

The Big Ol' Ubuntu Security Resource

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2007-06/msg00442.html>

- *From:* "Jose Manuel Tella Llop" <jmtella@xxxxxxxxx>
 - *Date:* Sat, 2 Jun 2007 16:45:10 +0200
-

Ubuntu is billed as ultra-secure, but its default install has flaws. Here are the mods you need to make to protect your system.
Brian Provost

If you've recently switched from Windows to the Linux distribution Ubuntu, you've probably experienced a decrease in spyware — and malware in general — on your system. But although Ubuntu is billed as the ultra-secure solution, you should know that even though Ubuntu's default install has its flaws, like every other operating system.

To combat these weaknesses, IT Security has prepared a guide to help you close your system's backdoors and protect you from some of the common Ubuntu exploits. Look at this big ol' Ubuntu security resource as an introductory guide to securing Ubuntu, along with a list of the software you'll need to stay protected.

Getting Started

Surprisingly, many new Ubuntu users fail to take the most basic steps towards securing their install, even when they know better. Thankfully, the list of critical changes isn't long. Making modifications may not excite you as much as, say, adding a whole new security program, but these simple changes will go a long way to closing up Ubuntu's security weaknesses.

Modifying Default Settings

The first set of basic critical changes requires you to modify three insecure default system settings:

a.. Reconfiguring shared memory

Load your favorite text editor, open the file `"/etc/fstab"` and add the following line of code:

```
tmpfs /dev/shm tmpfs defaults,ro 0 0
```

b.. Disabling SSH root login

Load your favorite text editor, open the file `"/etc/ssh/sshd_config"` and add change the following line of code:

```
PermitRootLogin yes
```

to

```
PermitRootLogin no
```

c.. Limiting access to the "su" program

Open the terminal by clicking "Applications" selecting "Accessories" and choosing "Terminal." From there enter the commands:

```
sudo chown root:admin /bin/su sudo
```

```
chmod 04750 /bin/su
```

Enabling Automatic Security Updates

Having made the three most critical default system settings changes, you have better ensured that your Ubuntu install will start out relatively secure. But keeping it that way means being vigilant about updating your system. Because so many of us forget to update regularly, enabling automatic security updates is one surefire way to make sure it gets done.

To enable automatic security updates, click on "System" select "Administration" and choose the "Software Sources" menu. From there select the "Internet Updates" tab and enable "Check for updates automatically" (specify "Daily"). Now every time Ubuntu issues a new security release you will be notified via the "Update Manager" icon in the system tray. From there it's up to you to click the icon and allow the Update Manager to download and install the files.

Securing the Home directory

The final critical change we recommend, is that you protect your personal documents by securing your home directory. The easiest way to do this is by clicking "Applications" selecting "Accessories" and choosing "Terminal."

From there enter the command:

```
chmod 0700 /home/username (replace username with the name you use to login to your computer).
```

Now that you've successfully made these basic system setting modifications, you're ready to move on and start installing software that protects your system from being compromised.

Essential Security Installs

Unlike the Windows operating system, the Ubuntu Linux distribution is not ultra vulnerable to widespread virus and spyware infections, therefore the style of security used to protect one's machine is slightly different than that of a typical Windows machine.

Instead of spending hundreds of dollars on sophisticated firewalls, spyware blockers and intrusion detection and prevention systems, Ubuntu users simply have to install several free programs that protect the kernel from

exploits, prevent the execution of malicious code and keep programs and users from accessing areas of the computer outside of their designated access level.

Important Software

To keep your computer secure, install the following software:

- a.. grsecurity – A complete security suite for protecting Linux's kernel.
- b.. PaX – The most critical piece of grsecurity, prevents memory exploits. (Comes standard with grsecurity, you only need to install this if you have no intention of installing grsecurity.)
- c.. Pro Police – IBM's solution for protecting against stack smash attacks.
- d.. DigSig – Verifies the integrity of executables via user defined digital signatures before running it. If a program is modified without your consent the digital signature changes and DigSig denies the program the ability to run.

Bootup Security

An often overlooked yet highly vulnerable area of computing is protection for machines while they're booting up. While simply keeping unauthorized users from having access to your computer is the best policy, sometimes that isn't possible. Thus this guide, over at the UbuntuForums, gives detailed instructions for protecting your computer while it's booting up.

The steps involved in this security measure are a bit more complex than the skillset of the average user, and it requires a small amount of scripting, so we recommend that you only attempt to perform this security measure if you're really comfortable with Ubuntu, and Linux in general.

Second Level Security Software Installs

Congratulations, by this point you have completed the mandatory steps for a baseline securing of your Ubuntu install. You can now feel reasonably comfortable in the security of your install, but there are certainly still some lingering vulnerabilities. At this point it's up to you whether you want to take your system's security to the next level by integrating a few more applications of your choice.

Rootkit Protection

Ahh yes rootkit, the ultimate swear word to a Linux user. Although this guide is designed to prevent attackers from installing rootkits and backdoors onto your machine in the first place, breakdowns can occasionally happen. Thus it's a good idea to regularly scan for rootkits using the following software to make sure that your computer hasn't been compromised.

- a.. chkrootkit – Scans your computer for rootkits, worms and LKM trojans.
- b.. Rootkit Hunter – Excellent tool for detecting rootkits.

Antivirus

I know what you're thinking, antivirus?...This is Linux! However true that may be, it is still important to provide protection for all inbound and outbound files you might be transmitting in order to protect the less than

fortunate Windows computers you might come in contact with.

- a.. Clam AntiVirus – One of the most popular UNIX based antivirus solutions. Works well with email gateways.
- b.. AVG Anti-Virus – Free version of a popular commercial virus scanner.
- c.. BitDefender – On demand command line/shell script scanner.
- d.. Panda Antivirus – Uses sophisticated software to remove viruses from workstations connected to a Linux server.

Firewall

Installing and configuring an efficient firewall is a great way to keep attackers out. The stricter your rule-set and security policies are, the less likely it is that an attacker will find a way to exploit your system.

- a.. Firestarter – Versatile user friendly firewall.
- b.. SmoothWall – Highly configurable and extremely powerful network firewall solution.
- c.. HardWall Firewall – Iptables based packet filterer.
- d.. Firewall Builder – Generates rule sets for popular firewalls including iptables, ipfilter and pf.
- e.. BullDog – Very restrictive iptables based firewall. Recommended for advanced users only.

Network Tools

These tools are essential for monitoring and securing your network.

- a.. Nagios – Complete network monitoring suite.
- b.. Network Mapper – Uses IP packets to scan the network and determine various security information on the available hosts and network nodes.
- c.. Wireshark – Comprehensive tool for monitoring and analyzing network protocols.
- d.. Nessus – The definitive solution for scanning networks for vulnerabilities.
- e.. EtherApe – Graphical network monitoring suite.
- f.. tcpdump – Simple yet powerful tool for network monitoring.
- g.. tcptrace – Analyzes tcpdump output.

Miscellaneous

In addition to the above resources, here are a few other programs we recommend for getting the most out of your computing experience.

- a.. Snort – The leading open source solution for intrusion prevention and detection.
- b.. OpenSSH – Allows you to secure transfer data to remote hosts.
- c.. OpenVPN – Secure virtual private network.
- d.. strongSwan – IPsec based virtual private network.
- e.. Kismet – Wireless network detector, sniffer and intrusion detection system.
- f.. GNU Privacy Guard – A superb command line encryption and digital signature tool.
- g.. TrueCrypt – Allows you to create virtual encrypted disks.
- h.. Thunderbird – Mozilla's secure email client.

One Last Note

Remember your computer (and network for that matter) can only be secure as the users allow it. Failing to use strong passwords, falling victims to social engineering scams, installing software without first verifying its integrity and over using the root account are all common ways to have your network compromised. To have a truly safe system, you must be committed to

The Big Ol' Ubuntu Security Resource

having a secure mindset and you must layout strict guidelines for the people using your computer and or network. Otherwise one of them might misplace a password one day, and your entire client database or purchasing records will be stolen the next.

Sources

For more information on securing Ubuntu, check out the sources we used when writing this article.

- a.. Security Guides
- b.. Proactive Security
- c.. Installing Security Tools
- d.. Security on Ubuntu
- e.. Locking Down Ubuntu
- f.. Security Analysis Tools

<http://www.itsecurity.com/features/ubuntu-secure-install-resource/>