރާ 9000ރ

އަގު. ކޮޕީރައިޓާ އެއްބަޔަކު، އެކިކޮމްޕިއުޓަރ

ބޭނުންކުރާ އަދި އެހެން އެޕްލިކޭޝަން

ސަރުކާރުގެ ފަރާތުން. ލައިސަންސް ވަރުގަދަ އެކި

ގިނަ ދުވަސް ކޮމްޕިއުޓަރ 2500ރ އަގު.

ވިންޑޯސް ވިސްޓާ ވިންޑޯސް 7 ގިނަ ދުވަސް

3000ރ އަގު. މިހެން އަދި ނުލިބޭނެ ނަމަވެ.

ބޭނުންވާ އެހެން ސޮފްޓްވެއަރ ފަދަ އެންމެ ބޮޑު

ބާއި އަދި އަހަރެން ސޮފްޓްވެއަރ ގިނަ ދުވަހު

ހިނގާނެ. މީގެ ލޯނު އިތުރު އެބައި

ރާއްޖޭގައި ކޮޕީރައިޓް ބަލަހައްޓާ ހިއްސާ ގޮތް

ހަރަދު ކުރަންޖެހޭ ބޭނުންކުރާ ސޮފްޓްވެއަރ ބަލަން

އެބައި ދިވެހިރާއްޖެ ވަރަށް ގިނަ ހަރަދު ބާކީ

ހުރީ ގިނަ ސަރުކާރު ބެލެނިވެރިން ސޮފްޓްވެއަރ

ގިނަ ޢާންމު ހަރަދު ބަލާ ހިނގާނެ ކަމަށް.

ވިއުމާ އެކު މިހާރު ފަހަރުގަ ބޭނުންކުރާ ކަމުގައި

އެހެން ގޮތްތަކުން ހަމައެކަނި ބޭނުންކުރެވޭ.

ހަމައެކަނި ފަސް ވަރަށް ހުރިހާ ފަރާތަކަށް

ކޮމްޕައުންޑް ސަރުކާރުގެ ދާއިރާގައި ޙައްލު

އާއި ވިޔަފާރި ތަކުން ފަރާތުން ސޮފްޓްވެއަރ

އެކި ޢާއްމު ފަސޭހަ ހިނގާ އަދި ރިސާލާ ވަޒީފާ

ހިނގާ ދިގު ސަރުކާރުގެ ފަރާތުން ހުރި

ކޮންމެ އަހަރަކު އަގުގަ ފަސޭހަ ވަރަށް ދިވެހިން

ވަރަށް ގިނަ ބާ ލައިސަންސްތައް ގަތުމަށް އެބަ

ކޮމްޕިއުޓަރ ބޭނުންކުރާ ދުވަސް. ކޮންމެ

ގޮތަކަށް ވެސް ސަރުކާރު ފަރާތުން ދިވެހިރާއްޖެ

ވަރަށް އަގުބޮޑު ސޮފްޓްވެއަރ ބޭނުންކުރޭ.

ކޮޕީރައިޓްއާ ގުޅޭ އިތުރު މަޢުލޫމާތަށް

ގިނަ ކަމަކީ ފައިސާ ހަރަދު ނުކުރުމަށް

ސަރުކާރުގެ ސޮފްޓްވެއަރ ބަދަލުކުރަން ހުށަހެޅީ.

ސޮފްޓްވެއަރ ބަދަލު ކުރުމާއި ބޭނުން

ކުރެވޭ ސޮފްޓްވެއަރ ބޭނުންކުރާ މީހުން

ވަރަށް ކުރިއަށް ގެންދިއުމަށް ބޭނުން.

އާ ލިނަކްސް ބޭނުން ކުރާނެ ސަރުކާރު

ސިސްޓަމް ހިފެހެއްޓުމަށް ހެދި ކޮމްޕިއުޓަރ

ކޮމްޕިއުޓަރ ހަރަދު ކުރުމުގެ ފަސޭހަ ޚިދުމަތް

ވަރަށް ހިނގާފައި. ސަރުކާރު ފަރާތުން ދިވެހިން

ކަމަށް ލިބޭނެ ހަމައެކަނި ޙައްލެއް.

ކޮމްޕިއުޓަރ ބޭނުންކުރާ ގިނަ ފަރާތްތަކަކީ

އަދި "ހަރަދު" ކުރަން ދޫކުރާ ސޮފްޓްވެއަރ

ބޭނުންކުރާ ސޮފްޓްވެއަރ ގެ ބޭނުން "ލިނަކްސް"

އެއީ ބަލަ ހަމައެކަނި ކޮމްޕިއުޓަރ ގެ ބޭނުންކުރާ

ސޮފްޓްވެއަރ މިނިވަން ކޮމްޕިއުޓަރތައް. އެއިން

ވަކި ވަރަށް ގިނަ ފަރާތްތަކެއް ބޭނުންކުރާ

ވަގުތު ބޭނުން ކުރެވޭ. ސަރުކާރު ދޫކުރާ

ސޮފްޓްވެއަރ ބޭނުންކުރާ ކަމާއި ބަދަލު

ދިވެހި ސަރުކާރުން "ލިނަކްސް" ބޭނުން ކުރާ

ބޭނުން "އެއްވެސް ކަމަކާ ނުލައި" ކޮމްޕިއުޓަރ

ބޭނުންކުރާ ފަސޭހަ ސޮފްޓްވެއަރ އަދި ބޭނުންކުރާ

ބޭނުނުން ހިސާބުތަކެއް ދީފައި ހުރި.

ކޮމްޕިއުޓަރ ބޭނުންކުރާ ގިނަ ފަރާތްތަކުން

ކުރާ ހަރަދު ކުރުމުގެ ބަދަލުގައި ބޭނުންކުރޭ

ކޮމްޕިއުޓަރ އަގުބޮޑު ސޮފްޓްވެއަރ ފުރުޞަތު

ދިނުމަށް ސަރުކާރު ފަރާތުން ކަމާބެހޭ

ވިސްނުމާއި ބޭނުން ބަލާ ކަމަކީ ހަމައެކަނި

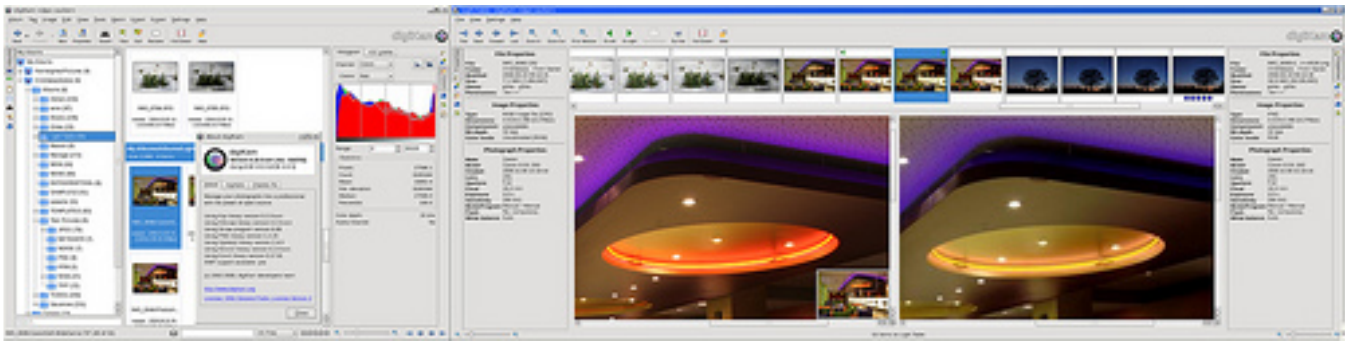
"ލިނަކްސް" އެއީ ހަމައެކަނި

ޙައްލެވެ"

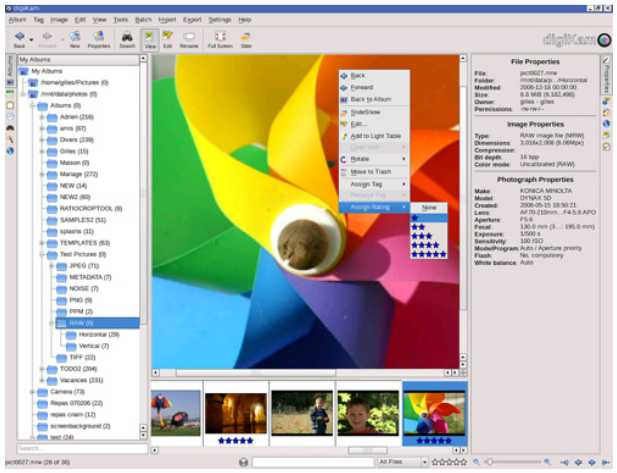
ބޭނުނުން ހިސާބުތަކެއް ދީފައި ހުރި.

Digikam: Manage your photographs like a professional with the power of open source

Mohamed Malik > mohamedmalik.com

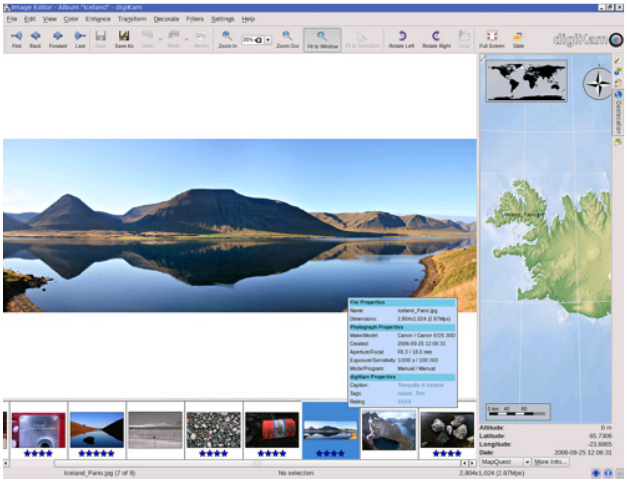


Digikam is definitely the best image management tool that is available to Linux users. It support all major image formats, even RAW files from all major DSLR camera manufactures Canon, Nikon etc.. Nevertheless it can organize collections of photographs in directory-based albums, or dynamic albums by date, timeline, or by tags. Users can also add captions and ratings to their images, search through them and save searches for later use. With the plugins they can also export albums to 23hq, Facebook, Flickr, Gallery2, Google Earth's KML files, SmugMug, Simpleviewer, burn them on CD, or create web galleries.

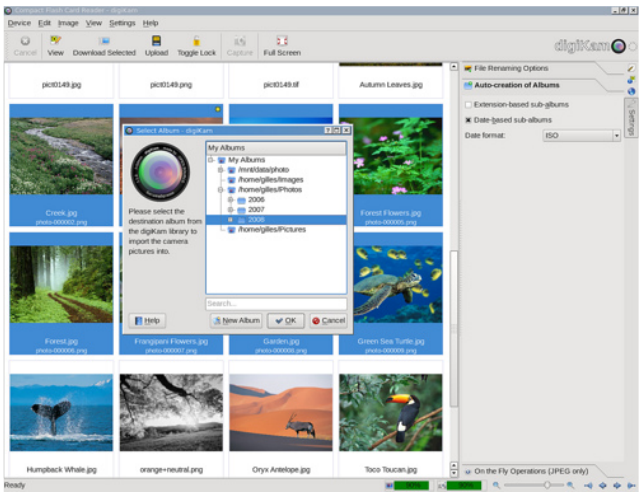


Features

Digikam provides functions for organizing, previewing, downloading and/or deleting images from digital cameras. Basic auto-transformations can also be deployed on the fly during picture downloading. In addition, Digikam offers image enhancement tools through its KIPI (KDE Image Plugins Interface) framework and its own plugins, like red-eye removal, color management, image filters, or special effects. Digikam is the only free photo management application on Linux that can handle 16 bit/channel images. Digital Asset Management is the mainstay of DigiKam.

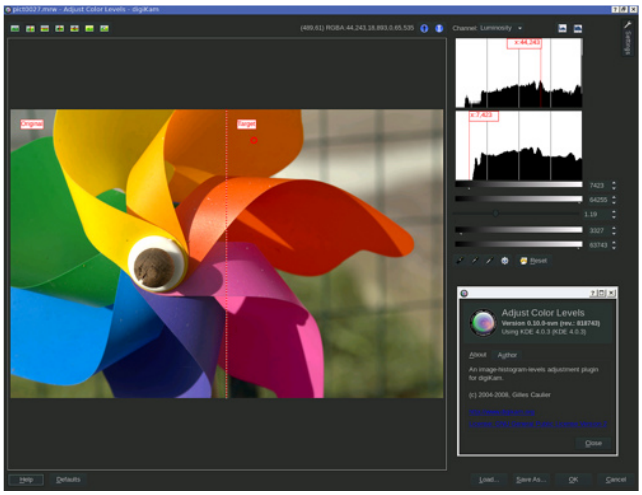


Digikam²



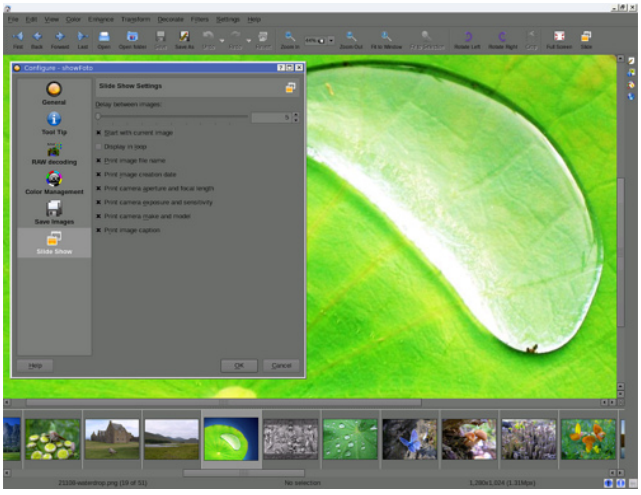
The 0.10 version is a hallmark in development as it integrates DigiKam in the KDE4/Qt4 desktop environment, which is now available on all major platforms as Unix-like, OS X and Windows (XP and Vista). New features are: XMP metadata, DNG format read and write, database file is independent of photo libraries, enabling remote paths, multiple roots and offline archives, improved database with many more metadata that can be searched, e.g. camera or lens, Marble integration for geolocation, non-modal image editor, live search boxes in both sidebars and main window, and many more.

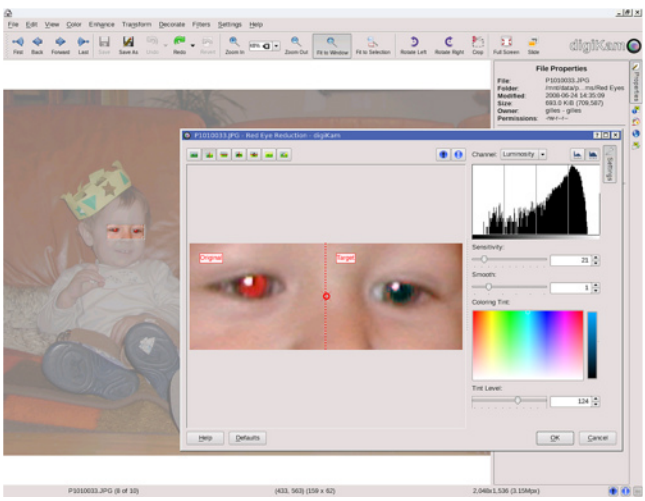
Due to these high end features that are available on Digikam it can even satisfy the most serious photographers or people who have tons of pictures in there collection.

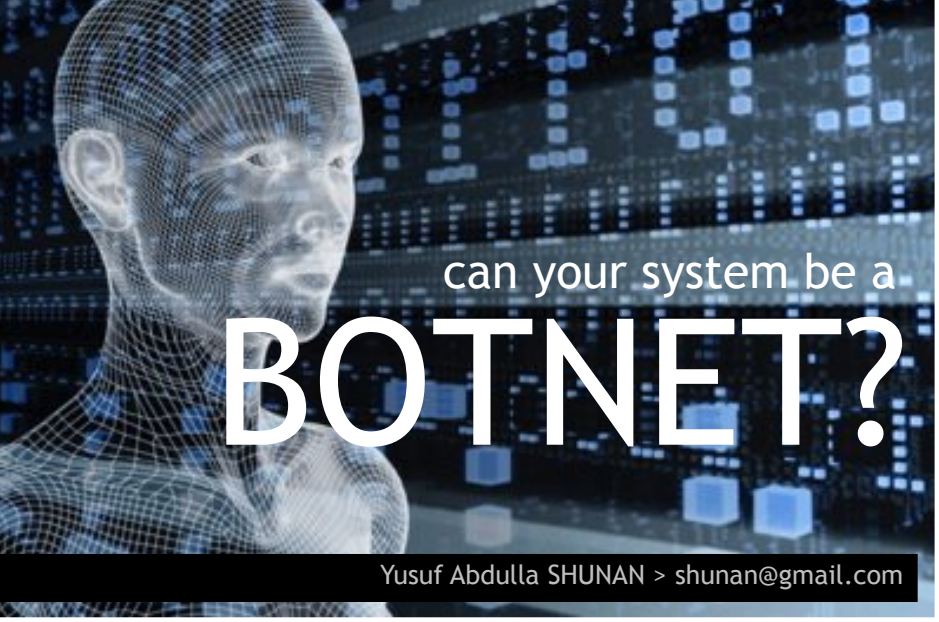


Digikam has two views, one is the default viewer and the other is the editor view. In editor view, users can edit the picture by using various tools which are available. In this regard, many filters such as artistic, color paint and emboss are available. By using the editor view users can apply various effects to their pictures as well. In this manner it can be regarded as a fully fledged replacement for proprietary photo management tools like Apple's Aperture and Adobe's Lightroom.

Due to its usefulness and popularity it has been awarded the TUX 2005 and 2008 Readers' Choice Award in the category Favorite Digital Photo Management Tool.







can your system be a BOTNET?

Yusuf Abdulla SHUNAN > shunan@gmail.com

We all know of the Dhiraagu and ROL targeted series of cyber attacks on August 2009. They were "denial of service" (DOS) or "distributed denial of service" (DDOS) attacks, where the attacker overflow the network with fake messages, causing the servers (computers that serve as a core in a network) to over burden to a slow or crash status.

The attacks got a lot of media attention, basically because today we all are so dependent on the Internet and it's services with only two service providers. However, it was funny how easily people were ready to start a blame game and pin pointing, some even wanted to take credit (funny way to get famous!). Like many things that happen on the Internet, it is hard to tell who could have been in the other end of the Internet, as most DOS attacks use "botnets". Botnets - short for robot networks - are the toys of the cyber criminals. A cyber criminal takes control of a computer via the Internet by secretly installing software on it. This is usually done without the slightest knowledge of the computer user. There are known cases of huge botnets, with tens of thousands of computers from all corners of the globe. Cyber criminals take control of all these computers as a network to send thousands of fake messages at a chosen interval overloading servers and causing them to crash. This is kind of the same thing that happens when we all try sending greeting text messages at the same time but DOS attacks take place in a bigger scale and for a longer duration.

In the world of the Internet, the use of Botnets is common — most of the spam that you receive are sent by botnets — and for cyber criminals they are normal day to day toys. Hence in cyberspace DOS attacks are common. In addition, even attacks on servers and Web sites, like MSN, Facebook or Twitter, with botnets, hacks, and graffiti do occur.

DOS attacks are a less destructive form of attack, a more destructive attack would have been when a cyber criminal penetrated computers and databases and scrambled or erased the data. If data like records and accounts were deleted, it would have been really destructive.

Can your system become a Botnet? Illegal pirated software is one major cause, as nobody has anyway of knowing what it contain or what additional codes are in it and some are known to have back doors that cyber criminals can come in to take control of your system. Other ways include installing untrusted software from unknown sources, un-patches vulnerabilities, virus, Trojans and worms.

With such a high volume of pirated software usage in the Maldives, many computers are insecure. We are left in the dark with no way to know which is infected or not. All will be made clear when it is another turn to be attacked, but it might be better to find and fix vulnerable systems before this occurs. Free Libre Open Source Software is a cost effective choice for such freedom. Do you want your system to be a botnet?

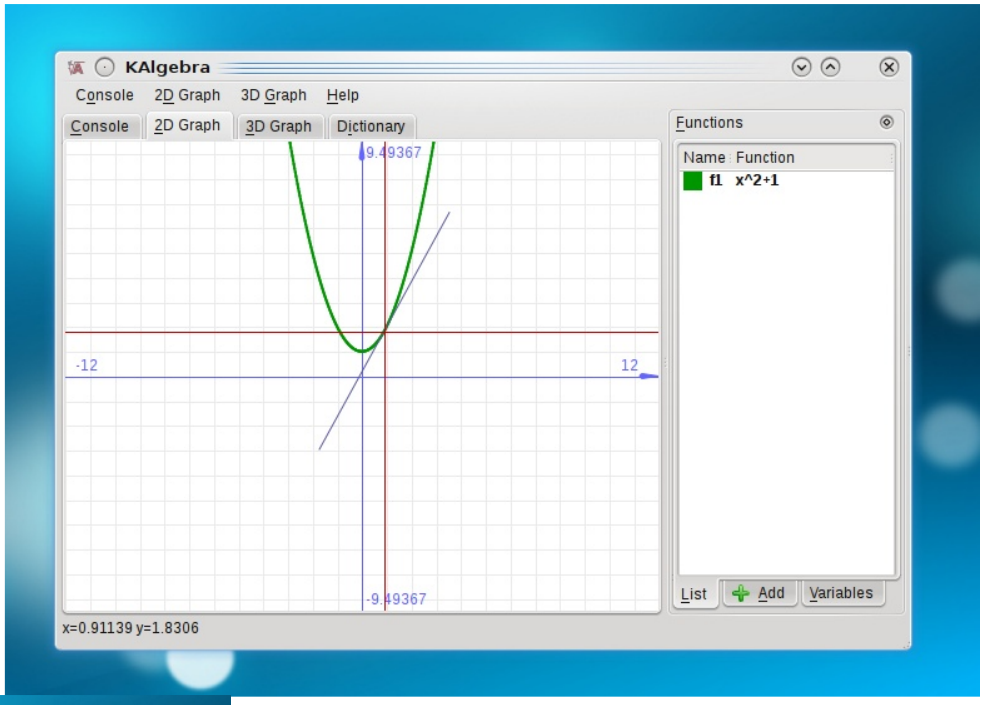
KDE Educational Applications

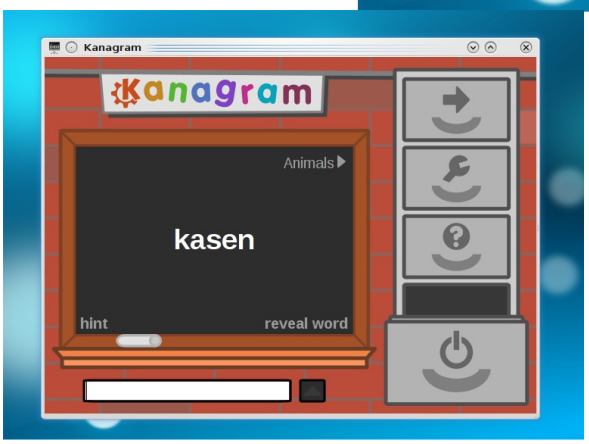
The Perfect Solution For Schools

Mohamed MALIK
mohamedmalik.com

In the previous issue of MOSS we looked at a number of applications from the KDE educational package, as discussed in the previous issue it contains a number of applications that can be used and implemented in schools. In this issue we will be taking a look at some of the other applications that are available in the KDE Educational package.

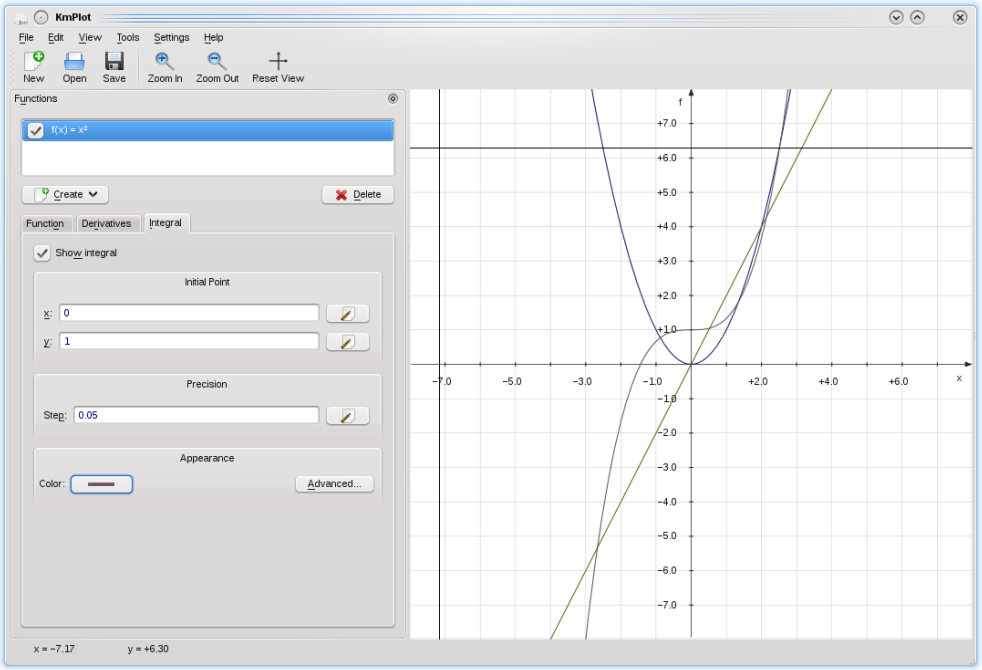
KAlgebra is a mathematical calculator based on content markup MathML language, capable to make simple MathML operations (arithmetic and logical) and to represent 2D and 3D graphs.





Kanagram is a game based on anagrams of words: the puzzle is solved when the letters of the scrambled word are put back in the correct order. There is no limit on either time taken, or the amount of attempts to solve the word.

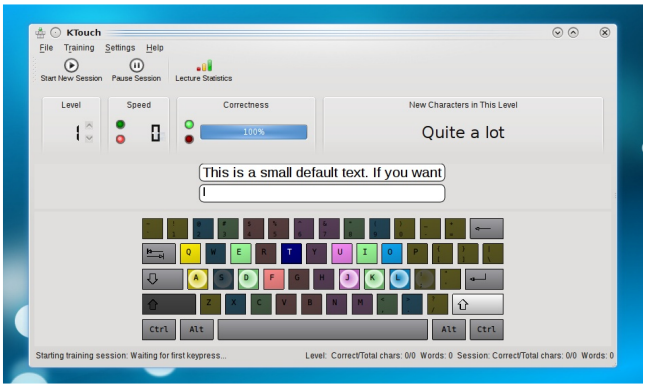
KDE Educational Applications^2



KmPlot is a program to draw graphs, their integrals or derivatives. It supports different systems of coordinates like the Cartesian or the polar coordinate system. The graphs can be colorized and the view is scalable, so that you are able to zoom to the level you need.

KTouch is a program for learning to touch type. It provides you with text to train on and adjusts to different levels depending on how good you are. It also displays which key to press next and the correct finger to use.

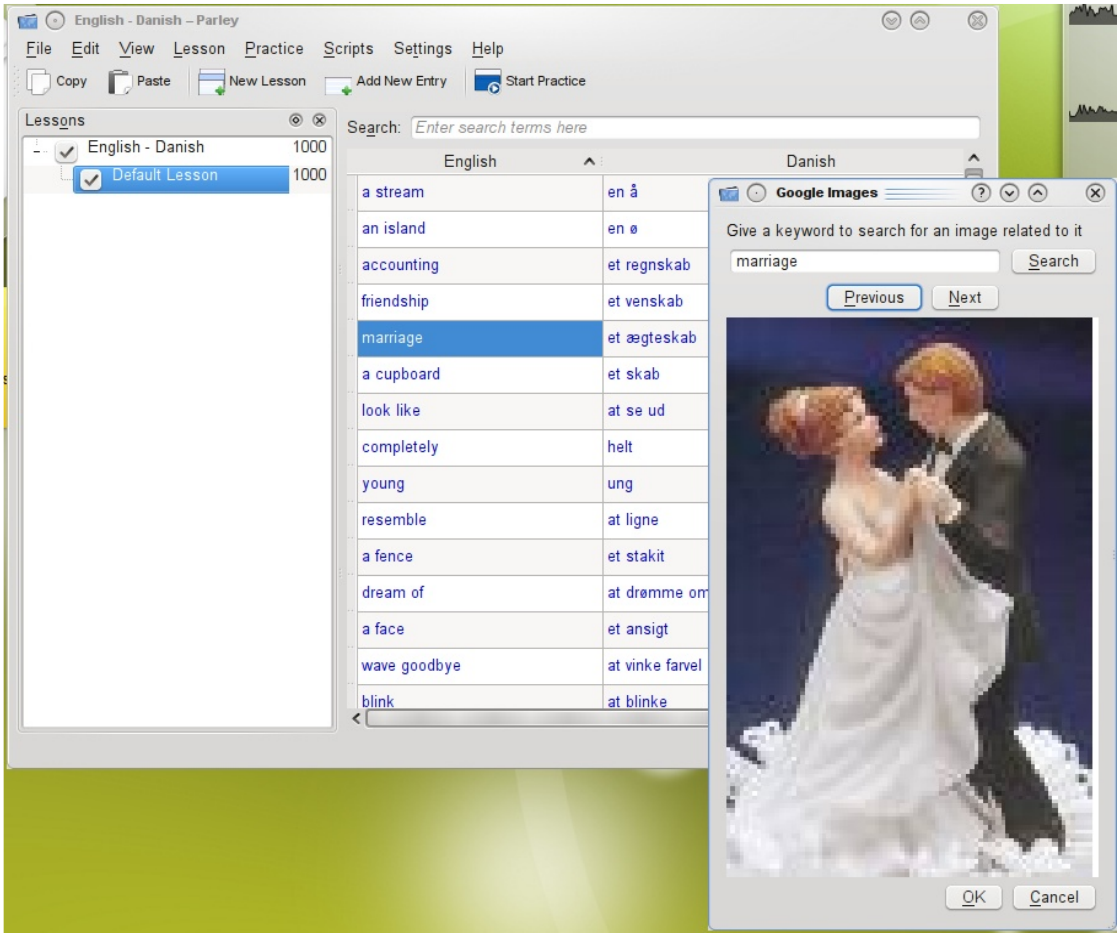
You learn typing with all fingers, step by step, without having to look down at the keyboard all the time to find your keys (which slows you down a lot). It is convenient for all ages and the perfect typing tutor for schools, universities and individuals.



Features

Support for many different training lectures
Support for many languages including language specific text fonts
Comfortable lecture editor
Support for different keyboard layouts, with the ability to use user-defined layouts
During training sessions comprehensive statistical informations are shown to help you analyze your progress

KDE Educational Applications[3]



Parley is a program to help you memorize things.
Parley supports many language specific features but can be used for other learning tasks just as well. It uses the spaced repetition learning method, also known as flash cards.
Creating new vocabulary collections with Parley is easy, but of course it is even better if you can use some of our premade files. Have a look at the KDE-Files.org page or use the "Download New Collections" feature directly.

Features

Different test types
- Mixed Letters (order the letters, anagram like) to get to know new words
- Multiple choice
- Written tests - type the words (including clever correction mechanisms)
- Example sentences can be used to create 'fill in the gap' tests
- Article training
- Comparison forms (adjectives and/or adverbs)
- Conjugations
- Synonym/Antonym/Paraphrase

Fast test setup with all options in one dialog
More than two languages (for example English, Chinese Traditional and Chinese Simplified)
Find words (also by word type) quickly
Easy lesson management
Premade vocabulary files ready to use
Share and download vocabulary using Get Hot New Stuff
Open XML file format (shared with KWordQuiz, Kanagram and KHangMan) that can be edited by hand and is easily usable with scripts

These are only some of the applications that the KDE community has to offer. For more information on the KDE Educational project visit http://kde.org/applications/education/

/dev/null

Enabling Projects

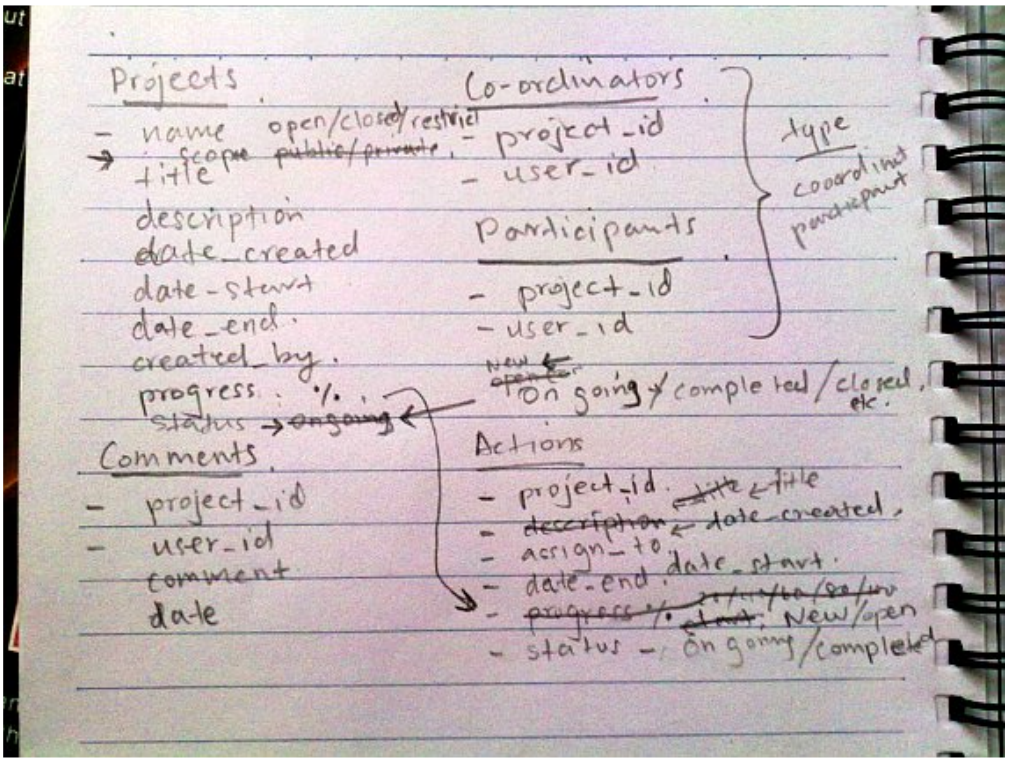
INASH Zubair

On one fine Friday, during mid February, me and Hussain got together to discuss about planning and organizing work and resources within MOSS. It's very pleasant to know that there are people who're concerned with a steady health of the organization as well as the community at the same time who think that the way to get to a level where everything is well managed and overseen is through planning. Hussain is one of those people who're very into organizing and planning things ahead of time so that things won't fall out of place without a sign.

The evening was mostly spent on the topic of community growth and engagement. We assumed that if tasks and projects were an aspect of the website which can be interactive and managed by the community, it would engage the community a little more. At the time of this writing, there are 62 registered members on the website, and we're assuming most of them have a direct relationship with free and open source software, and that figure is not small if we're looking at people with technical skills and knowledge and who have experience working in corporate environments.

We set out to plan and design the basics for a small function that would allow the creation and management of projects on the website. We would build it gradually phase by phase outlining the features for each milestone along the way. Although we didn't brainstorm little, at some point the whole component bloated to be a full stack project management system with Gantt charts and fully fledged reporting, etc.

Below is a picture of the initial components and their ERD diagram. As you can see it is very simple and we have removed most of the high level extra ideas for the time being.



Enabling Projects^2

The projects will come in three types: Open, Closed and Restricted, the differences being that an Open project will fully be publicly visible and open for participation from the public for all registered members on the website; a Closed project will be partially displayed to the public and participation will be through invitation or by requesting to join; and Restricted being completely hidden off from the face of the public and will only be accessible and visible to it's coordinators and members.

Projects will have comments and a project's participants will be able to leave comments on the project page. A project must at least have one coordinator, although participants can vary or can be none. The project will further be broken down by tasks which will outline it's individual bits and pieces of actions that will be required sequentially for it's progress and completion.

Once this is complete, it will gradually be open to all the members and they can start creating their own projects and participating in other non-restricted projects. Eventually we can have a nice map of MOSS related projects that are being executed here and there, disparately.

Projects does not have to be nature specific. It can be for planning of an event or perhaps the development of a software or even the progress of this specific function for the website. Anything that requires planning, coordination, actions and execution and which are related to MOSS and the community can somehow be hosted and managed here.

I'm hoping that if at the least this will help and enhance the level of coordination and the quality of work here amongst the members at present, it certainly will come as a major hand in connecting with the community and accounting for most of the things that happen in and around our society.

For starters, here's the phases and milestones that will be completed step by step and which will be rolled out one by one.

Enabling Projects[3]

Phase 1

- Creating and listing Open projects
- Set it's basic information such as the start and end dates and description.
- Set it's status manually through phases from On Going, Completed and Closed.

Phase 2

- Members can participate in Open projects, Coordinators can manage membership.
- Actions can be set and either assigned to or assigned by one self.
- Actions can also be managed by coordinators as well as participants by setting it's properties along with the progress of it.

Phase 3

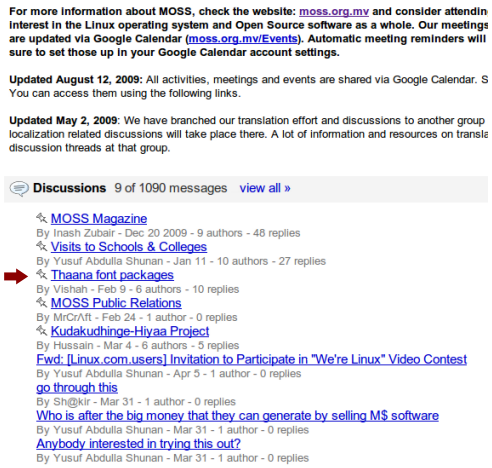
- Comment on projects.

So between each phase, there will be rigorous testing of those functions. Since this component is developed for the website, the development will be available for the public to see and track at [Github](http://github.com/inash/moss.org.mv). Once functions are rolled out expect to see announcements on the website or through the announcements syndication and I shall do follow up articles as well.

So if you would like to share your ideas, join our mailing list at http://groups.google.com/group/mlugmv and start discussing about it. I would love ideas and early feedback. Cheers.

INASH Zubair
9 March, 2010 12:52 AM

HOW TO
ADD DHIVEHI FONTS
on ubuntu


For more information about MOSS, check the website: moss.org.mv and consider attendin
interest in the Linux operating system and Open Source software as a whole. Our meetings
are updated via Google Calendar (moss.org.mv/Events). Automatic meeting reminders will
sure to set those up in your Google Calendar account settings.

Updated August 12, 2009: All activities, meetings and events are shared via Google Calendar. S
You can access them using the following links.

Updated May 2, 2009: We have branched our translation effort and discussions to another group
localization related discussions will take place there. A lot of information and resources on transla
discussion threads at that group.

Discussions 9 of 1090 messages view all »

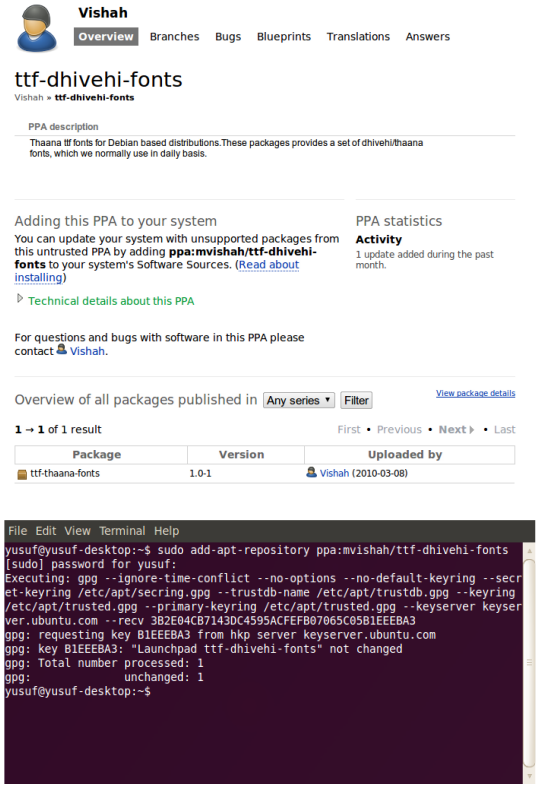
MOSS Magazine
By Inash Zubair - Dec 20 2009 - 9 authors - 48 replies
Visits to Schools & Colleges
By Yusuf Abdulla Shunan - Jan 11 - 10 authors - 27 replies
Thaana font packages
By Vishah - Feb 9 - 6 authors - 10 replies
MOSS Public Relations
By MrCrAft - Feb 24 - 1 author - 0 replies
Kudakudhinge-Hiyaa Project
By Hussain - Mar 4 - 6 authors - 5 replies
Fwd: [Linux.com.users] Invitation to Participate in "We're Linux" Video Contest
By Yusuf Abdulla Shunan - Apr 5 - 1 author - 0 replies
go through this
By Sh@kir - Mar 31 - 1 author - 0 replies
Who is after the big money that they can generate by selling M$ software
By Yusuf Abdulla Shunan - Mar 31 - 1 author - 0 replies
Anybody interested in trying this out?
By Yusuf Abdulla Shunan - Mar 31 - 1 author - 0 replies

On February 2010 Vishah started the ttf-dhivehi-font project by a post on the MOSS mailing list.

This gave birth to a deb file, which you can use to easily install dhivehi fonts on Debian based distributions.

http://mlugmv.googlegroups.com/web/dv-mv-fonts_1.0-1_i386.deb

Today the project is hosted and maintained via launchpad.net


Vishah

Overview Branches Bugs Blueprints Translations Answers

ttf-dhivehi-fonts

Vishah » ttf-dhivehi-fonts

PPA description

Thaana ttf fonts for Debian based distributions.These packages provides a set of dhivehi/thaana fonts, which we normally use in daily basis.

Adding this PPA to your system

You can update your system with unsupported packages from this untrusted PPA by adding **ppa:mvishah/ttf-dhivehi-fonts** to your system's Software Sources. (Read about installing)

Technical details about this PPA

For questions and bugs with software in this PPA please contact Vishah.

PPA statistics

Activity

1 update added during the past month.

Overview of all packages published in Any series Filter

View package details

1 → 1 of 1 result

First • Previous • Next • Last

Package	Version	Uploaded by
ttf-thaana-fonts	1.0-1	Vishah (2010-03-08)

File Edit View Terminal Help

```
yusuf@yusuf-desktop:~$ sudo add-apt-repository ppa:mvishah/ttf-dhivehi-fonts
[sudo] password for yusuf:
Executing: gpg --ignore-time-conflict --no-options --no-default-keyring --secr
et-keyring /etc/apt/secring.gpg --trustdb-name /etc/apt/trustdb.gpg --keyring
/etc/apt/trusted.gpg --primary-keyring /etc/apt/trusted.gpg --keyserver keyser
ver.ubuntu.com --recv 3B2E04CB7143DC4595ACFEFB07065C05B1EEEBA3
gpg: requesting key B1EEEBA3 from hkp server keyserver.ubuntu.com
gpg: key B1EEEBA3: "Launchpad ttf-dhivehi-fonts" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
yusuf@yusuf-desktop:~$
```

https://launchpad.net/~mvishah/+archive/ttf-dhivehi-fonts

This means on Ubuntu you can use the Ubuntu Software Center to install, update or remove the fonts.

To use the fonts from Personal Package Archive (PPA) you must first tell Ubuntu where to find the PPA.

For Ubuntu 9.10 (Karmic) and later open a terminal and enter the following command.

sudo add-apt-repository ppa:mvishah/ttf-dhivehi-fonts

Next you should tell your system to pull down the latest list of software from each archive it knows about, including the ttf-thaana-fonts PPA you just added. To do so issue the following command in a terminal.

sudo apt-get update

Now you are ready to install the fonts from the PPA either by using the following terminal command or Ubuntu Software Center.

sudo apt-get install ttf-thaana-fonts

This Magazine was created using FLOSS

Graphic Design

GIMP

http://www.gimp.org/

Layout Setting

Scribus

http://scribus.net/

Type Setting

OpenOffice.org

http://www.openoffice.org/

Operating System

Ubuntu 10.04 Lucid beta2

http://www.ubuntu.com/

Release License

Creative Commons

http://www.creativecommons.org/

Creative Commons is a nonprofit corporation dedicated to making it easier for people to share and build upon the work of others, consistent with the rules of copyright.

Creative Commons provide free licenses and other legal tools to mark creative work with the freedom the creator wants it to carry, so others can share, remix, use commercially, or any combination thereof.