NDHU ISC Information Security Club
IAN YANG

Linux Shell

Ian

Who am I?

- Name：Ian
- Department：東華大學資管系(NDHU IM)
- Grade：大三(Junior)
- 學習資安一年多，忝為副社長

Kali Linux

- A Debian-based Linux distribution
- Aimed at advanced Penetration Testing and Security Auditing.
- Include 600 penetration testing tools
- Single user, root access by design

User

- Root (uid 0) – the God of the local host
  - The most privileged account on a Unix/Linux system.
  - Execute the initial program
  - Able to control and modify anything

Shell

- The shell is a program that takes your commands to the operating system to perform.

Syntax

prompt

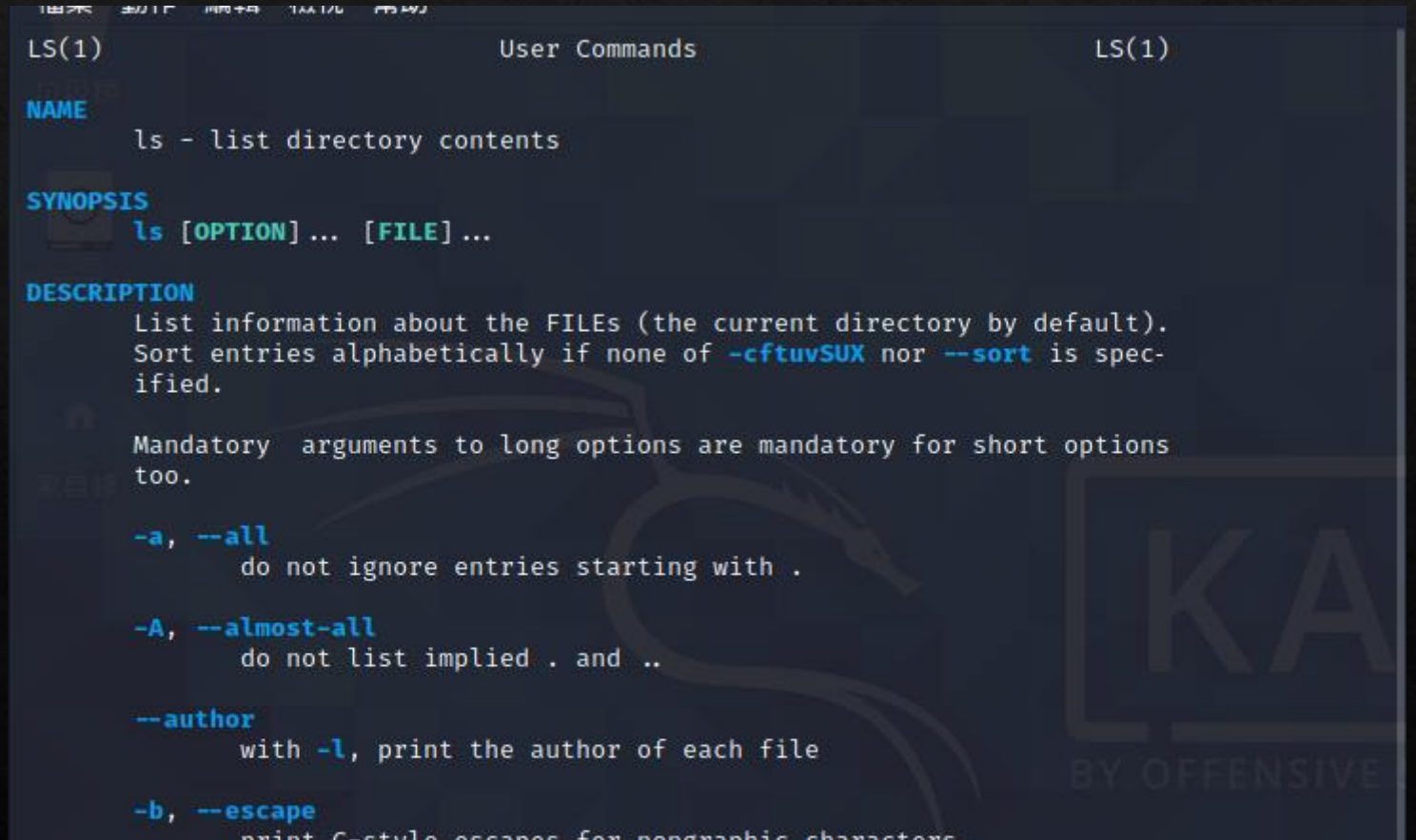
[user]@[host]:[directory]$ [command] -[short opt] --[long opt] args

ls

- List directory contents
  - -a :do not ignore entries starting with “ . ”
  - -l :use a long listing format
  - -R :list subdirectories recursively
  - .
  - .
  - .
  - Too many options!

But a command has a lot of options in facts Too hard to remember all of them!!

- Let's welcome the greatest man in the Unix/Linux world
- The "man" command - an interface to the reference manuals



```
LS(1)                          User Commands                          LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List information about the FILEs (the current directory by default).
       Sort entries alphabetically if none of -cftuvSUX nor --sort is spec-
       ified.

       Mandatory  arguments to long options are mandatory for short options
       too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
              do not list implied . and ..

       --author
              with -l, print the author of each file

       -b, --escape
```

Common command

comm	description	example
cd	change the working directory	cd /tmp ; cd - ;
echo	display a line of text	echo “hello world”; echo –e “hello\tworld\n”;
cat	concatenate files and print on the standard output	cat /etc/passwd;
ps	report a snapshot of the current processes	ps auxww;
top	display processes	top;
kill	terminate a process	kill 5566;
nc (netcat)	arbitrary TCP and UDP connections and listens	nc ip/hostname port;
apt-get	APT package handling utility	apt-get install packages;

Common command 2

comm	description	example
su	run a command with substitute user and group ID	su nobody;
touch	create a empty file	touch file;
mkdir	create a directory	mkdir dir;
cp	copy files and directories	cp file file2; cp –r dir/ /otherdir ;
mv	move (rename) files	mv file ooxx; mv dir/ newdir/
rm	remove files or directories	rm file2; rm –r newdir/
chmod	change the privilege of file	chmod 755 file; chmod [u|g|o|a][-|+][r|w|x] file;
chown	change the owner of file	chown nobody test;
exit	exit from shell	exit;

Variables & Quotes

var=value	Assign value to variable	var=“test” ;
$var ${var}	Get shell variable	echo $var;
`cmd` $(cmd)	Substitution stdout	echo `date`; $(bash);
‘string’	Quote character without substitution	echo ‘This is a $var’;
“string”	Quote character with substitution	echo “This is a $var”;

Special skill !!

Skill	Purpose	Example
*	Match any string of characters	`ls test*`
?	Match any single alphanumeric character	`ls test?`
[…]	Match any single character within […]	`ls test[123]`
[!…]	Match any single character not in […]	`ls test[!234]`
~	Home directory	`ls ~`

Special skill 2 !!

Skill	Purpose	Example
#	Start a shell comment	# this is a comment
;	Command separator	cd /tmp ; ls
&&	executes the first command, and then executes the second if first command success (exit code=0)	cd /fake/dir && touch test cd /tmp && touch test
||	executes the first command, and then executes the second if first command fail (exit code≠0)	cp x y || touch y
&	Background execution	yes &
\	Escape character	touch test*; ls

Pipe and redirect !!

Skill	Purpose	Example
cmd1 | cmd2	Pipe stdout of cmd1 as stdin of cmd2 (Note : except stderr)	ls | grep ‘c’
cmd > file	Write stdout of cmd into the file	echo “I love 5566” > lies.txt
cmd >> file	Append stdout of cmd into the file	echo “It’s true” >> lies.txt
cmd < file	Read the file as stdin to cmd	tr ‘ ’ ‘_’ < lies.txt
2>&1	Redirect stderr to stdout	ls file_not_exist 2>&1 | less

Bash Keyboard Shortcuts

- Up (Down) key : Previous (Next) command
- Ctrl + C : Send kill interrupt to the current process
- Ctrl + Z : Suspend the current process, wake up it with “fg” command
- Ctrl + D : Send EOF marker
- Ctrl + L : Clear screen
- Ctrl + A : Go to the beginning of line
- Ctrl + E : Go to the end of line
- Alt + B : Backward a word
- Alt + F : Forward a word

- More detail : http://ss64.com/bash/syntax-keyboard.html

Let’s play a game !!

- This game is Can_you _pass .
- How to play? Just input wget 134.208.97.233/Can_you _pass
- And you can get the shell (pwn).

- Source code is already in the project.

How to?

- Writing a socket program with Python?
- But I am lazy and just want using built-in command.

Demo time

Service

- service [services] start|stop|restart|reload|status
- Services are located at /etc/init.d/

- For example
  - xinetd
  - sshd
  - httpd (apache)
  - ftpd

Thank you

- The more knowledge about Linux : http://linux.vbird.org/