Chapter 9 - Exploit

Do not blindly run exploits

Searchploit - make sure you update

--what was the main point here?

-can find exploits - need to know how to read and modify. Very few will work as is.

--mingw-w64 (i686-w64-mingw32-gcc) - what does this do?

Compiles windows c code on linux

--wine

Execute windows executable on linux

Chapter 10 - File Transfer Methods

--What were the main themes?

What were the methods?

-what is meaning of interactive?

-TFTP

- pros (windows non interactive)
- cons (no longer installed by default)

-script language (copy and paste)

-powershell

-vbs

-other options?

-python simple http server

-upx (file compression via optimization - can still be executed)

-exe2bat

-converts an exe to a .txt file. Can be simply copied and pasted.

File Paths:

--If I run `cat test.txt`, where is test.txt?

--What if I run `atftp --daemon --port 69 tftp`

The point is sometimes file paths are from your perspective, sometimes from the program running. The best method is to always use the full path

--Where is your root ftp directory? Root web? Root ssh?

-/etc is where config files are. In here, you find a file or dir per service. Use these files to determine root directories.

Finally, do not run any commands from PWK without fully understanding what you are doing

--what does apt-get update do? Apt-get install? Apt-get upgrade?

--what does your ftp bash script do?

Groupadd ftypgroup?

Useradd -g ftpgroup -d /dev/null -s /etc ftpuser, etc.

What about ftp.txt?

Chapter 11 - Priv Esc

This is the weakest chapter in the book. There are many better blog posts on how to do priv esc:
Linux: https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
Windows: http://www.fuzzysecurity.com/tutorials/16.html
https://github.com/pentestmonkey
https://netsec.ws/?p=309

General Categories:
--password reuse / password cracking
--config files / script with creds
--sudo / file permissions / groups
--services with writeable executables
--new ports / avenues of approach (i.e. internally accessible services)
--Kernel exploits

What does pyinstaller.py do?

Windows priv esc commands example:

for /f "tokens=2 delims='='" %a in ('wmic service list full^|find /i "pathname"^|find /i /v "system32"') do @echo %a >> c:\windows\temp\permissions.txt

for /f eol^=^"^ delims^=^" %a in (c:\windows\temp\permissions.txt) do cmd.exe /c icacls "%a" >> c:\windows\temp\icalcsresults.txt

http://travisaltman.com/windows-privilege-escalation-via-weak-service-permissions/