

KALI LINUX CERTIFIED PROFESSIONAL

Practice Quiz FAQ

Here are some important notes to help you understand what the practice quizzes are and what they are not.

We did not use questions from the official pool for these quizzes. That would disqualify a percentage of the exam pool. We generally did not grab questions from the pool and make slight changes to the question and answers. That's basically the same thing as duplicating a question. In addition, the real exam does not provide instant feedback about your answers, making it impossible to learn potential future answers from previous questions. The practice quizzes provide this feedback, allowing you to learn from previous questions. There are no true/false questions on the final exam. Try Harder.

In order to avoid overlap, we dodged the objects of the official question pool entirely. Because of this, the vast majority of the objects of the practice questions are completely different than what's in the official pool. However, in some very rare cases, we threw in a few questions that are fairly similar to the exam, but with (often vastly) different answers to throw you off just a bit. Because of this, you can never be completely sure what, exactly, is on the final. You guessed it: Try Harder.

An astute reader and student will "fill in the blanks" between the practice quizzes, and realize that there were foundational commands, topics and processes in the book that we did not cover in the practice quizzes. You might also notice that we dive into some deeply technical topics in the practice quizzes but omit less-specific topics in that section. These topical omissions could be considered perfect candidates for the exam.

Overall, we wanted to give you a true taste of what you can expect during the exam. We probed the book equally for both the practice quizzes and the official exam in order to clearly illustrate the depth of knowledge of the Kali Revealed book you'll need to pass the final exam.

On a practical note, our team spent months creating the official exam question pool. We voted on each question, balanced the answers to avoid give-aways, attended several meetings with Pearson, nuked several questions and generally poured over the question pool. On the other hand, the practice exam was created by one person over a few weeks followed by a cursory team review. The practice quizzes contain some silly, unbalanced, give-away questions and answers; the final exam does not. In short, these practice questions were not given the same care as the official pool and are a poor reflection of the quality of the KLCP test.

But to reiterate, the practice quizzes give you a feel of what's to come, and reveal the attention you'll need to pay to our free training resources. Please let us know if you have any questions or concerns in our forums.



KLCP Practice Questions

Chapter 1

1. The most current version of Kali is:

- A rolling distribution based on Debian testing
- A rolling distribution based on Debian Wheezy stable
- A static, versioned distribution based on Debian Wheezy testing
- A static, versioned distribution based on Debian Jessie stable

Chapter 2

1. If you have a 64-bit Intel desktop, which Kali image will boot on your machine? Select all that apply.

- Kali 32-bit
- Kali 64-bit
- Kali armhf
- Kali armel

2. How can you determine whether the CPU in your Kali Linux machine is 32 or 64-bit?

- `/proc/cpuflags`
- `/proc/cpu`
- `/proc/cpuinfo`
- `/proc/system`

3. Which command will download and import the Kali public key over https?

- `gpg_import https://www.kali.org/archive-key.asc`
- `lynx http://www.kail.org/archive-key.asc | gpg_import`
- `wget -q -O - https://www.kali.org/archive-key.asc | gpg --import`
- `echo archive-key.asc | gpg --import`

4. When installing Kali Linux to a virtual machine, which installation method will most likely produce a clean install?

- Install from official, validated Kali 32-bit ISO burned to USB
- Install from official, validated Kali 32-bit ISO burned to USB with official `preseed.cfg` file
- Load official, validated Kali VM image
- Import previously installed, validated and test Kali 32-bit machine

Chapter 3

1. Which character is used to represent the user's home directory?

- ~
- !
- ?
- &

2. Which tools can be used to get file information? Check all that apply.

- pwd
- type
- which
- cat
- echo

3. Which of the following files is not a block or character device?

- `drwxr-xr-x 2 root root 60 Mar 21 08:30 vfio`
- `crw----- 1 root root 10, 63 Mar 21 08:30 vga_arbiter`
- `crw-rw---- 1 root tty 7, 132 Mar 21 08:30 vcsa4`
- `brw-rw---- 1 root disk 8, 0 Mar 21 08:30 sda`

4. How can the file permissions `-r---w----` be represented in octal notation?

- 200
- 110
- 411
- 420
- 751

5. Based on the following partial directory listing, what permissions does user have on the file test?

```
-r-x--x--- 1 user root 0 Mar 24 01:19 test
```

- Read, Write, Execute
- Read, Execute
- Execute
- No permissions

6. You have two jobs running in the background. How do you kill the first job you executed?

- killall
- kill %1
- kill -signal pid
- CTRL-C

7. Which command does not control the permissions or user attributes associated with a file ?

- chown
- chgrp
- chperm
- chmod

8. Which command displays the identity of the user running the session along with the list of groups they belong to?

- id
- whoami
- cat /etc/passwd
- who

9. Which command summarizes the PCI hardware through the /proc and /sys virtual filesystems?

- pci -v
- pciutil
- lspci
- cat /proc/pci

10. According to the FHS, which directory contains log files, queues, spools and cache data handled by daemons?

- /proc
- /var
- /sbin
- /bin

Chapter 4

1. Which is the recommended configuration for simple Intel-based Kali SSH server with no desktop (headless)?

- 128 MB RAM / 1 GB hard drive free space
- 512 MB RAM / 2 GB hard drive free space
- 2048 MB RAM / 20 GB hard drive free space
- 4096 MB RAM / 40 GB hard drive free space

2. Generally speaking, which of these is not a minimum requirement for a Kali Linux desktop?

- 20GB hard disk space
- 2 GB RAM
- adm64, i386, armel, armhf, or arm64 CPU architecture
- 1024MB RAM GPU

3. True or False: The Kali Linux installation will fail if you do not select a network mirror.

- True
- False

4. True or False: When booted from the mini.iso, the Kali Linux installation will fail is network hardware can not be detected.

- True
- False

5. Which partitioning scheme is most likely to be affected by user error?

- Guided - use entire Disk
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual

6. Which partitioning method is preferred for servers and multi-user systems?

- No Partitions
- All files in one partition
- Separate /home/ partition
- Separate /home, /var, and /tmp partitions

7. Installing a modern version of Windows after a Kali installation will:

- Fail due to a previous grub installation
- Erase the boot loader and prevent Kali from booting
- Create a fail-safe boot for Kali Linux
- Erase Kali Linux

8. What is the purpose of preseed.conf?

- Set a random seed for cryptographic functions
- Create sensible defaults for most user-land settings
- The configuration file for the preseed daemon
- Provide predetermined answers to installation questions

9. What is the simplest and most effective procedure for installing Kali on an ARM device?

- Use live-build to generate an ARM-based ISO file
- Use mini.iso to create a base system, then run apt-get update
- Boot from an official, validated Kali ARM image and follow the installation steps
- Boot from an official, validated Kali ARM image and log in with root/toor

10. Which method is not readily available for saving debug logs during a failed install?

- Save to floppy disk
- Serve up logs from web server
- Save logs to Kali bug tracker
- Save logs to a mounted file system

Chapter 5

1. You can use GNOME's control center to graphically set network options with which tool?

- ifupdown
- systemctl
- NetworkManager
- /etc/network/interfaces

2. The interfaces file is an important part of command-line network configuration. What directory is it in?

- /etc/init.d
- /etc/network
- /etc/init
- /etc/networks

3. What is the name of a command-line package typically used in Kali to configure the network from the command line?

- systemctl
- init.d
- ifupdown
- hosts

4. When configuring a network from the command line (say with ifup or ifdown) which line will begin the section for a manual network configuration?

- `iface eth0 inet dhcp`
- `iface eth0 inet static`
- `iface eth0 inet auto`
- `auto eth0`

5. Which methods can be used to configure network devices in Kali Linux? Choose all that apply:

- On the command line with `ifupdown`
- On the command line with `systemd-networkd`
- On the command line via the `/etc/network/interfaces` file
- On the command line with `.network` files in the `/etc/systemd/network` directory
- Graphically with NetworkManager
- None of the above

6. Which file contains encrypted user passwords?

- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`
- None of the above

7. Which command is used to add users to the system?

- `passwd -l`
- `adduser`
- `chuser`
- `useradd`

8. Which command will suspend a user account?

- `useradd -s olduser`
- `passwd -l olduser`
- `passwd -s olduser`
- `rmuser -l olduser`

9. Which is true of the SSH service on a default Kali install? Select all that apply.

- The SSH service is installed by default
- The SSH service is disabled by default
- The default configuration file blocks certificate-based logins
- The default configuration blocks password-based logins
- The default keys from a live image are pre-generated

10. Which command is commonly used to start services like ssh and postgresql?

- init
- run
- systemctl
- service

11. Which command can be used to create a new postgresql database?

- db_create
- createdb
- dropdb
- psql -n

12. Which command is not a postgresql command?

- psql
- createuser
- createdb
- pg_createuser

13. Which command will create a postgres database name db_new?

- createdb -T template0 -E UTF-8 -n db_new
- createdb -T template0 -E UTF-8 -O dbuser db_new
- psql -h localhost -c db_new -O dbuser dbuser
- pg_create -o dbuser -n db_new -E UTF-8

14. Which of the following are not associated with Apache2? Choose one.

- a2enmod
- /var/www/html
- /etc/apache2
- systemctl start apache

15. Which of the following are not associated with Apache2?

- DocumentRoot
- htpasswd
- .htaccess
- apachectl
- /etc/apache2/ports.conf
- /etc/apache2/mods-available

16. In Kali, what is responsible for the boot sequence, but also permanently acts as a full featured service manager, starting and monitoring services?

- systemctl
- systemd
- init.d
- grub

17. Which command will inspect the current status of the postgresql service?

- systemctl status postgresql
- sudo status postgresql
- /etc/init/postgresql status
- ps | grep postgresql

Chapter 6

1. Which command will determine if nmap has been modified by Kali?

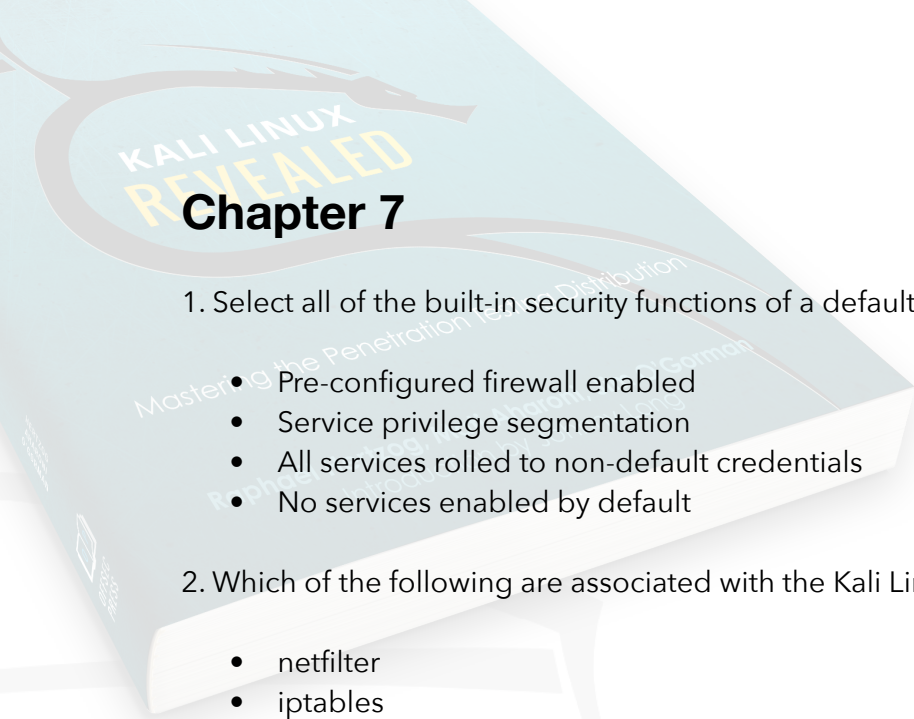
- dpkg -l | grep nmap
- dpkg -s nmap | grep ^Version
- dpkg-query -l | grep nmap
- All of the above
- None of the above

2. Which command is used to report a bug to the Kali Linux developers?

- kalibug
- bugreport
- reportbug
- irssi

3. Which of these actions can be used to submit a bug to the Debian developers? Select all that apply.

- Use the official Debian bug tracker at <https://bugs.debian.org>
- Send an email (with a special syntax) to submit@bugs.debian.org
- Use the kalidebug tool directly from Kali Linux and mark the issue as an upstream Debian issue.
- Submit the bug to the official Kali bug tracker at <https://bugs.kali.org> and mark the issue for an upstream Debian patch.



Chapter 7

1. Select all of the built-in security functions of a default installation of Kali Linux:

- Pre-configured firewall enabled
- Service privilege segmentation
- All services rolled to non-default credentials
- No services enabled by default

2. Which of the following are associated with the Kali Linux firewall? Select all that apply.

- netfilter
- iptables
- ip6tables
- fwbuilder

3. Which of the following is a default chain in the Kali Linux firewall?

- ALL
- DROP
- INPUT
- FILTER
- RAW

5. Place the chains in the proper processing order, from first to last:

- 1) PREROUTING
- 2) INPUT
- 3) FORWARD
- 4) OUTPUT
- 5) POSTROUTING

6. Which of the following will apply a special case of source NAT to packets in the Kali Linux firewall?

- SOURCE
- MASQUERADE
- DNAT
- POSTROUTE

7. Which of the following commands will block all packets originating from 8.8.8.8?

- `iptables -A ALL -s 8.8.8.8 -j DROP`
- `iptables -A INPUT -s 8.8.8.8 -t ALL -j DROP`
- `iptables -A INPUT -s 8.8.8.8 -j DROP`
- `iptables -A OUTPUT -s 8.8.8.8 -j DROP`

8. Which of the following commands is used to delete all rules in the INPUT chain?

- iptables -X INPUT
- iptables -F INPUT
- iptables -D INPUT
- iptables -R INPUT

9. Which of the following will explicitly allow SSH connections to your Kali Linux machine?

- iptables -A INPUT -p ssh -j ACCEPT
- iptables -A INPUT --dport 22 -j ACCEPT
- iptables -A INPUT --state NEW -p tcp --dport 22 -j ACCEPT
- iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT

10. Which file should be updated to enable custom firewall rules at boot-time?

- /etc/netfilter.conf
- /etc/netfilter/netfilter.conf
- /etc/init.d/netfilter
- /etc/network/interfaces

11. Which tool can be used to graphically monitor process status?

- gnome-system-monitor
- ps -ax
- ntop
- System Monitor

12. Which easily-subverted command can be used to detect suspicious packages?

- dpkg -l
- dpkg -v
- dpkg --checksum
- dpkg -V

13. Which of the following can be used to protect against brute-force logins?

- tripwire
- logcheck
- fail2ban
- AIDE



KALI LINUX REVEALED

Chapter 8

1. Which tool directly installs packages without regard for dependencies or other packages?

- dpkg
- apt
- apt-get
- aptitude
-

2. Which tool is a complete package management system designed to to install and remove applications, update packages, and even upgrade your entire system?

- /usr/bin/gnome-software
- Advanced Package Tool
- dpkg
- Package Updater

3. Which is the key configuration file for defining package sources?

- /etc/sources
- /etc/sources.list
- /etc/apt/sources.list
- /etc/apt/sources.list.d/list

4. Select the syntactically correct apt source description:

- deb http://http.kali.org/kali kali main non-free contrib
- deb ssh://http.kali.org/kali kali-rolling main non-free contrib
- deb http://http.kali.org/kali kali-rolling main free contrib
- deb http://http.kali.org/kali kali-rolling main non-free contrib

5. Which apt source description points to software that does not conform to the Debian Free Software Guidelines?

- deb http://http.kali.org/kali kali-rolling main contrib
- deb http://http.kali.org/kali kali-rolling main free contrib
- deb http://http.kali.org/kali kali-rolling main extras contrib
- deb http://http.kali.org/kali kali-rolling main non-free contrib

6. Which of the following repositories is recommended for most users?

- kali-linux
- kali-linux-full
- kali-rolling
- kali-dev
- kali bleeding-edge

7. Which command will install the man-db package?

- dpkg man-db_2.7.0.2-5_amd64.deb
- dpkg -l man-db_2.7.0.2-5_amd64.deb
- dpkg -install man-db_2.7.0.2-5_amd64.deb
- dpkg -i man-db_2.7.0.2-5_amd64.deb

8. Which command should be used for regular updates of Kali Linux and will remove obsolete packages and install new dependencies?

- apt-get update
- apt-get full-update
- apt-get upgrade
- apt-get full-upgrade

9. Which of the following commands downloads the latest list of available packages and should be run before working with apt?

- apt-update
- apt update
- apt-get update

11. Which command will show all the files installed by the metasploit-framework package?

- dpkg -L metasploit-framework
- apt list metasploit-framework
- apt-search metasploit-framework
- aptitude search metasploit-framework

12. Which of the following commands will display the name of the package that installed the file "msfconsole"?

- dpkg -S msfconsole
- apt list msfconsole
- apt-search msfconsole
- aptitude search msfconsole

13. Which of the following commands will list all packages installed on the system?

- `dpkg -l`
- `apt list`
- `apt search`
- `apt-search`

14. You need to install a package for a CPU other than the one on the current system. How would you enable this?

- `apt config --enable-foreign-architecture`
- `dpkg --add-architecture`
- `apt -a`
- `apt-get install kali-linux-foreign`

15. Which of the following are graphical front ends to Kali's package manager?

- `aptitude`
- `synaptic`
- `apt`
- `dpkg`

16. Which of the following commands shows the architectures that are installed on the current system?

- `apt print architectures`
- `dpkg --print-architecture`
- `arch --list`
- `aptitude list architectures`

17. Which file contains the most vital information about a Debian package?

- `.deb`
- `package-list`
- `control.tar.gz`
- `.pkginfo`

18. Which of the following is not a part of a standard Debian package?

- `debian-binary`
- `manifest`
- `control.tar.gz`
- `data.tar.xz`

19. Which file in a Debian package contains the actual files to be installed on the file system?

- debian-binary
- data.tar.xz
- package.tar.gz
- manifest

21. Which field in the package header will cause dpkg to refuse to install a package and trigger apt to resolve the problem by updating the incompatible package to a newer version?

- Incompat
- Breaks
- Conflicts
- Updates

22. Which of the following is not a valid Debian package configuration script?

- postinst
- preinst
- postconf
- postrm

Chapter 9

1. Which of the following commands will download the source of a Debian package?

- apt-get -S
- dpkg --source
- apt source
- aptitude --source

2. Which command will retrieve sources from a GIT repository?

- apt-get --git
- git clone
- git-get
- git-clone

3. Assuming that you are in a directory containing an unpacked source package, which command will install build dependencies listed in the Build-Depends field of the debian/control file?

- dpkg --build_dep
- apt build-dep ./
- dpkg-buildpackage
- dch --build-dep

4. Which file or command will reveal whether or not your changes to a Debian package "stuck"?

- `dch --updates`
- `debian/changelog`
- `DEBCHANGES`
- `dch --local`

5. When applying changes, which command will update the prefix used in a Debian package to "kali"?

- `dch --local kali`
- `dch --prefix kali`
- `dpkg-update -p kali`
- `dpkg-buildpackage -u kali`

6. What is the proper command for copying the config file from a running Kali Linux instance to a downloaded Kali source tree in the current directory?

- `cp /boot/config-4.9.0-kali1-amd64 ~/kernel/linux-source-4.9/.config`
- `cp /boot/kali-linux-4.9.0-kali1-amd64/ ~/kernel/linux-source-4.9/`
- `cp /boot/kali-linux-4.9.0-kali1-amd64/.config ~/kernel/linux-source-4.9/.config`
- `cp /boot/kali-linux-4.9.0-kali1-amd64/.config ~/kernel/linux-source-4.9/`

7. Which command will execute the graphical kernel configuration tool?

- `make config`
- `make menuconfig`
- `make gconfig`
- `make textconfig`

8. Which command will install the prerequisites for the Kali Linux build environment?

- `apt install livebuild`
- `apt install git livebuild`
- `apt install curl git livebuild`
- `apt install curl git live-build`

9. A user on a 32-bit operating system wishes to create a custom Kali Linux ISO image for the 64-bit architecture with the XFCE desktop environment. Assuming they are in the "live-build-config" directory, which command will accomplish their goal?

- `# ./build.sh -xfce::x64 --verbose`
- `# ./build.sh -xfce::amd64`
- `# ./build.sh --variant x64 --verbose`
- `# ./build.sh --arch amd64 --variant xfce --verbose`

10. Which metapackage installs all the tools in the default Kali Linux installation?

- kali-linux
- kali-linux-full
- kali-linux-default
- kali-linux-all

11. Which file contains the data of persisted directories?

- persist.conf
- persistence
- persistence.conf
- /union/persistence.conf

12. Which command will create an EXT3 filesystem with a label of "persistence" on the third partition of the third drive attached to the system?

- mkfs.ext3 -L persistence /dev/sdc3
- mkfs.ext3 -l persistence /dev/sdc3
- mkfs.ext3 -l persistence --part sdc3
- mkfs.ext3 -L persistence -p sdc3

13. Which command could prepare a LUKS container on /dev/sdb3 for user interaction?

- cryptsetup open -t LUKS /dev/sdb3 kali_persistence
- cryptsetup open --type LUKS /dev/sdb3 kali_persistence
- cryptsetup luksOpen /dev/sdb3 kali_persistence
- cryptsetup -o /dev/sdb3 kali_persistence

14. Which of the following will add a "nuke" password to the LUKS partition on /dev/sdb4?

- cryptsetup convert --type luksAddNuke
- cryptsetup open --type LUKS -a nuke /dev/sdb4
- cryptsetup luksAddNuke /dev/sdb4
- cryptsetup luksNukeAdd /dev/sdb4

Chapter 10

1. Which of the following are required to install Kali over the network on a machine without an operating system?

- PXE
- TFTP
- DHCP
- BOOTP
- (all)

2. Which of the following commands will install the dnmap package on salt minions?

- salt '*' -i dnmap
- salt '*' --install dnmap
- salt '*' install dnmap
- salt '*' pkg.install dnmap

3. Which of these commands will execute 'uptime; uname -a' on the kali-scratch minion?

- salt kali-scratch -x 'uptime; uname -a'
- salt kali-scratch cmd 'uptime; uname -a'
- salt kali-scratch --shell 'uptime; uname -a'
- salt kali-scratch cmd.shell 'uptime; uname -a'

4. Which of the following commands will generate a binary package from and unsigned source package with unsigned .buildinfo and .changes file?

- dpkg --build -u
- dpkg-build -p -us -ub
- dpkg-buildpackage -us -uc
- dpkg-buildpackage -us -ub

5. Which command is used to create and manage Debian repositories?

- debrepo
- reprepo
- pkgrepo
- deb_repo

6. Select all of the fields required in a repo configuration file:

- Codename
- Architectures
- Components
- Status

7. Which file should be updated on client machines wishing to access a custom repository?

- repo.conf
- sources.conf
- sources.list
- repo.list

The image shows the cover of the book 'Kali Linux Revealed: Mastering Penetration Testing Distribution'. The cover is light blue with a dark blue dragon logo at the top. The title 'KALI LINUX REVEALED' is written in large, bold, yellow and white letters. Below the title, the subtitle 'Mastering Penetration Testing Distribution' is visible in smaller white text. The authors' names, 'Rophy Aharoni, John Long', are also present. The book is shown at an angle, with its white pages visible at the bottom.

Chapter 11

1. Which of the following are not a part of the "CIA triad"?

- Confidentiality
- Classification
- Integrity
- Accessibility
- Authentication
- Availability

2. An organization owns a web server which generates revenue based on uptime. Which of the following security attributes of the system will be the primary focus of the organization?

- Accessibility
- Integrity
- Availability
- Confidentiality

3. A flaw has been found in a cryptographic algorithm that weakens the cryptographic system. Which of the following elements of the CIA triad are affected by this?

- Confidentiality
- Authentication
- Accessibility
- Classification

4. Which of the following best describes software that can be used to take advantage of a security weakness?

- vulnerability
- exploit
- patch
- race condition

5. Which of the following (derived from likelihood of occurrence and impact) provides guidance to those responsible for securing and maintaining the systems in question?

- Overall Risk
- Compliance
- Adversarial Rating
- Deviation



6. Which of the following leverages identified issues to uncover the worst-case scenario?

- Penetration Test
- Vulnerability Assessment
- Compliance Test
- Application Assessment?

7. Which of the following best describes a technique that is used to target the various applications installed on the workstation of an employee within a target organization?

- Client-Side Attack
- Denial of Service
- Memory Corruption
- SQL Injection