ZROC102

Module 1 – Introduction to Kali Linux

Kali Linux

Kali Linux is developed, funded and maintained by Offensive Security.

It is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing.

Kali contains several hundred tools that are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

Linux File System

- Kali Linux adheres to the filesystem hierarchy standard (FHS), which provides a familiar and universal layout for all Linux users. The directories you will find most useful are:
  - /bin - basic programs (ls, cd, cat, etc.)
  - /sbin - system programs (fdisk, mkfs, sysctl, etc)
  - /etc - configuration files
  - /tmp - temporary files (typically deleted on boot)
  - /usr/bin - applications (apt, ncat, nmap, etc.)
  - /usr/share - application support and data files

Navigating the File System

Man Pages

Most executable programs intended for the Linux command line provide a formal piece of documentation often called manual or man pages.

- $ man ls

Listing Files

The “ls” command prints out a basic file listing to the screen. We can modify the output results with various wildcards.

- The -a option is used to display all files (including hidden ones).
- The -1 option displays each file on a single line, which is very useful for automation.

Moving Around

We can use the “cd” command followed by a path to change to the specified directory.

The “pwd” command will print the current working directory.

cd ~ will return you to the home directory.

Cont’d

- Creating Directories
  - The “mkdir” command followed by the name of a directory creates the specified directory.
  - Directory names can contain spaces, but we can save ourselves a lot of trouble by using hyphens or underscores instead.
    - $ mkdir notes
    - $ mkdir -p test/{recon,exploit,report}
- Finding Files
  - **Which**: searches through the directories that are defined in the $PATH environment variable for a given file name.
    - which filename
  - **Locate:** searches a built-in database named locate.db rather than the entire hard disk itself. searches a built-in database named locate.db rather than the entire hard disk itself
    - Locate filename
  - **Find:** is the most complex and flexible search tool among the three. With this command, we can perform a recursive search starting from the root file system directory and look for any file that starts with the letters “con”
    - Sudo find / -name con*
- The main advantage of find over locate is that it can search for files and directories by more than just the name. With find, we can search by file age, size, owner, file type, timestamp, permissions, and more.

Users and Privileges

- Linux is a multi-user system, so it is necessary to provide a permissions system to control the set of authorized operations on files and directories.
  - on a Unix system, any device is represented by a file or directory.
- Each file or directory has specific permissions for three categories of users:
  - Its owner (symbolized by u, as in User)
  - Its owner group (symbolized by g, as in Group), representing all the members of the group
  - The others (symbolized by o, as in Other)
- Three types of rights can be combined:
  - Reading (symbolized by r, as in Read);
  - Writing (or modifying, symbolized by w, as in Write);
  - Executing (symbolized by x, as in eXecute).

Users and Privileges

In the case of a file;

- read access allows reading the content (including copying).
- write access allows changing it.
- execute access allows running it (which will only work if it is a program).

In the case of a directory;

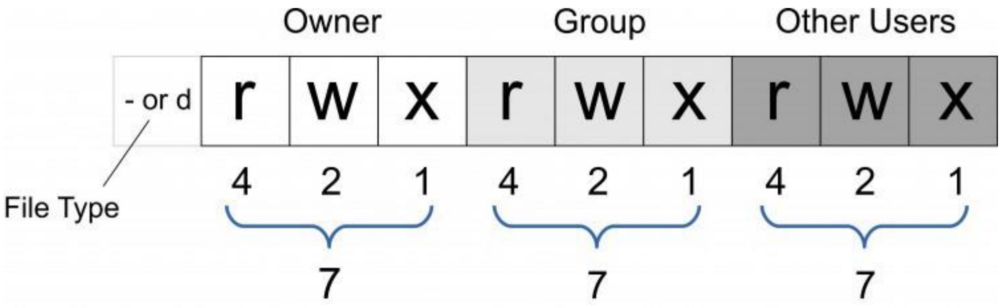
- Read access gives the right to consult the list of its contents (files and directories).
- write access allows creating or deleting files.
- execute access allows entry to the directory to access its contents.

Users and Privileges

- Three commands control the permissions associated with a file:
  - chown “user” “file” changes the owner of the file.
  - chgrp “group” “file” alters the owner group.
  - chmod “rights” “file” changes the permissions for the file.

Users and Privileges

Number	Octal Permission Representation	Ref
0	No permission	---
1	Execute permission	--x
2	Write permission	-w-
3	Execute and write permission: 1 (execute) + 2 (write) = 3	-wx
4	Read permission	r--
5	Read and execute permission: 4 (read) + 1 (execute) = 5	r-x
6	Read and write permission: 4 (read) + 2 (write) = 6	rw-
7	All permissions: 4 (read) + 2 (write) + 1 (execute) = 7	rwx



Common Linux Commands

Command	Description
cat [filename]	Display file’s contents to the standard output device (usually your monitor).
cd /directorypath	Change to directory.
chmod [options] mode filename	Change a file’s permissions.
chown [options] filename	Change who owns a file.
clear	Clear a command line screen/window for a fresh start.
cp [options] source destination	Copy files and directories.
date [options]	Display or set the system date and time.
df [options]	Display used and available disk space.
rm [options] directory	Remove (delete) file(s) and/or directories.
ps [options]	Display a snapshot of the currently running processes.
pwd	Display the pathname for the current directory.
file [options] filename	Determine what type of data is within a file.
find [pathname] [expression]	Search for files matching a provided pattern.
grep [options] pattern [filesname]	Search files or output for a particular pattern.
kill [options] pid	Stop a process. If the process refuses to stop, use kill -9 pid.
less [options] [filename]	View the contents of a file one page at a time.
su [options] [user [arguments]]	Switch to another user account.
locate filename	Search a copy of your filesystem for the specified filename.
passwd [name [password]]	Change the password or allow (for the system administrator) to change any password.
ls [options]	List directory contents.
rm [options] directory	Remove (delete) file(s) and/or directories.
mkdir [options] directory	Create a new directory.
mv [options] source destination	Rename or move file(s) or directories.

File Manipulation

The “cat” file command reads a file and displays its contents on the terminal.

cat “filename”

Most Linux Distros come with one or more text editors installed:

CLI editors e.g. Vi, Nano

GUI based Editors e.g. Mousepad, Gedit etc

simple files can sometimes be created directly from the command interpreter using redirection:

Echo “hello world!” > hello.txt creates a file with the text “hello world” inside.

Echo “hello world!” >> hello.txt appends to the file instead of overwriting it.

Managing Services

- **systemctl** with the **start** option followed by the service name is used to start services.
- SSH Service
  - The Secure SHell (SSH) 43 service is mostly used to remotely access a computer, using a secure, encrypted protocol.
  - TCP based listening by default on port 22.
    - $ sudo systemctl start ssh.
    - $ sudo systemctl enable ssh (start SSH automatically on boot).
- Confirm the SSH service is listening
    - Sudo ss –antlp | grep sshd

Managing Services

- HTTP service
  - The Apache HTTP service is often used during a penetration test, either for hosting a site, or providing a platform for downloading files to a victim machine.
  - TCP based service that listens by default on port 80
    - $ sudo systemctl start apache2
    - $ sudo systemctl enable apache2

Installing and Removing Apps

- Kali Linux makes use of the Advanced Package Tool (APT) toolset to manage application and packages.
- **Apt update**
  - it is always good practice to update the list of available packages, including information related to their versions, descriptions, etc
- **Apt upgrade**
  - After the APT database has been updated, we can upgrade the installed packages and core system to the latest versions using this command
- **apt-cache search**
  - find out whether or not an application is present in the Kali Linux repositories.

Installing and Removing Apps

- **apt Install**
  - used to add a package to the system.
    - $ sudo apt install “package name”.
- **apt remove --purge**
  - completely removes packages from Kali.
  - Adding the –purge removes all package data.
    - $ sudo apt remove –purge “package name”
- **dpkg**
  - Mainly used when operating offline to install already downloaded packages.
    - $ sudo dpkg –I “package name.deb”

Bash Environment

- Bash (Bourne Again Shell) is an sh-compatible shell that allows us to run complex commands and perform different tasks from a terminal window.
- Environmental Variables
  - They are a form of global storage for various settings inherited by any applications that are run during that terminal session. E.g.
    - PATH, USER, PWD, HOME (echo $PATH)
    - An environment variable can be defined with the export command e.g.
      - $ export b=20
      - $ print $b

Bash Environment

Tab Completion

- The Bash shell auto-complete function allows us to complete filenames and directory paths with the tab key.

Bash History

- Bash maintains a history of commands that have been entered, which can be displayed with the history command.
  - !"history number" will execute that command.
  - !! Will execute the last command.

Piping and Redirection

- Redirecting to a new file using the ">"
- Redirecting to an existing file using the ">>"
- Redirecting from a file using "<" (wc –m < ping.txt) *character count

Bash Environment

- Piping
  - redirecting the output from one command into the input of another.
    - $ cat ping.txt | wc –m > fig.txt
- Text Searching and Manipulation
  - grep: searches text files for the occurrence of a given regular expression and outputs any line containing a match.
    - $ Ls –la /usr/bin | grep conf
  - Sed: it is a very powerful and complex stream editor. Can be used to replace strings.
    - Echo “I hate hacking” | sed ‘s/hate/love/’
  - Cut: It is used to extract a section of text from a line and output it to the standard output. –f (field number) –d (delimiter)
    - $ echo “give me binaries,web apps,mobile apps, and just about anything else but nothing" | cut -f 3 -d ",“
  - Awk: is a programming language designed for text processing and is typically used as a data extraction and reporting tool. –F (field separator)
    - echo “give me binaries,web apps,mobile apps, and just about anything else but nothing“ | awk –F “,” ‘{print $1,$3}’

Bash Environment

- CLI Editors
  - Nano
    - Crtl O – write changes
    - Ctrl k – cut current line
    - Ctrl w – search
    - Ctrl X – exit
  - Vi
    - Press ‘I’ – insert mode
    - dd – delete current line
    - yy – copy current line
    - :wq – save and quit

Bash Environment

- Downloading files
  - wget: wget –o “filename” http://download
  - Curl: curl –o “filename” http://download
  - Axel: download accelerator. axel -a -n 20 –o “filename” http://download

References

- Kali Revealed 2021 edition - https://kali.training/downloads/Kali-Linux-Revealed-2021-edition.pdf