QuickStart Guide

Introduction to grsecurity

This guide will lead you through the process of downloading, configuring, installing, and maintaining grsecurity. This guide was written to be as clear as possible and to provide only the details necessary to get you up and running with grsecurity. For more in-depth information, links to outside resources will be located where appropriate.

grsecurity Philosophy

There is a philosophy behind the project that governs the kind of features you see and will see in grsecurity. The project is based on the belief that:

- Security cannot be solved in a single layer
- Additional security, if not user friendly, is useless
- You should be able to protect any third-party software you have installed, not only the software that is provided by your distribution
- Humans are often the weakest link in security

grsecurity Overview

For a complete list of grsecurity's features, please visit http://www.grsecurity.net/features.php . Grsecurity includes several main features:

- Buffer overflow exploitation prevention from the PaX project (http://pax.grsecurity.net)
- Role-Based Access Control (RBAC)
- Randomization of Process IDs and in the TCP/IP stack
- Restricted viewing of processes
- Change root (chroot) hardening
- /tmp race vulnerability protection

Conventions Used in this Document

The following writing conventions will be used throughout the rest of the document.

Read these notes very carefully to avoid possibly dangerous results.

Pay careful attention to these notes, as the information will be very important to the current topic.

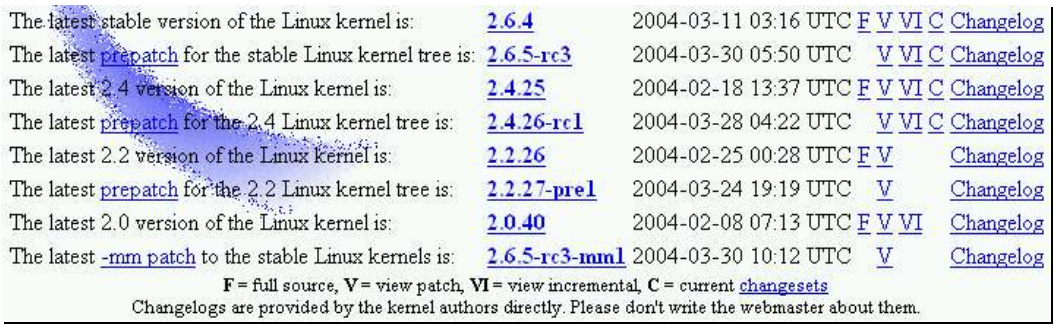
```
This font will be used in cases where you have to
enter commands into a shell.  Enter only the text
in this font into the shell.
```

Pre-Installation Tasks

The following instructions will lead you through the process of downloading all the components necessary for using grsecurity on your system, as well as how to patch your kernel for use with grsecurity. Download each component to the same directory on your computer.

Downloading the Linux Kernel

Point your browser to http://www.kernel.org. Locate the image below on your screen. For the purposes of this document, we will be installing the "latest 2.4 version of the Linux kernel." Click on the "F" link to download the kernel.



The latest stable version of the Linux kernel is:	2.6.4	2004-03-11 03:16 UTC	F V VI C Changelog
The latest prepatch for the stable Linux kernel tree is:	2.6.5-rc3	2004-03-30 05:50 UTC	V VI C Changelog
The latest 2.4 version of the Linux kernel is:	2.4.25	2004-02-18 13:37 UTC	F V VI C Changelog
The latest prepatch for the 2.4 Linux kernel tree is:	2.4.26-rc1	2004-03-28 04:22 UTC	V VI C Changelog
The latest 2.2 version of the Linux kernel is:	2.2.26	2004-02-25 00:28 UTC	F V Changelog
The latest prepatch for the 2.2 Linux kernel tree is:	2.2.27-pre1	2004-03-24 19:19 UTC	V Changelog
The latest 2.0 version of the Linux kernel is:	2.0.40	2004-02-08 07:13 UTC	F V VI Changelog
The latest -mm patch to the stable Linux kernels is:	2.6.5-rc3-mm1	2004-03-30 10:12 UTC	V Changelog

F = full source, V = view patch, VI = view incremental, C = current changesets
Changelogs are provided by the kernel authors directly. Please don't write the webmaster about them.

Figure 1: kernel.org download page

Downloading grsecurity

Now point your browser to http://www.grsecurity.net. Click on the "download" link. For the purposes of this document, we will be installing the latest development release of grsecurity for the 2.4 kernel. Click on the bold filename to download the patch.

For security reasons, it is recommended that you download the signature file for grsecurity and verify the patch you download with gpg. eg:

```
gpg --verify ./grsecurity-2.0-
2.4.26.patch.sign
```

Downloading gradm

When downloading gradm, the administration utility for grsecurity's RBAC system, you must download the version that matches the version of the grsecurity patch you downloaded. Gradm is located on the same download page as

grsecurity. The recommendation above about verifying the download also applies here with gradm.

Patching Your Kernel with grsecurity

This section will assume the version of grsecurity we downloaded is 2.0 for the 2.4.26 kernel. If the version you downloaded differs from this, adjust the below commands accordingly. Change to the root user and execute the following commands in the directory you downloaded the files to.

```
tar –jxf ./linux-2.4.26.tar.bz2
patch –p0 < ./grsecurity-2.0-2.4.26.patch
```

Configuration and Installation

In this section, you will configure both the Linux kernel and grsecurity. Pay close attention, as an improperly configured kernel may not boot.

Configuring the Linux Kernel

Since a description of every configuration option in the Linux kernel would be far out of the scope of the document, and systems are different in terms of hardware configuration, for novice users a generic configuration is recommended. Download the configuration file at http://grsecurity.net/generic-config and place it in the same directory that grsecurity and gradm were downloaded to. Since your kernel is unpacked and patched, we can change into the directory holding the kernel's source code (eg. linux-2.4.26 if 2.4.26 is the version of the kernel you downloaded). Execute the following command:

```
make menuconfig
```

The following menu should then be visible:

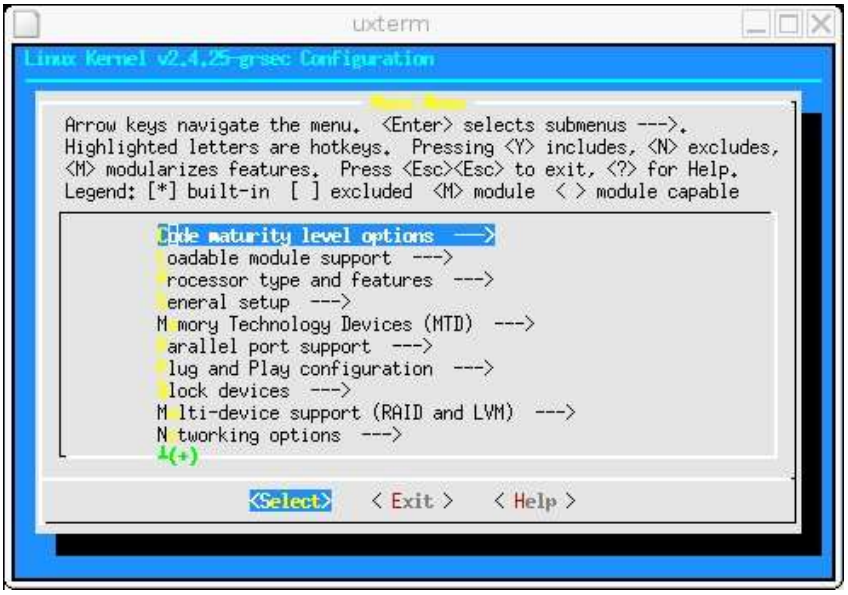


Figure 2: Kernel configuration menu

Scroll down to the bottom of the menu using the down arrow key. Press enter on the "Load an Alternate Configuration File" entry. Then enter the pathname you downloaded the files to, followed by "generic-config." If you downloaded the files to /usr/src, the filename entered would be /usr/src/generic-config. Press enter, then scroll up using the up arrow key to the entry named "Grsecurity."

By configuring your kernel manually, you can increase security by having a smaller amount of privileged code running on the system all the time. For information on how to configure your kernel manually, visit http://www.digitalhermit.com/~kwan/kernel.html.

Configuring grsecurity

Now that you are in the grsecurity menu, press the space bar to enable grsecurity for your system. You will see a new menu labeled "Security level." Select it using the down arrow key. This document will outline the steps to configure a customized grsecurity. Customizing grsecurity allows you to enable more features and tailor the installation to your needs. Press enter to choose the customized security level. You should then see a screen similar to the following:

Figure 3: grsecurity configuration menu

To view all configuration help for each grsecurity option, including what features are present in each security level, please visit http://grsecurity.net/confighelp.php . It is necessary to review this information before using your new grsecurity-enabled system.

Since this is a quick-start guide, each feature will not be discussed. Rather, an overview of each submenu will be provided and a recommended configuration will be presented.

PaX Control

This section allows you to specify the methods recognized to mark binaries on your system for use with PaX. Configure this section as follows:

- Support soft mode OFF
- Use legacy ELF header marking ON
- Use ELF program header marking ON
- MAC system integration NONE

Address Space Protection

This section allows you to configure PaX, as well as a small number of other related features. PaX is a separate project, but is included in grsecurity as it is a crucial component of grsecurity's security philosophy. PaX provides buffer overflow exploitation prevention and randomization of how a process is laid out in memory, both of which serve as an incredibly effective protection against attackers. Configure this section as follows:

- Enforce Non-executable pages ON
- Paging based non-executable pages ON
- Segmentation based non-executable pages ON
- Emulate trampolines OFF
- Restrict mprotect() ON
- Address Space Layout Randomization ON
- Randomize kernel stack base ON
- Randomize user stack base ON
- Randomize mmap() base ON
- Randomize ET_EXEC base ON
- Deny writing to /dev/kmem, /dev/mem, and /dev/port ON
- Disable privileged I/O OFF
- Remove addresses from /proc/pid/[maps|stat] ON
- Hide kernel symbols OFF

Role Based Access Control Options

This section allows you to configure options related to the RBAC system in grsecurity, including how many failed authentications can occur within a given period of time until authentication is locked. Configure this section as follows:

- Hide kernel processes ON
- Maximum tries before password lockout 3
- Time to wait after max password tries, in seconds 30

Filesystem Protections

This section allows you to configure features related to the filesystem, including /proc restrictions, which allow a user to view only the processes they are running, /tmp race protections, and change root restrictions that greatly increase the security of a change root (chroot) in an application. Configure this section as follows:

- Proc restrictions ON
- Restrict to user only OFF
- Allow special group ON
- GID for special group 1001
- Additional restrictions ON
- Linking restrictions ON
- FIFO restrictions ON
- Chroot jail restrictions ON
- Deny mounts ON
- Deny double-chroots ON
- Deny pivot_root in chroot ON
- Enforce chdir("/") on all chroots ON
- Deny (f)chmod +s ON
- Deny fchdir out of chroot ON
- Deny mknod ON
- Deny shmat() out of chroot ON
- Deny access to abstract AF_UNIX sockets out of chroot ON
- Protect outside processes ON
- Restrict priority changes ON
- Deny sysctl writes in chroot ON
- Capability restrictions within chroot ON

Kernel Auditing

This section allows you to configure various auditing options. That is, these features do not provide any inherent security, but provide useful information to the administrator that may be security relevant. Configure this section as follows:

- Single group for auditing OFF
- Exec logging OFF
- Resource logging ON

- Log execs within chroot OFF
- Chdir logging OFF
- (Un)Mount logging OFF
- IPC logging OFF
- Signal logging ON
- Fork failure logging ON
- Time change logging ON
- /proc/<pid>/ipaddr support OFF
- ELF text relocations logging OFF

Executable Protections

This section allows you to configure options dealing with process creation and what binaries can be accessed on the system. Configure this section as follows:

- Enforce RLIMIT_NPROC on execs ON
- Dmesg(8) restriction ON
- Randomized PIDs ON
- Trusted path execution OFF

Network Protections

This section allows you to configure options related to randomization of the TCP/IP stack and restrictions on what kinds of sockets users can use. Configure this section as follows:

- Larger entropy pools ON
- Truly random TCP ISN selection ON
- Randomized IP IDs ON
- Randomized TCP source ports ON
- Randomized RPC XIDs ON
- Socket restrictions OFF

Sysctl support

This section allows you to enable sysctl support for grsecurity. Enabling this would allow you modify the configuration of most grsecurity features at runtime. Because it defaults to disabling all features at startup, requiring you to modify your system initialization scripts, it is recommended that you not enable this feature.

Logging options

This section allows you to specify flood rate and burst rate settings for all logs produced by grsecurity Configure this section as follows:

- Seconds in between log messages (minimum) 10
- Number of messages in a burst (maximum) 4

Installing the New Kernel

To compile and install your new kernel, enter:

```
make dep bzImage modules modules_install install
```

During installation of the kernel, it will ask if you want to update LILO (or grub). Enter “Y” at this point, and the system will be updated to boot your new kernel. You may now issue the command:

```
/sbin/reboot
```

to reboot your system with the new grsecurity-enabled kernel.

Role-Based Access Control Quick-Start

Now that you are running your new grsecurity-enabled kernel, it is highly recommended that you use the RBAC system grsecurity provides.

RBAC Overview

Since the general strategy of grsecurity is "detection, prevention, and containment," the RBAC system is key to the containment component. Grsecurity's RBAC system allows you to grant only the privileges necessary for a process or user to accomplish their tasks. Unlike other systems, grsecurity's RBAC system provides a functional, human-readable, centralized configuration file, and does not require much manual configuration.

Installing gradm

To install gradm, the administration utility for the RBAC system, change to the directory you downloaded gradm and grsecurity to earlier. We will assume the version of gradm downloaded is 2.0 for this example. Execute the following commands to compile and install gradm:

```
tar -zxf gradm-2.0.tar.gz
cd gradm2
make
make install
```

Basic Commands

To enable the system:

```
gradm -E
```

To disable the system:

```
gradm -D
```

To authenticate to the administration role:

```
gradm -a admin
```

To de-authenticate from the administration role, either exit your shell, or enter:

```
gradm -u admin
```

Full-System Learning

Full-system learning will generate a least privilege policy for your entire system that anticipates normalized usage. In other words, it is not necessary to run the learning mode for weeks and use every single utility on your system several times in every possible combination. The learning mode will anticipate this usage while still enforcing a secure policy. Through graph and heuristic analysis, a secure policy is generated. A few basic rules are followed when generating the policy. If a process uses special "root" privileges, accesses the Internet, or modifies

important files or directories, it is marked as a privileged process and segmented from the rest of the system. The learning mode is designed to be as easy to use as possible. To begin full system learning, enter:

```
gradm -F -L /etc/grsec/learning.log
```

Then use your system normally. It may be necessary to run the system for more than a day so that time-based applications such as cron can be recognized and profiled.

Do not perform any administrative tasks while running in learning mode. This includes starting/stopping system services, adding or removing users from the system, or adding or removing new software. These kinds of tasks should only be performed under the administration role once the learning phase is over. Remember that "root" can no longer be trusted, so assume root is the attacker and do not do anything you would allow an attacker to do.

When you decide to end the learning phase, enter:

```
gradm -F -L /etc/grsec/learning.log -O /
etc/grsec/acl
```

You will now be able to enable the RBAC system with your new learned policy.

Maintaining grsecurity

Though grsecurity's design goal is to require little maintenance after installation, you should know a few things about maintaining your grsecurity-enabled system.

Monitoring Log Files

It is important to monitor your log files to look for intrusion attempts. A log from PaX about an execution attempt in a network service you are running signifies that an attacker was attempting to exploit an unpatched vulnerability in the network service. It would be wise to make sure you are running the latest version of the service, and if so, investigate the intrusion from the IP provided with the log. Take note that some logs from grsecurity are not evidence of an intrusion and are simply providing useful information. For instance, seeing a log about a signal being sent a certain process is not evidence of an intrusion and is not caused by grsecurity.

Troubleshooting

If you execute an application and see "Killed" immediately after and a log on your system similar to:
PAX: execution attempt in: /usr/lib/tls/libGL.so.1.0.5336, 22669000-22677000 0004b000
PAX: terminating task: /usr/bin/khelpcenter(khelpcenter):4143, uid/euid: 1001/1001, PC: 2266ef20, SP: 5b404d10
PAX: bytes at PC: b8 c8 ff ff ff e9 2b 73 fe ff b8 cc ff ff ff e9 31 73 fe ff
PAX: bytes at SP: 2264437a 20dc8c20 225b64f8 20dc8e58 5b404d54 5b404d54 20dbe0de 00000001 5b404da4 5b404dac 5b404d98 20db2f3b 5b404da0 20db3270 20dc8c20 00000013 20dc8e58 5b404d94 20dbe1ca 225b64f8
The binary is using code that is not written properly, and thus PaX must be disabled on it. To disable PaX for a single binary, you must first download chpax from http://pax.grsecurity.net/. After compiling and installing chpax, run the following command:

```
chpax -spmr /path/to/binary
```

In this case, we would run chpax against /usr/bin/khelpcenter.