سرفصل آموزشی

پک پایه متخصص امنیت

فهرست سرفصل‌های دوره‌های آموزشی

سرفصل‌های دوره آموزشی

LPIC-1

Topic 101: System Architecture

101.1 Determine and configure hardware settings

Weight: 2

Description: Candidates should be able to determine and configure fundamental system hardware

Key Knowledge Areas:

- Enable and disable integrated peripherals.
- Differentiate between the various types of mass storage devices.
- Determine hardware resources for devices.
- Tools and utilities to list various hardware information (e.g. lsusb, lspci, etc.).
- Tools and utilities to manipulate USB devices.
- Conceptual understanding of sysfs, udev and dbus.

The following is a partial list of the used files, terms and utilities:

- /sys/
- /proc/
- /dev/

- modprobe
- lsmod
- lspci
- lsusb

101.2 Boot the system

Weight: 3

Description: Candidates should be able to guide the system through the booting process.

Key Knowledge Areas:

- Provide common commands to the boot loader and options to the kernel at boot time.
- Demonstrate knowledge of the boot sequence from BIOS/UEFI to boot completion.
- Understanding of SysVinit and systemd.
- Awareness of Upstart.
- Check boot events in the log files.

The following is a partial list of the used files, terms and utilities:

- dmesg
- journalctl
- BIOS
- UEFI
- bootloader
- kernel
- initramfs
- init

- SysVinit
- systemd

101.3 Change runlevels / boot targets and shutdown or reboot system

Weight: 3

Description: Candidates should be able to manage the SysVinit runlevel or systemd boot target of the system. This objective includes changing to single user mode, shutdown or rebooting the system. Candidates should be able to alert users before switching runlevels / boot targets and properly terminate processes. This objective also includes setting the default SysVinit runlevel or systemd boot target. It also includes awareness of Upstart as an alternative to SysVinit or systemd.

Key Knowledge Areas:

- Set the default runlevel or boot target.
- Change between runlevels / boot targets including single user mode.
- Shutdown and reboot from the command line.
- Alert users before switching runlevels / boot targets or other major system events.
- Properly terminate processes.
- Awareness of acpid.

The following is a partial list of the used files, terms and utilities:

- /etc/inittab
- shutdown
- init
- /etc/init.d/

- telinit
- systemd
- systemctl
- /etc/systemd/
- /usr/lib/systemd/
- wall

Topic 102: Linux Installation and Package Management

102.1 Design hard disk layout

Weight: 2

Description: Candidates should be able to design a disk partitioning scheme for a Linux system.

Key Knowledge Areas:

- Allocate filesystems and swap space to separate partitions or disks.
- Tailor the design to the intended use of the system.
- Ensure the /boot partition conforms to the hardware architecture requirements for booting.
- Knowledge of basic features of LVM.

The following is a partial list of the used files, terms and utilities:

- / (root) filesystem
- /var filesystem
- /home filesystem
- /boot filesystem

- EFI System Partition (ESP)
- swap space
- mount points
- partitions

102.2 Install a boot manager

Weight: 2

Description: Candidates should be able to select, install and configure a boot manager.

Key Knowledge Areas:

- Providing alternative boot locations and backup boot options.
- Install and configure a boot loader such as GRUB Legacy.
- Perform basic configuration changes for GRUB 2.
- Interact with the boot loader.

The following is a partial list of the used files, terms and utilities:

- menu.lst, grub.cfg and grub.conf
- grub-install
- grub-mkconfig
- MBR

102.3 Manage shared libraries

Weight: 1

Description: Candidates should be able to determine the shared libraries that executable programs depend on and install them when necessary.

Key Knowledge Areas:

- Identify shared libraries.
- Identify the typical locations of system libraries.
- Load shared libraries.

The following is a partial list of the used files, terms and utilities:

- ldd
- ldconfig
- /etc/ld.so.conf
- LD_LIBRARY_PATH

102.4 Use Debian package management

Weight: 3

Description: Candidates should be able to perform package management using the Debian package tools.

Key Knowledge Areas:

- Install, upgrade and uninstall Debian binary packages.
- Find packages containing specific files or libraries which may or may not be installed.
- Obtain package information like version, content, dependencies, package integrity and installation status (whether or not the package is installed).
- Awareness of apt.

The following is a partial list of the used files, terms and utilities:

- /etc/apt/sources.list
- dpkg
- dpkg-reconfigure
- apt-get
- apt-cache

102.5 Use RPM and YUM package management

Weight 3

Description: Candidates should be able to perform package management using RPM, YUM and Zypper.

Key Knowledge Areas:

- Install, re-install, upgrade and remove packages using RPM, YUM and Zypper.
- Obtain information on RPM packages such as version, status, dependencies, integrity and signatures.

- Determine what files a package provides, as well as find which package a specific file comes from.
- Awareness of dnf.

The following is a partial list of the used files, terms and utilities:

- rpm
- rpm2cpio
- /etc/yum.conf
- /etc/yum.repos.d/
- yum
- zypper

102.6 Linux as a virtualization guest

Weight: 1

Description: Candidates should understand the implications of virtualization and cloud computing on a Linux guest system.

Key Knowledge Areas:

- Understand the general concept of virtual machines and containers.
- Understand common elements virtual machines in an IaaS cloud, such as computing instances, block storage and networking.
- Understand unique properties of a Linux system which have to changed when a system is cloned or used as a template.
- Understand how system images are used to deploy virtual machines, cloud instances and containers.
- Understand Linux extensions which integrate Linux with a virtualization

product.
- Awareness of cloud-init.

The following is a partial list of the used files, terms and utilities:

- Virtual machine
- Linux container
- Application container
- Guest drivers
- SSH host keys
- D-Bus machine id

Topic 103: GNU and Unix Commands

103.1 Work on the command line

Weight: 4

Description: Candidates should be able to interact with shells and commands using the command line. The objective assumes the Bash shell.

Key Knowledge Areas:

- Use single shell commands and one line command sequences to perform basic tasks on the command line.
- Use and modify the shell environment including defining, referencing and exporting environment variables.
- Use and edit command history.
- Invoke commands inside and outside the defined path.

The following is a partial list of the used files, terms and utilities:

- bash
- echo
- env
- export
- pwd
- set
- unset
- type
- which
- man
- uname
- history
- .bash_history
- Quoting

103.2 Process text streams using filters

Weight: 2

Description: Candidates should be able to apply filters to text streams.

Key Knowledge Areas:

- Send text files and output streams through text utility filters to modify the output using standard UNIX commands found in the GNU textutils package.

The following is a partial list of the used files, terms and utilities:

- bzcat
- cat
- cut
- head
- less
- md5sum
- nl
- od
- paste
- sed
- sha256sum
- sha512sum
- sort
- split
- tail
- tr
- uniq
- wc
- xzcat
- zcat

103.3 Perform basic file management

Weight: 4

Description: Candidates should be able to use the basic Linux commands to manage files and directories.

Key Knowledge Areas:

- Copy, move and remove files and directories individually.
- Copy multiple files and directories recursively.
- Remove files and directories recursively.
- Use simple and advanced wildcard specifications in commands.
- Using find to locate and act on files based on type, size, or time.
- Usage of tar, cpio and dd.

The following is a partial list of the used files, terms and utilities:

- cp
- find
- mkdir
- mv
- ls
- rm
- rmdir
- touch
- tar
- cpio
- dd
- file
- gzip
- gunzip
- bzip2
- bunzip2
- xz
- unxz
- file globbing

103.4 Use streams, pipes and redirects

Weight: 4

Description: Candidates should be able to redirect streams and connect them in order to efficiently process textual data. Tasks include redirecting standard input, standard output and standard error, piping the output of one command to the input of another command, using the output of one command as arguments to another command and sending output to both stdout and a file.

Key Knowledge Areas:

- Redirecting standard input, standard output and standard error.
- Pipe the output of one command to the input of another command.
- Use the output of one command as arguments to another command.
- Send output to both stdout and a file.

The following is a partial list of the used files, terms and utilities:

- tee
- xargs

103.5 Create, monitor and kill processes

Weight: 4

Description: Candidates should be able to perform basic process management.

Key Knowledge Areas:

- Run jobs in the foreground and background.
- Signal a program to continue running after logout.
- Monitor active processes.
- Select and sort processes for display.
- Send signals to processes.

The following is a partial list of the used files, terms and utilities:

- &
- bg
- fg
- jobs
- kill
- nohup
- ps
- top
- free
- uptime
- pgrep
- pkill
- killall
- watch
- screen
- tmux

103.6 Modify process execution priorities

Weight: 2

Description: Candidates should should be able to manage process execution priorities.

Key Knowledge Areas:

- Know the default priority of a job that is created.
- Run a program with higher or lower priority than the default.
- Change the priority of a running process.

The following is a partial list of the used files, terms and utilities:

- nice
- ps
- renice
- top

103.7 Search text files using regular expressions

Weight: 3

Description: Candidates should be able to manipulate files and text data using regular expressions. This objective includes creating simple regular expressions containing several notational elements as well as understanding the differences between basic and extended regular expressions. It also includes using regular expression tools to perform searches through a filesystem or file content.

Key Knowledge Areas:

- Create simple regular expressions containing several notational elements.
- Understand the differences between basic and extended regular expressions.
- Understand the concepts of special characters, character classes, quantifiers and anchors.
- Use regular expression tools to perform searches through a filesystem or file content.
- Use regular expressions to delete, change and substitute text.

The following is a partial list of the used files, terms and utilities:

- grep
- egrep
- fgrep
- sed
- regex(7)

103.8 Basic file editing

Weight: 3

Description: Candidates should be able to edit text files using vi. This objective includes vi navigation, vi modes, inserting, editing, deleting, copying and finding text. It also includes awareness of other common editors and setting the default editor.

Key Knowledge Areas:

- Navigate a document using vi.
- Understand and use vi modes.
- Insert, edit, delete, copy and find text in vi.
- Awareness of Emacs, nano and vim.
- Configure the standard editor.

Terms and Utilities:

- vi
- /, ?
- h,j,k,l
- i, o, a
- d, p, y, dd, yy
- ZZ, :w!, :q!
- EDITOR

Topic 104: Devices, Linux Filesystems, Filesystem Hierarchy Standard

104.1 Create partitions and filesystems

Weight: 2

Description: Candidates should be able to configure disk partitions and then create filesystems on media such as hard disks. This includes the handling of swap partitions.

Key Knowledge Areas:

- Manage MBR and GPT partition tables
- Use various mkfs commands to create various filesystems such as:
- ext2/ext3/ext4
- XFS
- VFAT
- exFAT
- Basic feature knowledge of Btrfs, including multi-device filesystems, compression and subvolumes.

The following is a partial list of the used files, terms and utilities:

- fdisk
- gdisk
- parted
- mkfs
- mkswap

104.2 Maintain the integrity of filesystems

Weight: 2

Description: Candidates should be able to maintain a standard filesystem, as well as the extra data associated with a journaling filesystem.

Key Knowledge Areas:

- Verify the integrity of filesystems.
- Monitor free space and inodes.
- Repair simple filesystem problems.

The following is a partial list of the used files, terms and utilities:

- du
- df
- fsck
- e2fsck
- mke2fs
- tune2fs
- xfs_repair
- xfs_fsr
- xfs_db

104.3 Control mounting and unmounting of filesystems

Weight: 3

Description: Candidates should be able to configure the mounting of a filesystem.

Key Knowledge Areas:

- Manually mount and unmount filesystems.
- Configure filesystem mounting on bootup.
- Configure user mountable removable filesystems.
- Use of labels and UUIDs for identifying and mounting file systems.
- Awareness of systemd mount units.

The following is a partial list of the used files, terms and utilities:

- /etc/fstab
- /media/
- mount
- umount
- blkid
- lsblk

104.4 Removed

104.5 Manage file permissions and ownership

Weight: 3

Description: Candidates should be able to control file access through the proper use of permissions and ownerships.

Key Knowledge Areas:

- Manage access permissions on regular and special files as well as directories.
- Use access modes such as suid, sgid and the sticky bit to maintain security.
- Know how to change the file creation mask.
- Use the group field to grant file access to group members.

The following is a partial list of the used files, terms and utilities:

- chmod
- umask
- chown
- chgrp

104.6 Create and change hard and symbolic links

Weight: 2

Description: Candidates should be able to create and manage hard and symbolic links to a file.

Key Knowledge Areas:

- Create links.
- Identify hard and/or soft links.
- Copying versus linking files.
- Use links to support system administration tasks.

The following is a partial list of the used files, terms and utilities:

- ln
- ls

104.7 Find system files and place files in the correct location

Weight: 2

Description: Candidates should be thoroughly familiar with the Filesystem Hierarchy Standard (FHS), including typical file locations and directory classifications.

Key Knowledge Areas:

- Understand the correct locations of files under the FHS.
- Find files and commands on a Linux system.
- Know the location and purpose of important file and directories as defined in the FHS.

The following is a partial list of the used files, terms and utilities:

- find
- locate
- updatedb
- whereis
- which
- type
- /etc/updatedb.conf

Topic 105: Shells and Shell Scripting

105.1 Customize and use the shell environment

Weight: 4

Description: Candidates should be able to customize shell environments to meet users' needs. Candidates should be able to modify global and user profiles.

Key Knowledge Areas:

- Set environment variables (e.g. PATH) at login or when spawning a new shell.
- Write Bash functions for frequently used sequences of commands.
- Maintain skeleton directories for new user accounts.
- Set command search path with the proper directory.

The following is a partial list of the used files, terms and utilities:

- source
- /etc/bash.bashrc
- /etc/profile
- env
- export
- set
- unset
- ~/.bash_profile
- ~/.bash_login
- ~/.profile
- ~/.bashrc

- ~/.bash_logout
- function
- alias

105.2 Customize or write simple scripts

Weight: 4

Description: Candidates should be able to customize existing scripts, or write simple new Bash scripts.

Key Knowledge Areas:

- Use standard sh syntax (loops, tests).
- Use command substitution.
- Test return values for success or failure or other information provided by a command.
- Execute chained commands.
- Perform conditional mailing to the superuser.
- Correctly select the script interpreter through the shebang (#!) line.
- Manage the location, ownership, execution and suid-rights of scripts.

The following is a partial list of the used files, terms and utilities:

- for
- while
- test
- if
- read
- seq
- exec
- ||
- &&

Topic 106: User Interfaces and Desktops

106.1 Install and configure X11

Weight: 2

Description: Candidates should be able to install and configure X11.

Key Knowledge Areas:

- Understanding of the X11 architecture.
- Basic understanding and knowledge of the X Window configuration file.
- Overwrite specific aspects of Xorg configuration, such as keyboard layout.
- Understand the components of desktop environments, such as display managers and window managers.
- Manage access to the X server and display applications on remote X servers.
- Awareness of Wayland.

The following is a partial list of the used files, terms and utilities:

- /etc/X11/xorg.conf
- /etc/X11/xorg.conf.d/
- ~/.xsession-errors
- xhost
- xauth
- DISPLAY
- X

106.2 Graphical Desktops

Weight: 1

Description: Candidates should be aware of major Linux desktops. Furthermore, candidates should be aware of protocols used to access remote desktop sessions.

Key Knowledge Areas:

- Awareness of major desktop environments
- Awareness of protocols to access remote desktop sessions

The following is a partial list of the used files, terms and utilities:

- KDE
- Gnome
- Xfce

- X11
- XDMCP
- VNC
- Spice
- RDP

106.3 Accessibility

Weight: 1

Description: Demonstrate knowledge and awareness of accessibility technologies.

Key Knowledge Areas:

- Basic knowledge of visual settings and themes.
- Basic knowledge of assistive technology.

The following is a partial list of the used files, terms and utilities:

- High Contrast/Large Print Desktop Themes.
- Screen Reader.
- Braille Display.
- Screen Magnifier.
- On-Screen Keyboard.
- Sticky/Repeat keys.
- Slow/Bounce/Toggle keys.
- Mouse keys.
- Gestures.
- Voice recognition.

Topic 107: Administrative Tasks

107.1 Manage user and group accounts and related system files

Weight: 5

Description: Candidates should be able to add, remove, suspend and change user accounts.

Key Knowledge Areas:

- Add, modify and remove users and groups.
- Manage user/group info in password/group databases.
- Create and manage special purpose and limited accounts.

The following is a partial list of the used files, terms and utilities:

- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/skel/
- chage
- getent
- groupadd
- groupdel
- groupmod
- passwd
- useradd
- userdel
- usermod

107.2 Automate system administration tasks by scheduling jobs

Weight: 4

Description: Candidates should be able to use cron and systemd timers to run jobs at regular intervals and to use at to run jobs at a specific time.

Key Knowledge Areas:

- Manage cron and at jobs.
- Configure user access to cron and at services.
- Understand systemd timer units.

The following is a partial list of the used files, terms and utilities:

- /etc/cron.{d,daily,hourly,monthly,weekly}/
- /etc/at.deny
- /etc/at.allow
- /etc/crontab
- /etc/cron.allow
- /etc/cron.deny
- /var/spool/cron/
- crontab
- at
- atq
- atrm
- systemctl
- systemd-run

107.3 Localisation and internationalisation

Weight: 3

Description: Candidates should be able to localize a system in a different language than English. As well, an understanding of why LANG=C is useful when scripting.

Key Knowledge Areas:

- Configure locale settings and environment variables.
- Configure timezone settings and environment variables.

The following is a partial list of the used files, terms and utilities:

- /etc/timezone
- /etc/localtime
- /usr/share/zoneinfo/
- LC_*
- LC_ALL
- LANG
- TZ
- /usr/bin/locale
- tzselect
- timedatectl
- date
- iconv
- UTF-8
- ISO-8859
- ASCII
- Unicode

Topic 108: Essential System Services

108.1 Maintain system time

Weight: 3

Description: Candidates should be able to properly maintain the system time and synchronize the clock via NTP.

Key Knowledge Areas:

- Set the system date and time.
- Set the hardware clock to the correct time in UTC.
- Configure the correct timezone.
- Basic NTP configuration using ntpd and chrony.
- Knowledge of using the pool.ntp.org service.
- Awareness of the ntpq command.

The following is a partial list of the used files, terms and utilities:

- /usr/share/zoneinfo/
- /etc/timezone
- /etc/localtime
- /etc/ntp.conf
- /etc/chrony.conf
- date
- hwclock
- timedatectl
- ntpd
- ntpdate
- chronyc
- pool.ntp.org

108.2 System logging

Weight: 4

Description: Candidates should be able to configure rsyslog. This objective also includes configuring the logging daemon to send log output to a central log server or accept log output as a central log server. Use of the systemd journal subsystem is covered. Also, awareness of syslog and syslog-ng as alternative logging systems is included.

Key Knowledge Areas:

- Basic configuration of rsyslog.
- Understanding of standard facilities, priorities and actions.
- Query the systemd journal.
- Filter systemd journal data by criteria such as date, service or priority.
- Configure persistent systemd journal storage and journal size.
- Delete old systemd journal data.
- Retrieve systemd journal data from a rescue system or file system copy.
- Understand interaction of rsyslog with systemd-journald.
- Configuration of logrotate.
- Awareness of syslog and syslog-ng.

Terms and Utilities:

- /etc/rsyslog.conf
- /var/log/
- logger
- logrotate
- /etc/logrotate.conf
- /etc/logrotate.d/
- journalctl

- systemd-cat
- /etc/systemd/journald.conf
- /var/log/journal/

108.3 Mail Transfer Agent (MTA) basics

Weight: 3

Description: Candidates should be aware of the commonly available MTA programs and be able to perform basic forward and alias configuration on a client host. Other configuration files are not covered.

Key Knowledge Areas:

- Create e-mail aliases.
- Configure e-mail forwarding.
- Knowledge of commonly available MTA programs (postfix, sendmail, exim) (no configuration).

Terms and Utilities:

- ~/.forward
- sendmail emulation layer commands
- newaliases
- mail
- mailq
- postfix
- sendmail
- exim

108.4 Manage printers and printing

Weight: 2

Description: Candidates should be able to manage print queues and user print jobs using CUPS and the LPD compatibility interface.

Key Knowledge Areas:

- Basic CUPS configuration (for local and remote printers).
- Manage user print queues.
- Troubleshoot general printing problems.
- Add and remove jobs from configured printer queues.

The following is a partial list of the used files, terms and utilities:

- CUPS configuration files, tools and utilities
- /etc/cups/
- lpd legacy interface (lpr, lprm, lpq)

Topic 109: Networking Fundamentals

109.1 Fundamentals of internet protocols

Weight: 4

Description: Candidates should demonstrate a proper understanding of TCP/IP network fundamentals.

Key Knowledge Areas:

- Demonstrate an understanding of network masks and CIDR notation.
- Knowledge of the differences between private and public “dotted quad” IP addresses.
- Knowledge about common TCP and UDP ports and services (20, 21, 22, 23, 25, 53, 80, 110, 123, 139, 143, 161, 162, 389, 443, 465, 514, 636, 993, 995).
- Knowledge about the differences and major features of UDP, TCP and ICMP.
- Knowledge of the major differences between IPv4 and IPv6.
- Knowledge of the basic features of IPv6.

The following is a partial list of the used files, terms and utilities:

- /etc/services
- IPv4, IPv6
- Subnetting
- TCP, UDP, ICMP

109.2 Persistent network configuration

Weight: 4

Description: Candidates should be able to manage the persistent network configuration of a Linux host.

Key Knowledge Areas:

- Understand basic TCP/IP host configuration.

- Configure ethernet and wi-fi network using NetworkManager.
- Awareness of systemd-networkd.

The following is a partial list of the used files, terms and utilities:

- /etc/hostname
- /etc/hosts
- /etc/nsswitch.conf
- /etc/resolv.conf
- nmcli
- hostnamectl
- ifup
- ifdown

109.3 Basic network troubleshooting

Weight: 4

Description: Candidates should be able to troubleshoot networking issues on client hosts.

Key Knowledge Areas:

- Manually configure network interfaces, including viewing and changing the configuration of network interfaces using iproute2.
- Manually configure routing, including viewing and changing routing tables and setting the default route using iproute2.
- Debug problems associated with the network configuration.
- Awareness of legacy net-tools commands.

The following is a partial list of the used files, terms and utilities:

- ip
- hostname
- ss
- ping
- ping6
- traceroute
- traceroute6
- tracepath
- tracepath6
- netcat
- ifconfig
- netstat
- route

109.4 Configure client side DNS

Weight: 2

Description: Candidates should be able to configure DNS on a client host.

Key Knowledge Areas:

- Query remote DNS servers.
- Configure local name resolution and use remote DNS servers.
- Modify the order in which name resolution is done.
- Debug errors related to name resolution.
- Awareness of systemd-resolved.

The following is a partial list of the used files, terms and utilities:

- /etc/hosts
- /etc/resolv.conf
- /etc/nsswitch.conf
- host
- dig
- getent

Topic 110: Security

110.1 Perform security administration tasks

Weight: 3

Description: Candidates should know how to review system configuration to ensure host security in accordance with local security policies.

Key Knowledge Areas:

- Audit a system to find files with the suid/sgid bit set.
- Set or change user passwords and password aging information.
- Being able to use nmap and netstat to discover open ports on a system.
- Set up limits on user logins, processes and memory usage.
- Determine which users have logged in to the system or are currently logged in.
- Basic sudo configuration and usage.

The following is a partial list of the used files, terms and utilities:

- find
- passwd
- fuser
- lsof
- nmap
- chage
- netstat
- sudo
- /etc/sudoers
- su
- usermod
- ulimit
- who, w, last

110.2 Setup host security

Weight: 3

Description: Candidates should know how to set up a basic level of host security.

Key Knowledge Areas:

- Awareness of shadow passwords and how they work.
- Turn off network services not in use.
- Understand the role of TCP wrappers.

The following is a partial list of the used files, terms and utilities:

- /etc/nologin
- /etc/passwd
- /etc/shadow
- /etc/xinetd.d/
- /etc/xinetd.conf
- systemd.socket
- /etc/inittab
- /etc/init.d/
- /etc/hosts.allow
- /etc/hosts.deny

110.3 Securing data with encryption

Weight: 4

Description: The candidate should be able to use public key techniques to secure data and communication.

Key Knowledge Areas:

- Perform basic OpenSSH 2 client configuration and usage.
- Understand the role of OpenSSH 2 server host keys.
- Perform basic GnuPG configuration, usage and revocation.
- Use GPG to encrypt, decrypt, sign and verify files.
- Understand SSH port tunnels (including X11 tunnels).

The following is a partial list of the used files, terms and utilities:

- ssh
- ssh-keygen
- ssh-agent
- ssh-add
- ~/.ssh/id_rsa and id_rsa.pub
- ~/.ssh/id_dsa and id_dsa.pub
- ~/.ssh/id_ecdsa and id_ecdsa.pub
- ~/.ssh/id_ed25519 and id_ed25519.pub
- /etc/ssh/ssh_host_rsa_key and ssh_host_rsa_key.pub
- /etc/ssh/ssh_host_dsa_key and ssh_host_dsa_key.pub
- /etc/ssh/ssh_host_ecdsa_key and ssh_host_ecdsa_key.pub
- /etc/ssh/ssh_host_ed25519_key and ssh_host_ed25519_key.pub
- ~/.ssh/authorized_keys
- ssh_known_hosts
- gpg
- gpg-agent
- ~/.gnupg/

Future Change Considerations

Future changes to the objective will/may include:

- Remove ifup/ifdown and legacy net-tools command
- Remove TCP wrappers

LPIC-2

Topic 200: Capacity Planning

200.1 Measure and Troubleshoot Resource Usage

Weight: 6

Description: Candidates should be able to measure hardware resource and network bandwidth, identify and troubleshoot resource problems.

Key Knowledge Areas:

- Measure CPU usage
- Measure memory usage
- Measure disk I/O
- Measure network I/O
- Measure firewalling and routing throughput
- Map client bandwidth usage
- Match / correlate system symptoms with likely problems
- Estimate throughput and identify bottlenecks in a system including networking

The following is a partial list of the used files, terms and utilities:

- iostat
- netstat
- w
- top
- sar
- processes blocked on I/O
- blocks out
- vmstat
- pstree, ps
- lsof
- uptime
- swap
- blocks in

200.2 Predict Future Resource Needs

Weight: 2

Description: Candidates should be able to monitor resource usage to predict future resource needs.

Key Knowledge Areas:

- Use monitoring and measurement tools to monitor IT infrastructure usage.
- Predict capacity break point of a configuration
- Observe growth rate of capacity usage
- Graph the trend of capacity usage
- Awareness of monitoring solutions such as Icinga2, Nagios, collectd, MRTG and Cacti

The following is a partial list of the used files, terms and utilities:

- diagnose
- predict growth
- resource exhaustion

Topic 201: Linux Kernel

201.1 Kernel Components

Weight: 2

Description: Candidates should be able to utilize kernel components that are necessary to specific hardware, hardware drivers, system resources and requirements. This objective includes implementing different types of kernel images, identifying stable and development kernels and patches, as well as using kernel modules.

Key Knowledge Areas:

- Kernel 2.6.x, 3.x and 4.x documentation

Terms and Utilities:

- /usr/src/linux/
- /usr/src/linux/Documentation/
- zImage
- bzImage
- xz compression

201.2 Compiling a kernel

Weight: 3

Description: Candidates should be able to properly configure a kernel to include or disable specific features of the Linux kernel as necessary. This objective includes compiling and recompiling the Linux kernel as needed, updating and noting changes in a new kernel, creating an initrd image and installing new kernels.

Key Knowledge Areas:

- /usr/src/linux/
- Kernel Makefiles
- Kernel 2.6.x/3.x make targets
- Customize the current kernel configuration.
- Build a new kernel and appropriate kernel modules.
- Install a new kernel and any modules.
- Ensure that the boot manager can locate the new kernel and associated files.
- Module configuration files
- Use DKMS to compile kernel modules.
- Awareness of dracut

Terms and Utilities:

- mkinitrd
- mkinitramfs
- make
- make targets (all, config, xconfig, menuconfig, gconfig, oldconfig, mrproper, zImage, bzImage, modules, modules_install, rpm-pkg, bin-rpm-pkg, deb-pkg)

- gzip
- bzip2
- module tools
- /usr/src/linux/.config
- /lib/modules/kernel-version/
- depmod
- dkms

201.3 Kernel runtime management and troubleshooting

Weight: 4

Description: Candidates should be able to manage and/or query a 2.6.x, 3.x or 4.x kernel and its loadable modules. Candidates should be able to identify and correct common boot and run time issues. Candidates should understand device detection and management using udev. This objective includes troubleshooting udev rules.

Key Knowledge Areas:

- Use command-line utilities to get information about the currently running kernel and kernel modules
- Manually load and unload kernel modules
- Determine when modules can be unloaded
- Determine what parameters a module accepts
- Configure the system to load modules by names other than their file name.
- /proc filesystem
- Content of /, /boot/ , and /lib/modules/
- Tools and utilities to analyze information about the available hardware
- udev rules

Terms and Utilities:

- /lib/modules/kernel-version/modules.dep
- module configuration files in /etc/
- /proc/sys/kernel/
- /sbin/depmod
- /sbin/rmmod
- /sbin/modinfo
- /bin/dmesg
- /sbin/lspci
- /usr/bin/lsdev
- /sbin/lsmod
- /sbin/modprobe
- /sbin/insmod
- /bin/uname
- /usr/bin/lsusb
- /etc/sysctl.conf, /etc/sysctl.d/
- /sbin/sysctl
- udevmonitor
- udevadm monitor
- /etc/udev/

Topic 202: System Startup

202.1 Customizing SysV-init system startup

Weight: 3

Description: Candidates should be able to query and modify the behaviour of system services at various targets / run levels. A thorough understanding of the systemd, SysV Init and the Linux boot process is required. This objective includes interacting with systemd targets and SysV init run levels.

Key Knowledge Areas:

- Systemd
- SysV init
- Linux Standard Base Specification (LSB)

Terms and Utilities:

- /usr/lib/systemd/
- /etc/systemd/
- /run/systemd/
- systemctl
- systemd-delta
- /etc/inittab
- /etc/init.d/
- /etc/rc.d/
- chkconfig
- update-rc.d
- init and telinit

202.2 System Recovery

Weight: 4

Description: Candidates should be able to properly manipulate a Linux system during both the boot process and during recovery mode.
This objective includes using both the init utility and init-related kernel options. Candidates should be able to determine the cause of errors in loading and usage of bootloaders. GRUB version 2 and GRUB Legacy are the bootloaders of interest. Both BIOS and UEFI systems are covered.

Key Knowledge Areas:

- BIOS and UEFI
- NVMe booting
- GRUB version 2 and Legacy
- grub shell
- boot loader start and hand off to kernel
- kernel loading
- hardware initialisation and setup
- daemon/service initialisation and setup
- Know the different boot loader install locations on a hard disk or removable device.
- Overwrite standard boot loader options and using boot loader shells.
- Use systemd rescue and emergency modes.

Terms and Utilities:

- mount
- fsck
- inittab, telinit and init with SysV init
- The contents of /boot/, /boot/grub/ and /boot/efi/
- EFI System Partition (ESP)
- GRUB
- grub-install
- efibootmgr
- UEFI shell
- initrd, initramfs
- Master boot record
- systemctl

202.3 Alternate Bootloaders

Weight: 2

Description: Candidates should be aware of other bootloaders and their major features.

Key Knowledge Areas:

- SYSLINUX, ISOLINUX, PXELINUX
- Understanding of PXE for both BIOS and UEFI
- Awareness of systemd-boot and U-Boot

Terms and Utilities:

- syslinux
- extlinux
- isolinux.bin
- isolinux.cfg
- isohdpfx.bin
- efiboot.img
- pxelinux.0
- pxelinux.cfg/
- uefi/shim.efi
- uefi/grubx64.efi

Topic 203: Filesystem and Devices

203.1 Operating the Linux filesystem

Weight: 4

Description: Candidates should be able to properly configure and navigate the standard Linux filesystem. This objective includes configuring and mounting various filesystem types.

Key Knowledge Areas:

- The concept of the fstab configuration
- Tools and utilities for handling swap partitions and files
- Use of UUIDs for identifying and mounting file systems
- Understanding of systemd mount units

Terms and Utilities:

- /etc/fstab
- /etc/mtab
- /proc/mounts
- mount and umount
- blkid
- sync
- swapon
- swapoff

203.2 Maintaining a Linux filesystem

Weight: 3

Description: Candidates should be able to properly maintain a Linux filesystem using system utilities. This objective includes manipulating standard filesystems and monitoring SMART devices.

Key Knowledge Areas:

- Tools and utilities to manipulate and ext2, ext3 and ext4
- Tools and utilities to perform basic Btrfs operations, including subvolumes and snapshots
- Tools and utilities to manipulate XFS
- Awareness of ZFS

Terms and Utilities:

- mkfs (mkfs.*)
- mkswap
- fsck (fsck.*)
- tune2fs, dumpe2fs and debugfs
- btrfs, btrfs-convert
- xfs_info, xfs_check, xfs_repair, xfsdump and xfsrestore
- smartd, smartctl

203.3 Creating and configuring filesystem options

Weight: 2

Description: Candidates should be able to configure automount filesystems using AutoFS. This objective includes configuring automount for network and device filesystems. Also included is creating filesystems for devices such as CD-ROMs and a basic feature knowledge of encrypted filesystems.

Key Knowledge Areas:

- autofs configuration files
- Understanding of automount units
- UDF and ISO9660 tools and utilities
- Awareness of other CD-ROM filesystems (HFS)
- Awareness of CD-ROM filesystem extensions (Joliet, Rock Ridge, El Torito)
- Basic feature knowledge of data encryption (dm-crypt / LUKS)

Terms and Utilities:

- /etc/auto.master
- /etc/auto.[dir]
- mkisofs
- cryptsetup

Topic 204: Advanced Storage Device Administration

204.1 Configuring RAID

Weight: 3

Description: Candidates should be able to configure and implement software RAID. This objective includes using and configuring RAID 0, 1 and 5.

Key Knowledge Areas:

- Software raid configuration files and utilities

Terms and Utilities:

- mdadm.conf
- mdadm
- /proc/mdstat
- partition type 0xFD

204.2 Adjusting Storage Device Access

Weight: 2

Description: Candidates should be able to configure kernel options to support various drives. This objective includes software tools to view & modify hard disk settings including iSCSI devices.

Key Knowledge Areas:

- Tools and utilities to configure DMA for IDE devices including ATAPI and SATA
- Tools and utilities to configure Solid State Drives including AHCI and NVMe
- Tools and utilities to manipulate or analyse system resources (e.g. interrupts)
- Awareness of sdparm command and its uses
- Tools and utilities for iSCSI
- Awareness of SAN, including relevant protocols (AoE, FCoE)

Terms and Utilities:

- hdparm, sdparm
- nvme
- tune2fs
- fstrim
- sysctl
- /dev/hd*, /dev/sd*, /dev/nvme*
- iscsiadm, scsi_id, iscsid and iscsid.conf
- WWID, WWN, LUN numbers

204.3 Logical Volume Manager

Weight: 3

Description: Candidates should be able to create and remove logical volumes, volume groups, and physical volumes. This objective includes snapshots and resizing logical volumes.

Key Knowledge Areas:

- Tools in the LVM suite
- Resizing, renaming, creating, and removing logical volumes, volume groups, and physical volumes
- Creating and maintaining snapshots
- Activating volume groups

Terms and Utilities:

- /sbin/pv*
- /sbin/lv*
- /sbin/vg*
- mount
- /dev/mapper/
- lvm.conf

Topic 205: Network Configuration

205.1 Basic networking configuration

Weight: 3

Description: Candidates should be able to configure a network device to be able to connect to a local, wired or wireless, and a wide-area network. This objective includes being able to communicate between various sub-nets within a single network including both IPv4 and IPv6 networks.

Key Knowledge Areas:

- Utilities to configure and manipulate ethernet network interfaces
- Configuring basic access to wireless networks

Terms and Utilities:

- ip
- ifconfig
- route
- arp
- iw
- iwconfig
- iwlist

205.2 Advanced Network Configuration and Troubleshooting

Weight: 4

Description: Candidates should be able to configure a network device to implement various network authentication schemes.
This objective includes configuring a multi-homed network device and resolving communication problems.

Key Knowledge Areas:

- Utilities to manipulate routing tables
- Utilities to configure and manipulate ethernet network interfaces
- Utilities to analyze the status of the network devices
- Utilities to monitor and analyze the TCP/IP traffic

Terms and Utilities:

- ip
- ifconfig
- route
- arp
- ss
- netstat
- lsof
- ping, ping6
- nc
- tcpdump
- nmap

205.3 Troubleshooting Network Issues

Weight: 4

Description: Candidates should be able to identify and correct common network setup issues, to include knowledge of locations for basic configuration files and commands.

Key Knowledge Areas:

- Location and content of access restriction files
- Utilities to configure and manipulate ethernet network interfaces
- Utilities to manage routing tables
- Utilities to list network states.
- Utilities to gain information about the network configuration
- Methods of information about the recognized and used hardware devices
- System initialization files and their contents (SysV init process)
- Awareness of NetworkManager and its impact on network configuration

Terms and Utilities:

- ip
- ifconfig
- route
- ss
- netstat
- /etc/network/, /etc/sysconfig/network-scripts/
- ping, ping6
- traceroute, traceroute6
- mtr

- hostname
- System log files such as /var/log/syslog, /var/log/messages and the systemd journal
- dmesg
- /etc/resolv.conf
- /etc/hosts
- /etc/hostname, /etc/HOSTNAME
- /etc/hosts.allow, /etc/hosts.deny

Topic 206: System Maintenance

206.1 Make and install programs from source

Weight: 2

Description: Candidates should be able to build and install an executable program from source. This objective includes being able to unpack a file of sources.

Key Knowledge Areas:

- Unpack source code using common compression and archive utilities
- Understand basics of invoking make to compile programs
- Apply parameters to a configure script
- Know where sources are stored by default

Terms and Utilities:

- /usr/src/
- gunzip
- gzip
- bzip2
- xz
- tar
- configure
- make
- uname
- install
- patch

206.2 Backup operations

Weight: 3

Description: Candidates should be able to use system tools to back up important system data.

Key Knowledge Areas:

- Knowledge about directories that have to be include in backups
- Awareness of network backup solutions such as Amanda, Bacula, Bareos and BackupPC
- Knowledge of the benefits and drawbacks of tapes, CDR, disk or other backup media
- Perform partial and manual backups.
- Verify the integrity of backup files.
- Partially or fully restore backups.

Terms and Utilities:

- /bin/sh
- dd
- tar
- /dev/st* and /dev/nst*
- mt
- rsync

206.3 Notify users on system-related issues

Weight: 1

Description: Candidates should be able to notify the users about current issues related to the system.

Key Knowledge Areas:

Automate communication with users through logon messages
Inform active users of system maintenance

Terms and Utilities:

- /etc/issue
- /etc/issue.net
- /etc/motd
- wall
- /sbin/shutdown
- systemctl

Topic 207: Domain Name Server

207.1 Basic DNS server configuration

Weight: 3

Description: Candidates should be able to configure BIND to function as a caching-only DNS server. This objective includes the ability to manage a running server and configuring logging.

Key Knowledge Areas:

- BIND 9.x configuration files, terms and utilities
- Defining the location of the BIND zone files in BIND configuration files
- Reloading modified configuration and zone files
- Awareness of dnsmasq, djbdns and PowerDNS as alternate name servers

The following is a partial list of the used files, terms and utilities:

- /etc/named.conf
- /var/named/
- /usr/sbin/rndc
- kill
- host
- dig

207.2 Create and maintain DNS zones

Weight: 3

Description: Candidates should be able to create a zone file for a forward or reverse zone and hints for root level servers. This objective includes setting appropriate values for records, adding hosts in zones and adding zones to the DNS. A candidate should also be able to delegate zones to another DNS server.

Key Knowledge Areas:

- BIND 9 configuration files, terms and utilities
- Utilities to request information from the DNS server
- Layout, content and file location of the BIND zone files
- Various methods to add a new host in the zone files, including reverse zones

Terms and Utilities:

- /var/named/
- zone file syntax
- resource record formats
- named-checkzone
- named-compilezone
- masterfile-format
- dig
- nslookup
- host

207.3 Securing a DNS server

Weight: 2

Description: Candidates should be able to configure a DNS server to run as a non-root user and run in a chroot jail. This objective includes secure exchange of data between DNS servers.

Key Knowledge Areas:

- BIND 9 configuration files
- Configuring BIND to run in a chroot jail
- Split configuration of BIND using the forwarders statement
- Configuring and using transaction signatures (TSIG)
- Awareness of DNSSEC and basic tools
- Awareness of DANE and related records

Terms and Utilities:

- /etc/named.conf
- /etc/passwd
- DNSSEC
- dnssec-keygen
- dnssec-signzone

Topic 208: Web Services

208.1 Implementing a web server

Weight: 4

Description: Candidates should be able to install and configure a web server. This objective includes monitoring the server's load and performance, restricting client user access, configuring support for scripting languages as modules and setting up client user authentication. Also included is configuring server options to restrict usage of resources. Candidates should be able to configure a web server to use virtual hosts and customize file access.

Key Knowledge Areas:

- Apache 2.4 configuration files, terms and utilities
- Apache log files configuration and content
- Access restriction methods and files
- mod_perl and PHP configuration
- Client user authentication files and utilities
- Configuration of maximum requests, minimum and maximum servers and clients
- Apache 2.4 virtual host implementation (with and without dedicated IP addresses)
- Using redirect statements in Apache's configuration files to customize file access

Terms and Utilities:

- access logs and error logs
- .htaccess
- httpd.conf
- mod_auth_basic, mod_authz_host and mod_access_compat
- htpasswd
- AuthUserFile, AuthGroupFile
- apachectl, apache2ctl
- httpd, apache2

208.2 Apache configuration for HTTPS

Weight: 3

Description: Candidates should be able to configure a web server to provide HTTPS.

Key Knowledge Areas:

- SSL configuration files, tools and utilities
- Generate a server private key and CSR for a commercial CA
- Generate a self-signed Certificate
- Install the key and certificate, including intermediate CAs
- Configure Virtual Hosting using SNI
- Awareness of the issues with Virtual Hosting and use of SSL
- Security issues in SSL use, disable insecure protocols and ciphers

Terms and Utilities:

- Apache2 configuration files
- /etc/ssl/, /etc/pki/
- openssl, CA.pl
- SSLEngine, SSLCertificateKeyFile, SSLCertificateFile
- SSLCACertificateFile, SSLCACertificatePath
- SSLProtocol, SSLCipherSuite, ServerTokens, ServerSignature, TraceEnable

208.3 Implementing a proxy server

Weight: 2

Description: Candidates should be able to install and configure a proxy server, including access policies, authentication and resource usage.

Key Knowledge Areas:

- Squid 3.x configuration files, terms and utilities
- Access restriction methods
- Client user authentication methods
- Layout and content of ACL in the Squid configuration files

Terms and Utilities:

- squid.conf
- acl
- http_access

208.4 Implementing Nginx as a web server and a reverse proxy

Weight: 2

Description: Candidates should be able to install and configure a reverse proxy server, Nginx. Basic configuration of Nginx as a HTTP server is included.

Key Knowledge Areas:

- Nginx
- Reverse Proxy
- Basic Web Server

Terms and Utilities:

- /etc/nginx/
- nginx

Topic 209: File Sharing

209.1 SAMBA Server Configuration

Weight: 5

Description: Candidates should be able to set up a Samba server for various clients. This objective includes setting up Samba as a standalone server as well as integrating Samba as a member in an Active Directory. Furthermore, the configuration of simple CIFS and printer shares is covered. Also covered is a configuring a Linux client to use a Samba server. Troubleshooting installations is also tested.

Key Knowledge Areas:

- Samba 4 documentation
- Samba 4 configuration files
- Samba 4 tools and utilities and daemons
- Mounting CIFS shares on Linux
- Mapping Windows user names to Linux user names
- User-Level, Share-Level and AD security

Terms and Utilities:

- smbd, nmbd, winbindd
- smbcontrol, smbstatus, testparm, smbpasswd, nmblookup
- samba-tool
- net
- smbclient
- mount.cifs
- /etc/samba/
- /var/log/samba/

209.2 NFS Server Configuration

Weight: 3

Description: Candidates should be able to export filesystems using NFS. This objective includes access restrictions, mounting an NFS filesystem on a client and securing NFS.

Key Knowledge Areas:

- NFS version 3 configuration files
- NFS tools and utilities
- Access restrictions to certain hosts and/or subnets
- Mount options on server and client
- TCP Wrappers
- Awareness of NFSv4

Terms and Utilities:

- /etc/exports
- exportfs
- showmount
- nfsstat
- /proc/mounts
- /etc/fstab
- rpcinfo
- mountd
- portmapper

Topic 210: Network Client Management

210.1 DHCP configuration

Weight: 2

Description: Candidates should be able to configure a DHCP server. This objective includes setting default and per client options, adding static hosts and BOOTP hosts. Also included is configuring a DHCP relay agent and maintaining the DHCP server.

Key Knowledge Areas:

- DHCP configuration files, terms and utilities
- Subnet and dynamically-allocated range setup
- Awareness of DHCPv6 and IPv6 Router Advertisements

Terms and Utilities:

- dhcpd.conf
- dhcpd.leases
- DHCP Log messages in syslog or systemd journal
- arp
- dhcpd
- radvd
- radvd.conf

210.2 PAM authentication

Weight: 3

Description: The candidate should be able to configure PAM to support authentication using various available methods. This includes basic SSSD functionality.

Key Knowledge Areas:

- PAM configuration files, terms and utilities
- passwd and shadow passwords
- Use sssd for LDAP authentication

Terms and Utilities:

- /etc/pam.d/
- pam.conf
- nsswitch.conf
- pam_unix, pam_cracklib, pam_limits, pam_listfile, pam_sss
- sssd.conf

210.3 LDAP client usage

Weight: 2

Description: Candidates should be able to perform queries and updates to an LDAP server. Also included is importing and adding items, as well as adding and managing users.

Key Knowledge Areas:

- LDAP utilities for data management and queries
- Change user passwords
- Querying the LDAP directory

Terms and Utilities:

- ldapsearch
- ldappasswd
- ldapadd
- ldapdelete

210.4 Configuring an OpenLDAP server

Weight: 4

Description: Candidates should be able to configure a basic OpenLDAP server including knowledge of LDIF format and essential access controls.

Key Knowledge Areas:

- OpenLDAP
- Directory based configuration
- Access Control
- Distinguished Names
- Changetype Operations
- Schemas and Whitepages
- Directories
- Object IDs, Attributes and Classes

Terms and Utilities:

- slapd
- slapd-config
- LDIF
- slapadd
- slapcat
- slapindex
- /var/lib/ldap/
- loglevel

Topic 211: E-Mail Services

211.1 Using e-mail servers

Weight: 4

Description: Candidates should be able to manage an e-mail server, including the configuration of e-mail aliases, e-mail quotas and virtual e-mail domains. This objective includes configuring internal e-mail relays and monitoring e-mail servers.

Key Knowledge Areas:

- Configuration files for postfix
- Basic TLS configuration for postfix
- Basic knowledge of the SMTP protocol
- Awareness of sendmail and exim

Terms and Utilities:

- Configuration files and commands for postfix
- /etc/postfix/
- /var/spool/postfix/
- sendmail emulation layer commands
- /etc/aliases
- mail-related logs in /var/log/

211.2 Managing E-Mail Delivery

Weight: 2

Description: Candidates should be able to implement client e-mail management software to filter, sort and monitor incoming user e-mail.

Key Knowledge Areas:

- Understanding of Sieve functionality, syntax and operators
- Use Sieve to filter and sort mail with respect to sender, recipient(s), headers and size
- Awareness of procmail

Terms and Utilities:

- Conditions and comparison operators
- keep, fileinto, redirect, reject, discard, stop
- Dovecot vacation extension

211.3 Managing Remote E-Mail Delivery

Weight: 2

Description: Candidates should be able to install and configure POP and IMAP daemons.

Key Knowledge Areas:

- Dovecot IMAP and POP3 configuration and administration
- Basic TLS configuration for Dovecot
- Awareness of Courier

Terms and Utilities:

- /etc/dovecot/
- dovecot.conf
- doveconf
- doveadm

Topic 212: System Security

212.1 Configuring a router

Weight: 3

Description: Candidates should be able to configure a system to forward IP packet and perform network address translation (NAT, IP masquerading) and state its significance in protecting a network. This objective includes configuring port redirection, managing filter rules and averting attacks.

Key Knowledge Areas:

- iptables and ip6tables configuration files, tools and utilities
- Tools, commands and utilities to manage routing tables.
- Private address ranges (IPv4) and Unique Local Addresses as well as Link Local Addresses (IPv6)
- Port redirection and IP forwarding
- List and write filtering and rules that accept or block IP packets based on source or destination protocol, port and address
- Save and reload filtering configurations

Terms and Utilities:

- /proc/sys/net/ipv4/
- /proc/sys/net/ipv6/
- /etc/services
- iptables
- ip6tables

212.2 Securing FTP servers

Weight: 2

Description: Candidates should be able to configure an FTP server for anonymous downloads and uploads. This objective includes precautions to be taken if anonymous uploads are permitted and configuring user access.

Key Knowledge Areas:

- Configuration files, tools and utilities for Pure-FTPd and vsftpd
- Awareness of ProFTPd
- Understanding of passive vs. active FTP connections

Terms and Utilities:

- vsftpd.conf
- important Pure-FTPd command line options

212.3 Secure shell (SSH)

Weight: 4

Description: Candidates should be able to configure and secure an SSH daemon. This objective includes managing keys and configuring SSH for users. Candidates should also be able to forward an application protocol over SSH and manage the SSH login.

Key Knowledge Areas:

- OpenSSH configuration files, tools and utilities
- Login restrictions for the superuser and the normal users
- Managing and using server and client keys to login with and without password
- Usage of multiple connections from multiple hosts to guard against loss of connection to remote host following configuration changes

Terms and Utilities:

- ssh
- sshd
- /etc/ssh/sshd_config
- /etc/ssh/
- Private and public key files
- PermitRootLogin, PubKeyAuthentication, AllowUsers, PasswordAuthentication, Protocol

212.4 Security tasks

Weight: 3

Description: Candidates should be able to receive security alerts from various sources, install, configure and run intrusion detection systems and apply security patches and bugfixes.

Key Knowledge Areas:

- Tools and utilities to scan and test ports on a server
- Locations and organizations that report security alerts as Bugtraq, CERT or other sources
- Tools and utilities to implement an intrusion detection system (IDS)
- Awareness of OpenVAS and Snort

Terms and Utilities:

- telnet
- nmap
- fail2ban
- nc
- iptables

212.5 OpenVPN

Weight: 2

Description: Candidates should be able to configure a VPN (Virtual Private Network) and create secure point-to-point or site-to-site connections.

Key Knowledge Areas:

- OpenVPN

Terms and Utilities:

- /etc/openvpn/
- openvpn

LPIC3-303

Topic 325: Cryptography

325.1 X.509 Certificates and Public Key Infrastructures

Weight: 5

Description: Candidates should understand X.509 certificates and public key infrastructures. They should know how to configure and use OpenSSL to implement certification authorities and issue SSL certificates for various purposes.

Key Knowledge Areas:

- Understand X.509 certificates, X.509 certificate lifecycle, X.509 certificate fields and X.509v3 certificate extensions
- Understand trust chains and public key infrastructures
- Generate and manage public and private keys
- Create, operate and secure a certification authority
- Request, sign and manage server and client certificates
- Revoke certificates and certification authorities

The following is a partial list of the used files, terms and utilities:

- openssl, including relevant subcommands
- OpenSSL configuration
- PEM, DER, PKCS
- CSR
- CRL
- OCSP

325.2 X.509 Certificates for Encryption, Signing and Authentication

Weight: 4

Description: Candidates should know how to use X.509 certificates for both server and client authentication. Candidates should be able to implement user and server authentication for Apache HTTPD. The version of Apache HTTPD covered is 2.4 or higher.

Key Knowledge Areas:

- Understand SSL, TLS and protocol versions
- Understand common transport layer security threats, for example Man-in-the-Middle
- Configure Apache HTTPD with mod_ssl to provide HTTPS service, including SNI and HSTS
- Configure Apache HTTPD with mod_ssl to authenticate users using certificates
- Configure Apache HTTPD with mod_ssl to provide OCSP stapling
- Use OpenSSL for SSL/TLS client and server tests

Terms and Utilities:

- Intermediate certification authorities
- Cipher configuration (no cipher-specific knowledge)
- httpd.conf
- mod_ssl
- openssl

325.3 Encrypted File Systems

Weight: 3

Description: Candidates should be able to setup and configure encrypted file systems.

Key Knowledge Areas:

- Understand block device and file system encryption
- Use dm-crypt with LUKS to encrypt block devices
- Use eCryptfs to encrypt file systems, including home directories and
- PAM integration
- Be aware of plain dm-crypt and EncFS

Terms and Utilities:

- cryptsetup
- cryptmount
- /etc/crypttab

- ecryptfsd
- ecryptfs-* commands
- mount.ecryptfs, umount.ecryptfs
- pam_ecryptfs

25.4 DNS and Cryptography

Weight: 5

Description: Candidates should have experience and knowledge of cryptography in the context of DNS and its implementation using BIND. The version of BIND covered is 9.7 or higher.

Key Knowledge Areas:

- Understanding of DNSSEC and DANE
- Configure and troubleshoot BIND as an authoritative name server serving DNSSEC secured zones
- Configure BIND as an recursive name server that performs DNSSEC validation on behalf of its clients
- Key Signing Key, Zone Signing Key, Key Tag
- Key generation, key storage, key management and key rollover
- Maintenance and re-signing of zones
- Use DANE to publish X.509 certificate information in DNS
- Use TSIG for secure communication with BIND

Terms and Utilities:

- DNS, EDNS, Zones, Resource Records
- DNS resource records: DS, DNSKEY, RRSIG, NSEC, NSEC3, NSEC3PARAM, TLSA
- DO-Bit, AD-Bit
- TSIG
- named.conf
- dnssec-keygen
- dnssec-signzone
- dnssec-settime
- dnssec-dsfromkey
- rndc
- dig
- delv
- openssl

Topic 326: Host Security

326.1 Host Hardening

Weight: 3

Description: Candidates should be able to secure computers running Linux against common threats. This includes kernel and software configuration.

Key Knowledge Areas:

- Configure BIOS and boot loader (GRUB 2) security
- Disable useless software and services
- Use sysctl for security related kernel configuration, particularly ASLR, Exec-Shield and IP / ICMP configuration

- Exec-Shield and IP / ICMP configuration
- Limit resource usage
- Work with chroot environments
- Drop unnecessary capabilities
- Be aware of the security advantages of virtualization

Terms and Utilities:

- grub.cfg
- chkconfig, systemctl
- ulimit
- /etc/security/limits.conf
- pam_limits.so
- chroot
- sysctl
- /etc/sysctl.conf

326.2 Host Intrusion Detection

Weight: 4

Description: Candidates should be familiar with the use and configuration of common host intrusion detection software. This includes updates and maintenance as well as automated host scans.

Key Knowledge Areas:

- Use and configure the Linux Audit system
- Use chkrootkit
- Use and configure rkhunter, including updates
- Use Linux Malware Detect
- Automate host scans using cron
- Configure and use AIDE, including rule management
- Be aware of OpenSCAP

Terms and Utilities:

- auditd
- auditctl
- ausearch, aureport
- auditd.conf
- auditd.rules
- pam_tty_audit.so
- chkrootkit
- rkhunter
- /etc/rkhunter.conf
- maldet
- conf.maldet
- aide
- /etc/aide/aide.conf

326.3 User Management and Authentication

Weight: 5

Description: Candidates should be familiar with management and authentication of user accounts. This includes configuration and use of NSS, PAM, SSSD and Kerberos for both local and remote directories and authentication mechanisms as well as enforcing a password policy.

Key Knowledge Areas:

- Understand and configure NSS
- Understand and configure PAM
- Enforce password complexity policies and periodic password changes
- Lock accounts automatically after failed login attempts
- Configure and use SSSD
- Configure NSS and PAM for use with SSSD
- Configure SSSD authentication against Active Directory, IPA, LDAP, Kerberos and local domains
- Kerberos and local domains
- Obtain and manage Kerberos tickets

Terms and Utilities:

- nsswitch.conf
- /etc/login.defs
- pam_cracklib.so
- chage
- pam_tally.so, pam_tally2.so
- faillog
- pam_sss.so

- sssd
- sssd.conf
- sss_* commands
- krb5.conf
- kinit, klist, kdestroy

326.4 FreeIPA Installation and Samba Integration

Weight: 4

Description: Candidates should be familiar with FreeIPA v4.x. This includes installation and maintenance of a server instance with a FreeIPA domain as well as integration of FreeIPA with Active Directory.

Key Knowledge Areas:

- Understand FreeIPA, including its architecture and components
- Understand system and configuration prerequisites for installing FreeIPA
- Install and manage a FreeIPA server and domain
- Understand and configure Active Directory replication and Kerberos cross-realm trusts
- Be aware of sudo, autofs, SSH and SELinux integration in FreeIPA

Terms and Utilities:

- 389 Directory Server, MIT Kerberos, Dogtag Certificate System, NTP, DNS, SSSD, certmonger
- ipa, including relevant subcommands

- ipa-server-install, ipa-client-install, ipa-replica-install
- ipa-replica-prepare, ipa-replica-manage

Topic 327: Access Control

327.1 Discretionary Access Control

Weight: 3

Description: Candidates are required to understand Discretionary Access Control and know how to implement it using Access Control Lists. Additionally, candidates are required to understand and know how to use Extended Attributes.

Key Knowledge Areas:

- Understand and manage file ownership and permissions, including SUID and SGID
- Understand and manage access control lists
- Understand and manage extended attributes and attribute classes

Terms and Utilities:

- getfacl
- setfacl
- getfattr
- setfattr

327.2 Mandatory Access Control

Weight: 4

Description: Candidates should be familiar with Mandatory Access Control systems for Linux. Specifically, candidates should have a thorough knowledge of SELinux. Also, candidates should be aware of other Mandatory Access Control systems for Linux. This includes major features of these systems but not configuration and use.

Key Knowledge Areas:

- Understand the concepts of TE, RBAC, MAC and DAC
- Configure, manage and use SELinux
- Be aware of AppArmor and Smack

Terms and Utilities:

- getenforce, setenforce, selinuxenabled
- getsebool, setsebool, togglesebool
- fixfiles, restorecon, setfiles
- newrole, runcon
- semanage
- sestatus, seinfo
- apol
- seaudit, seaudit-report, audit2why, audit2allow
- /etc/selinux/*

327.3 Network File Systems

Weight: 3

Description: Candidates should have experience and knowledge of security issues in use and configuration of NFSv4 clients and servers as well as CIFS client services. Earlier versions of NFS are not required knowledge.

Key Knowledge Areas:

- Understand NFSv4 security issues and improvements
- Configure NFSv4 server and clients
- Understand and configure NFSv4 authentication mechanisms (LIPKEY, SPKM, Kerberos)
- Understand and use NFSv4 pseudo file system
- Understand and use NFSv4 ACLs
- Configure CIFS clients
- Understand and use CIFS Unix Extensions
- Understand and configure CIFS security modes (NTLM, Kerberos)
- Understand and manage mapping and handling of CIFS ACLs and SIDs in a Linux system

Terms and Utilities:

- /etc/exports
- /etc/idmap.conf
- nfs4acl
- mount.cifs parameters related to ownership, permissions and security modes
- winbind
- getcifsacl, setcifsacl

Topic 328: Network Security

328.1 Network Hardening

Weight: 4

Description: Candidates should be able to secure networks against common threats. This includes verification of the effectiveness of security measures.

Key Knowledge Areas:

- Configure FreeRADIUS to authenticate network nodes
- Use nmap to scan networks and hosts, including different scan methods
- Use Wireshark to analyze network traffic, including filters and statistics
- Identify and deal with rogue router advertisements and DHCP messages

Terms and Utilities:

- radiusd
- radmin
- radtest, radclient
- radlast, radwho
- radiusd.conf
- /etc/raddb/*
- nmap
- wireshark
- tshark
- tcpdump
- ndpmon

328.2 Network Intrusion Detection

Weight: 4

Description: Candidates should be familiar with the use and configuration of network security scanning, network monitoring and network intrusion detection software. This includes updating and maintaining the security scanners.

Key Knowledge Areas:

- Implement bandwidth usage monitoring
- Configure and use Snort, including rule management
- Configure and use OpenVAS, including NASL

Terms and Utilities:

- ntop
- Cacti
- snort
- snort-stat
- /etc/snort/*
- openvas-adduser, openvas-rmuser
- openvas-nvt-sync
- openvassd
- openvas-mkcert
- /etc/openvas/*

328.3 Packet Filtering

Weight: 5

Description: Candidates should be familiar with the use and configuration of packet filters. This includes netfilter, iptables and ip6tables as well as basic knowledge of nftables, nft and ebtables.

Key Knowledge Areas:

- Understand common firewall architectures, including DMZ
- Understand and use netfilter, iptables and ip6tables, including standard modules, tests and targets
- Implement packet filtering for both IPv4 and IPv6
- Implement connection tracking and network address translation
- Define IP sets and use them in netfilter rules
- Have basic knowledge of nftables and nft
- Have basic knowledge of ebtables
- Be aware of conntrackd

Terms and Utilities:

- iptables
- ip6tables
- iptables-save, iptables-restore
- ip6tables-save, ip6tables-restore
- ipset
- nft
- ebtables

328.4 Virtual Private Networks

Weight: 4

Description: Candidates should be familiar with the use of OpenVPN and IPsec.

Key Knowledge Areas:

- Configure and operate OpenVPN server and clients for both bridged and routed VPN networks
- Configure and operate IPsec server and clients for routed VPN networks using IPsec-Tools / racoon
- Awareness of L2TP

Terms and Utilities:

- /etc/openvpn/*
- openvpn server and client
- setkey
- /etc/ipsec-tools.conf
- /etc/racoon/racoon.conf