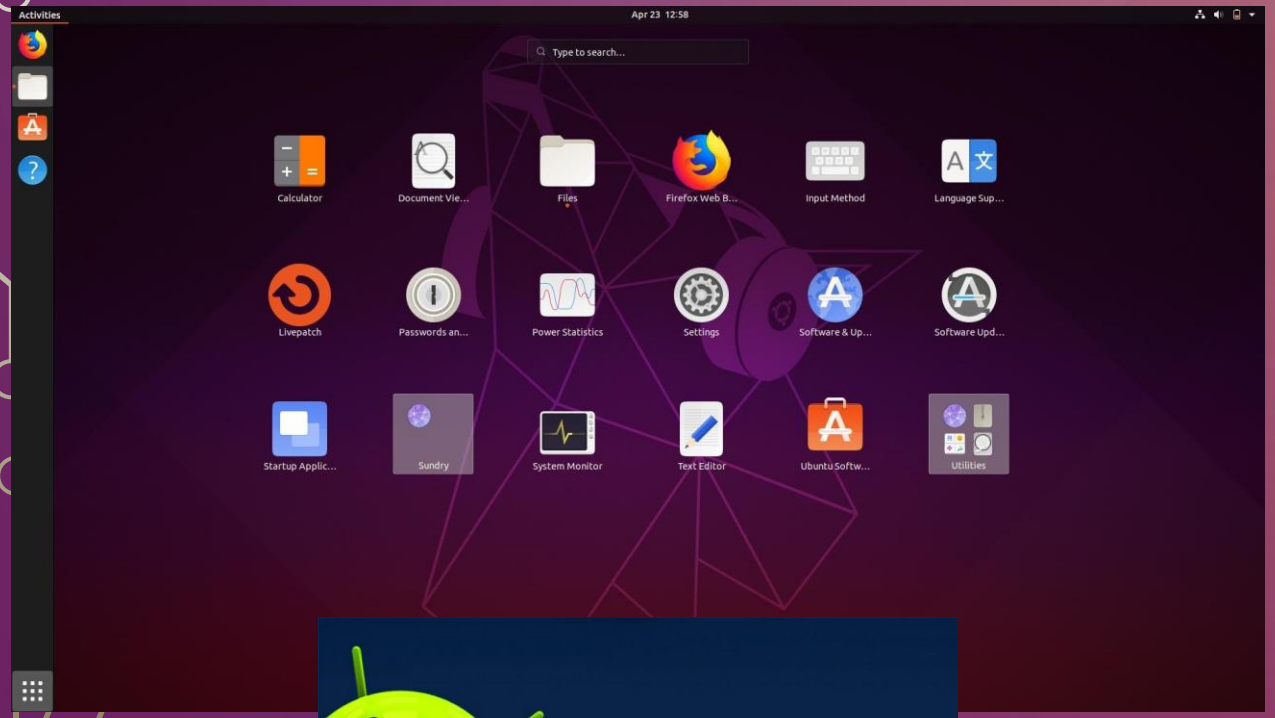
MODULE 4B: AUDITING UNIX AND LINUX OPERATING SYSTEMS

OBJECTIVES

- Basic commands for getting around in the *nix environment
- How to audit Unix and Linux systems, focusing on the following main areas:
- Account management
- Permissions management
- Network security and controls
- Security monitoring and other general controls
- Tools and resources for enhancing your *nix audits

UNIX OS “*NIX”

Linux



Mac OS X

UNIX AND LINUX AUDITING ESSENTIALS

- Everything in Unix is a file. For example, if you type in a command and press ENTER, you are actually executing a file within the system that has the same name as the command you entered. And if you attach a device, such as a printer or storage, to your Unix system, it will be represented on the system as a file.
- The root of the Unix file system is the directory called root or /. Every directory and every file branches off this root directory. Since everything in Unix is a file, if you do a recursive listing off of the / directory, you will see every component of the system.
- The system administrator (or superuser) account in Unix is called “root.” This account has full control over the system.
- If you can alter a file that someone is executing, you can easily capture (i.e., compromise or “become”) his or her account.

LINUX SECURITY ARCHITECTURE

- Linux root is just a slash (/)
- Important locations
  - / - root directory
  - /**bin** - basic Linux commands
  - /**dev** - contains pointer locations to various storage and input/output systems
  - /**etc** - all administration files and passwords. Both password and shadow files are here
  - /**home** - holds the user home directories
  - /**mnt** - holds the access locations you've mounted
  - /**sbin** - system binaries folder which holds more administrative commands
  - /**usr** - holds almost all of the information, commands and files unique to the user.
- *When navigating a *nix system, the presence or absence of the leading / in the path is very important; if present, it serves to anchor the path at the root directory. Thus, if you are currently in /usr, cd /bin and cd bin will take you to two different places (/bin and /usr/bin, respectively). These are known as absolute or relative path names. The absolute path always starts with / and traces the entire path from the root directory. The relative path, with no leading /, starts with the present directory.

LINUX COMMANDS

Command	Description
adduser	Adds a user to the system
cat	Displays contents of file
cp	Copies
ifconfig	Displays network configuration information
kill	Kills a running process
ls	Displays the contents of a folder. -l option provides most information.
man	Displays the manual page for a command
passwd	Used to change password
ps	Process status. -ef option shows all processes
rm	Removes files. -r option recursively removes all directories and subdirectories
Su or sudo	Allows you to perform functions as another user (super user)

LINUX FILE PERMISSIONS

- Permissions:
  - Read (R) = 4
  - Write (W) = 2
  - Execute (X) = 1
  - None (-) = 0
- Permission groups:
  - Users (U)
  - Groups (G)
  - Other (O / A)

- Chmod 777 file.exe
- Users, Groups, and Others have Read Write and Execute permissions
- File would read as
- u/g/o 7/7/7 file.exe
- What would 570 securefile.dat mean?

Permissions on a file or directory:

	Owner			Group			World		
Available permissions	Read	Write	Execute	Read	Write	Execute	Read	Write	Execute
Assigned permissions	r	w	x	r		x	r		
Binary (1 = Yes, 0 = No)	1	1	1	1		1	1		
Decimal value	4	2	1	4		1	4		
Cumulative result	7			5			4		

Resulting permissions: 754 (or) rwxr-xr--

LINUX SECURITY

- **pwd** - displays curennt directory
- **chmod** - changes the permissions of a folder or file
- Passwords are stored in /etc/shadow for most current systems
- /etc/password stores passwords in hashes.
- /etc/shadow stores passwords encrypted (hashed and salted) and is only accessible by root

UNIX PASSWORD FILE

- The /etc/passwd file contains account information for all users. Each account on the local system will have a single line in the /etc/passwd file. The system refers to this file when a user attempts to authenticate.

- account:password:UID:GID:GECOS:directory:shell

Field	Use
account	Represents the user to the system. This name is used when the user logs in.
password	Encrypted password. It may be kept in /etc/shadow instead; if so, this field simply will contain an `*`, `x`, `!`, or other character.
UID	Numeric user ID.
GID	Numeric group ID for the user's primary group.
GECOS	Optional field used to store arbitrary additional information about the account. A typical use would be the real name and/or employee ID of the user.
directory	Location of the user's home directory.
shell	User's default shell, the command-line environment that interprets commands and passes them to the kernel.

UNIX SHADOW FILE

- By design, the /etc/passwd allows world read access. Therefore, if the encrypted password is kept in that file, any user on the system would be able to download all users' encrypted passwords and attempt to crack them using freely available password-cracking software. To mitigate this risk, most systems store the encrypted password inside a shadow password file, which is readable only by root. The shadow password file is complementary to the /etc/passwd file, with a corresponding line for each user.

Field	Use
account	Name representing the user to the system.
password	Encrypted password; `*LK*` indicates that the account is locked.
lastchange	Number of days since the password was changed.
min	Minimum number of days allowed between password changes.
max	Maximum number of days allowed between password changes.
warn	Number of days before max, at which point the user will be warned to change his or her password.
inactive	Number of days of inactivity after which the user's account will be disabled.
expired	Number of days since January 1, 1970, that the account has been disabled.
reserved	An extra field that is not used.

LDAP, NIS, OR NIS+

- In more complicated cases, credentials can be checked against an authentication database located on the network; typically, this is Lightweight Directory Access Protocol (LDAP), Active Directory, Network Information System (NIS), or NIS+. You may be able to determine whether one of these is used in preliminary discussions with the system administrator, or you may want to look at the systems yourself.
- Determine whether NIS, NIS+, or LDAP is used by looking at the line beginning with passwd in /etc/nsswitch.conf. The presence of nis, nisplus, or ldap on that line indicates use of those protocols.

AUDITING LINUX ACCOUNT MANAGEMENT

Checklist for Auditing Account Management	
❑	1. Review and evaluate procedures for creating Unix or Linux user accounts and ensuring that accounts are created only when there's a legitimate business need. Also, review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.
❑	2. Ensure that all user IDs in the password file(s) are unique.
❑	3. Ensure that passwords are shadowed and use strong hashes where possible.
❑	4. Evaluate the file permissions for the password and shadow password files.
❑	5. Review and evaluate the strength of system passwords and use of stronger forms of authentication.
❑	6. Evaluate the use of password controls such as aging.
❑	7. Review the process used by the system administrator(s) for setting initial passwords for new users and communicating those passwords.
❑	8. Ensure that each account is associated with and can be traced easily to a specific employee.
❑	9. Ensure that invalid shells have been placed on all disabled accounts.
❑	10. Review and evaluate access to superuser (root-level) accounts and other administration accounts.
❑	11. Review controls for preventing direct root logins.
❑	12. Review and evaluate the use of groups, and determine the restrictiveness of their use.
❑	13. Evaluate the use of passwords at the group level.
❑	14. Review and evaluate the security of directories in the default path used by the system administrator when adding new users. Evaluate the use of the "current directory" in the path.
❑	15. Review and evaluate the security of directories in root's path. Evaluate the use of the "current directory" in the path.
❑	16. Review and evaluate the security of user home directories and config files. They generally should be writable only by the owner.

AUDITING PERMISSIONS MANAGEMENT

Checklist for Auditing Permissions Management	
❑	17. Evaluate the file permissions for a judgmental sample of critical files and their related directories.
❑	18. Look for open directories (directories with permission set to `drwxrwxrwx`) on the system and determine whether they should have the sticky bit set.
❑	19. Evaluate the security of all SUID files on the system, especially those that are SUID to root.
❑	20. Review and evaluate security over the kernel.
❑	21. Ensure that all files have a legal owner in the /etc/passwd file.
❑	22. Ensure that the `chown` command cannot be used by users to compromise user accounts.
❑	23. Obtain and evaluate the default umask value for the server.
❑	24. Examine the system's crontabs, especially root's crontab, for unusual or suspicious entries.
❑	25. Review the security of the files referenced within crontab entries, particularly root's crontab. Ensure that the entries refer to files that are owned by and writable only by the owner of the crontab and that those files are located in directories that are owned by and writable only by the owner of the crontab.
❑	26. Examine the system's scheduled atjobs for unusual or suspicious entries.

AUDITING NETWORK SECURITY AND CONTROLS

Checklist for Auditing Network Security and Controls	
❑	27. Determine what network services are enabled on the system, and validate their necessity with the system administrator. For necessary services, review and evaluate procedures for assessing vulnerabilities associated with those services and keeping them patched.
❑	28. Execute a network vulnerability scanning tool to check for current vulnerabilities in the environment.
❑	29. Review and evaluate the use of trusted access via the /etc/hosts.equiv file and user .rhosts files. Ensure that trusted access is not used or, if deemed to be absolutely necessary, is restricted to the extent possible.
❑	30. Review and evaluate the usage of trusted access via SSH keys.
❑	31. If anonymous FTP is enabled and genuinely needed, ensure that it is locked down properly.
❑	32. If NFS is enabled and genuinely needed, ensure that it is secured properly.
❑	33. Review for the use of secure protocols.
❑	34. Review and evaluate the use of .netrc files.
❑	35. Ensure that a legal warning banner is displayed when a user connects to the system.
❑	36. Review and evaluate the use of modems on the server.

AUDITING SECURITY MONITORING AND OTHER GENERAL CONTROLS

Checklist for Auditing Security Monitoring and Other General Controls	
❑	37. Review the `su` and `sudo` command logs to ensure that when these commands are used, they are logged with the date, time, and user who typed the command.
❑	38. Evaluate the syslog to ensure that adequate information is being captured.
❑	39. Evaluate the security and retention of the wtmp log, sulog, syslog, and any other relevant audit logs.
❑	40. Evaluate security over the utmp file.
❑	41. Review and evaluate system administrator procedures for monitoring the state of security on the system.
❑	42. If you are auditing a larger Unix/Linux environment (as opposed to one or two isolated systems), determine whether a standard build exists for new systems and whether that baseline has adequate security settings. Consider auditing a system freshly created from the baseline.
❑	43. Perform steps from Chapter 5 as they pertain to the system you are auditing.