BSD Professional Certification Requirements

The official exam objectives for the BSD Professional (BSDP) certification exam including task descriptions, practical details, and supporting information about the exam.

Cover graphics design by Ryan Hall

Version History

Version No.	Date	Author	Reviewed	Comments
1.0	2010-08-31	BSD Certification Group	Y	Released version.

Preface

The BSD Professional (BSDP) certification is an advanced level, psychometrically[1] valid certification for BSD system administrators offered by the BSD Certification Group (BSDCG). The requirements for the BSDP examination were developed with active input from the BSD community, system administrators, and organizations that use BSD systems in their IT infrastructure. A Job Task Analysis Survey was conducted in late 2009 and approximately 190 tasks were analyzed for both Importance and Frequency. The BSD Professional Certification Job Task Analysis Survey Report[2], published in March, 2010, served as the basis for the development of the objectives contained within this BSDP Certification Requirements document. Additional work with Subject Matter Experts (SMEs) from the BSD community further refined the objectives in this document.

The BSDCG may eventually submit this certification program for international accreditation defined by the ANSI/ISO/IEC 17024[3] standard. The process for achieving accreditation imposes certain requirements on this certification program. These requirements include many organizational and procedural changes for the BSDCG itself, but they also include requirements such as recertification and periodic communication with the BSDCG. Further details on these aspects will be published on the BSDCG website as they become available.

It takes a considerable amount of time and effort to develop a cerfication program such as the BSD Professional certification. The BSD Certification Group would like to thank all those who took the Job Task Analysis Survey, those who participated in the SME sessions, those who will participate as BSDP beta exam testers, our dedicated proctors, the supporting training organizations, and everyone who is interested in the advancement of BSD systems.

The BSD Certification Group, Inc.

www.bsdcertification.org

August 31, 2010

---

1 See our publication on The Importance of Psychometrics: http://www.bsdcertification.org/downloads/psychometric.pdf
2 http://www.bsdcertification.org/downloads/BSDP_JTA_Report.pdf
3 https://www.ansica.org/wwwversion2/outside/PERgeneral.asp?menuID=2

Table of Contents

Executive Summary

This document describes the requirements of the BSD Professional (BSDP) certification developed by the BSD Certification Group (BSDCG). It outlines eleven study domains, each containing a dozen or so exam objectives. These objectives describe the topics that must be mastered by prospective candidates for the certification.

The BSDP certification requires successful completion of both a written test and a hands-on lab exam. The hands-on lab exam consists of a collection of exercises that the candidate performs using BSD systems networked together within a virtual environment. The certification is BSD agnostic, meaning BSDP exam candidates can choose which BSD version(s) to use during the lab portion of the exam. Questions in the written portion of the exam are independent of the BSD version.

BSDP candidates are expected to be very proficient in at least one of the following BSD versions:

- NetBSD: 5.1 or higher

- FreeBSD: 8.1 or higher

- OpenBSD: 4.7 or higher

- Dragonfly BSD: 2.6.3 or higher

The BSDP exam was created by the BSDCG to help employers, managers, recruiters, and others have confidence in the skill levels of senior level BSD system administrators. The certification is designed for a BSD system administrator experienced in using one or more versions of NetBSD, FreeBSD, OpenBSD, or DragonFly BSD for several years. The BSDP candidate generally has a well developed knowledge of common system administration activities including user administration, file and filesystem maintenance, kernel tuning, script writing, and many other technical tasks.

The successful candidate has a proven ability to perform complex system administration tasks and can be immediately productive in the administration of BSD systems.

1 Introduction to the BSDP Exam Objectives

This document describes the examination objectives for the BSD Professional (BSDP) certification. The BSDP exam is comprehensive and consists of both a written exam and a hands-on lab exam to provide the opportunity for the candidate to demonstrate knowledge comprehension as well as practical skill. The objectives listed in this document describe the required knowledge and comprehension elements for the written exam, as well as suggested time estimates for tasks that the candidate may be asked to perform during the lab portion of the exam.

1.1 Audience

This document is written for individuals interested in achieving the BSDP certification. The BSDP candidate is experienced in using one or more versions of NetBSD, FreeBSD, OpenBSD, or DragonFly BSD for several years. The candidate may be engaged as a senior BSD system administrator by an employer, may be active in open source projects where BSD systems are used, or may have gained experience in using BSD systems over the years in a variety of settings. The candidate generally has a well developed knowledge of shell scripting, networking, user administration, file and filesystem maintenance, kernel tuning, and many other technical tasks.

The document is also of interest to individuals and organizations who wish to develop training materials or educational programs geared towards advanced BSD system administration. The objectives in this document cover the tasks that employers require of a senior system administrator and are representative of a comprehensive training program. Use of these materials is subject to the copyright requirements specified on page 2 of this document and the disclaimer found in Section 2.1.

1.2 Purpose

The objectives in this document cover the tasks that a senior level BSD system administrator with a minimum of three years experience would be expected to be able to perform. The objectives are intended to help candidates prepare for both the written and lab sections of the exam. BSDP candidates should study and practice all of the objectives and concentrate on the areas they are unfamiliar with.

1.3 Methodology

These objectives were constructed from the results of the BSDP Job Task Analysis Survey[4] (JTA). The survey, held in late 2009, was composed of approximately 190 technical tasks covering twelve different knowledge domains. The survey attempted to determine the Importance and Frequency of each item. Psychometric analysis[5] of the results was used to select the preliminary list of objectives which were further refined through BSD community involvement.

Table 1 shows the key for interpreting the numerical results for the JTA survey graphs.

---

4   http://www.bsdcertification.org/news/pr058.html
5   Http://www.bsdcertification.org/downloads/psychometric.pdf

Table 1: Key for Importance and Frequency

Importance	Very Low	Low	Medium	High	Very High
	1	2	3	4	5
Frequency	**Less 1X/Month**	**Monthly**	**Weekly**	**Daily**	**Multiple X/Day**
	1	2	3	4	5

Many survey responders pointed out that there are some tasks that are generally only done once in the life of the system, such as formatting the root filesystem, or performing an initial installation. These were generally assumed to be Frequency "Less Than 1X/Month".

Objective Numbering

JTA tasks with an Importance less than 3.0 or a Frequency less than 1.5 were reviewed and discussed by SMEs and several were removed during the course of the development of these objectives. Some objectives were reworded slightly from the original JTA tasks to clarify their purpose or to make them applicable to all BSD systems. All these changes have been reviewed and approved by the BSDCG psychometrician. Therefore, all objectives in this document are valid for the BSDP exam.

In order to provide an easy to use reference, the objectives in this document are numbered consecutively. Organizations creating BSDP training materials should use the objective numbers used in this document. Objectives in the wiki[6] (see below) are numbered twice, to correspond to the numbers in this document as well as their original JTA number.

A Note on the BSDP Wiki

The BSDP wiki contains commentary on each objective defined by the JTA. Objectives that have been retired appear in light grey type and contain comments on why and when the objective was retired. Active objectives may contain additional information added by the BSD community to assist in the study of that objective or in the creation of study materials. Anyone is welcome to add useful commentary to the wiki. However, the official exam objectives, their descriptions, and their numbers are contained within this document.

1.4 Operating System Versions Covered by BSDP

In order for a certification to be practical, it must cover working knowledge in versions of BSD operating systems most likely to be seen in the workplace. The BSDP exam requires proficiency in one or more of the following versions of these operating systems:

- NetBSD: 5.1 or higher
- FreeBSD: 8.1 or higher
- OpenBSD: 4.7 or higher

---

6   http://bsdwiki.reedmedia.net/wiki/BSDP.html

- DragonFly BSD: 2.6.3 or higher

The testing candidate should keep in mind that the base utilities most likely to be encountered in the BSDP examination rarely change from one operating system revision to another. Many tasks in these objectives also apply to earlier versions of each BSD system, and will likely remain in later versions.

1.5 Blooms Taxonomy

Blooms Taxonomy[7] is a commonly used classification of learning objectives. Each BSDP exam objective contains at least one of the following three Bloom types:

- **K- Knowledge:** indicates that BSDP candidates should be familiar with basic concepts and can recall facts and terms about the objective.

- **C- Comprehension:** indicates that BSDP candidates exhibit understanding by being able to compare, contrast, and organize information about the objective.

- **A- Application:** indicates that BSDP candidates use knowledge to solve problems by applying the knowledge to specific tasks. Exam objectives that may show up on the lab portion of the exam will include Bloom type **A**.

Some exam objectives are not well suited to a lab scenario. They will be marked as **K** or **K**,**C**.

1.6 Recertification Requirements

As noted in the Preface, the BSD Certification Group may eventually submit this certification program for ANSI/ISO/IEC 17024[8] accreditation. To be compliant with the ANSI/ISO/IEC 17024 standard, a time limit for a valid certification must be established. Once a BSDP candidate meets the certification requirements, their BSDP certification will be valid for a period of 5 years. At the end of that time, the candidate will need to recertify. Details on how to recertify will be publicly available in a document to be published on the BSDCG website once the recertification requirements are finalized.

---

7   http://en.wikipedia.org/wiki/Bloom%27s_Taxonomy
8   https://www.ansica.org/wwwversion2/outside/PERgeneral.asp?menuID=2

2 Exam Description

2.1 Official BSDP Examination Description

The following is the official BSDP examination description, suitable for display by training and testing centers and for use within training materials:

"The BSDP (BSD Professional) Certification is for those with strong to expert skills in BSD Unix system administration. The successful candidate understands and uses both basic and advanced system administration commands, demonstrating proficiency in the following eleven domains:

1. Installation and Setup

2. Security

3. Filesystems and Files

4. User Administration

5. General Administration

6. Common Services

7. General Networking

8. Backup and Restore

9. Virtualization

10. Logging and Monitoring

11. High Availability

Additional information about the BSD Professional Certification is available at the BSD Certification Group website (www.bsdcertification.org)."

Organizations using these objectives to develop their own training programs should also include the following disclaimer regarding the use of these materials:

"These training materials were developed using publicly available information provided by the BSD Certification Group (www.bsdcertification.org)."

3 Using the BSDP Exam Objectives

In order to assist candidates in their studies as well as organizations wishing to provide training and study materials, each exam objective has five components:

1. *Number and name*- of the exam objective.
2. *Importance, Frequency, and Bloom Type(s)*- metrics that can guide the candidate in understanding which tasks are the most important and frequently performed.
3. *Concept*- describes the task and background material the candidate should master in order to effectively put the exam objective to use.
4. *Practical*- provides a list of possible commands and software that may be used to perform the tasks described in the objective. Unless otherwise specified, the commands are available on each BSD. Note that the *Practical* section contains commands that apply to the task, but *does not contain all possible commands*. Candidates are advised to use the listed commands as starting points for study. Referencing the listed commands with the "SEE ALSO" section in manual pages is highly recommended.
5. *Estimated Time*- an estimate to use as a guide for completing the task during the BSDP lab exam. When studying, candidates should practice the objective until they can complete it within the suggested time period.

Note: When studyng the exam objectives, keep the following points in mind:

- The BSDP certification exam tests practical skills, so you should not simply memorize written materials. Instead, continually practice the tasks described in the objectives until you fully understand them and can perform the requested operations within the estimated time.

- The BSDP is an advanced level examination. You are not expected to know *everything*, but you are expected to know *a lot of things.* You need to demonstrate that you have experience completing complex administrative tasks within the time restraints imposed by the exam.

- Watch for the words "install", "configure", "perform", "set up", and similar action words in an exam objective. They indicate that you need to know how to perform these operations.

- During the lab portion of the exam, you will have access to the latest releases of all 4 BSDs, their packages and pkgsrc repositories, as well as any manual pages and documentation included with the operating systems. These will be provided on a file server. Internet access will *not* be available during the exam, meaning you will be limited to the resources that come with the operating systems and to the applications contained within the official packages and pkgsrc repositories.

- The BSDP certification exam is meant to assess *what* should be accomplished, not *how* it should be accomplished.

Additional Notes

A few objectives contain features that may not be present in all BSDs or which may require the installation of additional software or the creation of scripts in order to perform that objective on certain BSDs. In each case, the objective is marked accordingly. During the lab exam, BSDP candidates should be aware of such differences and be time efficient in how they decide to perform a task. The candidate may choose to use a different BSD system that comes with the feature built-in or may choose to create a more imaginative solution that works on their BSD of choice. For the written portion of the exam, questions will be weighted so that BSDP candidates are not penalized for features that are not present on all BSD systems.

The rest of this document describes the eleven study domains and the objectives within each domain.

3.1 Installation and Setup

System installation and setup is a basic but important job of a BSD system administrator. Beyond getting the system up and running, the BSDP candidate must be able to perform more complex tasks such as preparing and updating automated installation scripts, using a serial console for installation, restoring a corrupted boot sector, and other similar tasks.

3.1.1 Build and install system from source code.

Importance: 3.6, Frequency: 1.7, Bloom: K,C

Concept:

BSD systems allow the administrator to compile both the kernel and userland from source in order to upgrade an existing operating system. The commands provided for this purpose vary between the BSDs.

BSDP candidates should be familiar with the steps required to compile both kernel and userland from source and to install the new kernel and userland for their BSD of choice.

Practical:

DragonFly BSD: build(7), development(7), make(1)

FreeBSD: config(8), make(1), mergemaster(8)

NetBSD: build.sh, etcupdate(8), postinstall(8)

OpenBSD: config(8), make(1), sysmerge(8)

Estimated Time:

10 minutes to describe the steps required to build and install a system from source code.

3.1.2 Use disklabel to modify or create partitions.

Importance: 3.5, Frequency: 1.4, Bloom: K,C,A

Concept:

The disklabel utility can be used to install, examine, or modify the label on a hard drive. The disk label contains information about the size and type of disk and the partition layout. While each BSD provides the disklabel utility, its command parameters and usage vary by BSD.

BSDP candidates should be able to view, modify, or create the disk label on a BSD system.

Practical:

disklabel(8)

Estimated Time:

10 minutes to create or modify an existing disk label according to a specification.

3.1.3 Use fdisk tool.

Importance: 3.3, Frequency: 1.5, Bloom: K,C,A

Concept:

On BSD systems, the built-in fdisk utility is either used to view and modify the disk slice table or to view and modify the master boot record.

BSDP candidates should be able to either modify the disk slice table or the master boot record using the built-in fdisk utility, depending upon their BSD of choice.

Practical:

fdisk(8)

Estimated Time:

10 minutes to create or edit the disk slice table or master boot record according to a specification.

3.1.4 Create FAT32, NTFS, or other non-BSD partitions.

Importance: 2.5, Frequency: 1.3, Bloom: K,C,A

Concept:

Creating a non-BSD disk partition is the first step in creating a filesystem used by other operating systems. The partition is assigned an identifier that marks it as a non-BSD partition.

BSDP candidates should be familiar with all the steps in the creation of a filesystem and be able to configure a disk partition as the first step in preparing a non-BSD filesystem.

Practical:

fdisk(8), disklabel(8)

Estimated Time:

10 minutes to create a non-BSD partition according to a specification.

3.1.5 Create an install script or configuration for unattended installation.

Importance: 3.2, Frequency: 1.4, Bloom: K,C,A

Concept:

Creating a script for unattended installation relieves the BSD system administrator of manually repeating the same task when installing multiple systems.

BSDP candidates should be able to configure a script for unattended installation or post-installation configuration of a BSD system.

Practical:

software of choice in packages/pkgsrc

FreeBSD: sysinstall(8)

O*penBSD:* install.site or upgrade.site

Estimated Time:

20 minutes to create, install, and test an install script according to a specification.

3.1.6 Configure startup scripts to be run at boot time.

Importance: 3.3, Frequency: 1.9, Bloom: K,C,A

Concept:

BSD systems perform startup operations by means of scripts that are run at boot time.

BSDP candidates should be able to enable and disable system, third-party, and custom services at boot time, as well as temporarily start a service without configuring it to start at boot time.

Practical:

rc(8), rc.conf(5)

Estimated Time:

5 minutes to enable or disable a service to start at boot time.

3.1.7 Restore a corrupted boot sector.

Importance: 3.6, Frequency: 1.3, Bloom: K,C,A

Concept:

A corrupted boot sector prevents the system from booting normally. Restoring the boot sector can enable the system to boot, or enable the administrator to access files on the affected disk.

BSDP candidates should be able to restore the master boot record of a disk.

Practical:

software of choice for packages/pkgsrc

fdisk(8)

NetBSD, OpenBSD: scan_ffs(8)

Estimated Time:

10 minutes to restore a corrupted boot sector.

3.1.8 Boot via the serial console.

Importance: 2.9, Frequency: 1.6, Bloom: K

Concept:

Using a serial device for booting the system permits the system to be booted when there is no attached keyboard and/or display device.

BSDP candidates should know how to configure a BSD system to use an attached serial device during the boot loader and kernel load, all the way to a login prompt.

Practical:

ttys(5)

FreeBSD: loader.conf(5)

OpenBSD: boot(8)

Estimated Time:

20 minutes to configure and test booting the system from a serial console.

3.1.9 Configure sysctl values to be loaded at system startup.

Importance: 4.0, Frequency: 1.9, Bloom: K,C, A

Concept:

BSD systems utilize an internal Management Information Base (MIB) that contains a collection of variables and values that maintain kernel state. The values of some of these variables can be changed by the system administrator.

BSDP candidates should understand the use of the MIB to maintain kernel state, be able to configure custom MIB values on a live system, and configure the system to preserve custom values after a system boot.

Practical:

sysctl(7) or (8), sysctl.conf(5)

Estimated Time:

10 minutes to set custom MIB values and configure the system to preserve the values after a system boot, according to a specification.

3.1.10 Configure BSD system for PXE booting.

Importance: 3.1, Frequency: 1.6, Bloom: K,C,A

Concept:

Preboot Execution Environment (PXE) allows diskless systems to access a network's resources using a network interface.

BSDP candidates should understand the PXE boot process and be able to configure a BSD PXE boot server to enable diskless systems to boot and access network resources. Candidates should also be able to configure the services necessary for a PXE boot environment: i) DHCP or bootp server; and ii) TFTP or NFS.

Practical:

software of choice from packages/pkgsrc

pxeboot(8), diskless(8)

Estimated Time:

30 minutes to configure a BSD PXE boot server and test a diskless workstation according to a specification.

3.1.11 Configure system to mount remote network filesystems at boot.

Importance: 3.7, Frequency: 2.2, Bloom: K,C,A

Concept:

BSD systems can be configured to access remote Network File System (NFS) shares over a network at boot time.

BSDP candidates should be able to configure a BSD system to access NFS shares over a network.

Practical:

fstab(5)

DragonFly BSD, FreeBSD: rc.conf(5)

Estimated Time:

15 minutes to configure a BSD system to mount remote NFS shares at boot time according to a specification.

3.1.12 Create a local package repository.

Importance: 3.3, Frequency: 1.7, Bloom: K,C,A

Concept:

While each BSD project provides its own official package repository, it is often desirable for a system administrator to create a local repository containing only those packages needed by the organization.

BSDP candidates should be able to configure a local repository containing a subset of the packages collection or pkgsrc. In addition, BSDP candidates should be aware of the environment variables and program switches needed to modify the default path used when installing packages.

Practical:

pkg_add(1)

Estimated Time:

20 minutes to configure and test a local package repository according to a specification.

3.1.13 Compile a customized binary using ports or pkgsrc.

Importance: 4.2, Frequency 3.0, Bloom: K,C,A

Concept:

System administrators often need to install customized software compiled from source code.

BSDP candidates should be able to compile a customized binary using either the ports collection or pkgsrc. This may require the use of make(1) targets, customizing a port's Makefile, or setting pkgsrc environmental variables.

Practical:

The pkgsrc Guide

make(1)

FreeBSD, OpenBSD: ports(7)

Estimated Time:

10 minutes to compile and test customized software according to a specification.

3.2 Security

BSD systems have a long history of attention to detail regarding security, and are often considered the most secure systems in the enterprise. However, security is as much a function of good system administration as it is good code. The BSDP candidate must be able to configure various security features on a BSD system, maintain them over time, and know how to assess the security of a BSD system.

3.2.1 Raise or lower security level.

Importance: 3.7, Frequency: 1.9, Bloom: K,C,A

Concept:

BSD systems have the capability to change their operational security through a facility known as securelevels. The name of the secureleves and their effects vary by BSD system.

BSDP candidates should understand the nature of higher security level environments and should be able to modify the current security level.

Practical:

sysctl(8), init(8)

DragonFly BSD, *FreeBSD:* security(7)

NetBSD: secmodel(9)

OpenBSD: securelevel(7)

Estimated Time:

5 minutes to be able to configure the securelevel of the system according to a specification.

3.2.2 Configure system to deny local root logins.

Importance: 4.1, Frequency: 2.0, Bloom: K,C,A

Concept:

Due to the elevated permissions of the root (superuser) account, many security policies disallow the practice of logging in as the root user.

BSDP candidates should be familiar with how BSD systems perform console and serial logins, and should be able to configure the system to deny root logins from these types of devices.

Practical:

login(1), login.conf(5), getty(8), gettytab(5), init(8), ttys(5)

DragonFly BSD, *FreeBSD*, *OpenBSD: fbtab(5)*

DragonFly BSD, *FreeBSD*, *NetBSD: login.access(5)*

Estimated Time:

15 minutes to configure the system to deny root logins according to a specification.

3.2.3 Configure support for an alternative authentication mechanism.

Importance: 3.5, Frequency: 1.8, Bloom: K,C,A

Concept:

BSD systems provide either the Pluggable Authentication Model (PAM) or the BSD Authentication libraries in order to supplement the traditional Unix authentication model.

BSDP candidates should understand the authentication framework for their BSD of choice and know how to configure a BSD system to use alternate authentication methods.

Practical:

DragonFly BSD, *FreeBSD*, *NetBSD:* pam(3), pam.conf(5)

OpenBSD: authenticate(3), bsd_auth(3)

Estimated Time:

15 minutes to configure and test alternative authentication according to a specification.

3.2.4 Understand how ACLs augment traditional Unix permissions.

Importance: 3.4, Frequency: 2.0, Bloom: K,C

Concept:

Some filesystems support Access Control Lists (ACLs). These provide extensions that allow for the use of fine grained discretionary and mandatory access control by the system administrator.

BSDP candidates should have an understanding of how ACLs extend basic Unix permissions and be able to recognize a correct usage of ACL entries.

Practical:

FreeBSD: setfacl(1), getfacl(1), acl(3), getextattr(8), setextattr(8), acl(9), extattr(9), lsextattr(8)

Estimated Time:

5 minutes to review a file's ACL entry.

3.2.5 Change the flags on sensitive files.

Importance: 3.9, Frequency: 2.3, Bloom: K,C,A

Concept:

File flags provide extended attributes that allow the administrator to control certain operations such as making files undeleteable. By setting certain flags, the system administrator can exercise greater control over files than is possible with simple Unix-style permissions.

BSDP candidates should understand the effects of each flag and be able to configure file flags.

Practical:

chflags(1), ls(1)

Estimated Time:

5 minutes to change file flags according to a specification.

3.2.6 Configure SSH to restrict or allow logins.

Importance: 4.3, Frequency: 2.4, Bloom: K,A

Concept:

Many security policies require the administrator to deny or permit specific users the ability to login over the network using the SSH protocol.

BSDP candidates should know how to configure sshd(8) to deny or permit specified users or network addresses. In addition, candidates should be familiar with the various settings available for SSH logins.

Practical:

sshd_config(5), sshd(8)

Estimated Time:

15 minutes to configure and test SSH logins according to a specification.

3.2.7 Configure a Network Intrusion Detection System.

Importance: 3.7, Frequency: 1.8, Bloom: K,C,A

Concept:

A Network Intrusion Detection System (NIDS) listens to network traffic and raises an alert when certain traffic is detected.

BSDP candidates should be able to install and configure a NIDS that can watch for and display network traffic.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

30 minutes to configure, implement, and test a simple NIDS according to a specification.

3.2.8 Configure and use sudo.

Importance: 4.0, Frequency: 2.8, Bloom: K,A

Concept:

sudo(8) allows a user to run commands as another user .The sudoers(5) file contains details on which users can run specific commands, and under what conditions. sudo(8) is helpful where certain privileged programs must be run by unprivileged users.

BSDP candidates should be familiar with setting up sudo and configuring the sudoers file to permit programs to be run according to a specification.

Practical:

sudo from packages/pkgsrc when not installed by default

sudo(8), sudoers(5), visudo(8)

Estimated Time:

15 minutes to create, implement, and test a working sudo configuration according to a specification.

3.2.9 Download and apply security patches.

Importance: 4.7, Frequency: 3.1, Bloom: K,C,A

Concept:

Security advisories are released by a BSD project whenever a flaw or bug is discovered in supported software. The technical details of the advisories vary between the projects, but each advisory contains instructions on how to fix the specific problem.

BSDP candidates should be familiar with implementing the instructions within security advisories, including how to download and apply software patches and recompile the affected software.

Practical:

make(1), patch(1)

FreeBSD: freebsd-update(8)

NetBSD: cvs(1), build.sh

Estimated Time:

10 minutes to perform the instructions within a specified security advisory.

3.2.10 Scan and review open ports.

Importance: 4.0, Frequency: 2.8, Bloom: K,A

Concept:

Daemons that listen on the network for incoming connections do so by opening a socket on a specific port. While these sockets are actively listening, the ports are considered "open" and ready to serve requests.

BSDP candidates should be able to use common security tools to scan a local or a remote system for open ports.

Practical:

software of choice from packages/pkgsrc

netstat(1)

DragonFly BSD, FreeBSD, NetBSD: sockstat(1)

Estimated Time:

15 minutes to scan a host for open ports according to a specification.

3.2.11 Generate self-signed certificates.

Importance: 3.7, Frequency: 1.9, Bloom: K,C,A

Concept:

Self-signed certificates are useful in software testing and in limited use deployments of secured systems.

BSDP candidates should understand the certification deployment framework and be able to configure a Certificate Authority according to a specification. Candidates should then be able to use that Authority to sign certificates.

Practical:

openssl(1)

DragonFly BSD, FreeBSD: verify(1), x509(1), CA.pl(1), ca(1), req(1)

NetBSD: openssl.cnf(5), openssl_ca(1), and related openssl_*(1) utilities

Estimated Time:

45 minutes to set up a Certificate Authority and use that Authority to generate and verify a self-signed certificate according to a specification.

3.2.12 Scan a password file for weak passwords.

Importance: 3.6, Frequency: 2.2, Bloom: K,A

Concept:

Some security policies require periodic scanning of the password database to ensure that users are complying with the password policy.

BSDP candidates should be aware of the legal and moral obligations involved in password scanning and, as required by their employment duties, know how to perform both a dictionary and brute force password cracking exercise.

Practical:

software of choice from packages/pkgsrc

passwd(5), master.passwd(5)

Estimated Time:

20 minutes to configure and review the results from a dictionary scan.

3.2.13 Configure kernel to prevent ability to perform network sniffing.

Importance: 3.4, Frequency: 1.5, Bloom: K,A

Concept:

The Berkeley Packet Filter (bpf) enables a BSD system to acquire and process packets directly off the network interface and is necessary to perform network packet sniffing on a BSD system.

BSDP candidates should know how to disable the operation of bpf on their BSD system of choice.

Practical:

bpf(4)

Estimated Time:

5 minutes to configure a kernel without bpf.

3.2.14 Configure a firewall to act as an authentication gateway.

Importance: 3.5, Frequency: 1.6, Bloom: K,C,A

Concept:

An authentication gateway is one that permits traffic to pass after a valid authentication mechanism approves the flow. Once authentication is successful, predetermined rules are applied to the traffic flow.

BSDP candidates should be able to configure an authentication gateway.

Practical:

software of choice from packages/pkgsrc

pf(4), pfctl(8), authpf(8), pf.conf(5)

Estimated Time:

30 minutes to configure and test an authentication gateway according to a specification.

3.2.15 Configure a firewall for greylisting or blacklisting.

Importance: 3.7, Frequency: 2.1, Bloom: K,C,A

Concept:

System administrators can configure a firewall to recognize when suspicious traffic occurs and to block the offending network or host temporarily (greylisting) or permanently (blacklisting).

BSDP candidates should be able to configure their BSD firewall of choice to recognize a traffic pattern designated as suspicious and restrict the source temporarily or permanently.

Practical:

software of choice from packages/pkgsrc

pf(4), pfctl(8), pf.conf(5)

DragonFly BSD, FreeBSD: ipfw(8)

Estimated Time:

20 minutes to configure and test a firewall to greylist or blacklist traffic according to a specification.

3.2.16 Configure a firewall to deny multiple connection attempts from an attacker.

Importance: 4.0, Frequency: 2.4, Bloom: K,C,A

Concept:

In the case of multiple connection attempts, network traffic is considered to be malicious when the number of connection attempts exceeds a predetermined threshold.

BSDP candidates should be able to configure their BSD firewall of choice to deny connection attempts that exceed a connection threshold.

Practical:

software of choice from packages/pkgsrc

pf(4), pfctl(8), pf.conf(5)

DragonFly BSD, FreeBSD: ipfw(8)

Estimated Time:

20 minutes to configure and test the denial of connection attempts according to a specification.

3.2.17 Configure a firewall with custom packet filtering rules.

Importance: 4.3, Frequency: 2.7, Bloom: K,C,A

Concept:

Configuring a firewall to permit and deny traffic is a common system administration task. Traffic is often constrained by security policies that restrict traffic flows to those officially approved.

BSDP candidates should be able to configure their BSD firewall of choice to permit and deny traffic based on a specification.

Practical:

pf(4), pfctl(8), pf.conf(5)

DragonFly BSD, FreeBSD: ipfw(8)

Estimated Time:

20 minutes to configure and test firewall rules according to a specification.

3.2.18 Configure TCP wrappers.

Importance: 3.4, Frequency: 1.9, Bloom: K,C,A

Concept:

TCP wrappers allows a system administrator to exercise fine grained control over remote access to network services.

BSDP candidates should understand the capabilities offered by TCP wrappers and be able to configure the system to allow or deny remote users access to specific services.

Practical:

inetd(8), inetd.conf(5), hosts_access(5), hosts_options(5)

Estimated Time:

20 minutes to configure and test a system to use TCP wrappers according to a specification.

3.2.19 Configure a file integrity checking utility.

Importance: 3.5, Frequency: 2.0, Bloom: K,C,A

Concept:

BSD systems have integrity checking utilities present in the base system. These utilities can be used to produce MD5, SHA, and RIPE hashes of individual files, directories, or whole filesystems.

BSDP candidates should be able to produce file integrity hash collections and use those hashes to determine if there have been any changes to file content or file attributes.

Practical:

software of choice from packages/pkgsrc

mtree(8), cksum(1), stat(1)

Estimated Time:

20 minutes to create a hash collection according to a specification and to detect changes to file content or attributes.

3.2.20 Configure One-Time Passwords (OTP).

Importance: 3.0, Frequency: 1.5, Bloom: K,C,A

Concept:

One Time Passwords (OTP) restrict users from reusing the same password for subsequent authentication. This significantly reduces the chance that an attacker can gain access by reusing another user's password. OTP utilizes S/KEY (RFC 2289) to secure the password against replay attacks.

BSDP candidates should know how to configure and test OTP.

Practical:

DragonFly BSD, FreeBSD: opie(4), opiekeys(5), opieaccess(5), opiekey(1), opieinfo(1), opiepasswd(1)

NetBSD, OpenBSD: skey(1), skeyaudit(1), skeyinfo(1), skeyinit(1)

Estimated Time:

30 minutes to configure and test OTP.

3.2.21 Configure a password policy.

Importance: 3.5, Frequency: 1.6, Bloom: K,C,A

Concept:

Many security policies require require the use of advanced controls on password usage.

Given a specification, BSDP candidates should be able to configure a password policy. Possible specifications include: login backoff delay, number of login attempts, allowable login times, and minimum password length.

Practical:

software of choice from packages/pkgsrc

login.conf(5)

DragonFly BSD, FreeBSD: pam_passwdqc(8), pam.conf(5)

Estimated Time:

20 minutes to configure a password policy according to a specification.

3.2.22 Utilize daily security checks to monitor system for common security threats.

Importance: 4.3, Frequency: 3.3, Bloom: K, A

Concept:

BSD systems provide a set of scripts and programs that perform security monitoring on a periodic basis. The scripts examine files and perform operations to gather relevant security information which is provided to the administrator in a daily email summary.

BSDP candidates should be familiar with the location and use of these monitoring scripts and be able to configure them to be turned on or off.

Practical:

DragonFly BSD, FreeBSD: periodic(8), periodic.conf(5), security(7)

NetBSD: security.conf(5)

OpenBSD: security(8)

Estimated Time:

15 minutes to attend to the security email and enable or disable monitoring scripts according to a specification.

3.2.23 Configure an IPSec VPN.

Importance: 3.3, Frequency: 1.2, Bloom: K,C,A

Concept:

IPSec is a set of protocols- ESP (for Encapsulating Security Payload), AH (for Authentication Header), and IPComp (for IP Payload Compression Protocol)- that provide security services for IP packets.

BSDP candidates should understand the differences between IPSec transport and tunnel modes. Candidates should also be able to configure an IPSec Virtual Private Network (VPN) in tunnel mode between two networks.

Practical:

software of choice from packages/pkgsrc

sysctl(7) or (8), ipsec(4)

DragonFly BSD, *FreeBSD:* setkey(8), ipsec_set_policy(3)

NetBSD: racoon(8), setkey(8), racoon.conf(5)

OpenBSD: enc(4), pf.conf(5), ipsecctl(8), isakmpd(8)

Estimated Time:

45 minutes to configure, setup, and test an IPSec VPN according to a specification.

3.2.24 Configure process accounting or security event auditing.

Importance: 3.9, Frequency: 2.2, Bloom: K,C,A

Concept:

BSD systems provide various facilities for determining activity on a system. Process accounting provides statistics on system resources and their allocation among users. Security event auditing, available on FreeBSD only, provides more fine-grained logging of a variety of security-relevant system events, including logins, configuration changes, and file and network access.

BSDP candidates should be familiar with the accounting and auditing capabilities provided by their BSD of choice and be able to configure the system to collect, process, and report on notifications.

Practical:

sa(8), lastcomm(1), acct(5), ac(8), accton(8)

FreeBSD: audit(4), audit_class(5), audit_control(5), audit_event(5), audit_warn(5), auditd(8), audit(8)

Estimated Time:

30 minutes to configure accounting or auditing according to a specification.

3.3 Filesystems and Files

Files and filesystems are essential components of a BSD system. The BSDP candidate must be able to configure new filesystems, adjust various filesystem parameters, take filesystem snapshots, and perform other complex tasks according to a specification.

3.3.1 Format an FFS filesystem.

Importance: 3.9, Frequency: 2.0, Bloom: K,C,A

Concept:

Before a hard disk can store data it must first be partitioned and then formatted with a filesystem.

BSDP candidates should be able to create a hard disk partition, format it with the Fast File System (FFS), and specify its blocksize, inode density, and other common parameters found in newfs(8).

Practical:

disklabel(8), newfs(8)

Estimated Time:

10 minutes to partition and format a FFS filesystem according to a specification.

3.3.2 Manually run file system checker and repair tool.

Importance: 4.1, Frequency: 2.1, Bloom: K,C,A

Concept:

Over time, filesystems can become damaged due to physical deterioration or data corruption.

BSDP candidates should be able to assess whether a corrupted filesystem can be recovered and use the tools available to recover the filesystem and data.

Practical:

fsck(8), fsdb(8), mount(8)

Estimated Time:

20 minutes to fix a filesystem according to a specification.

3.3.3 Restore system files from single user mode.

Importance: 4.1, Frequency: 1.5, Bloom: K,C,A

Concept:

Some files are necessary to the operation of a BSD system. Should a critical system file become corrupted or deleted, it may render the system inaccessible.

BSDP candidates should be able to boot a system in single user mode and fix or restore the specified

system file.

Practical:

shutdown(8), mount(8), cp(1), cpio(1), tar(1), dd(1), restore(8)

Estimated Time:

15 minutes to recover system files and successfully boot into an operational system.

3.3.4 Resolve full filesystem issues.

Importance: 4.2, Frequency: 1.8, Bloom: K,C,A

Concept:

Filesystems can become full due to excessive use.

BSDP candidates should know how to find and remove specified files from a filesystem in order to recover disk space. They should also be able to create symbolic links to help prevent the filesystem from becoming full again.

Practical:

rm(1), find(1), rmdir(1), ln(1), df(1), du(1)

Estimated Time:

10 minutes to recover disk space according to a specification.

3.3.5 Set up filesystem quotas for users.

Importance: 3.4, Frequency: 1.7, Bloom: K,C,A

Concept:

Filesystem quotas allow the system administrator to place restrictions on disk usage. Restrictions may be enforced on a particular user or group or on all users and groups.

BSDP candidates should understand how quotas are enabled, disabled, edited, and reported. Candidates should also be able to configure quotas for a given filesystem.

Practical:

quotaon(8), quota(1), quotackeck(8), edquota(8), repquota(8), fstab(5)

Estimated Time:

20 minutes to configure quotas for a filesystem according to a specification.

3.3.6 Enable or disable a mounted filesystem's write status.

Importance: 3.5, Frequency: 1.8, Bloom: K,C,A

Concept:

Filesystems can be mounted as read-only file storage, in which case no writing is permitted while the filesystem is mounted.

BSDP candidates should be able to mount a filesystem as read-only and change the read-write status of a currently mounted filesystem.

Practical:

mount(8), chflags(1)

Estimated Time:

10 minutes to configure a filesystem's read/write status according to a specification.

3.3.7 Configure software RAID.

Importance: 3.8, Frequency: 1.6, Bloom: K,C,A

Concept:

Redundant Array of Inexpensive Disks (RAID) is used to provide increased storage reliability through redundant disks. Should one disk fail, the data is maintained by other disks within the array.

BSDP candidates should be familiar with basic RAID concepts and understand RAID levels 0, 1, 4, and 5. Candidates should also be able to configure the requested RAID type for their BSD of choice.

Practical:

ccd(4), ccdconfig(8)

FreeBSD: vinum(8), gstripe(8), gmirror(8)

NetBSD, OpenBSD: raid(4), raidctl(8)

Estimated Time:

30 minutes to configure software RAID according to a specification.

3.3.8 Encrypt a file.

Importance: 3.7, Frequency: 2.5, Bloom: K,C,A

Concept:

File encryption protects the confidentiality of data within a file. There are a variety of ways to encrypt and decrypt a file, depending on user requirements.

BSDP candidates should be able to use their cryptographic utility of choice to encrypt and decrypt a given file. Candidates should also be familiar with the differences between symmetric and asymmetric encryption.

Practical:

software of choice from packages/pkgsrc

openssl(1)

Estimated Time:

10 minutes to encrypt or decrypt a file according to a specification.

3.3.9 Configure an encrypted disk or partition.

Importance: 3.5, Frequency: 1.7, Bloom: K,C,A

Concept:

An encrypted disk or partition adds an additional layer of security as a passphrase is required before the data can be accessed.

BSDP candidates should be able to encrypt the specified disk or partition and verify that the data is only accessible when the correct passphrase is used.

Practical:

software of choice from packages/pkgsrc

FreeBSD: gbde(4), gbde(8), geli(8)

NetBSD: cgd(4), cgdconfig(8)

OpenBSD: vnconfig(8)

Estimated Time:

20 minutes to create and test an encrypted disk or partition according to a specification.

3.3.10 Create a filesystem snapshot.

Importance: 3.8, Frequency: 2.5, Bloom: K,C,A

Concept:

Snapshots allow a user to create images of specified filesystems and treat them as files. Snapshots can be used for backup purposes or to study the state of the filesystem at a given point in time.

BSDP candidates should be able to take a snapshot of the specified filesystem on their BSD of choice.

Practical:

software of choice from packages/pkgsrc

DragonFly BSD: hammer(8)

FreeBSD: mksnap_ffs(8)

NetBSD: fss(4), fssconfig(8)

Estimated Time:

15 minutes to take a snapshot of a filesystem according to a specification.

3.3.11 Configure filesystem journaling or soft updates.

Importance: 3.8, Frequency: 1.9, Bloom: K,C,A

Concept:

A journaling filesystem keeps track of pending changes before committing them. Soft updates use a memory cache to improve performance. In the event of a system crash or power failure, these types of filesystems are quicker to bring back online and less likely to become corrupted.

BSDP candidates should be able to format a partition with a journaled filesystem or enable soft updates on a BSD system.

Practical:

DragonFly BSD, FreeBSD, NetBSD: tunefs(8)

DragonFly BSD: mountctl(8), ffs(5)

FreeBSD: gjournal(8)

NetBSD: wapbl(4), fstab(5)

OpenBSD: mount(8)

Estimated Time:

20 minutes to configure a journaling filesystem or to enable soft updates according to a specification.

3.4 User Administration

Many BSD systems have a large user base and the BSD system administrator often needs to perform a specialized task for multiple users. The BSDP candidate must be able to configure user accounts and to automate many tasks associated with user account management.

3.4.1 Customize the login class capability database.

Importance: 3.3, Frequency: 1.6, Bloom: K,C,A

Concept:

Part of the login(1) process is to check various attributes in the login class capability database to see if the current login should be permitted or denied.

BSDP candidates should understand the capabilities offered by the login class database and be able to configure a login class.

Practical:

login(1), login.conf(5)

DragonFly BSD, FreeBSD: login.access(5)

OpenBSD: authenticate(3), bsd_auth(3)

Estimated Time:

15 minutes to configure and test a user account in the login capability database.

3.4.2 Script the creation/deletion/modification of multiple user accounts.

Importance: 3.3, Frequency: 1.8, Bloom: K,A

Concept:

Manually adding, deleting, and modifying individual user accounts is practical when the number of users is small. However, it is often easier to create a script to perform basic account management operations for large numbers of users.

BSDP candidates should be able to script the creation, deletion, and modification of user accounts using their scripting language of choice.

Practical:

scripting language of choice

adduser(8), rmuser(8) or userdel(8), usermod(8) or vipw(8)

DragonFly BSD, FreeBSD: pw(8)

Estimated Time:

15 minutes to create and test user accounts modified by a script according to a specification.

3.4.3 Prevent regular users from viewing who is logged on and seeing what others are doing.

Importance: 3.5, Frequency: 1.8, Bloom: K,C

Concept:

Some BSD systems provide kernel MIBS which can be used to prevent users from snooping on each other. Additionally, SSH users can be constrained to their own chroot environment.

BSDP candidates should be able to configure their BSD system to prevent users from seeing the activities of other users.

Practical:

sshd_config(8)

FreeBSD: sysctl(8)

NetBSD: sysctl(7)

Estimated Time:

5 minutes to configure the system to prevent users from viewing the activities of other users.

3.4.4 Restrict the commands available to a user.

Importance: 3.7, Frequency: 1.9, Bloom: K,C,A

Concept:

One way to increase the security of a system is to restrict the commands that are available to logged-in users. This can be achieved through the installation and configuration of a restricted shell or by adding commands to the user's SSH authorized_keys file.

BSDP candidates should be able to restrict the commands available to a given user.

Practical:

software of choice from packages/pkgsrc

sshd(8)

Estimated Time:

20 minutes to configure a restricted shell according to a specification.

3.4.5 Create or modify skeleton files for new users' home directories.

Importance: 3.5, Frequency: 1.7, Bloom: K,A

Concept:

It is possible to automatically populate the home directories of new users with "dot" files. These files can be preconfigured with aliases, environment variables, and shell functions.

BSDP candidates should be able to configure a skeleton "dot" file and have it populate the home directories of new users automatically.

Practical:

shell configuration file(s) of choice

/skel/ directories on BSD of choice

Estimated Time:

15 minutes to configure and test skeleton files for new user accounts according to a specification.

3.4.6 Force an active user off the system.

Importance: 3.6, Frequency: 1.8, Bloom: K,A

Concept:

It is sometimes necessary to force malicious users off the system.

BSDP candidates should be able to force a specified user off the system and prevent them from regaining access.

Practical:

ps(1), kill(1), pkill(1), hosts_access(5), hosts_options(5), vipw(8)

DragonFly BSD, FreeBSD: pw(8)

NetBSD, OpenBSD: usermod(8)

Estimated Time:

5 minutes to force a user off the system and configure the system to disallow logins for that user.

3.4.7 Set shell limits.

Importance: 3.6, Frequency: 1.9, Bloom: K,A

Concept:

A user's shell can be configured to limit the number of open files, the number of blocks for core dumps, and other similar limits.

BSDP candidates should be able to configure shell limits for their shell of choice.

Practical:

man page for shell of choice

Estimated Time:

15 minutes to configure and test shell limits according to a specification.

3.4.8 Configure resource limits.

Importance: 3.5, Frequency: 1.8, Bloom: K,A

Concept:

BSD systems use login.conf(5) to limit resources such as CPU and memory usage.

BSDP candidates should understand the difference between hard and soft limits, be able to create a login class, and add resource limits to that class.

Practical:

login.conf(5)

Estimated Time:

5 minutes to configure resource limits according to a specification.

3.4.9 Generate a key and configure the system to use it for SSH authentication.

Importance: 4.3, Frequency: 2.4, Bloom: K,C,A

Concept:

SSH key based authentication is a secure method for authenticating remote users.

BSDP candidates should be able to configure, install, and test SSH keys for authentication, troubleshoot authentication problems, and change key formats between OpenSSH and RFC 4716.

Practical:

ssh-keygen(1), sshd(8), sshd_config(5)

Estimated Time:

20 minutes to generate, install, and test a key for SSH authentication.

3.4.10 Configure users to autologout after a period of inactivity.

Importance: 3.3, Frequency: 1.7, Bloom: K,A

Concept:

Setting an idle timeout on user sessions is a best practice. The method for configuring autologout of users is shell dependent and should be enforced at the system level.

BSDP candidates should be able to configure autologout for their shell of choice.

Practical:

man page for shell of choice

Estimated Time:

15 minutes to configure and test autologout according to a specification.

3.4.11 Log a user's activity on a terminal.

Importance: 3.3, Frequency: 1.7, Bloom: K,A

Concept:

Logging all user input and terminal output is desirable in many situations.

BSDP candidates should be able to configure a user login to record all user activity on a terminal.

Practical:

script(1), configuration file for shell of choice

Estimated Time:

10 minutes to configure and test a shell to log all activity according to a specification.

3.4.12 Configure a user account to expire on a specified date.

Importance: 3.2, Frequency: 1.7, Bloom: K,A

Concept:

User accounts can be created or modified to expire on a certain date.

BSDP candidates should understand account expiration capabilities and be able to configure and test user account expiration.

Practical:

adduser(8) or useradd(8), login.conf(5)

DragonFly BSD, FreeBSD, NetBSD: pw(8)

Estimated Time:

10 minutes to configure a user account to expire according to a specification.

3.4.13 Create a system account.

Importance: 3.8, Frequency: 2.2, Bloom: K,A

Concept:

System accounts are created for use by applications, and for security reasons, should not be available for users to login to the system. These accounts do not need a login shell and generally do not need resources.

BSDP candidates should be able to create and test a system account.

Practical:

adduser(8) or useradd(8), nologin(8)

Estimated Time:

10 minutes to create and test a system account according to a specification.

3.5 General Administration

General administration tasks include many of the day-to-day activities performed by a BSD system administrator. The BSDP candidate should know how to perform all of these tasks in an efficient manner.

3.5.1 Configure shared library cache.

Importance: 3.0, Frequency: 1.5, Bloom: K,C,A

Concept:

The ldconfig utility is used to prepare a set of hints to facilitate quick lookup of shared libraries spanning multiple directories. The libraries which are found will be automatically available when a program is loaded.

BSDP candidates should be able to list the current library paths and add a new path using ldconfig(8).

Practical:

ldconfig(8), ld(1)

NetBSD: ld.so.conf(5)

Estimated Time:

5 minutes to configure the shared library cache according to a specification.

3.5.2 Enable or disable virtual consoles.

Importance: 3.0, Frequency: 1.5, Bloom: K,A

Concept:

Virtual consoles are additional terminal sessions that are accessed by a function key sequence.

BSDP candidates should be able to recognize how many virtual consoles are enabled on the system and change the number of available virtual consoles.

Practical:

ttys(5)

Estimated Time:

5 minutes to enable or disable a specified number of virtual consoles.

3.5.3 Configure and recompile a kernel.

Importance: 4.4, Frequency: 2.0, Bloom: K,C,A

Concept:

A system administrator sometimes needs to recompile a kernel in order to add or remove kernel

functionality.

BSDP candidates should be able to add or delete a specified functionality to the kernel configuration file of their BSD of choice, then compile and install the new kernel.

Practical:

config(8), make(1)

NetBSD, OpenBSD: options(4)

Estimated Time:

15 minutes to configure and install a kernel. BSDP lab exam candidates should perform other tasks while the kernel is compiling.

3.5.4 Boot an alternate kernel.

Importance: 4.3, Frequency: 1.8, Bloom: K,A

Concept:

It is possible to compile and store multiple kernels on a BSD system. The system administrator can choose which kernel is used when the system boots.

BSDP candidates should be able to interrupt the boot process and load an alternate kernel.

Practical:

boot(8)

NetBSD: boot.cfg(5)

Estimated Time:

5 minutes to load a specified kernel.

3.5.5 Load and unload kernel modules.

Importance: 4.0, Frequency: 2.3, Bloom: K,A

Concept:

Kernel modules allow the system administrator to add or remove functionality on a running system without having to recompile and install a new kernel.

BSDP candidates should be able to view which modules are currently loaded and to load or unload a specified kernel module.

Practical:

DragonFly BSD, FreeBSD: kldload(8), kldstat(8), kldunload(8)

NetBSD, OpenBSD: modload(8), modstat(8), modunload(8)

Estimated Time:

5 minutes to load or unload a kernel module according to a specification.

3.5.6 Install perl modules.

Importance: 3.5, Frequency: 2.1, Bloom: K,A

Concept:

Perl is a popular scripting language which provides a large collection of modules that perform a wide variety of programming tasks. Many perl modules are available through packages and pkgsrc.

BSDP candidates should be familiar with the availability of perl packages and be able to install a given perl module from either packages or pkgsrc.

Practical:

pkg_add(1)

Estimated Time:

5 minutes to install a perl module according to a specification.

3.5.7 Retrieve updates from a code repository.

Importance: 4.1, Frequency: 2.7, Bloom: K,A

Concept:

BSD projects maintain official repositories containing operating system source as well as the source for software which has been ported to the operating system.

BSDP candidates should be able to sync their system of choice with the specified subset of a source collection.

Practical:

DragonFly BSD: git(1)

FreeBSD: csup(1)

FreeBSD, NetBSD, OpenBSD: cvs(1)

Estimated Time:

15 minutes to synchronize a local repository with a remote repository according to a specification.

3.5.8 Use ktrace to troubleshoot software issues.

Importance: 3.4, Frequency: 2.0, Bloom: K,C,A

Concept:

The ktrace utility can be used to track kernel system calls and I/O for the specified application.

BSDP candidates should be able to enable and disable kernel tracing and review the generated trace file.

Practical:

ktrace(1), kdump(1)

Estimated Time:

15 minutes to troubleshoot a software issue according to a specification.

3.5.9 Update system configuration files during a system upgrade.

Importance: 4.0, Frequency: 2.1, Bloom: K,A

Concept:

During a system upgrade it is important that all system configuration files contain both the new settings required by the operating system as well as any existing customizations required by the local environment.

BSDP candidates should be able to merge any changes to system configuration files during an upgrade.

Practical:

software of choice from packages/pkgsrc

diff(1)

DragonFly BSD: make(1)

FreeBSD: mergemaster(8)

NetBSD: etcupdate(8)

OpenBSD: sysmerge(8)

Estimated Time:

15 minutes to merge system configuration files according to a specification.

3.5.10 Tune the operating system.

Importance: 4.3, Frequency: 2.4, Bloom: K,C,A

Concept:

There are many factors that can contribute to the speed and efficiency of a running system. Some factors are pre-installation decisions, such as the size and number of partitions and their selected block sizes. The tunefs utility allows the administrator to tune some filesystem parameters and the sysctl utility provides the capability to change MIB parameters to improve the performance of a system.

BSDP candidates should be able to tune their BSD system.

Practical:

tunefs(8), sysctl (7) or (8)

DragonFly BSD, FreeBSD: tuning(7)

Estimated Time:

5 minutes to tune the operating system according to a specification.

3.5.11 View interrupt rate.

Importance: 3.3, Frequency: 2.2, Bloom: K,A

Concept:

Devices communicate updates in the hardware state via interrupts. The interrupt number of a device can usually be seen in the system boot messages. To get more information about the runtime behavior of a device, interrupt statistics need to be reviewed.

BSDP candidates should be able to view the runtime interrupt statistics using the utilities provided by their BSD system.

Practical:

iostat(8), pstat(8), systat(1)

Estimated Time:

5 minutes to review the interrupt rate.

3.5.12 Enable logins on serial console.

Importance: 3.2, Frequency: 1.6, Bloom: K,A

Concept:

Serial communications allow an administrator to access a system that does not have an attached keyboard or monitor.

BSDP candidates should be able to configure their BSD of choice to accept logins over a serial port.

Practical:

ttys(5), boot(8)

Estimated Time:

10 minutes to enable serial logins according to a specification.

3.5.13 Add additional swap space.

Importance: 3.4, Frequency: 1.5, Bloom: K,A

Concept:

One way to improve system performance is to increase the memory available to applications. When it is not possible to add more physical memory, the system administrator can increase virtual memory by adding swap space.

BSDP candidates should be able to create and enable additional swap space.

Practical:

dd(1), rc.conf(5), chmod(1), fstab(5), vnconfig(8), swapon(8)

Estimated Time:

10 minutes to create and enable new swap space according to a specification.

3.5.14 Insert entries in the system log.

Importance: 3.2, Frequency: 2.0, Bloom: K,A

Concept:

When troubleshooting a system, it can be useful to add comments to the log file to mark certain actions.

BSDP candidates should be able to add entries to the system log file.

Practical:

logger(1)

Estimated Time:

5 minutes to add a log entry according to a specification.

3.5.15 Configure the system for Linux binary compatibility.

Importance: 3.2, Frequency: 1.6, Bloom: K,A

Concept:

Binary compatibility allows a system to run applications that were compiled for a different operating system. BSD systems are able to provide binary compatibility for Linux applications.

BSDP candidates should be able to install the Linux runtime libraries for their BSD system of choice, install a precompiled Linux binary, and verify that Linux emulation is enabled. They should also be able to mount /proc for Linux binaries that require this filesystem.

Practical:

software of choice from packages/pkgsrc

fstab(5)

DragonFly BSD, FreeBSD: kldload(8), linprocfs(5), linux(4), brandelf(1)

NetBSD, OpenBSD: mount_procfs(8), compat_linux(8)

Estimated Time:

30 minutes to load the libraries, install the application, configure the environment, and run a Linux binary according to a specification.

3.5.16 Configure a network service to use a sandbox environment.

Importance: 3.5, Frequency: 1.8, Bloom: K,C,A

Concept:

The chroot command can be used to change the apparent disk root directory for a process and its children. A program that is re-rooted to another directory cannot access files outside of that directory.

BSDP candidates should be able to create a chroot for a specified service and ensure that all of the libraries that program needs are contained within the chroot.

Practical:

chroot(8), ldd(1)

Estimated Time:

20 minutes to configure a sandbox environment for a network service according to a specification.

3.5.17 Setup on-going software vulnerability audit reports.

Importance: 4.0, Frequency: 2.5, Bloom: K,A

Concept:

Tracking security vulnerabilities for software is an important task.

BSDP candidates should be able to track security vulnerabilities for software that was installed using pkgsrc or packages.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

15 minutes to automate the tracking of security vulnerabilities according to a specification.

3.5.18 Capture performance data using standard tools.

Importance: 4.1, Frequency: 3.2, Bloom: K,A

Concept:

An important administrative task is proactively monitoring system performance to become aware of potential bottlenecks or issues.

BSDP candidates should be able to use common utilities to monitor performance data such as CPU usage, RAM usage, network usage, and disk I/O.

Practical:

vmstat(8) or vmstat(1), iostat(8), systat(1), netstat(1), ps(1), top(1)

Estimated Time:

10 minutes to collect performance data using standard tools according to a specification.

3.5.19 Localize a server for another language.

Importance: 2.5, Frequency: 1.4, Bloom: K,A

Concept:

Localization adds support for non-English characters and can be added to the environment settings of a BSD system.

BSDP candidates should be able to configure their BSD of choice to support the specified locale.

Practical:

environment settings for shell of choice

DragonFly BSD, FreeBSD, NetBSD: locale(1), setlocale(3)

Estimated Time:

10 minutes to configure localization according to a specification.

3.6 Common Services

Providing access to and configuring services, both locally and on a network, is a key skill of a BSD system administrator.

BSDP candidates should understand the options available for providing a service and be proficient in installing, configuring, and monitoring the specified service. Candidates are free to implement the service through any software provided with the four supported BSD systems, or available through packages or pkgsrc. Candidates are expected to use their knowledge of the service described and the capabilities of their preferred platform to implement the objectives in a time efficient manner.

3.6.1 Configure and enable a DHCP server.

Importance: 3.8, Frequency: 1.9, Bloom: K,C,A

Concept:

A Dynamic Host Configuration Protocol (DHCP) server is used to provide network addressing information to systems running DHCP client software.

BSDP candidates should know how to install and configure the DHCP server software of their choice to provide IPv4 addressing information.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

20 minutes to install, configure, and test a DHCP server according to a specification.

3.6.2 Override settings a DHCP client receives from a DHCP server.

Importance: 3.4, Frequency: 1.9, Bloom: K,A

Concept:

A system administrator can configure a DHCP client to override the settings received from a DHCP server. BSD systems provide a dhclient.conf(5) file which contains configuration directives for this purpose.

BSDP candidates should know how to use this file's directives to either override settings received or to specify default settings.

Practical:

dhclient.conf(5), dhclient(8)

Estimated Time:

10 minutes to configure a dhclient.conf file according to a specification.

3.6.3 Enable a DNS caching server.

Importance: 3.9, Frequency: 2.0, Bloom: K,C,A

Concept:

A caching name server provides name services for clients but may not be authoritative for the domains being queried. A caching server retains name resolution data for all domains that it resolves on behalf of clients.

BSDP candidates should know how to configure and operate a caching name serveras well as how to dump and clear the cache of the name server.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

20 minutes to set up and operate a caching name server.

3.6.4 Configure a primary DNS server.

Importance: 4.0, Frequency: 2.0, Bloom: K,C, A

Concept:

A primary name server serves information found in a master zone. Names resolved in this fashion are considered authoritative.

BSDP candidates should be able to configure a primary name server that provides authoritative replies from a master zone file.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

20 minutes to set up a primary name server according to a specification.

3.6.5 Configure a secondary DNS server.

Importance: 3.8, Frequency: 1.9, Bloom: K,C, A

Concept:

A secondary DNS server serves data from secondary zones. The secondary name server needs to refresh data from a primary server through a zone transfer of the selected zone.

BSDP candidates should be able to configure a secondary name server. Candidates should also be able to configure the server to refresh zone data from a master server via a zone transfer.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

15 minutes to set up a secondary server according to a specification.

3.6.6 Determine which DNS servers are authoritative for a specified hostname.

Importance: 4.0, Frequency: 2.5, Bloom: K,C, A

Concept:

DNS queries that return IP addresses include data in the reply that indicates whether or not the information returned is considered authoritative for the domain or host requested. Authority is determined by configuration of the zone file for that domain.

BSDP candidates should understand the difference between authoritative and non-authoritative DNS replies. They should be able to retrieve replies for any domain and check the authority of the reply.

Practical:

software of choice from packages/pkgsrc

host(1), dig(1)

Estimated Time:

5 minutes to retrieve a DNS reply, determine its authority, and determine what server(s) are authoritative for a host or domain.

3.6.7 Configure a DNS server to permit or deny zone transfers.

Importance: 3.9, Frequency: 1.8, Bloom: K,C,A

Concept:

Primary name servers can be configured to permit or deny zone transfers from specific hosts or from all hosts.

BSDP candidates should know how to configure a primary name server to permit zone transfers from specific hosts, from any host, or not at all.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

10 minutes to configure a name server to permit zone transfers according to a specification.

3.6.8 Configure a DNS server to provide reverse lookups.

Importance: 3.9, Frequency: 2.0, Bloom: K,C,A

Concept:

DNS servers can be configured to return name information when queried with a PTR resource record

containing an IP address. Many applications, such as mail servers, expect this functionality.

BSDP candidates should know how to configure a DNS server for reverse lookups and test that it is able to return a hostname for an IP address.

Practical:

software of choice from packages/pkgsrc

dig(1), host(1)

Estimated Time:

15 minutes to configure a DNS server to provide reverse lookups and test the configuration according to a specification.

3.6.9 Change the order of name resolution.

Importance: 3.5, Frequency: 1.7, Bloom: K,C, A

Concept:

BSD systems can use text files, DNS, a DNS caching daemon, or Network Information Service (NIS) for name resolution. The system administrator can configure the order of these name resolution methods.

BSDP candidates should be able to configure the order of name resolution on their BSD system.

Practical:

DragonFly BSD, FreeBSD, NetBSD: nsswitch.conf(5)

OpenBSD: resolv.conf(5)

Estimated Time:

5 minutes to configure the order of name resolution on a BSD system according to a specification.

3.6.10 Configure an NTP server.

Importance: 3.0, Frequency: 1.5, Bloom: K,C, A

Concept:

Network Time Protocol (NTP) is capable of synchronizing time across multiple disparate devices. This is useful in environments that require precision timekeeping.

BSDP candidates should have a general understanding of NTP operation and be able to configure a BSD system to operate as an NTP server.

Practical:

software of choice from packages/pkgsrc

FreeBSD: ntpd(8), ntp.conf(5), ntpdate(8), ntpdc(8), ntpq(8)

NetBSD: ntpd(1)

OpenBSD: ntpd(8), ntpd.conf(5)

Estimated Time:

25 minutes to configure and test an NTP server according to a specification.

3.6.11 Install and configure an FTP server.

Importance: 3.6, Frequency: 1.8, Bloom: K,C,A

Concept:

File Transfer Protocol (FTP) enables authenticated users to transfer files between computer systems. An FTP server accepts connection requests from FTP clients and uploads or downloads data according to requests from the client.

BSDP candidates should be able to configure and test an FTP server.

Practical:

software of choice from packages/pkgsrc

ftpd(8), ftp(1), services(5), inetd(8)

DragonFly BSD, FreeBSD: ftpchroot(5)

NetBSD: ftpd.conf(5), ftpusers(5)

OpenBSD: ftp-proxy(8)

Estimated Time:

15 minutes to configure and test an FTP server according to a specification.

3.6.12 Configure a Mail Transfer Agent (MTA) to send and receive email.

Importance: 4.1, Frequency: 2.0, Bloom: K,C,A

Concept:

A mail server is one of the most important and widely used components of an organization's IT infrastructure. A system administrator needs to be able to configure an MTA to send and receive email to and from a domain and subdomains, rewrite source addresses, issue custom replies for unknown users, manage mail aliases, and perform other similar technical tasks.

BSDP candidates should know how to configure the MTA of their choice to send and receive email, and verify that the configuration is working correctly.

Practical:

MTA of choice either included with the BSD system or installed from packages/pkgsrc

Estimated Time:

30 minutes to configure an MTA to send and receive email according to a specification.

3.6.13 Manually send an email using SMTP protocol.

Importance: 3.8, Frequency: 2.4, Bloom: K,C, A

Concept:

It is occasionally necessary to test an MTA by manually sending a test email.

BSDP candidates should to be able to connect to an MTA using an ASCII data stream and process a test email. The email should arrive at the assigned destination, which may or may not be on the local system.

Practical:

RFC 821 (updated by RFC 2821)

telnet(1)

DragonFly BSD, FreeBSD, OpenBSD: nc(1)

Estimated Time:

10 minutes to manually connect to an MTA and process an email according to a specification.

3.6.14 Configure MTA for outgoing mail only.

Importance: 3.7, Frequency: 1.9, Bloom: K,A

Concept:

An MTA can be configured to only send email or to relay outgoing mail to another mail server.

BSDP candidates should know how to configure their MTA for outbound only operation, either as a main mail server or a forwarding mail server.

Practical:

MTA of choice either included with the BSD system or installed from packages/pkgsrc

Estimated Time:

15 minutes to configure MTA for outbound only operation according to a specification.

3.6.15 Configure MTA to use SASL.

Importance: 3.4, Frequency: 1.7, Bloom: K,C,A

Concept:

RFC 4422 describes the Simple Authentication and Security Layer (SASL), a framework for adding authentication support to connection-based protocols. When added to an MTA, the mail server will first authenticate users to determine if they are allowed to establish a connection to the mail server.

BSDP candidates should be able to add SASL support to their MTA of choice and confirm that authentication is working properly.

Practical:

MTA of choice either included with the BSD system or installed from packages/pkgsrc

SASL implementation from packages/pkgsrc

Estimated Time:

45 minutes to configure a SASL enabled MTA according to a specification.

3.6.16 Configure MTA to use TLS.

Importance: 3.5, Frequency: 1.7, Bloom: K,C,A

Concept:

RFC 5246 describes how SMTP servers can use Transport Layer Security (TLS) to provide private, authenticated communication over the Internet. TLS enables an MTA to encrypt email communications.

BSDP candidates should be able to add TLS support to their MTA of choice and confirm that mail communications over the network are encrypted.

Practical:

MTA of choice, either included with the BSD system or installed from packages/pkgsrc

software of choice from packages/pkgsrc

tcpdump(1)

Estimated Time:

45 minutes to configure TLS for an MTA according to a specification.

3.6.17 Configure MTA to filter SPAM.

Importance: 4.0, Frequency: 2.2, Bloom: K,C,A

Concept:

BSD administrators should be aware of various options for filtering SPAM. Common requirements include rejecting email from misconfigured systems that violate the SMTP protocol, filtering on keywords, or rejecting email from systems on blacklists.

BSDP candidates should be able to configure their MTA or SPAM filtering utility of choice to reject a SPAM email.

Practical:

software of choice either included with the BSD system or installed from packages/ pkgsrc

Estimated Time:

45 minutes to configure an MTA to reject a SPAM message according to a specification.

3.6.18 Configure MTA to use a virus scanner.

Importance: 3.8, Frequency: 2.0, Bloom: K,C,A

Concept:

BSD system administrators should be aware of the various options for deploying virus detection and removal systems. Common requirements include identifying and filtering email from systems containing attachments of specific file types ("file.exe", "file.pdf", "file.xyz", etc.), accepting email from systems on a sender whitelist even if an attachment contains a virus, and creating sender blacklists for known virus senders.

BSDP candidates should be able to configure an MTA to accept or reject email containing an attachment with a virus.

Practical:

software of choice either included with the BSD system or installed from packages/pkgsrc

Estimated Time:

45 minutes to configure an MTA to reject an email message containing a virus in an attachment according to a specification.

3.6.19 Install and configure an IMAP server.

Importance: 3.7, Frequency: 1.8, Bloom: K,C,A

Concept:

Internet Message Access Protocol (IMAP) is widely used by organizations as it allows users the flexibility of deciding which emails to download and which to store on the mail server.

BSDP candidates should be able to configure and test their IMAP server of choice.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

30 minutes to install, configure, and test an IMAP server according to a specification.

3.6.20 Install and configure a POP3 server.

Importance: 3.6, Frequency: 1.8, Bloom: K,C,A

Concept:

Post Office Protocol version 3 (POP3) is a commonly used protocol for downloading email from a mail server.

BSDP candidates should be able to configure and test their POP3 server of choice.

Practical:

software of choice from packages/pkgsrc

telnet(1)

OpenBSD: popa3d(8)

Estimated Time:

30 minutes to install, configure, and test a POP3 server according to a specification.

3.6.21 Configure an email client to send encrypted emails.

Importance: 3.2, Frequency: 1.8, Bloom: K,C,A

Concept:

An email client can be configured to automatically send and receive encrypted emails.

BSDP candidates should be able to configure their email client of choice to provide encryption and decryption using PGP, PGPi, GnuPG, or any related encryption solution. Solutions may encompass either symmetric or asymmetric encryption techniques, but should not require manual encryption of individual files.

Practical:

software of choice either included with the BSD system or installed from packages/pkgsrc

Estimated Time:

30 minutes to install, configure, and test an encrypted email solution according to a specification.

3.6.22 Install and configure a webmail server.

Importance: 3.4, Frequency: 1.6, Bloom: K,C,A

Concept:

Webmail provides an easy way to send and receive mail when computer access is limited to a browser-only environment, or when technical requirements disallow the use of standard SMTP protocols for Mail User Agents (MUAs).

BSDP candidates should be able to configure a webmail solution that provides the capability to create, send, receive, and manage email messages.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

45 minutes to install, configure, and test a webmail server according to a specification.

3.6.23 Install and configure a webserver.

Importance: 4.1, Frequency: 2.2, Bloom: K,C,A

Concept:

Web services are a key business requirement for all Internet connected businesses and organizations.

BSDP candidates should be able to configure a webserver that provides the capability to display pages and execute simple scripts.

Practical:

software of choice from packages/pksgrc

NetBSD, *OpenBSD*: httpd(8)

Estimated Time:

30 minutes to install, configure, and test a webserver according to a specification.

3.6.24 Configure webserver for HTTPS / SSL.

Importance: 4.2, Frequency: 2.1, Bloom: K,C,A

Concept:

Enabling secure communications for web traffic provides businesses with the ability to complete secure transactions over the Internet.

BSDP candidates should be able to install, modify, or configure a webserver to utilize Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption for secure communications using an existing certificate.

Practical:

software of choice from packages/pksgrc

openssl(1)

NetBSD, *OpenBSD:* httpd(8)

Estimated Time:

45 minutes to install, configure, and test an HTTPS connection according to a specification.

3.6.25 Enable NFS server and share a local directory for network usage.

Importance: 3.8, Frequency: 2.1, Bloom: K,A

Concept:

Network File System (NFS) provides the capability to access files remotely over a network.

BSDP candidates should be able to configure, test, and operate an NFS server to serve files over a network.

Practical:

mountd(8), nfsd(8), exports(5), mount(8), nfsstat(1)

Estimated Time:

20 minutes to setup, configure, and test an NFS server according to a specification.

3.6.26 Enable and configure NIS service.

Importance: 2.6, Frequency: 1.4, Bloom: K,A

Concept:

Network Information Service (NIS) maintains a centralized directory of user and group information, hostnames, email aliases and configuration files and makes them available to other Unix systems in a network.

BSDP candidates should be able to configure a master NIS server and verify that the data is available to clients within the NIS domain.

Practical:

rc.conf(5), yp(8), ypinit(8), ypserv(8), ypcat(1), ypbind(8)

Estimated Time:

30 minutes to configure a master NIS server and verify its operation according to a specification.

3.6.27 Install and configure an RDBMS.

Importance: 3.6, Frequency: 1.9, Bloom: K,A

Concept:

A Relational Data Base Management System (RDBMS) is used to collect, organize, operate on, and report about collections of information that contain interrelated attributes. Setting up the correct relationships is usually the job of a database administrator. However, system administrators are often required to setup and manage the database server themselves.

BSDP candidates should have a basic understanding of setting up a relational database with one or two tables. Some experience with Structured Query Language (SQL) will be required, though use will be limited to table management, data insertion, and simple data retrieval.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

30 minutes to install, configure, and test an RDBMS according to a specification.

3.6.28 Configure an RDBMS to allow specific logins.

Importance: 3.6, Frequency: 1.9, Bloom: K,A

Concept:

It is often desirable to limit database connections to authorized users.

BSDP candidates should be able to configure a database for non-privileged as well as privileged access. Requirements may include the name and password of the database user and basic security settings such as limiting who can access the database.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

15 minutes to configure a database to allow logins according to a specification.

3.7 General Networking

Many of the Internet networking protocols widely used today were originally developed on BSD systems. The celebrated "Berkeley tapes", originally sent out from the University of California at Berkeley, dramatically advanced the state of the art for computer to computer communications. Even without this historical background, BSD system administrators are often looked upon as some of the most knowledgeable networking professionals in their organizations.

The BSDP candidate must be well versed in all aspects of IP networking, must be able to rapidly configure multiple computer systems to communicate using IP based protocols, and troubleshoot various problems when communication fails.

3.7.1 Configure networking with PPP or PPPoE.

Importance: 2.9, Frequency: 1.5, Bloom: K,C,A

Concept:

Point to Point Protocol (PPP) allows dialup modems to access the Internet over telephone lines. PPP over Ethernet (PPPoE) is used by some DSL modems to access the Internet.

BSDP candidates should be able to configure their BSD system of choice for either outbound or incoming PPP or outbound PPPoE. They should also understand general concepts such as PAP and CHAP authentication and PPPoE service tags.

Practical:

ppp(4) or (8)

FreeBSD: pppctl(8), pppoed(8)

NetBSD: pppd(8), pppoectl(8), ifconfig(8)

OpenBSD: pppd(8), pppoe(4) and (8)

Estimated Time:

20 minutes to configure a BSD system to use PPP or PPPoE according to a specification.

3.7.2 Configure BSD system to be a router.

Importance: 4.1, Frequency: 2.0, Bloom: K,C,A

Concept:

BSD systems containing multiple interfaces are capable of forwarding packets between interfaces. This capability is turned off by default as required by RFC 1122.

BSDP candidates should be able to configure a system to perform packet forwarding and configure routing table routes to individual hosts or networks using the utilities provided with the BSD system.

Practical:

sysctl(8), sysctl.conf(5), route(8), netstat(1)

Estimated Time:

15 minutes to configure the system for packet forwarding and to configure routes according to a specification.

3.7.3 Configure BSD system to act as a traffic shaper.

Importance: 3.7, Frequency: 1.9, Bloom: K,C,A

Concept:

Traffic shaping is the control of computer network traffic by enforcing different scheduling and queue management policies that apply bandwidth and queue size limitations.

BSDP candidates should be able to configure a traffic shaper on their BSD of choice.

Practical:

altq(4) or (9), pf(4), pf.conf(5), pfctl(8)

DragonFly BSD, FreeBSD: dummynet(4), ipfw(8)

Estimated Time:

20 minutes to configure a BSD system as a traffic shaper according to a specification.

3.7.4 Configure BSD system to act as a bridge.

Importance: 3.4, Frequency: 1.7, Bloom: K,C,A

Concept:

BSD systems have the capability to bridge network interfaces together in order to combine multiple segments using the bridge(4) capability.

BSDP candidates should be able to create a bridge interface, add and delete other interfaces to the bridge, and configure the bridge interface for bridge and port control. Familiarity with the Spanning Tree Protocol (STP) is recommended.

Practical:

bridge(4), ifconfig(8)

NetBSD, OpenBSD: brconfig(8)

Estimated Time:

15 minutes to create and configure the bridge device and to add, delete, or configure additional interfaces according to a specification.

3.7.5 Determine which address is abusing the network.

Importance: 4.5, Frequency: 3.1, Bloom: K,C,A

Concept:

Detrimental network activity can take many forms such as packet overloading, SYN flooding, bruteforce login attempts, deliberate packet corruption (fuzzing), Ethernet address duplication, and other abusive activity.

BSDP candidates should be able to identify that detrimental network activity is occurring and identify the IP address or MAC address causing the problem.

Practical:

software of choice from packages/pkgsrc

sysctl(8), dmesg(8), netstat(1), tcpdump(1)

Estimated Time:

10 minutes to identify detrimental network activity and determine the address(es) responsible.

3.7.6 Partition an IP address space for new subnets.

Importance: 4.1, Frequency: 2.3, Bloom: K,C,A

Concept:

Configuring multiple IP subnets within an address space is a key skill for a network or system administrator.

BSDP candidates should be able to create multiple IP address ranges either manually or using their application of choice, according to a specification.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

10 minutes for allocating network subnets within a larger IP address space according to a specification.

3.7.7 Enable network interface IP aliases.

Importance: 4.2, Frequency: 2.5, Bloom: K,A

Concept:

An IP alias is used to associate multiple IP addresses to one network interface. This allows the administrator to configure each IP address to be associated with a different service or purpose.

BSDP candidates should be able to configure two or more IP addresses on a single interface and should be able to identify IP aliases given output from the ifconfig(8) command.

Practical:

ifconfig(8)

Estimated Time:

5 minutes to configure one or more IP aliases on a network interface according to a specification.

3.7.8 Troubleshoot network traffic issues using a sniffer program.

Importance: 4.4, Frequency: 3.2, Bloom: K,C,A

Concept:

Beyond identifying deliberate network abuse, system administrators should be able to identify other network problems such as duplicate IP addresses, DNS resolution issues, routing issues, or MTU packet loss.

BSDP candidates should be able to identify and resolve network traffic issues according to a specification .

Practical:

software of choice from packages/pkgsrc

tcpdump(1), netstat(1), dmesg(8)

Estimated Time:

10 minutes to identify network traffic issues.

3.7.9 View network protocol statistics.

Importance: 4.2, Frequency: 3.2, Bloom: K,C,A

Concept:

Gathering network statistics within a specified time frame can provide important information that can be used in troubleshooting. Commonly gathered statistics include the number of packets inbound and outbound, packet TTL values, TCP vs UDP packet usage, and ICMP packet utilization.

BSDP candidates should be able to use the utilities present on a BSD system to view network protocol statistics.

Practical:

netstat(1), systat(1)

Estimated Time:

10 minutes to gather network statistics according to a specification.

3.7.10 Change network parameters such as TTL and MTU.

Importance: 3.6, Frequency: 1.9, Bloom: K,C,A

Concept:

Certain network parameters, such as the packet Time To Live (TTL) and the Maximum Transmission Unit (MTU), are adjustable on BSD systems. Adjusting network parameters is generally done only when needed, but is essential in certain circumstances.

BSDP candidates should be familiar with the network parameters that are tunable on their BSD system. Candidates should be aware of the implications of tuning network stack parameters and should be able to configure network parameters as needed.

Practical:

sysctl(7) or (8), ifconfig(8)

Estimated Time:

10 minutes to adjust and test network parameters according to a specification.

3.7.11 Configure interface for special options or media types.

Importance: 3.4, Frequency: 1.8, Bloom: K,C,A

Concept:

Physical network interfaces often have special modes or options that can be set for specific operations. Examples include full duplex mode to enable simultaneous use of transmit and receive channels, transmission speed and media types, and other specialized options.

BSDP candidates should know how to configure interfaces for various modes of operation and should also know how to determine the full range of options available.

Practical:

ifconfig(8)

Estimated Time:

10 minutes to find mode and option information and to configure the interface according to a specification.

3.7.12 Join the system to an IPv6 network.

Importance: 3.3, Frequency: 1.8, Bloom: K,C,A

Concept:

IP version 6 (IPv6) is designed as the successor to IP version 4 (IPv4), as explained in RFC 2460. IPv6 uses several addressing modes and an IP addressing format that consists of a 128 bit address with a flexible notation syntax. See RFC 3513 for a complete description and examples.

BSDP candidates should understand the basics of IPv6 addressing and should be able to configure an IPv6 address on a network interface. Candidates should also be able to use IPv6-enabled programs to test network communications on a local network.

Practical:

ip6(4), inet6(4), ifconfig(8), ping6 or (8), telnet(1), ssh(1), rc.conf(8), ndp(8)

Estimated Time:

15 minutes to configure and test an interface to use an IPv6 address according to a specification.

3.7.13 Configure network interface for multiple VLANs.

Importance: 3.7, Frequency: 2.1, Bloom: K,C,A

Concept:

Virtual LANs (VLANs, defined by IEEE 802.1Q) are used to separate packet traffic on an interface into separate streams based on a tagging scheme. BSD systems have the capability to create, interpret, and operate on VLAN tags.

BSDP candidates should be able to create a VLAN interface and use VLAN tags to separate network traffic.

Practical:

vlan(4), ifconfig(8)

Estimated Time:

10 minutes to set up a VLAN interface and configure it for one or more VLANs according to a specification.

3.7.14 Configure the system to restrict ICMP types.

Importance: 3.3, Frequency: 1.8, Bloom: K,C,A

Concept:

ICMP uses several message types and codes to relay messages between networked systems. Many security policies specify the restriction of certain ICMP message types.

BSDP candidates should be familiar with ICMP and which message types are necessary for successful network communication and which can be restricted for security reasons. Candidates should be able to restrict the use of ICMP on their BSD system of choice.

Practical:

http://www.iana.org/assignments/icmp-parameters

sysctl(8), pf(4), pfctl(8), pf.conf(5)

DragonFly BSD,FreeBSD: blackhole(4)

Estimated Time:

15 minutes to configure a BSD system to restrict ICMP messages types and codes according to a specification.

3.7.15 Configure access to data hosted on Microsoft systems.

Importance: 3.2, Frequency: 1.9, Bloom: K,C,A

Concept:

Accessing file and print services using Common Internet File Services (CIFS), and authenticating to

Windows standalone or Active Directory environments, are important capabilities for many enterprises.

BSDP candidates should have a basic understanding of Windows networking capabilities, be able to use compatible protocols to connect to Microsoft systems, authenticate to either standalone servers or servers within a domain environment, and map a Unix directory onto a Windows folder for read-only or read/write access.

Practical:

software of choice from packages/pkgsrc

Estimated Time:

30 minutes to install, test, and configure software on a BSD system to perform read/write file operations on a Microsoft server according to a specification.

3.8 Backup and Restore

The importance of backups and tested restores is recognized when the BSD system administrator successfully recovers from a disaster or business disruption by rapidly restoring from a backup data set.

The BSDP candidate should be able to take a backup and successfully restore files, filesystems, and whole disks, with and without encryption, locally or over a network.

3.8.1 Perform a backup of a data set.

Importance: 4.6, Frequency: 3.4, Bloom: K,A

Concept:

To perform a backup means saving data in case it is needed later. Such a need can arise due to corruption or loss of a single file or an entire disk. Backups can be performed on single files, whole file systems or entire disks including all partitions, the partition table and boot blocks.

BSDP candidates should be able to backup a variety of different data sets.

Practical:

software of choice from packages/pkgsrc

tar(1), cpio(1), pax(1), dump(8), dd(1)

Estimated Time:

20 minutes to backup a data set according to a specification.

3.8.2 Restore a portion of a system from a backup.

Importance: 4.6, Frequency: 2.3, Bloom: K,A

Concept:

Backing up data is only one half of what is needed to provide a reliable service. Restoring data from a backup data set is just as important.

BSDP candidates must know how to retrieve all or a portion of a backup data set.

Practical:

software of choice from packages/pkgsrc

tar(1), cpio(1), pax(1), restore(8), dd(1)

Estimated Time:

20 minutes to retrieve and verify all or a set of files from a backup data set according to a specification.

3.8.3 Maintain synchronized files on two or more systems.

Importance: 4.3, Frequency: 3.2, Bloom: K,C,A

Concept:

Maintaining synchronized data across multiple systems is often necessary for operational reasons.

BSDP candidates should be able to configure synchronization of data files across two or more systems.

Practical:

software of choice from packages/pkgsrc

scp(1), cron(8), crontab(1) and (5)

Estimated Time:

30 minutes to set up multiple systems to synchronize files according to a specification.

3.8.4 Perform an encrypted backup over the network.

Importance: 4.1, Frequency: 2.8, Bloom: K,C,A

Concept:

The ability to perform a remote backup is a common component of many disaster recovery plans. Encrypting the transmission link between the source and destination during the backup ensures confidentiality of the backup data.

BSDP candidates should be able to configure an encrypted backup over a network connection.

Practical:

software of choice from packages/pkgsrc

tar(8), cpio(1), dump(8), dd(1), ssh(8), scp(1)

Estimated Time:

20 minutes to configure and perform an encrypted backup according to a specification.

3.8.5 Perform a distributed backup on multiple systems.

Importance: 3.7, Frequency: 2.5, Bloom: K,C,A

Concept:

Backups can be distributed across multiple systems in order to decrease risk due to loss of both the source and backup system. Multiple backup systems allow for data recovery in the event of such a disaster.

BSDP candidates should be able to perform a backup over a network to multiple systems.

Practical:

software of choice from packages/pkgsrc

tar(8), cpio(1), dump(8), dd(1), ssh(8), scp(1)

Estimated Time:

30 minutes to configure and perform a backup to multiple systems over a network connection.

3.8.6 Backup Windows shares to a BSD system.

Importance: 3.1, Frequency: 2.4, Bloom: K,C,A

Concept:

BSD systems are capable of being configured to mount, read, and write to Windows shares.

BSDP candidates must be able to access files on Windows shares, back them up to remote storage facilities which may not use native Windows filesystems, restore the files to a (possibly different) Windows share, and keep user, system, and file attributes intact.

Practical:

software of choice from packages/pkgsrc

DragonFly BSD, FreeBSD, NetBSD: mount_smbfs(8)

Estimated Time:

35 minutes to configure and perform a backup of a Windows share over a network connection, restore the backup, and verify the results.

3.8.7 Backup and restore an RDBMS.

Importance: 3.7, Frequency: 2.5, Bloom: K,C,A

Concept:

RDBMS vendors provide tools to export and import the database and schema for backup and restore purposes.

BSDP candidates should be able to backup and restore a database using tools provided by the database vendor.

Practical:

software of choice from packages /pkgsrc

Estimated Time:

30 minutes to backup and restore an RDBMS according to a specification.

3.9 Virtualization

Virtualization provides many benefits to an organization as it allows multiple business units to use the same server hardware for diverse purposes. By enabling virtualization technologies, system administrators can improve the overall utilization of existing equipment and provide additional services for lower cost. Virtualization consists of a host system that provides one or more virtualized machine (guest system) environments.

The BSDP candidate should be familiar with the virtualization technologies available for BSD systems and be able to configure host and guest virtualization on their BSD of choice.

3.9.1 Configure a BSD system to host virtualized environments.

Importance: 3.6, Frequency: 1.8, Bloom: K,A

Concept:

Some preparation is required before a BSD system can host virtual environments. Depending upon the system and application used, the system administrator may have to perform one or more of the following tasks: install and configure software, prepare a vkernel(7) environment, install a privileged Xen Dom(0), or setup a jail(8) directory tree.

BSDP candidates should be able to perform the steps required to setup their virtualization software of choice on a BSD system.

Practical:

Virtualization software of choice either installed with BSD or from packages/pkgsrc

Estimated Time:

30 minutes to prepare the system to host virtual environments.

3.9.2 Create a virtual environment and install a BSD system as a guest.

Importance: 3.6, Frequency: 1.9, Bloom: K,A

Concept:

Once the host system is prepared, virtual environments can be created and installed with a guest operating system. Depending upon the virtualization product being used, the system administrator may need to perform one or more of the following tasks: install a world, create a Xen Dom(U), or create and start a jail.

BSDP candidates should be able to create a virtualized environment and install a BSD operating system as a guest virtual machine.

Practical:

tools provided by virtualization software of choice

Estimated Time:

30 minutes to install a BSD guest operating system according to a specification.

3.9.3 Start or shutdown a virtualized guest system.

Importance: 3.8, Frequency: 2.5, Bloom: K,A

Concept:

Once installed, a virtualized guest system can be treated as any other installed operating system. The system administrator needs to know how to properly shutdown or start the guest system.

BSDP candidates should know the procedure for properly starting or shutting down a guest system within their virtualized environment.

Practical:

tools provided by virtualization software of choice

Estimated Time:

5 minutes to properly start or shutdown a guest system.

3.9.4 Clone a virtualized instance.

Importance: 3.5, Frequency: 1.9, Bloom: K,C,A

Concept:

It is often useful to make a clone of a virtualized instance that can be used as a backup or installed as a separate guest with a different name and IP address. How this is accomplished depends upon the virtualization software being used. If the virtualization software does not provide a tool for this purpose, the administrator can consider creating a snapshot of the guest.

BSDP candidates should be able to replicate a guest system and install it as a separate instance.

Practical:

tool provided by virtualization software or installed from packages/pkgsrc

DragonFly BSD: hammer(8)

FreeBSD: zfs(1M), mksnap_ffs(8)

NetBSD: lvcreate(8), lvm(8)

Estimated Time:

30 minutes to clone a guest system according to a specification.

3.10 Logging and Monitoring

System monitoring and event logging are key tasks for a BSD system administrator. The BSDP candidate should understand the available options for logging and monitoring a BSD system and be able to configure various logging subsystems to record system events. The candidate should be well versed in methods used to extract information from log repositories.

3.10.1 Configure a log server.

Importance: 3.9, Frequency: 1.9, Bloom: K,A

Concept:

Collecting and analyzing system messages is an important administrative task. A BSD system can be configured to log events on the local system only or as a centralized logging server that collects logs from remote systems.

BSDP candidates must be able to configure a logging server.

Practical:

software of choice from packages/pkgsrc

syslogd(8), syslog.conf(5), logger(1)

Estimated Time:

15 minutes to configure a log server according to a specification.

3.10.2 Configure automatic rotation of log files.

Importance: 4.2, Frequency: 2.1, Bloom: K,A

Concept:

Organization of logs is an important administrative task. System administrators need to ensure that sufficient space is available for logs and that log files are configured to rotate on key parameters such as time of day and size of logfile.

BSDP candidates must be able to configure rotation of log files.

Practical:

software of choice from packages/pkgsrc

newsyslog(8)

Estimated Time:

15 minutes to configure and test automatic rotation of log files according to a specification.

3.10.3 Search for patterns in logfiles using regular expressions.

Importance: 4.1, Frequency: 3.3, Bloom: K,C,A

Concept:

A system administrator needs to be able to quickly find important system messages.

BSDP candidates must be able to use regular expressions to search for specific patterns in logfiles. Candidates should also be able to automate the task of searching for a list of patterns in text or binary form.

Practical:

scripting language of choice

re_format(7), grep(1), sed(1)

Estimated Time:

10 minutes to set up a solution to search for patterns in a logfile according to a specification.

3.10.4 Monitor system for login abuses.

Importance: 4.3, Frequency: 3.5, Bloom: K,A

Concept:

Systems need to be monitored to ensure that only authorized users are able to login and that automated programs are unable to access resources only available to authorized users.

BSDP candidates should be able to enforce a policy that limits the number of login attempts and sends an alert when the login threshhold is reached.

Practical:

scripting language and/or software of choice from packages/pkgsrc

login.conf(5)

Estimated Time:

15 minutes to set up a solution to monitor the system for login abuses according to a specification.

3.11 High Availability

Businesses and organizations lose money and operational capability if a system crashes without any failover or high availability configuration. High availability ensures that operations continue as another system can take over should a critical system fail.

3.11.1 Configure high availability routing.

Importance: 3.6, Frequency: 1.8, Bloom: C, K, A

Concept:

A router is an important component of a network's infrastructure. Configuring a high availability routing environment ensures that routes continue to be advertised should a router fail.

BSDP candidates should understand the basics of routing and how to configure a BSD system to support high availability routing.

Practical:

software of choice either installed on BSD system or from packages/pkgsrc

carp(4), route(8), routed(8), ifconfig(8)

OpenBSD: bgpd(8), ripd(8), ospfd(8)

Estimated Time:

30 minutes to set up, test, and verify high availability routing according to a specification.

3.11.2 Configure a firewall for high availability.

Importance: 3.9, Frequency: 1.9, Bloom: K,C,A

Concept:

BSD systems acting as firewalls can be configured in a resilient architecture using multiple systems and special network interface configurations, to detect and respond to a failure by the master firewall.

BSDP candidates should be able to configure a high availability firewall architecture. Candidates should be able to configure the interfaces and protocols necessary to maintain packet traffic between multiple connected segments in spite of the loss of a single firewall.

Practical:

pf(4), pfsync(4), pfctl(8), carp(4), ifconfig(8), netstat(8)

Estimated Time:

45 minutes to configure and test a set of firewalls in a high availability architecture according to a specification.

4 Additional Program Information

This certification program is being actively developed by the BSD Certification Group. While the objectives in this document are an important element of the certification, there are other requirements that are yet to be finalized. These include:

- **Domain Percentages** – The BSDCG psychometrician establishes a percentage of total weight for each domain according to an analysis of the previously published BSDP JTA results. These percentages determine the relative number of questions for each domain on the written exam and the number of tasks for each domain on the lab exam. The total combined score on the exam is scaled by these percentages to determine whether a candidate passed the exam. The psychometrician depends on a finalized list of objectives (defined in this document) to determine the domain percentages. Domain percentages will be published as soon as they are available on the BSDCG website.

- **Passing Score, Number of Questions, and Time Limits** – These values cannot be established until after the BSDCG SMEs meet to decide how essential correct completion of each task is for an individual to be considered a BSD Professional. This session, known as an Anghoff session, enables the psychometrician to finalize the scaled passing score, the number of questions, and the time limits for the written and lab exams. All these values will be published as soon as they are available on the BSDCG website.

- **Additional Certification Elements Required by ANSI/ISO/IEC 17024** – As mentioned previously, the BSDCG may submit this certification program for formal accreditation by ANSI. By reciprocal agreement, ANSI accredited personnel certification programs are recognized by ISO/IEC. Requirements for individuals in these programs are established by the 17204 standard and exist primarily to protect the integrity of the program and its value to the individual. Requirements include a certification time limit and periodic communications between the BSDCG and those certified. A complete list of these additional requirements will be published on the BSDCG website as they finalized.

The BSDCG intends to fully disclose all certification requirements, changes to this certification program, and all other important information as soon as it becomes available.

Visit our website (www.bsdcertification.org) to learn more about upcoming SME sessions, exam locations, translation activities, news of upcoming events, and more information on how you can become involved.

5 Summary

Achieving a BSD Professional certification demonstrates that an individual has a solid background in using and managing the systems that have the most mature, tested, and innovative code in the open source community. As BSD systems continue to proliferate, there will continue to be a demand for experienced administrators with knowledge of BSD systems and their capabilities. Mastering the objectives in this document can help senior BSD administrators improve their skills in using BSD systems in complex environments. By studying these objectives, all BSD users and administrators, at any level of experience, can improve their knowledge of BSD systems.

The BSD Professional certification will continue to evolve over time. To keep up to date with the latest developments, visit www.bsdcertification.org.