Stealth Mode FOSS

Fouad Riaz Bajwa

Co-Founder & FOSS Advocate

FOSSFP - iFOSSF
International Free and open Source Software Foundation,
MI, USA.

www.ifossf.org

Scope

- Worst Security Threats
- Sharing Knowledge
- What makes FOSS secure?
- Development Security
- Platform Security
- Secure by Design & Secure by Default
- FOSS Community

Disclaimer

- **I am neither an expert in the Information Security domain nor do I have the relevant experience but I do have knowledge about security and that is what really matters.**
  - "Critical Thinking"
  - Knowledge Management (Implicit + Explicit)

Worst Security Threats?

- What are the worst information security threats today?
  - People?
  - Technology?
  - Internet?
  - Something else…….?

Worst Security Threats?

- **What about Knowledge?**
  - Positive or Constructive Perceptions
  - Negative or Destructive Perceptions
  - Neutrality

The 1st Worst Threat is.......

Being Dumb!

- Lacking an understanding of the operating environment thus cannot prevent security threats

The 2nd Worst Threat is…….

Being Dumber!

- Has the best tools in place but no knowledge of detection and prevention

The 3rd Worst Threat is…….

Being Dumbest!

- Considers Closed Source Software to be more secure then Open Source Software

The Final Worst Threat is…….

Being Insane!

- Consider they have absolute prevention in place?

Sharing Some Knowledge

- The Free and Open Source Software Community has the largest wealth of information and knowledge on Security related issues and shares it through the Internet/World Wide Web globally.
- Updated round the clock and in some cases by various concerned Governments and Defense institutions worldwide.

Free and Open Source Software

- Freely available for inspection by security professionals and enthusiasts throughout the world thus distributors ensure that any security vulnerabilities will be rapidly found and corrected

- Freely distributed to the community, distributors subject their services to the harsh realities of the IT World and receive constant feedback from thousands of users around the world in every imaginable academic, home, government and business setting.

- Resultant is secure and home-office-enterprise ready FOSS platforms.

Information Security

- Even a million tools cannot keep your data, software and hardware secure
- Information Security problems cannot be solved, they must be managed
- To manage Security problems, you must have a dedicated manager the right man for the job

The 3-Layers of Security

- Prevention
- Detection
- Response

* Schneier, B. Secrets and Lies: Digital Security in a Networked World. 1 edition. John Wiley & Sons.ISBN:0471253111. August 14, 2000. http://www.amazon.com/Secrets-Lies-Digital-Security-Networked/dp/0471253111

What Makes FOSS Secure?

- Knowledge and Management
  - Secure Design, Development and Administration Processes
  - The relationship between security and knowledge is what makes FOSS secure.
  - A community continuously endeavoring to keep FOSS as secure as possible

Development Security

- Is FOSS Development and Closed Development Security two different areas?

A result of

- Secure design
- Source code auditing
- Quality developers
- Design process
- All of the above play into the security of a project, and none of these are directly related to a project being open or closed source

Platform Security

- FOSS follows various fundamental rules of good security practice, knowledge and practice
- Should be Secure by Default – Unix/OpenBSD
- Should be Secure by Design - Linux Kernel

Linux is a registered trademark of Linus Torvalds

Secure by Default

- **The OpenBSD concept of shipping an operating system** "Secure by Default"!
  - OpenBSD is designed to be secure from the minute you finished installing.
  - Why, because all source code is audited.

Secure by Design

- **Linux Kernel and Distributions**
  - The Kernel is the most secure piece of software in GNU/Linux and what isn’t secure is of course not really a Linux problem.
  - Distributions have threats because distributors that build them sometimes configure them to have most services running and do not set them up with security in mind.

Securing Linux

- **SELinux - Enabling Security on Linux**
  - Developed by NSA and several vendors including Red Hat, Tresys, IBM, HP, and by individual FOSS developers.
- **Engarde Secure Linux -**
  - For secure Internet Services
- **AppArmour -**
  - Application level security proprietary source product for SuSE Linux by Novell – Prevents exploitations

Security Enhanced Linux

- Created by National Security Agency NSA
- Implements **mandatory access** control using **Linux Security Modules (LSM)** in the Linux kernel, based on the principle of **least privilege.**
- Not a Linux distribution, a set of modifications that can be applied to Unix-like operating systems, such as Linux and BSD.

SELinux

- – Shows mandatory access controls that can confine the actions of any process, including a super-user process, can be added into Linux.
- – Requires a system-wide "policy" configuration that describes what kinds of controls to enforce.
- – A large example policy is provided with NSA's SELinux releases to provide a starting point.

SELinux Features

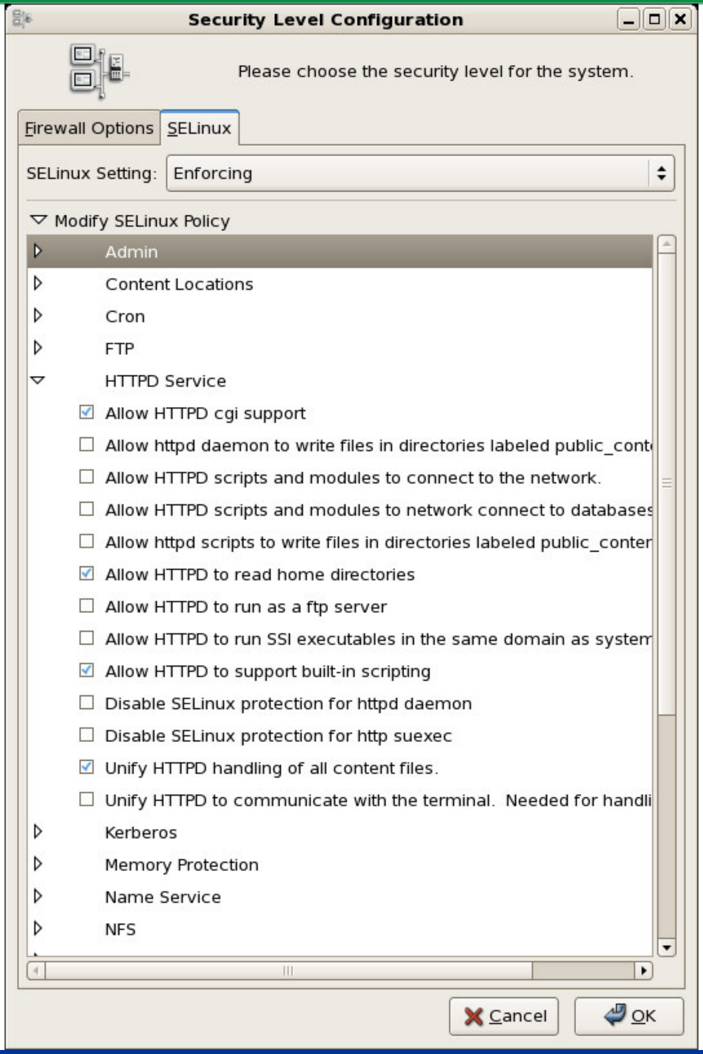
– Clean separation of policy from enforcement & well-defined policy interfaces. Independent of specific policies, policy languages, specific security label formats and contents

– Individual labels and controls for kernel objects and services

– Separate measures for protecting system integrity (domain-type) and data confidentiality

– Very flexible policy controls over process initialization, inheritance, program execution, file systems, sockets, messages, network interfaces, over use of "capabilities"

SELinux Security Configuration



Security Level Configuration

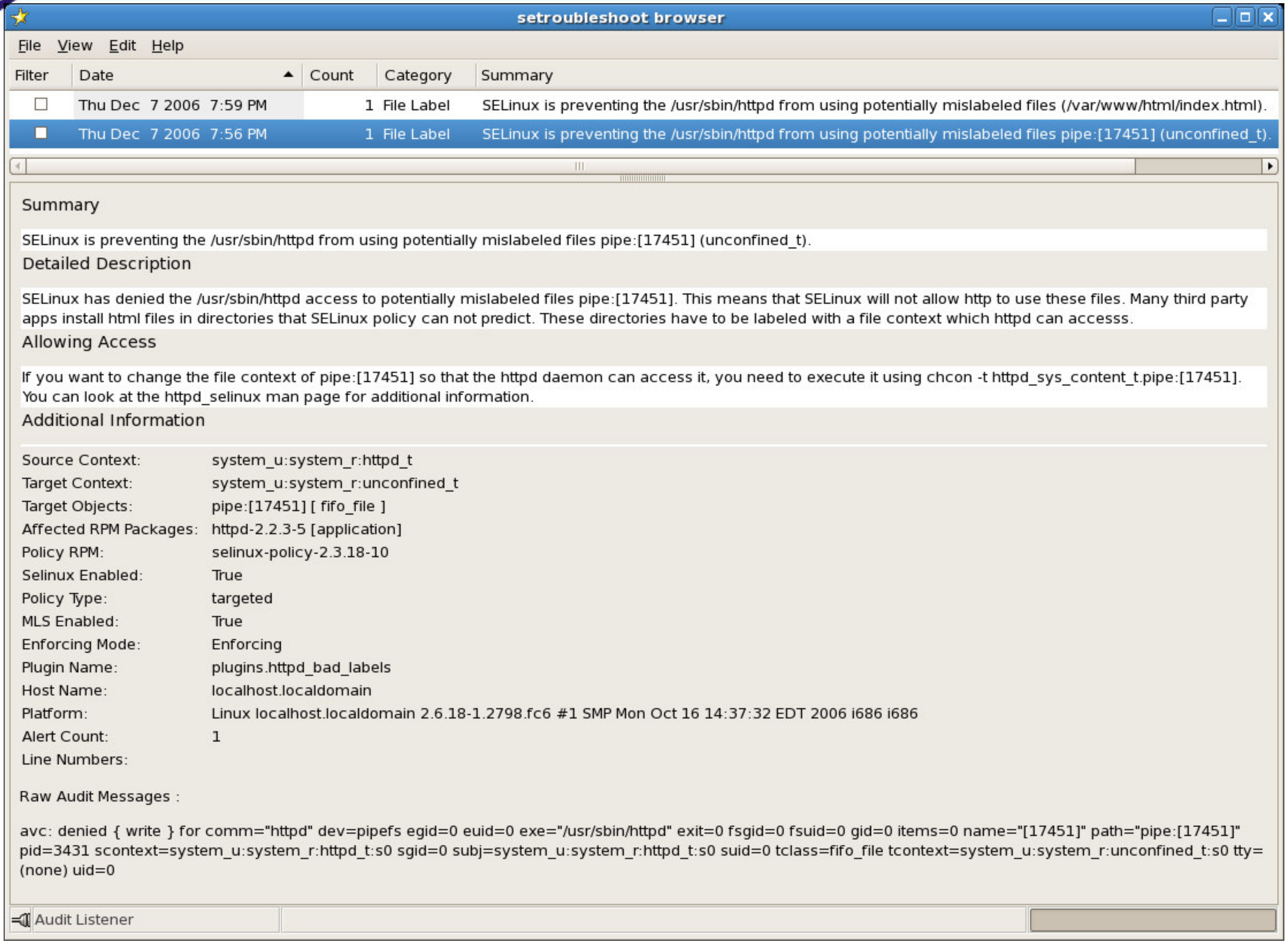
Please choose the security level for the system.

SELinux Setting: Enforcing

Modify SELinux Policy

- Admin
- Content Locations
- Cron
- FTP
- HTTPD Service
  - ☑ Allow HTTPD cgi support
  - □ Allow httpd daemon to write files in directories labeled public_conte
  - □ Allow HTTPD scripts and modules to connect to the network.
  - □ Allow HTTPD scripts and modules to network connect to databases
  - □ Allow httpd scripts to write files in directories labeled public_conter
  - ☑ Allow HTTPD to read home directories
  - □ Allow HTTPD to run as a ftp server
  - □ Allow HTTPD to run SSI executables in the same domain as system
  - ☑ Allow HTTPD to support built-in scripting
  - □ Disable SELinux protection for httpd daemon
  - □ Disable SELinux protection for http suexec
  - ☑ Unify HTTPD handling of all content files.
  - □ Unify HTTPD to communicate with the terminal. Needed for handli
- Kerberos
- Memory Protection
- Name Service
- NFS

SELinux – Troubleshooting Utility



Filter	Date	Count	Category	Summary
□	Thu Dec 7 2006 7:59 PM	1	File Label	SELinux is preventing the /usr/sbin/httpd from using potentially mislabeled files (/var/www/html/index.html).
□	Thu Dec 7 2006 7:56 PM	1	File Label	SELinux is preventing the /usr/sbin/httpd from using potentially mislabeled files pipe:[17451] (unconfined_t).

Summary

SELinux is preventing the /usr/sbin/httpd from using potentially mislabeled files pipe:[17451] (unconfined_t).

Detailed Description

SELinux has denied the /usr/sbin/httpd access to potentially mislabeled files pipe:[17451]. This means that SELinux will not allow http to use these files. Many third party apps install html files in directories that SELinux policy can not predict. These directories have to be labeled with a file context which httpd can accesss.

Allowing Access

If you want to change the file context of pipe:[17451] so that the httpd daemon can access it, you need to execute it using chcon -t httpd_sys_content_t.pipe:[17451]. You can look at the httpd_selinux man page for additional information.

Additional Information

Source Context:	system_u:system_r:httpd_t
Target Context:	system_u:system_r:unconfined_t
Target Objects:	pipe:[17451] [fifo_file]
Affected RPM Packages:	httpd-2.2.3-5 [application]
Policy RPM:	selinux-policy-2.3.18-10
Selinux Enabled:	True
Policy Type:	targeted
MLS Enabled:	True
Enforcing Mode:	Enforcing
Plugin Name:	plugins.httpd_bad_labels
Host Name:	localhost.localdomain
Platform:	Linux localhost.localdomain 2.6.18-1.2798.fc6 #1 SMP Mon Oct 16 14:37:32 EDT 2006 i686 i686
Alert Count:	1
Line Numbers:	

Raw Audit Messages :

```
avc: denied { write } for comm="httpd" dev=pipefs egid=0 euid=0 exe="/usr/sbin/httpd" exit=0 fsgid=0 fsuid=0 gid=0 items=0 name="[17451]" path="pipe:[17451]"
pid=3431 scontext=system_u:system_r:httpd_t:s0 sgid=0 subj=system_u:system_r:httpd_t:s0 suid=0 tclass=fifo_file tcontext=system_u:system_r:unconfined_t:s0 tty=
(none) uid=0
```

SELinux for Distributions

- **Distributions carrying SELinux userspace patches, labeling the files and necessary policy changes:**
  - Red Hat/Fedora
  - Debian
  - Gentoo
  - SuSE
  - Slackware
  - Ubuntu

* **http://selinux.sourceforge.net/**

SELinux on other distros

- Both Red Hat and SuSE provide a SE-Linux support in their modified kernel versions that is customized to work with their particular distros.

- This involves adding customized code that provides performance, stability and sometimes security enhancements to the vanilla kernel.

EnGarde Secure Linux

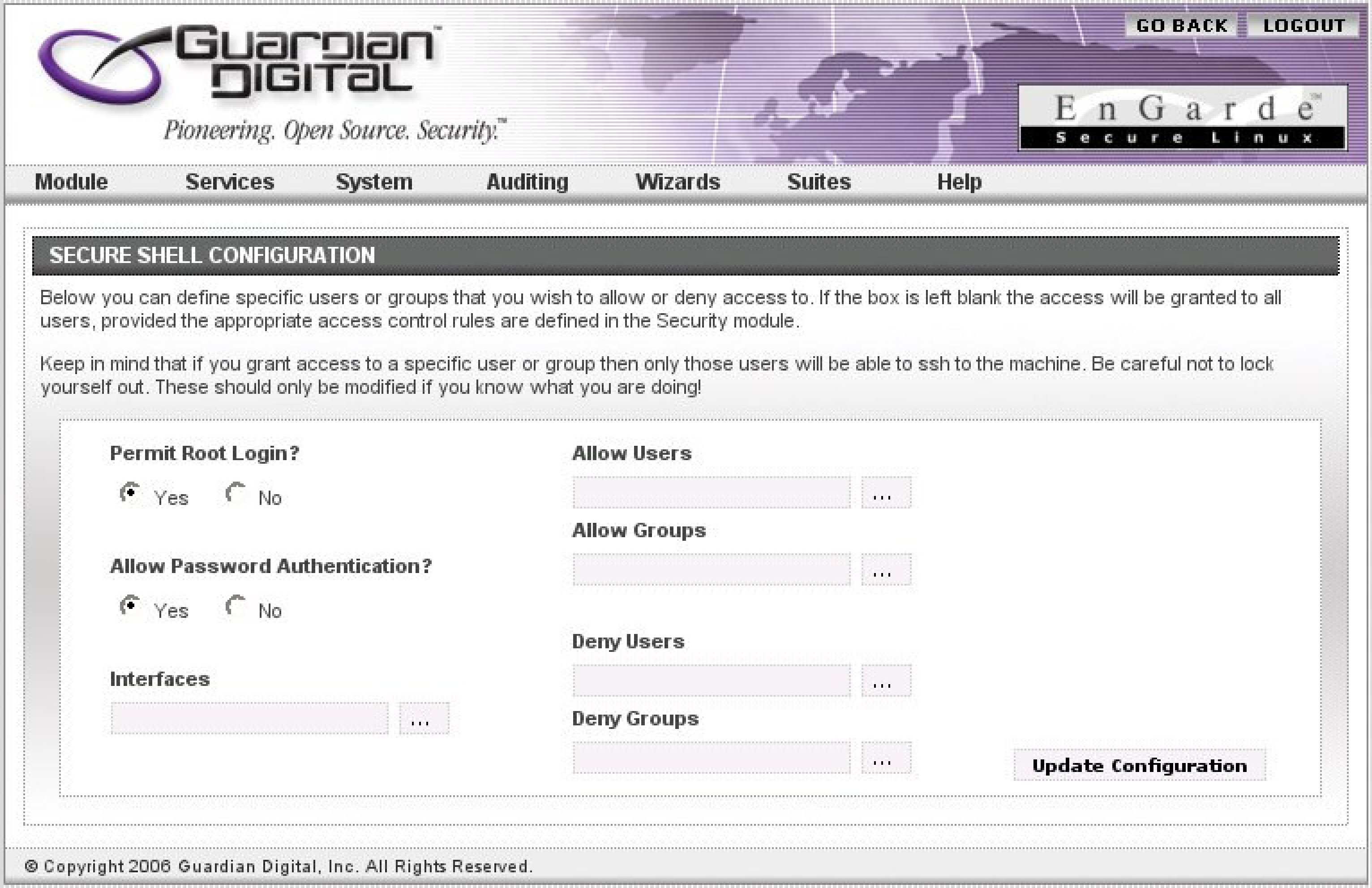
- Highly-secure OS built on SELinux policies incorporating security at all levels and includes tools like Postfix, BIND, and the LAMP stack.

- Offers simplified and secure remote management through a custom browser-based system of administration, the Guardian Digital WebTool.

EnGarde Secure Linux

- Builds on kernel-level security policies and incorporates a wide range of proven security tools like host and network intrusion detection.
- Delivers security for any Internet service, from Web and mail services to FTP and proxy services. Provides free access to updates and security notices through the Guardian Digital Secure Network.

Guardian WebTool



SECURE SHELL CONFIGURATION

Below you can define specific users or groups that you wish to allow or deny access to. If the box is left blank the access will be granted to all users, provided the appropriate access control rules are defined in the Security module.

Keep in mind that if you grant access to a specific user or group then only those users will be able to ssh to the machine. Be careful not to lock yourself out. These should only be modified if you know what you are doing!

Permit Root Login?

● Yes ○ No

Allow Password Authentication?

● Yes ○ No

Interfaces

Allow Users

Allow Groups

Deny Users

Deny Groups

© Copyright 2006 Guardian Digital, Inc. All Rights Reserved.

Keeping in Mind

- For both Open and Closed Source Software Systems, some risks are different, but as long as you're aware of them, you can manage them.

- The first and foremost defense against security threats will be first knowledgeable and then qualified developers and security professionals.

Conclusion

- **The problem for FOSS in Pakistan:**
  - Lack of not “expert” but knowledgeable FOSS Developers and Administrators.
  - This may lead to plenty of unsecured data and Linux machines both on the net and offline.
  - We need knowledgeable people, thus….

Be Part of the FOSS CoL-CoE

- **Join us at FOSS Meet-ups**
  - A fortnightly meeting/gathering of members of the Pakistani FOSS Movement and professionals from the IT Industry to discuss and share FOSS/Linux Knowledge.
  - These meetings are known as FOSS & Linux Club Meetings.
- **http://tech.groups.yahoo.com/group/foss_meetups**

FOSS-PDR Security Task Force

- – Civil Society Security Initiative
- – Maintain a mailing list and repository of knowledge on Prevention, Detection and Response *(PDR)
- – Discussions during FOSS Meet-ups
- – Online Meet-ups on Freenode IRC?
- – Suggestions

Reference Links

- **NSA SELinux:**
  - – http://www.nsa.gov/selinux/index.cfm
- **SELinux for Distributions**
  - – http://selinux.sourceforge.net
- **EnGarde Secure Linux**
  - – http://www.engardelinux.org
- **AppArmour**
  - – http://www.novell.com

Q & A Session

Thank You!