Unix-like OS Systems

A presentation to the
St. Louis Linux Users Group
On “Diversity in OS Systems”
Dave Forrest
17 MAR 2016

UNIX©

Unix (trademarked as UNIX) is a family of multitasking, multiuser computer operating systems that derive from the original AT&T Unix, developed in the 1970s at the Bell Labs research center by Ken Thompson, Dennis Ritchie, and others.

UNIX©

Initially intended for use inside the Bell System, AT&T licensed Unix to outside parties from the late 1970s, leading to a variety of both academic and commercial variants of Unix from vendors such as the University of California, Berkeley (BSD), Microsoft (Xenix), IBM (AIX) and Sun Microsystems (Solaris). AT&T finally sold its rights in Unix to Novell in the early 1990s, which then sold its Unix business to the Santa Cruz Operation (SCO) in 1995, but the UNIX trademark passed to the industry standards consortium, The Open Group, which allows the use of the mark for certified operating systems compliant with the Single UNIX Specification (SUS). Among these is Apple's OS X, which is the Unix version with the largest installed base as of 2014.

GNU (Gnu is Not Unix)

In 1983, Richard Stallman announced the GNU project, an ambitious effort to create a free software Unix-like system; "free" in the sense that everyone who received a copy would be free to use, study, modify, and redistribute it. The GNU project's own kernel development project, GNU Hurd, had not produced a working kernel, but then ...

Linux©

in 1991 Linus Torvalds released the Linux kernel as free software under the GNU General Public License. In addition to their use in the Linux operating system, many GNU packages – such as the GNU Compiler Collection (and the rest of the GNU toolchain), the GNU C library and the GNU core utilities – have gone on to play central roles in other free Unix-like systems as well.

Distributions

Linux distributions, consisting of the Linux kernel and large collections of compatible software have become popular both with individual users and in business.

Popular distributions include Red Hat Enterprise Linux, Fedora, SUSE Linux Enterprise, openSUSE, Debian GNU/Linux, Ubuntu, Linux Mint, Mandriva Linux, Slackware Linux, and Gentoo.

Many Distros

There are truly many distributions today. A site that watches what's happening and reports is: http://distrowatch.com/

In the week ending March 2 a couple of dozen different distribution updates were recorded with Mint, Debian, and Ubuntu (in that order) getting the hits on the site.

Unique IP sources hits per day by DistroWatch:
(1) Mint 3137 (2) Debian 1918 … (274) GuixSD 3

BSD Unix

A free derivative of BSD Unix, 386BSD, was released in 1992 and led to the NetBSD and FreeBSD projects. With the 1994 settlement of a lawsuit brought against the University of California and Berkeley Software Design Inc. (USL v. BSDi) by UNIX Systems Laboratories, it was clarified that Berkeley had the right to distribute BSD Unix for free, if it so desired. Since then, BSD Unix has been developed in several different product branches, including OpenBSD and DragonFly BSD

Diversity Abounds

Newcomers to the Linux® operating system are often bewildered by the many different flavors of systems being used and confused as to actual operating systems used on this fine Unix flavored system developed in the '90's by a computer science student that has since become a standard used by so many different entities for a variety of end purposes.

This or That?

Part of the misunderstandings arise from factions that have arisen that seem to maintain that their particular implementation is “The Holy Grail” and is the only true solution and none of the others is “worth a darn!” (really meaning: “My boss only allows DistroX” or “I only know DistroY”).

Working with life

This is a perfectly natural sentiment in any working environment; our system which I have spent innumerable hours (months – or years) learning is the only “real” answer to our now joint projects. … (Pause for a story)

But we learn from the traumatic events when jobs change or our smoothly running company buys or is bought by another group of plants and sales forces and the cycle repeats.

netfilter

As an example let's look at netfilter firewall applications. Netfilter is a system utility developed on Linux® to control the input and output internet packet flow in a machine; what kind of packet is allowed into the machine and what and where will they end up. The concept is clear but the implementation is quite varied. A quite good presentation by Elvir Kuric of HP is here:

https://ekuric.files.wordpress.com/2011/07/pf_iptables.pdf

A Firewall example

As an example I will write about netfilter firewall applications. Netfilter is a system developed on Linux® to control the input and output internet packet flow in a machine; what kind of packet is allowed into the machine and what and where will they end up. The concept is clear but the implementation is quite varied. A quite good presentation by Elvir Kuric of HP is here:

https://ekuric.files.wordpress.com/2011/07/pf_iptables.pdf

BSD ipfilter

In BSD based machines a typical firewall uses a different implementation than Linux: Instead, FreeBSD offers a choice of three kernel level firewalls: PF, IPFILTER, & IPFW.

I use the Linux netfilter and find the BSD dialect a tad strange and unfamiliar. But I'm sure folks are here to explain it if necessary.

Here are the rules for each to allow an outside connection to an internal Secure Shell server (SSH)

Vernaculars

With PF:

“pass in on $ext_if inet proto tcp from any to ($ext_if) port 22”

With IPFILTER/IPFW:

“pass in on $ext_if proto tcp from any to any port = 22”

With Linux iptables:

“-t INPUT -i $ext_if -p tcp -m state –state NEW --dport 22 -j ACCEPT”

iptables

Iptables comes by default installation within all Linux® distributions. On Debian, Red Hat, CentOS, it is present as the default packet handling system configured to allow almost no input from outside machines and no need to take any action regarding installation.

Also it's possible to install from source code. The option with pre-compiled packages can be more convenient.

Best?

Which is better? Both iptables and pf are very reliable and excellent solutions for firewalls. The choice is made by the OS we have installed (some GNU/Linux® =iptables, Open|Net|Free BSD =pf). PF has very similar (if not same) syntax as IPFilter on HP-UX system. It is necessary to understand TPC/IP protocol stack prior to starting firewall implementation.

It is easy to see the tendency to favor the system familiar to the administrator. Let's all agree on that!

Residential Users

I used the firewall illustration above because it introduced a topic that is primarily of interest to the administrator of the site using the machine. Most residential users do not run “services” that respond to inquiries originating outside of their premises. Many newcomers to our group are in this category of users and don't need to get into the technical subjects of system “hardening” or providing services such as web sites that serve information to the general public

They are looking for a reliable system that allows them to surf the web, use an internet mailing program, or run a personal financial system to track their tax information. We have had subjects presented on basic systems that fit into this area and address these basic concerns.

A recent presentation on how to keep information about one's personal information private comes to mind. It is not usually in one's thoughts that looking at a web page describing cute little dogs exposes an interest in dogs that may be of interest to a provider of dog grooming products and gives the company providing the access a customer name or address to target with advertising. Such has built the large companies like Google or Facebook who target those lists in a variety of ways for fairly substantial fees.

Administrative Users

But a portion of our membership is also interested in the server market. Servers are the web presence or information sites that listen on an internet address and act on the information sent with the inquiry and respond by processing and preparing the necessary response. This activity is fraught with risk of infection by undesirable processes and uses carefully constructed programs to insure that as few as possible ill results occur.

Usually professional technical savvy individuals have concocted these programs but even the gurus have stumbled at times. Many of our presentations are aimed to those who are so employed and may not be of interest to the residential membership. However, the interaction of those folks as they extol the superior actions of their each chosen tools can be most entertaining to all.

Unix-like OS Systems

Ah yes! The beauty of an open field such as is offered by the Unix/Linux family of operating systems at its most controversial heart!

But it does provide us with an opportunity to meet, discuss, and learn about alternate ways of “Skinning the cat”.

Questions?