Global Information Assurance Certification Paper

More Secure @home using Linux

Hans Lie

September 15, 2001

Introduction

I invested in a new PC at home and wanted to get a faster connection, than the current isdn setup I have today. Since I am starting to work with security I also wanted to find a good solution to protect the data I have. I have not decided what type of connection I will get, but it will be cable, adsl or wireless, so I have to make a flexible solution. It is my intent to stay connected to the Internet 24x7. I could have used one of the personal firewalls for Windows, but I feel more comfortable with a less graphical environment, where I have more control over what is happening. It forces me to know more about how things are interconnected. The best part of it, it's more fun. At least I thought so.

Threats

So what is it I try to protect, why bother?

Well, I have a small network with a few computers, mostly Linux, a Windows 98 computer, and a laser printer. I use them for several things:

Web surfing, On-line Banking and trading, mail and news, private economy programs, personal letters, genealogy research, store family pictures, contact information and connect my computer to the corporate LAN.

I believe several of these are common to a lot of people.

Today people have pretty speedy computers at home, and more connect them up to the Internet 24*7*365, through high-speed connections. Most of the day these computers are idle, and waiting for something to do. It is very tempting for a lot of people to break in to these computers, and use them for whatever cause they believe in. Some use them as a launch pad for other break-ins, making it harder to trace back the attack to the originator. Other uses could be as part of a bigger task, like a distributed cracking of passwords, or finding out if there is life in outer space. Whatever reasons people have, the default setup of today's computers makes it pretty easy to breaking, unless the owners take some measures to protect the computers.

I have asked myself, why people go online without protecting their computers. Most people lock up their home, when they leave it. I believe it is a basic trust in computers, and lack of knowledge.

Some years ago, viruses started to flow around. After some years, corporates realized

they had to protect themselves, and they did it in the perimeter, and on the servers. They started to inform the employees about the threat and said they should check all floppies for viruses. What we see today is that most people have anti-virus software programs on the desktops. Every new pc bought today is protected, with software, but the users don't update it, so they are not protected for long.

Seems like the same cycle is coming with firewalls. First businesses started putting up firewalls. Now more and more people have the same speedy connection at home, and the need also arises here. Many magazines now have started to write about the need to install personal firewalls at home, but will the consumers listen and act?

"*For consumers, no matter how many times you indicate to someone that they ought to have antivirus software and a firewall installed, they have to be in the right mindset or they don't do it*"

-- Eric Hemmendinger, research director for information security, Aberdeen Group.

According to the Cert Advisory: CA-2001-20, about home security

```
      This year, we have seen a significant increase in activity
      resulting in compromises of home user machines. In many cases,
      these machines are then used by intruders to launch attacks
against
      other organizations. Home users have generally been the least
      prepared to defend against attacks. Many home users do not keep
      their machines up to date with security patches and workarounds,
      do not run current anti-virus software, and do not exercise
caution
      when handling email attachments. Intruders know this, and we
have
      seen a marked increase in intruders specifically targeting home
      users who have cable modem and DSL connections.
```

Some of the information I keep in my computer I would like to keep secret. It should be available when I need them, and should not be altered without my knowledge. This brings us to the three pillars of security, which is fundamental in information security:

C-I-A triad

Confidentiality	Keeping information private or secret, and to avoid disclosing information to those who don't need it. It can be achieved by use of encryption, separate it from publicly available information or use access control to determine who gets to see the information.

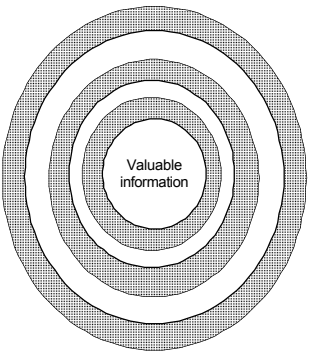
Integrity	Keeping the information complete and unaltered, keep a record of all changes of the information, and make sure only authorized personnel are allowed change it.
Availability	Having the information available to those who need it, when they need it.

What are the threats to my computers?

Physical	The computers are all situated in my condominium, and a burglar could just go in and grab the boxes.
Virus	There are a lot of mails circulating with attached viruses.
Script kiddies	People running scripts or programs to probe computers for vulnerabilities, exploiting these vulnerabilities to gain access to computer systems. Little knowledge required doing this, and the programs are easy to obtain. Once access is acquired they can install 'back-doors', to make it easier to return to the system.
Vandals	Wants to make visible damage to my data.

Protection

In order to protect my valuable information I will apply a principle known as defense-in-depth.



If you look at the figure, you see that we place the things we want to protect in the middle. Around the center we put successive (gray) layers of protection. Even though we use several means of protecting the data, does not make it impossible to get to the information, but it sure makes it harder. The concept of in-depth-in-depth is not limited to information only, but also useful in other areas, e.g. physical security, and other thing you might want to protect.

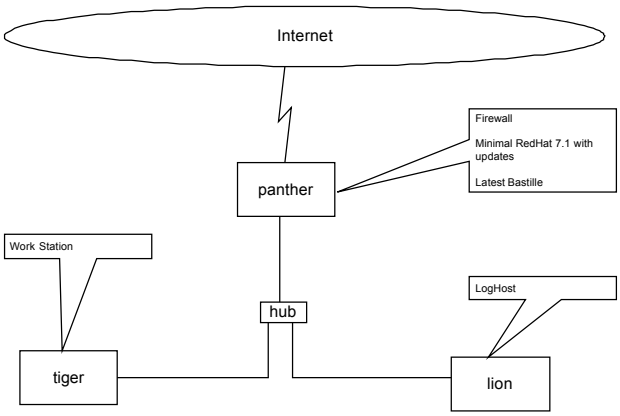
Another important thing is to know-your-system: If you know how your system behaves, it is much easier to tell if something is wrong. Ideally you should use some time every day to get to know it.

Implementation

Of course I could have used some sort of Windows type of firewall, but I kind of hate the feeling of not know what is happening on the system. Well I guess I have worked to long with UNIX, to even thing about using Microsoft stuff. I didn't want to pay too much either and I have a pile of old pentiums I could use, they should be good enough for the tasks.

I'll show you a picture of what I try to do. I have a network at home, with a few hosts. This is a simplified view, since I also got a Laser Printer and a few other hosts. I want

to be ready to get a speedier connection, as soon as it's available in my neighborhood. I hope to get a wireless connection, since they provide the best speed, but if it takes to long I will consider cable or adsl as well. Originally I hoped to use floppyfw, as my firewall, but I have not been able to verify, that they supports wireless connection.



When I started to implement the security I decided to go for RedHat-7.1 as a basis. The reason for this is that I have used RedHat for years, and it is the one Linux distribution I know best. If we take a look at the firewall, panther, I installed a customized version of RedHat-7.1. I installed as few packages as I could, in the spirit of 'small is beautiful'. It is also easier to get to know a smaller system, and there are fewer vulnerabilities to exploit. I installed the updates I could find, and keep checking for updates, to be released. There are lots of bugs ready to be exploited, and I want to get rid of them if I can. There are some tools, like autorpm for updating the systems automatically, but I like to check the system myself before installing the updates. I will probably look into a solution that will notify me when there is anything new.

There were some factors I knew I wanted in a new system, all part of my in-depth-in-depth strategy:

- Netfilter/IP Tables - to block all traffic except what I wanted to allow
- Network Address Translation (NAT) - to hide the ip-setup of my internal network to the world, so they can't scan the ports of my internal hosts.
- tcp_wrappers - to limit which ip-addresses are allowed to connect to the services I allow into the firewall
- A few user accounts with solid passwords, remove the rest
- ssh - only allow remote login to the system via secure channels. Disable telnet and ftp.
- Integrity of files on the system - tripwire and rpm -V
- syslog - remote logging to a dedicated host.
- ntp - to synchronize the time to a accurate time-source
- Use the SANS: Securing Linux: Step-by-step - to check other things I have forgotten. Get a copy of that paper, if you don't have it already.
- Need a regular backup of the system as well.
- Updated Anti-virus software, on MS Windows boxes.

I remembered hearing, a while ago, about Linux software that was supposed to tighten up the system. It was called Bastille, so I decided to take a closer look at it.

1) Bastille Linux

This is what they say about themselves:

The Bastille Hardening System attempts to "harden" or "tighten" the Linux operating system. It currently supports Red Hat and Mandrake systems. We attempt to provide the most secure, yet usable, system possible. The project is run by Jon Lasser, Lead Coordinator and Jay Beale, Lead Developer, and involves a number of developers, beta-testers and concept-creators. Bastille Linux was developed with several major goals:

Comprehensiveness	Bastille Linux draws from every available major reputable source on Linux Security. The initial development integrated Jay Beale's existing O/S hardening experience for Solaris and Linux with most major points from the SANS' Securing Linux Step by Step, Kurt Seifried's Linux Administrator's Security Guide, and countless other sources.
Instructiveness	Bastille Linux has been designed to educate the installing administrator about the security issues involved in each of the script's tasks, thereby securing both the box and the administrator. Each step is optional and contains a description of the security issues involved.
Community	Once the initial development was near complete, we brought the effort to the developers of the Bastille Discussion mailing list. Further, we began soliciting outside suggestions and testing. The script was GPL'd promptly and the Specification shared.

a) Features

- Packet Filters: IP Tables/Chains
- NAT
- Disables SUID programs
- Users: Password aging, Restrict root-login to local ttys at console, Password Protect single-user mode, and Restrict console-login to a few accounts
- Restrict use of cron to administrative accounts only (/etc/cron.allow)
- Password protect boot loader (LILO)
- Disable Ctrl-Alt-Del rebooting
- Setup a default deny on tcp-wrappers.
- Deactivates telnet and ftp
- Setup extra logging to tty's and files
- Log to a remote loghost

- Process accounting - log who's doing what, when
- Deactivate routing daemon
- Restrict sendmail

And even more. Bastille adapts to what is installed on the system. If you don't have a dns-server installed on the host, you will not get questions about securing the server.

Bastille has a lot of what I originally wanted and even more. It made the setup of the firewall much easier than I had expected.

b) Installing

It is really easy to install, just download three rpm-packages from www.bastille-linux.org and install them. You have to decide if you want to configure the firewall, using X-windows or the console (higher security). Depending on which interface you choose.

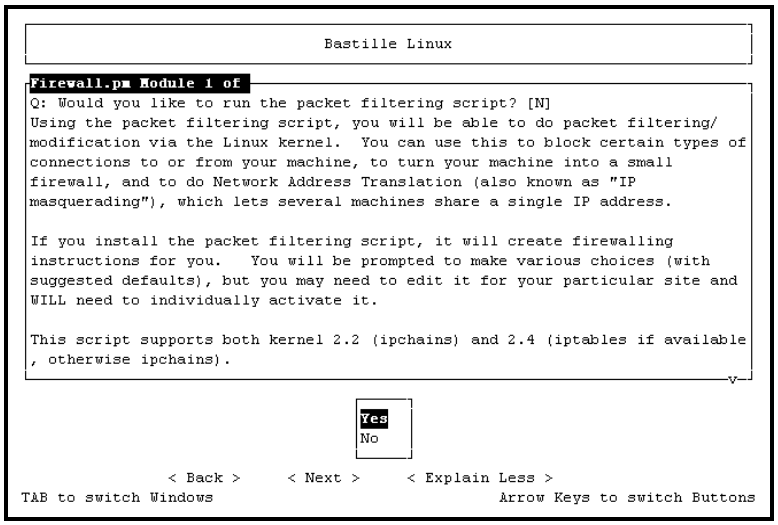
- Main RPM (Bastille)
- Using Console
  - Bastille-Curses-module
  - perl-Curses
- Using X-windows
  - Bastille-Tk-module
  - perl-Tk

I choose the console version, since I don't want X-windows on the firewall.

c) Configuring

After the packages are installed you just have to start: **InteractiveBastille**

Here is a screenshot from the configuration of Bastille:



The questions you have to answer are explained well, and it also gives you guidance it you are in doubt. If you have to give other input than yes or no, the examples are excellent.

At the end it asks if you want to use the firewall, and start it at every boot of the host. Then you're all set.

2) Other measures

Bastille did most of what I wanted, but I still lacked file integrity check. For this there are two things I do to check if anything has changed.

a) tripwire

is bundled with RedHat, so it's just to install the package.

- Then run /etc/tripwire/twinstall.sh, and follow the direction.
- Once that is finished you have to edit the policy file: /etc/tripwire/tw-pol.txt. In this file you setup which files you want to check regularly, and which alarm level to set if it has changed.
- Now you are able to apply the policy, using: twadmin -m P /etc/tripwire/tw-pol.txt
- Initialize tripwire using: `tripwire -init`
- Check the host for changes using: `tripwire --check`, this is done daily by cron, so all you have to do is to check the mail.
- If you have installed new files, and want to acknowledge the changes: `tripwire --update -r <report file>`, find the latest report-file in /var/lib/tripwire/report

b) rpm –V <package>

a way to check that the files in a package has not changed

c) ssh

in addition to using ssh instead of telnet I, used two additional measures secure the sshd on the host:

- Limit from which ip-addresses I can login to the firewall (/etc/hosts.allow)
- Only allow a few users to login via ssh. root is not one of them.

There is an option in /etc/ssh/sshd_config, called AllowGroups who let me say that only users of a certain Unix-group is allowed to login to the system. There is another option to disallow root to login: PermitRootLogin

Conclusion

To state is simple:

"If you are not connected to the Internet, then you don't need a firewall. Otherwise, you do"

"If you loose your data and identity, the ultimate impact on your life is real"

According to Gregor Freund, CEO of ZoneLabs

Check out Cert: "Home Network Security", for more information about threats and actions you can do to protect your computer.

It has been brought to my attention, that there are some problems with the wireless protocol 802.11b. Seems like it is possible to discover the 'secret' key that is used to encrypt the data. Check the reference for more information.

One thing is for sure, nothing is secure. If you use defense-in-depth, relying on several means, you are better protected than many others.

References

- RedHat http://www.redhat.com/
- Bastille Linux http://www.bastille-linux.org/
- IP Tables http://netfilter.samba.org/
- Home and Small Office http://www.sans.org/infosecFAQ/homeoffice/homeoffice_list.htm
- Step-by-Step Security Guides http://www.sansstore.org/
- floppyfw http://www.zelow.no/floppyfw/
- trinux http://trinux.sourceforge.net/tools.html
- Usefull security Articles http://www.bastille-linux.org/jay/security-articles-jjb.html
- autorpm http://www.kaybee.org/~kirk/html/linux.html
- Home PC users wake up to need for firewalls http://news.cnet.com/news/0-1006-200-6994590.html?tag=prntfr
- Home Network Security http://www.cert.org/tech_tips/home_networks.html
- tripwire http://www.tripwire.org/
- Wireless protocol problems http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
  http://www.powerbookcentral.com/columns/knowles/052101.shtml
  http://www.zdnet.com/special/stories/wireless/0,10676,5095205,00.html