



Newsletter #3

Table of Contents

Editorial

by MsMittensp. 3

Creating a Linux Distro Part I, II and III

by Andrew J. Benniestonp. 4

Hacker Periodic Table of Elements

submitted by psychosqueep. 7

Espionage and the Art of Information Warfare

by Echo5p. 8

The list command (ls)

by blackmaskp.11

Security Auditing Part II

by Remote_Access_p.18

Seek and Ye Shall Find.. Maybe

by Zigar_p.19

MsMittens' Editorial

Never say it's too quiet. I had a conversation with someone in IRC recently. I commented how quiet the Security/Hacking front seemed to be. As will often happen, someone will come along and make things more interesting for you. Today, I learned of the newest worm to grace our bits and bytes of the Internet: Benjamin. Not a fancy name. Not an unusual name. Very plain. Benjamin.

This new worm has opened an interesting idea for me when I discussed it with my students in class today.

The Benjamin worm was created as a method to go against the existing Kazaa users, particularly against software piracy distributors and child porn distributors. (<http://www.viruslist.com/eng/viruslist.html?id=49790>). It is apparently a "pilot test" if you will. Let's see what happens kind of idea. The worm basically infects the "victim" when they download a file (usually hidden as a popular form of pirated software or some type of porn). Once infected, the virus puts itself in the shared files folder of Kazaa and makes itself available for download so it can replicate. In addition, it then opens up multiple Internet Explorer windows, all attempting to access one site. IE remains permanently open, constantly attempting to connect to the site. It is interesting that the site that was used for the massive explorer pop-ups as part of the worm (<http://benjamin.xww.de/>) was shut down due to "massive abuse". Which certainly highlights the adage of "One born every minute".

Here's the big risk with this: the code for this worm will probably be available shortly. It wouldn't be that hard to modify it so that it's not noticed as much (aka massive pop-ups in IE) and with this modification set up a situation whereby these "innocent victims" become zombies. The new wave of DDoS (Distributed Denial of Service) would make MafiaBoy's little romp look like a kindergarten activity. To control thousands of machines easily due to the greed of many would be the easiest social engineering exercise to date.

I suspect that there will be more of these worms appearing as it becomes very evident as to how easy it is to manipulate users. Firewalls would be ineffective against this activity from the point of view of the "victim" in that users usually give full access for Kazaa to go out as well as Internet Explorer. Anti-virus manufacturers again will be the main defenders of this kind of thing plus vigilance by users. We, as security defenders, have to convince our users that Kazaa and like tools are not that beneficial, especially with the transmission of "warez" and "child porn".

This issue of the AO Newsletter covers off a wide variety of topics from Theory to better *nix understanding. Enjoy!

P.S.: We are looking for articles for Newsletter #4. Deadline will be June 26, 2002. Remember, that this newsletter is what the community makes it. Be part of it. ;)

Creating A Linux Distribution - Part I

Andrew J. Bennieston

1. Downloading The Linux Kernel Source
2. Choosing What To Build Into Your Kernel
3. Compiling The Kernel
4. Choosing A Boot Loader
5. [Part II - Installation]
6. [Part III - Adding Extras]

Kernel source can be obtained from www.kernel.org The latest stable version is 2.4.18 For this task, you require the Full source (denoted by an 'F') <http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.18.tar.gz> Whilst this is going, go make yourself a large cup of coffee... The download is about 28MB, so you'll have plenty of time, unless you're one of those lucky people on broadband.

Once the kernel source has downloaded, you'll need an existing Linux system on which to build it. Extract the kernel files from the tar.gz file, into a directory on your Linux machine, e.g. /kernel. Then do:

```
# cd /kernel/linux-2.4.18
# make xconfig
```

This command will run, and eventually take you to the X Kernel config tool. You should choose the functionality you will need to go into the kernel, and do not use modules at this point (configuration after primary installation will allow for extra modules to add support for new hardware etc). As a bare minimum, you'll need the drivers for ext2fs, FAT (To use Windows/DOS formatted floppy disks), generic CPUs, IDE Hard drives, ATAPI CDROM etc. You should know the basic config of your system... On top of this, you might want to include SCSI, USB or other support, which will obviously depend on your specific requirements (if you use a USB keyboard, for example, USB support is pretty much essential). Once you have chosen your kernel, you can progress to the build stage. Remember to save your settings in X Config

To compile the kernel, run these commands:

- make dep
- make bzImage
- make modules
- make modules_install

After all of this has run (this may take some time depending on processor speed. it took a good half hour on my old P120), you will be left with a compressed Linux kernel image in /kernel/linux-2.4.18/arch/i386/boot You should copy this image, and any associated modules (You were advised not to use modules for this!) to a working directory where you can get at them easily for the next stages.

There are many boot loaders for Linux, you will need to choose one for your new Linux system. Some are linked below:
LILO: http://software.freshmeat.net/projects/lilo/?topic_id=139 GRUB: <http://www.gnu.org/software/grub/> XOSL: <http://www.xosl.org/>

Creating A Linux Distribution - Part II

Andrew J. Bennieston

1. Partitioning
2. Formatting
3. Installing
4. Setting Up A Boot Loader
5. Restarting
6. Adding Extras [Part III]
7. Configuring [Part IV]

In order to do this, you'll need a partitioning program. <http://www.gnu.org/software/parted/http://www.users.intercom.com/~ranish/part/> Using one of the above, or your favourite partition program (I believe Partition Magic has ext2 support?), you should partition a hard disk as follows, for your new Linux installation:

LabelSizeType/boot10 MB to 20 MB**ext2fs[swap]**2 x System RAM**Linux Swap/Rest of Drive****ext2fs**

Save the changes to the partition table, and restart the computer.

GNU Parted can also format your partitions as Linux ext2fs and Linux Swap. Refer to the documentation, <http://www.gnu.org/software/parted/USER>

Boot from a Linux disk, or from a working system on a different hard drive or partition, and do the following:

1. Copy the boot loader and any files it needs to **/boot**
2. Copy the kernel image to **/boot**
3. Copy any kernel modules to **/boot** (I did warn you not to use kernel modules for now)
4. Create any files in your essential filesystem, such as **/usr** and **/home** directories, **/root**, **/etc**
5. Put "essential" tools (passwd, init, etc.) into their respective places (download the source, compile it, put it in the right place)
6. Create the **/dev/** directory and it's contents (best way is to mirror it from another, existing, Linux distro)

As for the specifics for step 5, I don't know. In theory nothing is essential, beyond the kernel and a boot loader, but you won't be able to do much with it. I'd also recommend putting a shell or two in, so that you can add extras and configure more easily. <http://www.gnu.org/software/bash/bash.html> <http://www.tcsh.org/>

This step will depend on your chosen boot loader. It is advantageous to have a working Linux system on which to modify config files and transfer across to your new build as and when they're needed. You will need to add your kernel image to the boot loader, and you will also get the opportunity to create options to boot Windows/DOS, floppy disks (*/dev/fd0*)

Hit the reset button, and choose your new kernel at the Boot loader prompt!!

Creating A Linux Distribution - Part III

Andrew J. Bennieston

1. Gnu Tools
2. The X Windowing System
3. Apache
4. Sendmail
5. KDE
6. GNOME
7. The GIMP
8. Other Useful Applications & Extras

These include gcc, the C compiler, amongst other tools. <http://www.gnu.org/order/ftp.html>. You may need a different Linux machine on which to compile these, or you can copy the relevant tools directly from an existing machine.

XFree86 can be downloaded from: <http://www.xfree86.org/http://ftp.xfree86.org/pub/XFree86/4.2.0/> You'll need the Gnu compiler and associated tools in order to make XFree86. After XFree86 has been installed, you should run FX86Setup or XF86Config to set up and configure your particular graphics card and monitor settings. The latest XFree86 is 4.2.0, although XFree86 v4 has been known not to work on some graphics cards, in which case you'll need XFree86 3.

The Apache HTTPd server can be downloaded from <http://httpd.apache.org/> You can download either a binary or source distribution... You might as well get the source and compile it on your system, it'll invariably work better! I think you'll also need inetd as well, in order for Apache to start properly and work as it should do. The latest Apache version is 1.3.24

The ever popular Sendmail can be downloaded from www.sendmail.org I will not begin to go into configuring Sendmail, since it is one of the most confusing and complicated packages on the modern Linux system, and I favour procmail, personally. Procmail can be downloaded from <http://www.procmail.org/>

KDE is one of two competitors for taking over the Linux desktop, the other being GNOME. KDE is available from <http://www.kde.org/> It can be downloaded as a series of .RPM files (In which case you'll need rpm, from <http://www.rpm.org/>) or as source code to compile

yourself. Once compiled and installed, it is extremely easy to set up, and comes with its own window manager, kwm.

GNOME has been around a little longer than KDE, and some prefer it to its younger rival. GNOME has the advantage of being completely free, whereas KDE is free only for personal use (As far as I know - I read that somewhere!). <http://www.gnome.org/> It is also easy to configure, and anyone who is considering making their own Linux distribution should have no problems setting up GNOME or KDE.

The Gnu Image Manipulation Program. The world's best, free, graphics tool. It is available as a binary download from www.gimp.org There is also a Windows version of The GIMP, available from the same place. It does, obviously, require X and a window manager such as KDE or Gnome.

- Nmap www.insecure.org/nmap
- X MultiMedia System www.xmms.org
- Linuxconf http://freshmeat.net/projects/linuxconf/?topic_id=89,149,154,253,150
- And, of course, any other packages you could possibly ever want to use... www.linuxapps.com is a good place to search for Linux software!

[www.firestormuk.cjb.net]

Hacker Periodic Table of Elements

Quiz later this week! Study hard!
submitted by psychosquee

Hk Hacker	Ex Exploit	Sc Scan	Kd Kiddie	Li Linux	La Lamer	Go Admin
Do DoS	Bk Backdoor	Bl Black	Wh White	Gr Grey	Pi Ping	
Dd DDoS	Bu Bugs	Sr Server	Rt Root	Pg Progs	Nw Newbie	Rm Remote
Dr DRDOS	Ck Cracker	Le Police	Kl Kernel	Pt Packet	Df DeFace	
	Sy SecuFity	Me Media	Rk Rootkit	Lt 1337	Ac Access	

Espionage and the Art of Information Warfare

by Echo5

[Edited for release]

The concept of “Espionage and the art of Information Warfare” brings to light the issues of espionage within a corporate as well as national level infrastructure. Espionage or spying can be considered as an action that seeks to obtain confidential information about the activities, plans, and methods, of an organization or person.

The subject selected is important to the field of networking and security due to its ability to cause irreparable damage to a company’s financial interests and reputation or on a national level to threaten the welfare and interest of national security.

One of the countries selected for review of their espionage actions is the Peoples Republic of China herein referred to as the PRC. The PRC has devoted numerous resources to gathering intelligence. The quest for information by the PRC is insatiable. The Ministry of State Security (MSS) and the General Staff’s Military Intelligence Department (MID) are the main intelligence services involved in acquisition of technological data. The PRC uses other sources to obtain information as well; these include, but are not limited to, research institutes and PRC military-industrial companies.

In 1997, the Chinese Communist Party (CCP) formally initiated the 16-Character Policy set forth by Deng Xiaoping’s 1978 pronouncement, that the military development is the sole object of general economic modernization. The sixteen characters literally mean:

- **Jun-min jiehe (Combine the military and civil)**
- **Ping-zhan jiehe (Combine peace and war)**
- **Jun-pin youxian (Give priority to military products)**
- **Yi min yan jun (Let the civil support the military)**

The efforts to obtain information on nuclear data is a prime example of how a person who has access to a controlled environment can utilize or manipulate the system’s network to accomplish a goal set forth by a foreign government. The PRC’s intelligence efforts to obtain and collect modern thermonuclear warhead data is targeted primarily against the U.S. Department of Energy’s National Laboratories at:

- **Los Alamos, New Mexico**
- **Lawrence Livermore, California**
- **Oak Ridge, Tennessee**
- **Sandia, New Mexico**

In the field of networking and security, cases of espionage at the Department of Energy's National Laboratories have been noted below.

In 1997 Peter Lee, a Chinese-born research physicist employed at the Lawrence Livermore lab in the mid-1980's admitted that he provided classified information to China during visits in 1985 and 1997.

On December 10th, 1999 computer scientist Wen Ho Lee (no relation to Peter Lee) was arrested and charged with removing nuclear secrets at Los Alamos. Mr. Lee created approximately 10 tapes containing legacy codes. The legacy codes provide a history of nuclear weapons development. Mr. Lee admitted that he had transferred thousands of computer codes from the Los Alamos highly secured computer system to his personal office computer considered less-secure in 1994 and also in 1995.

The second country selected for this topic is the country of Russia (formerly the Soviet Union). The two primary intelligence agencies in the Former Soviet Union were the Komitet Gosudarstvennoi Bezopasnosti (KGB) and the Glavnoye Razvedyvatelnoye Upravlenie (GRU).

Russia now maintains several different intelligence agencies, 4 of them are the

- **Federal'naya Sluzhba Bezopasnosti (FSB) -Counter-Intelligence**
- **Sluzhba Vneshney Razvedki (SVR)- Foreign Intelligence**
- **Federal'naya Agenstvo Pravitel'stvennoy Svayazi i Informatsii –(FAPSI) the Federal Agency for Government Communications and Information**
- **Glavnoye Razvedyvatelnoye Upravlenie (GRU) -Main Intelligence Administration (Military)**

The Russian Intelligence Services primarily, the SVR and GRU, maintain a thorough process of attempting to obtain technical information. On October 2, 1962, Colonel (Col) Oleg Vladimirovich Penkovsky of the GRU was arrested by Soviet State Security for passing secrets to the west. Some time prior to his arrest, Col. Penkovsky passed along a training doctrine used within the Intelligence Training School's.

Then (Soviet) Intelligence evaluated potential candidates that they could recruit to conduct espionage for them by using the four areas that could classify a person's level of weakness. The term of Money, Ideology, Compromise, and Ego was known under its acronym M.I.C.E.

Using this concept, Intelligence agents would evaluate prospects for recruitment and offer incentives that would appeal to the candidate's area of weakness.

Russian Intelligence has always been a formidable threat. Cases of espionage within the United States involving Russia and its intelligence apparatus are noted below.

In 1997 the Air Force Office of Special Investigations (OSI) and the Federal Bureau of Investigations (FBI) began an investigation code named Digital Demon. The investigation was based around the Vice President of Elegant Mathematics, Aleksey Yeremin, who was based in

Russia. At its peak, the company Elegant Mathematics employed personnel who were mathematicians, software experts, and physicists from the Russian Academy, the Steklov Mathematical Institute, and the Moscow State University.

Aleksey Yeremin, was allowed access to the Lockheed Martin supercomputer from Moscow, and is suspected of taking advantages in lax security measures to steal secret stealth technology. Yeremin had access to the performance characteristics of radar absorbing material that coat stealth planes, the MM3D (Method of Movement in 3 Dimensions, as well as the test fixtures (secret computer representations of stealth aircraft)

On February 20th, 2001 the announcement of the arrest of a veteran FBI agent working in the field of Counter-Intelligence plastered newspapers. US Counter-Intelligence officials stated that Robert Hanssen's use of computers greatly exceeded that of any other major spy case in US History. Hanssen was a regular user of the Automated Case Support System, which is the FBI's internal network which contains classified data of investigations.

With this information one can see the distressing issues at hand when a member of a staff who is allowed access to the inner sanctum violates the trust bestowed upon them. Though the threat from the inside is of a large concern, there is also the threat of espionage activity from the outside as well. Incidents as those noted below should be taken into consideration by those dealing within the networking and security field.

On April 5th, 1999 Network World reported that NATO computer systems were being attacked by anti-NATO hackers. Shortly there after an underground CD was made available see CD cover image below: [Edited]

On May 12th, 1999 the Associated Press reported that Dutch computer hackers had stolen US Military secrets during the Gulf War and had offered them to Iraq.

On March 16th, 2001 computer hackers suspected of having links to a foreign government. Successfully broke into the Sandia's computer system, and were able to access sensitive classified information. The suspected governments, according to the officials, include Russia, China, Iraq or North Korea .

There are various forms of espionage, and similar topics of interest to the reader may be:

SIGINT- Signals Intelligence is considered to be one of the most sensitive forms of intelligence and deals with the interception of foreign signals.

HUMINT- Human Intelligence is the use of individuals to obtain sensitive information.

Cryptography-Cryptography is the means of using numbers, letters, and or characters to encode or decode communications.

End Paper

[Edited by author]

ls - The list Command

(The essential command every *nix user should know)

By **blackmask**

Hello pals after seeing the two newsletters from the senior members, as a newbie I too got inspired to submit my own article. Even though it is a lame one, I hope it will benefit newbie's to *nix's. 'ls' is one of the essential commands that a *nix user should know. It is used to list the contents of a directory. I have given here almost all important flags that are used with 'ls'. A few combinations are also listed by the end of this document. Hope you will enjoy this.

ls -> The command itself. 'ls' lists the contents of the current directory.

Here it's my home directory. You can specify different directory/directories with 'ls' to see the contents of them.

```
[Matrix@localhost ~]$ ls
```

```
Art_of_assembly  mail          portsentry-1.1
Win              nasm-0.98    perl.programs
zips.rpms        hello.java    Notes
pics            webfiles
```

ls -l -> long listing format, it shows attributes, size, owner, group, modification time etc.

```
[Matrix@localhost ~]$ ls -l
```

```
total 52
```

```
drwxr-xr-T 20 Matrix Matrix 4096 Feb 19 22:59 Art_of_assembly
drwxrwxr-x  2 Matrix Matrix 4096 Mar 24 12:09 C
-rw-rw-r--  1 Matrix Matrix  92 Mar 24 12:04 hello.java
drwx----- 2 Matrix Matrix 4096 Mar 22 21:16 mail
drw-----  8 Matrix Matrix 4096 Jan 31 19:58 nasm-0.98
drwxr--r--  2 Matrix Matrix 4096 Mar 23 21:18 Notes
drwx-----  2 Matrix Matrix 4096 Mar  1 15:17 nsmail
drwxrwxr-x  2 Matrix Matrix 4096 Feb 15 22:47 perl.programs
drwxrwxr-x  2 Matrix Matrix 4096 Feb  2 11:22 pics
drwxr-xr-x  2 root  root  4096 Feb 11 23:07 portsentry-1.1
drwxrwxr-x  5 Matrix Matrix 4096 Mar  1 22:52 webfiles
drwxr-xr-x  2 root  root  4096 Feb  4 20:51 win
drwxrwxr-x  4 Matrix Matrix 4096 Mar 17 20:58 zips.rpms
```

ls -F -> Appends executables with *,directories with /,symbolic links with a @
 FIFO's with | and sockets with =.'ls -p' also appends / to directory.

```
[Matrix@localhost ~]$ ls -F
```

```
Art_of_assembly/  mail/  nsmail/  portsentry-1.1/  win/
C/                nasm-0.98/  perl.programs/  zips.rpms/
hello.java       Notes/  pics/    webfiles/
```

ls -R -> Recursive listing of all files in sub-directories. It was pretty long,
 so I had to delete some parts of it.

```
[Matrix@localhost ~]$ ls -R
```

```
.:
Art_of_assembly  mmail      portsentry-1.1
nasm-0.98        perl.programs  zips.rpms
hello.java       Notes      pics
webfiles        win
```

```
./Art_of_assembly:
```

```
Art of Assembly Chapter Eight-2_files
Art of Assembly Chapter Eight-2.htm
Art of Assembly Chapter Eight-3.htm
Art of Assembly Chapter Eight-5_files
Art of Assembly Chapter Eight-5.htm
Art of Assembly Chapter Eight.htm
Art of Assembly Chapter Five-2_files
```

```
./Art_of_assembly/Art of Assembly Chapter Eight-2_files:
```

```
ch08a1.gif  ch08a2.gif  ch08a3.gif
ch08a4.gif  ch08a5.gif  ch08a.gif
```

```
./Art_of_assembly/Art of Assembly Chapter Eight-5_files:
```

```
ch08a6.gif
```

```
./Art_of_assembly/Art of Assembly Chapter Five-2_files:
```

```
ch05a1.gif  ch05a2.gif  ch05a3.gif
ch05a4.gif  ch05a5.gif  ch05a.gif
```

```
./C:
```

```
asciiconv  astack.c  curmov.c
lsearch    makefile  window
asciiconv.cc  lsearch.c  window.c
```

./mail:

saved-messages sent-mail

ls: ./nasm-0.98/MODIFIED: Permission denied

ls: ./nasm-0.98/COPYING: Permission denied

ls: ./nasm-0.98/Changes: Permission denied

ls: ./nasm-0.98/Licence: Permission denied

./Notes:

PIC prglst tags timetbl

./nsmail:

Drafts Inbox Sent Templates Trash Unsent Messages

./perl.programs:

envar.pl senvar.pl

./pics:

philosophical-gnu-sm.jpeg Rock.jpeg takeittux.jpg

./portsentry-1.1:

CHANGES portsentry portsentry_io.c README.install

CREDITS portsentry.c portsentry_io.h

ls -s -> Prints size of files in blocks.

[Matrix@localhost ~]\$ **ls -s**

total 84

```
4 Art_of_assembly 4 nasm-0.98 4 pics
4 win 4 C 4 Notes
4 portsentry-1.1 4 zips.rpms 4 hello.java
4 nsmail 4 mail 4 perl.programs
4 webfiles
```

ls -a -> Lists all files in the directoy including the hidden ones whose names begin with a period.

[Matrix@localhost ~]\$ **ls -a**

```
. .calendar~ mail .screenrc
.. .cddbslave .mc .addressbook
```

```
.ee      .swp      nasm-0.98  .viminfo
Art_of_assembly .netscape  webfiles  win
Notes      nsmail      perl.programs .bash_profile
```

ls -x -> Lists contents in multiple columns.

```
[Matrix@localhost ~]$ ls -x
```

```
Art_of_assembly C      hello.java  mail      nasm-0.98
Notes          nsmail perl.programs pics      portsentry-1.1
webfiles      win      zips.rpms
```

ls -d -> Shows the directory, not its contents.

```
[Matrix@localhost ~]$ ls -d
```

ls -f -> Lists the contents exactly the way in which they are stored in the directory.

```
[Matrix@localhost ~]$ ls -f
```

```
.          .ICEauthority  .calendar      .netscape
..         .ee           .swp           Notes
.bash_logout .xauth        .gnome-help-browser win
.bash_profile .bash_history perl.programs  .esd_auth
.bashrc      nsmail        .newsrc-news   zips.rpms
.emacs       .cddbslave   .calendar~     nasm-0.98
.screenrc    pics         .pinerc        .gimp-1.2
.gnome       .viminfo     hello.java     portsentry-1.1
.gnome_private C            .aspell.english.pws .MCOP-random-seed
.sawfish     .gphoto     .aspell.english.prepl webfiles
.mc          Art_of_assembly .addressbook.lu
```

ls -i -> Shows the inode number of the contents.

```
[Matrix@localhost ~]$ ls -i
```

```
587133 Art_of_assembly 880194 Notes 163782 C
668467 nsmail 522061 webfiles 733339 hello.java
652101 perl.programs 440804 win 440134 mail
```

ls -t -> Lists contents in the order of their modification time.

```
[Matrix@localhost ~]$ ls -lu
```

```
total 52
drwxrwxr-x  2 Matrix  Matrix  4096 Mar 25 15:02 C
-rw-rw-r--  1 Matrix  Matrix   92 Mar 24 12:06 hello.java
drwx-----  2 Matrix  Matrix  4096 Mar 25 11:55 mail
drw-----  8 Matrix  Matrix  4096 Mar 25 11:55 nasm-0.98
drwxr--r--  2 Matrix  Matrix  4096 Mar 25 11:55 Notes
drwx-----  2 Matrix  Matrix  4096 Mar 25 11:55 nsmail
```

ls -u -> Lists contents in the order of their access time.

```
[Matrix@localhost ~]$ ls -lt
```

```
total 52
-rw-rw-r--  1 Matrix  Matrix   0 Mar 25 15:02 sessionlog
drwxrwxr-x  2 Matrix  Matrix  4096 Mar 24 12:09 C
-rw-rw-r--  1 Matrix  Matrix   92 Mar 24 12:04 hello.java
drwxr--r--  2 Matrix  Matrix  4096 Mar 23 21:18 Notes
drwx-----  2 Matrix  Matrix  4096 Mar 22 21:16 mail
```

ls -r -> Lists contents in the reverse order.

```
[Matrix@localhost ~]$ ls -r
```

```
zips.rpms  pics      nsmail
win        portsentry-1.1  mail
webfiles   perl.programs  Art_of_assembly
```

ls -lG -> Lists contents without group information.

```
[Matrix@localhost ~]$ ls -lG
```

```
total 84
drwxr-xr-T 20 Matrix  4096 Feb 19 22:59 Art_of_assembly
drwxrwxr-x  2 Matrix  4096 Mar 24 12:09 C
-rw-rw-r--  1 Matrix   92 Mar 24 12:04 hello.java
drwx-----  2 Matrix  4096 Mar 22 21:16 mail
drw-----  8 Matrix  4096 Jan 31 19:58 nasm-0.98
drwxr--r--  2 Matrix  4096 Mar 23 21:18 Notes
drwx-----  2 Matrix  4096 Mar  1 15:17 nsmail
drwxrwxr-x  2 Matrix  4096 Feb 15 22:47 perl.programs
drwxrwxr-x  2 Matrix  4096 Feb  2 11:22 pics
drwxr-xr-x  2 root    4096 Feb 11 23:07 portsentry-1.1
```

ls -A -> Lists all files including hidden but excluding . and .. directories.

```
[Matrix@localhost ~]$ ls -A
```

```
.addressbook      .cddbslave      mail      .sawfish
.addressbook.lu   .ee             .mc       Art_of_assembly  nasm-0.98      Notes      win
nsmail
```

ls -n -> Lists like -l flag but uses group-ID and user-ID numbers instead of owner and group names.

```
[Matrix@localhost ~]$ ls -ln
```

```
total 84
drwxr-xr-T 20 500 500 4096 Feb 19 22:59 Art_of_assembly
drwxrwxr-x 2 500 500 4096 Mar 24 12:09 C
-rw-rw-r-- 1 500 500 92 Mar 24 12:04 hello.java
drwx----- 2 500 500 4096 Mar 22 21:16 mail
drw----- 8 500 500 4096 Jan 31 19:58 nasm-0.98
drwxr--r-- 2 500 500 4096 Mar 23 21:18 Notes
drwx----- 2 500 500 4096 Mar 1 15:17 nsmail
drwxrwxr-x 2 500 500 4096 Feb 15 22:47 perl.programs
drwxrwxr-x 2 500 500 4096 Feb 2 11:22 pics
drwxr-xr-x 2 0 0 4096 Feb 11 23:07 portsentry-1.1
drwxr-xr-x 2 0 0 4096 Feb 4 20:51 mwin
drwxrwxr-x 4 500 500 4096 Mar 17 20:58 zips.rpms
```

Some combinations are given below. Try this out on your *nix box.

```
[Matrix@localhost ~]$ ls -asCF
```

```
total 248
4 ./      4 .esd_auth      4 perl.programs/
4 ../     4 .gimp-1.2/     4 pics/
0 .addressbook 4 .gnome/        16 .pinerc
4 .addressbook.lu 4 .gnome-desktop/ 4 portsentry-1.1/
4 Art_of_assembly 4 .gnome-help-browser/ 4 .sawfish/
[Matrix@localhost ~]$ ls -ld /bin /etc
```

```
drwxr-xr-x 2 root root 4096 Jan 29 17:15 /bin
drwxr-xr-x 42 root root 4096 Mar 25 11:17 /etc
```

```
[Matrix@localhost ~]$ ls -d | grep “^d”
```

```
drwxr-xr-T 20 Matrix Matrix 4096 Feb 19 22:59 Art_of_assembly
drwxrwxr-x 2 Matrix Matrix 4096 Mar 24 12:09 C
drwx----- 2 Matrix Matrix 4096 Mar 22 21:16 mail
drw----- 8 Matrix Matrix 4096 Jan 31 19:58 nasm-0.98
drwxr-r-- 2 Matrix Matrix 4096 Mar 23 21:18 Notes
drwx----- 2 Matrix Matrix 4096 Mar 1 15:17 nsmail
drwxrwxr-x 2 Matrix Matrix 4096 Feb 15 22:47 perl.programs
drwxrwxr-x 2 Matrix Matrix 4096 Feb 2 11:22 pics
drwxr-xr-x 2 root root 4096 Feb 11 23:07 portsentry-1.1
drwxrwxr-x 5 Matrix Matrix 4096 Mar 1 22:52 webfiles
drwxr-xr-x 2 root root 4096 Feb 4 20:51 win
drwxrwxr-x 4 Matrix Matrix 4096 Mar 17 20:58 zips.rpms
```

```
[Matrix@localhost ~]$ ls | wc -l
```

14

```
[Matrix@localhost ~]$ ls -a | wc -l
```

49

```
[Matrix@localhost ~]$ exit
```

Report bugs to virtualarun@yahoo.com

«BlâçkMâşk»

**We are looking for articles, tutorials, rants,
raves, etc.**

**Newsletter #4 Deadline is
June 26th, 2002**

Security Auditing: Part II

Hello everyone. Welcome to part II of security auditing. I apologize for not going into better detail. It's late and I don't really have the time. None the less, these topics should cover it:

Know Yourself: Vulnerability Assessments (<http://rr.sans.org/audit/know.php>)

Building a Security Toolkit (<http://rr.sans.org/audit/toolkit.php>)

The Ethics and Legality of Port Scanning (<http://rr.sans.org/audit/ethics.php>)

An Overview of Threat and Risk Assessment (<http://rr.sans.org/audit/overview.php>)

Port Scanning Techniques and the Defense Against Them
(http://rr.sans.org/audit/port_scan.php)

A Guide to Security Metrics (<http://rr.sans.org/audit/metrics.php>)

For more articles on security auditing and assessment visit the SANS Reading Room. The SANS reading room contains more than 1,300 research reports. You should be able to find proper reading material there.

If you plan on auditing your own computer, you'll need the right tools for the job. I would recommend browsing the Server Security Software archive from Hideaway.net If you don't find the tools you need there then try your luck at Google.

Remote_Access_

Got a funny bone?? Submit your humorous stories and tales to us. We are looking for articles, tutorials, rants, raves, etc.

Newsletter #4 Deadline is June 26, 2002

Seek and Ye Shall Find.. Maybe

by Zigar_

The web is a big place. Somewhere over 2 billion pages big. That's a lot of information and you want to find that "one" bit that answers that question you have. How do you find relevant answers to what you want to know? Knowing where to look is only the beginning. Over the next couple of issues, I hope to be able to help you make the most out of your searches.

The history of Internet searches presented by cartoon characters It's important to remember that in 1990, there was no world wide web (hard to believe but true). Most information on the internet was available only through ftp. The big problem was finding the information that you wanted or needed. There was no method of finding anything other than word of mouth. The first real search function on the internet was called Archie. Archie was developed by Alan Emtage, a student at McGill University in Montreal. The program was originally supposed to be called "archives" but in an effort to make the name somewhat cryptic and more unix friendly (read as: incomprehensible to most), it was shortened to Archie. Archie was simple but effective. It compiled listings of information on known ftp servers but the biggest advance was it's ability to enable a user to enter a regular expression(1) and get results from the archie database, making it the first widely used internet search tool.

Back around the same time, the other technology that was in widespread use was called gopher. Gopher was similar to ftp, except that gopher was strictly a text based document distribution system. In 1993, the folks at University of Nevada System Computing Services group developed Veronica, which was essentially the same type of system as archie except that it used gopher instead of ftp.

The birth of the web – thanks to high energy particle physics!

Back in 1990, a group of visionary geeks at CERN (European Organization for Nuclear Research, the world's largest particle physics center) were trying to figure out a way to disseminate large quantities of data in an easy to use and worldwide context. They understood that the internet was a potential tool, but also saw that there was a lack of a proper tool for using the net efficiently. Enter stage right, Tim Berners-Lee, a computer scientist at CERN. Berners_Lee along with Robert Cailliau wrote a program for NeXTStep, which was in fact the very first www client. Berners-Lee was the first to coin the term World Wide Web. 1991 saw the first web server in the US, being hosted at the Stanford Linear Accelerator Center. SLAC served mostly abstracts of physics papers to the particle physics community. By 1992, the number of web servers worldwide had risen to an incredible 50 (!). In this time, Berners-Lee was developing standards which we have now come to take for granted, such as URL, HTTP and HTML. It's important to note that at this time, the www was strictly the domain of unix based servers and browsers.

All of this work came to the attention of a young undergraduate student at the University of Illinois' NCSA (National Center for Supercomputing Applications) named Marc Andreessen. In

early 1993, Andreessen and the NCSA released the unix version of web browser as we know it today. By summer, the NCSA had released free versions of the browser known as Mosaic for Windows and Mac and the "internet" (although more correctly, the world wide web) as we know it was born. Andreessen later went on to commercialize his invention, to be known as Netscape. Netscape's IPO in 1995 became the single biggest of the 1990's and capitalized the company at \$2.6 billion. This IPO was credited with setting off the dotcom boom. (it should also be noted that Andreessen's last endeavour, Loudcloud, was one of the last "big" IPO's in March of 2001 with a paltry \$450 million at 6 bucks a share...and it's currently trading at about \$1.60 per share...)

Web Servers (2)

Jun 1993	130
Sep 1993	204
Oct 1993	228
Nov 1993	272
Dec 1993	623
Mar 1994	1265
Jun 1994	3184

WWW TRAFFIC OVER NSFNET BACKBONE - IN MEGABYTES/MONTH (2)

MONTH/YEAR	WWW	GOPHER
Dec 92	78	34,247
Jan 93	122	43,238
Feb 93	512	60,897
Mar 93	3,613	79,024
Apr 93	8,116	89,074
May 93	17,298	103,870
Jun 93	35,701	111,881
Jul 93	48,728	139,006
Aug 93	50,779	148,795
Sep 93	75,401	198,096
Oct 93	122,174	250,785
Nov 93	172,340	291,133
Dec 93	225,443	309,691
Jan 94	269,129	374,681
Feb 94	347,503	396,066
Mar 94	518,084	480,690
Apr 94	671,950	517,625
May 94	799,163	555,708
Jun 94	946,539	567,479
Jul 94	1,056,081	555,089

"The Web certainly needs solutions in information discovery and retrieval...The Web will also

need new protocols, tools, browsers, hypermedia interfaces, and software. But along with these tools for information discovery and delivery, we need to develop information shaping capabilities—skills to select and present information on the Web.” John December - Computer-Mediated Communication Magazine /Volume 1, Number 6 / October 1, 1994 / Page 8

Internet Domain Survey, July 2001 (3)
Number of Hosts advertised in the DNS
(IP addresses assigned a name – most are web servers)

Jul 2001		125,888,197
Jan 2001		109,574,429
Jul 2000		93,047,785
Jan 2000		72,398,092
Jul 1999		56,218,000
Jan 1999		43,230,000
Jul 1998		36,739,000
Jan 1998		29,670,000
Jul 1997		19,540,000
Jan 1997		16,146,000
Jul 1996		12,881,000
Jan 1996		9,472,000
Jul 1995		6,642,000
Jan 1995		4,852,000
Jul 1994		3,212,000
Jan 1994		2,217,000
Jul 1993		1,776,000
Jan 1993		1,313,000

Around this same time, people began developing tools to deal with the almost unimaginable growth in available information on the web. Matthew Grey, student at MIT, developed the World Wide Web Wanderer, with the intent of tracking the growth of the web. The first wanderer did little but count servers, but it was recognized early on that it could also collect and store urls. W4 was the webs first robot or bot as they are most often called now. It wasn't long before programmers realized the power of these automatons. The key was realizing that once you knew the first link to a site, a bot could easily find all the other pages within the site, just by following the links. In theory, if a bot knows all the addresses on the internet, it can follow all the links to every page on the internet or more poetically, trace all the strands of the web. Of course, this was the birth of the spider. The spider is the key element to a large portion of web searching today.

Captain Yahoo vs. The Spider

About this time, 2 grad students at Stanford were putting together some of their favorite links on a web page. Turns out that a lot of people liked the links and the page got a lot of visits.

These 2 guys, David Filo and Jerry Yang recognized that there might be a few people who would be interested in this type of searchable directory. It was different from a spider in that that all of the entries were reviewed and submitted by actual people. Turns out that a LOT of people liked this way of finding things on the web...and Do You Yahoo became synonymous with the explosion of growth on the web during the late 90's.

Goofy Names and Powerful Search Tools.

It was soon apparent that the web was going to be big. So big in fact that the tools of the day were lacking when it came to finding that specific piece of information you were looking for. In 1994, when there were only a few thousand web servers, finding what you needed was possible with basic tools. Today, with several million web servers and billions of pages, search tools have to be very advanced.

The first of the new generation search tools was AltaVista. AltaVista was the first search tool that allowed people to query using natural language. That is, it used relative importance of words to rank its findings. Words like "what" and "the" and "is" were given less importance so results of a query like "What is the Capital of Oregon" would look at Capital and Oregon and return more relevant results. If any of you run a web site, one of the more common server log entries will be something referencing "Slurp". Slurp was created by Inktomi Co. and was the first search engine to provide almost daily updates to its index. Metacrawler was one of the first Meta Search Engine.

That is, it was actually a place to go to enter a query which in turn queried other search engines. It did not actually do any searching of the web itself. It just submitted your request to multiple search engines and presented the data that they returned to you in a single location. Many found this a very attractive alternative as most of the search engines did things in a different way and Metacrawler was a single location to find diverse results. Fast forwarding to 1998, the current reigning champion of the search wars was founded. The name Google is a derivation of the term Googol, which is the mathematical term for 1 followed by 100 zero's (ie...a lot). Google's founders wanted to create the fastest and most comprehensive search engines available. And to most, they appear to have done just that. Google is now the number one search engine, and with good reason. It has indexed more than 2 billion urls and can return results of a query on those pages in fractions of a second. Google indexes standard urls, doc files, ppt presentation, pdf files, and even some dynamic content such as asp, php and cfm.

So many results...so little time

So you're having a problem with your display. Google says:

Searched the web for video card drivers. Results 1 - 10 of about 538,000. Search took 0.18 seconds. 538,000 results? Pretty impressive but what good is that. The key to getting results is knowing exactly how to ask the right question. Now that we know a bit about the history of the "search" and how these things work, we'll look at the best ways to use them next newsletter...until then...hsppy hunting.!

- (1) <http://hotwired.lycos.com/webmonkey/geektalk/97/33/index3a.html>
- (2) <http://www.ibiblio.org/cmc/mag/1994/oct/webip.html>
- (3) <http://www.isc.org/ds/WWW-200107/index.html>

Other references.

<http://www.wiley.com/legacy/compbooks/sonnenreich/history.html>
<http://www.ouc.bc.ca/libr/connect96/search.htm>
<http://www.netvalley.com/intvalweb.html>
<http://public.web.cern.ch/Public/ACHIEVEMENTS/WEB/Welcome.html>
http://www.hitmill.com/internet/web_history.html

And what are you looking at? Hey, if you read this far, it means we kept your interest. Now keep ours. Submit your article, story, rant, rave, cartoon, etc. today.

**Newsletter #4 Deadline is
June 26th, 2002**