Air Force Association's CyberPatriot

The National High School Cyber Defense Competition

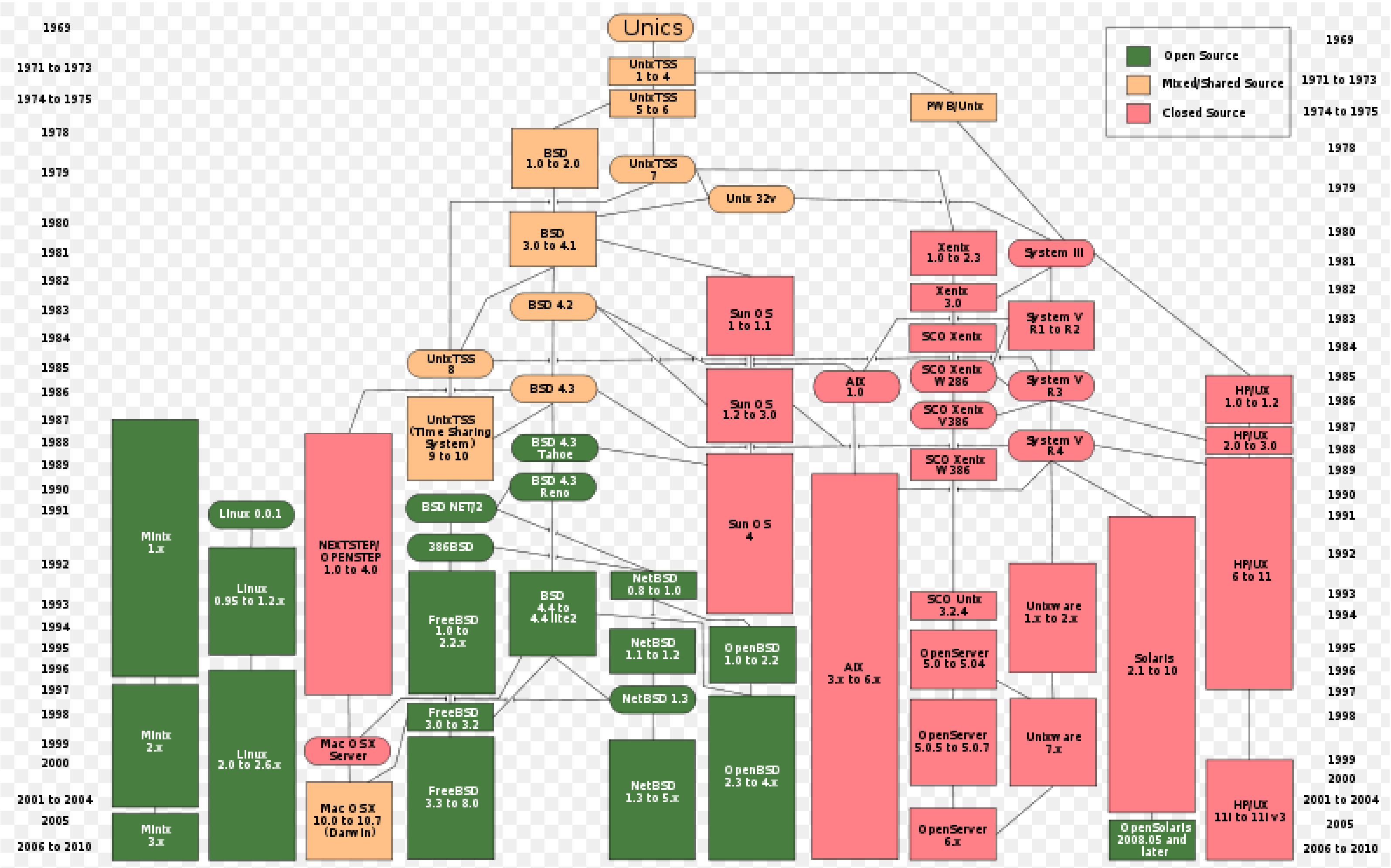
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL HIGH SCHOOL CYBER DEFENSE COMPETITION

Unix Operating Systems
Module 7

Unix Operating System

- Versions
- Basic Information
- User and Group Settings
- File Permissions
- Local Firewall
- Local Security Policies
- Permissions and Rights
- Tools
- Checklist

History of Versions



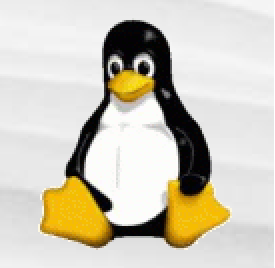
Current Versions

- Linux (Red Hat, Fedora, SUSE, Ubuntu, Mint)
- BSD (OpenBSD, FreeBSD, NetBSD)
- Mac OS X
- Sun OS
- AIX
- HP/UX
- Solaris
- OpenServer

http://www.sitepoint.com/unix-style-operating-systems/

Linux

- Different flavors of Linux may be used for the competition like:
  - Ubuntu
    - http://ubuntuguide.org/wiki/Ubuntu:Oneiric
  - Fedora Core
    - http://fedoraproject.org/



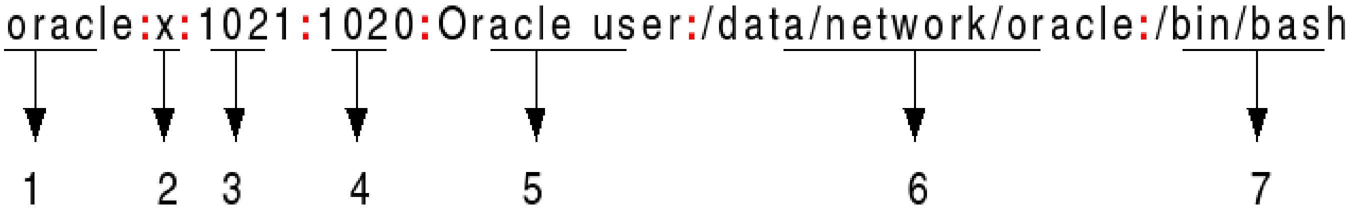
- Many flavors have GUIs for ease of use
- Command line interface
  - GUIs may not always be available
  - For consistency purposes, we will focus on command line rather than GUIs
- All flavors built around a "Kernel"
  - Main component of the OS
  - Made up of CPU, memory, and I/O (Input/Output) devices

Linux 101

- Root
  - The ‘administrator’ of the system
- Password files
  - Encrypt passwords
  - Located at /etc/passwd and /etc/shadow
- System Logs (syslog)
  - Configure the Syslog daemon to log messages and events
  - Located at the /etc/syslog.conf
- Daemon
  - A process that runs in the background
- Editor
  - VI is a text editor used on most Unix operating systems
  - Cheat sheet for commands at http://media.smashingmagazine.com/wp-content/uploads/2010/05/VI-Help-Sheet-011.pdf

Password Files

- Each user has an entry in the password file



```
oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash
```

1. **Username**: It is used when user logs in. It should be between 1 and 32 characters in length.
2. **Password**: An x character indicates that encrypted password is stored in /etc/shadow file.
3. **User ID (UID)**: Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.
4. **Group ID (GID)**: The primary group ID (stored in /etc/group file)
5. **User ID Info**: The comment field. It allows you to add extra information about the users such as user's full name, phone number etc. This field is used by the finger command.
6. **Home directory**: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory often becomes /
7. **Command/shell**: The absolute path of a command or shell (/bin/bash). Typically, this is a shell. Please note that it does not have to be a shell.

Password Files

- Passwords are usually not stored in the /etc/passwd file, but rather in the /etc/shadow file
  - Passwords are encrypted in the /etc/shadow file
- File permissions
  - /etc/passwd
    - Owned by Root
    - Read only to users
  - /etc/shadow
    - Owned by Root
    - Users should not have access to this file
- To crack Linux passwords you need the shadow file and sometimes have to merge the passwd and shadow file

User and Group Security

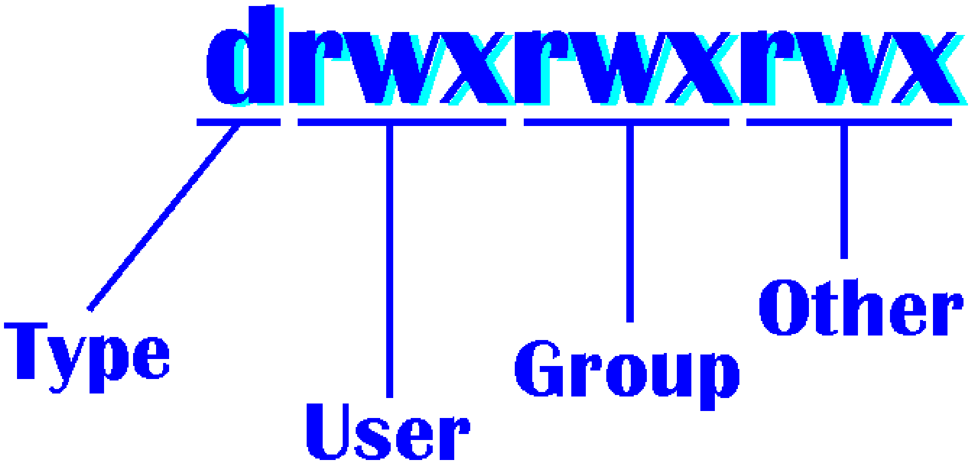
- Defaults Users and Groups
  - Permissions and privilege tips
    - Disable login for well known accounts (bin,sys,uucp)
    - Disable all account(s) with no password and lock them down
      - passwd -l {user-name}
  - Root

    $$\sqrt{x}$$

    - Disable direct login
    - Limit number of users with access
    - Regularly change password
    - For Ubuntu, the root account must be enabled by giving it a password using the **sudo** command
    - **Sudo** allows an authorized user to temporarily elevate their privileges using their own password instead of having to know the password belonging to the root account
  - Locking a user account may not prevent a user access. They may still be able to gain shell access, without the need for any password.

File Permissions

- File Type
  - Directory – d
  - File – ‘-’
- File Permissions
  - Read - r
  - Write (modify) - w
  - Execute – x



- The first segment defines permissions set for the **user**, or creator, of the file.
- The second segment of three bits defines permissions set for the **group** that can access the file.
- The last segment defines permission for **other**
- Use the *chmod* command to change user and group permissions
  - http://condor.depaul.edu/dpowebpg/support/chmod.html

Film System Security

- Network File System (NFS) Security
  - Method of sharing access to a filesystem between Unix systems
  - Only run NFS as needed, apply latest patches (including nfsd, mountd, statd, lockd)
  - Careful use of /etc/exports
  - Read-only if possible
  - No suid if possible
  - Fully qualified hostnames
- Device Security
  - Device files /dev/null, /dev/tty & /dev/console should be world writeable but NEVER executable
  - Most other device files should be unreadable and unwriteable by regular users

Services

- Disable unnecessary services (daemons)
  - If your system is configured with inetd, look at /etc/inetd.conf and prefix a line with a "#" character to make it a comment; then restart the inetd service or reboot
  - If you are using xinetd, its configuration will be in the directory **/etc/xinetd.d**.
    - Each file in the directory defines a service, and add disable = yes to any that you want to disable
  - Disable daemons not normally used such as
    - Telnet
    - Anonymous FTP
    - Remote processes (Rexec.Rlogin,Rsh)
    - Rstatd
    - Finger
    - Talk, Ntalk

Other Security Tips

- Monitor your processes
  - Use tools such as Snort, Nessus
  - Monitor syslog
- Monitor run levels (0 to 6)
  - Runlevels define what services or processes should be running on the system
    - http://www.unixtools.com/Linux-Runlevels.html
  - Make sure all processes are operating on the appropriate runlevel
- Encrypt network traffic
  - Install ssh
- Utilize access control
  - Configure *hosts.allow* and *hosts.deny* files for tcpd and sshd

Local Security Policies

- User profile
  - The **adduser** utility creates a brand new home directory named /home/username
  - */etc/default/useradd*
  - By default, user home directories in Ubuntu are created with world read/execute permissions

Local Security Policies

- Password Policy
  - Minimum Password Length
    - Add the ‘minlen = <x>’ parameter to the pam_unix configuration in the /etc/pam.d/common-password file – Set to 8
      - password required pam_cracklib.so retry=3 minlen=8 difok=3
    - By default, Ubuntu requires a minimum password length of 4 characters
  - Password Expiration
    - Needs a minimum and maximum password age forcing users to change their passwords when they expire
      - PASS_MIN_DAYS – Set to 7 days
        - Minimum number of days allowed between password changes
      - PASS_MAX_DAYS – Set from 30 to 90 days
        - Maximum number of days a password may be used
      - PASS_WARN_AGE – Set to 14 days
        - Number of days warning given before a password expires
    - Parameters can be set in */etc/login.defs*

Local Security Policies

- Password History (reuse)
  - Create an empty /etc/security/opasswd file for storing old user passwords
  - Set permissions to opasswd to the same as the /etc/shawdow file
  - Enable password history by adding the “remember=<x>” to the pam_unix configuration in the /etc/pam.d/common-password file
    - password required pam_unix.so md5 remember=12 use_authtok
    - The value of the "remember" parameter is the number of old passwords to store for a user
  - More explanation can be found at

    http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html

Local Security Policies

- Account Lockout
  - Set to a high enough number that authorized users are not locked out of their user accounts simply because they mistype a password
    - Usually set to 5
  - Add the following two lines highlighted in blue to the /etc/pam.d/system-auth file
    - auth required /lib/security/$ISA/pam_tally.so onerr=fail no_magic_root
    - account required /lib/security/$ISA/pam_tally.so per_user deny=5 no_magic_root reset
  - The first added line counts failed login and failed su attempts for each user. The default location for attempted accesses is recorded in /var/log/faillog
  - The second added line specifies to lock accounts automatically after 5 failed login or su attempts (deny=5)

Local Firewall

- Use a local firewall
  - UFW (Uncomplicated Firewall)
    - Default Ubuntu firewall; but not activated by default
    - Command line interface (frontend for iptables)
    - Configure and enable
      - Set default policies such as drop all connections (deny), then add (allow) rules for specific services
      - Enable logging
    - https://wiki.ubuntu.com/UncomplicatedFirewall?action=show&redirect=UbuntuFirewall
  - Gufw
    - Gui for ufw
      - Type “sudo apt-get install gufw” at the command line
    - Screenshots for Gufw at https://help.ubuntu.com/community/Gufw

Local Firewall

- Firestarter
  - Shows active connections and who they belong to
  - Controls inbound and outbound traffic
  - Displays intrusion attempts as they occur
  - Configure firewall to behave in a specific manner for certain types of connections
  - Create security policies
  - Screenshots can be found at http://www.fs-security.com/screenshots.php
  - Download at http://www.fs-security.com/
  - Installation directions can be found at http://www.howtogeek.com/howto/ubuntu/install-the-firestarter-firewall-on-ubuntu-linux/

Package Management

- Package
  - A compressed program or piece of software
- Package Managers
  - All software on a linux system is divided into RPM packages, which can be installed, upgraded, or uninstalled
  - Contain a list of software repositories
  - You will be prompted to enter the superuser (root) password before changes are made to the system
- RPM Package Manager
  - .rpm is the file format for the software package files
  - System administrators must manually install with dependencies
  - Instead, a front end can be used to automate this process

Package Managers

- Common Package Managers (front end)
  - YUM – automatic update and package installer
    - http://yum.baseurl.org/
  - PackageKit (GUI)
    - Open **Software Updates** by clicking **Applications** → **System Tools** → **Software Update** from the **Activities** menu within the GNOME desktop
  - apt-get
    - Command line tool
  - Aptitude
    - Menu driven text based tool (https://help.ubuntu.com/11.04/serverguide/C/aptitude.html)
  - Synaptic Package Manager (GUI)
    - http://www.nongnu.org/synaptic/

Checklist

- Disable unnecessary services
- Disable remote login
- Disable dangerous features
- Employ e-mail security practices
- Install and maintain malware protection software
- Patch more than just the OS
- Research and test updates
- Use a desktop/local firewall
- Look for alternatives to default applications

References

- http://www.sans.org/score/checklists/linuxchecklist.pdf
- http://oreilly.com/catalog/puis3/chapter/ch11.pdf
- http://linu-news.org/?p=1837
- http://www.sitepoint.com/unix-style-operating-systems/
- https://help.ubuntu.com/8.04/serverguide/C/security.html
- http://www.fs-security.com/
- https://help.ubuntu.com/community/UFW
- http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html
- Videos:
  - Securing Ubuntu
    - http://www.youtube.com/watch?v=H-c1LoVx0WY