Topic 207: Domain Name Server

207.1 Basic DNS server configuration

Weight: 3

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

Key Knowledge Areas:

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

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

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

207.2 Create and maintain DNS zones

Weight: 3

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

Key Knowledge Areas:

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

Terms and Utilities:

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

207.3 Securing a DNS server

Weight: 2

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

Key Knowledge Areas:

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

Terms and Utilities:

- /etc/named.conf
- /etc/passwd

- DNSSEC
- dnssec-keygen
- dnssec-signzone

Topic 208: Web Services

208.1 Implementing a web server

Weight: 4

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

Key Knowledge Areas:

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

Terms and Utilities:

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

- apachectl, apache2ctl
- httpd, apache2

208.2 Apache configuration for HTTPS

Weight: 3

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

Key Knowledge Areas:

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

Terms and Utilities:

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

208.3 Implementing a proxy server

Weight: 2

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

Key Knowledge Areas:

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

Terms and Utilities:

- squid.conf
- acl
- http_access

208.4 Implementing Nginx as a web server and a reverse proxy

Weight: 2

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

Key Knowledge Areas:

- Nginx
- Reverse Proxy
- Basic Web Server

Terms and Utilities:

- /etc/nginx/
- nginx

Topic 209: File Sharing

209.1 SAMBA Server Configuration

Weight: 5

Description: Candidates should be able to set up a Samba server for various clients. This objective includes setting up Samba as a standalone server as

well as integrating Samba as a member in an Active Directory. Furthermore, the configuration of simple CIFS and printer shares is covered. Also covered is a configuring a Linux client to use a Samba server. Troubleshooting installations is also tested.

Key Knowledge Areas:

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

Terms and Utilities:

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

209.2 NFS Server Configuration

Weight: 3

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

Key Knowledge Areas:

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

- TCP Wrappers
- Awareness of NFSv4

Terms and Utilities:

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

Topic 210: Network Client Management

210.1 DHCP configuration

Weight: 2

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

Key Knowledge Areas:

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

Terms and Utilities:

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

- radvd.conf

210.2 PAM authentication

Weight: 3

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

Key Knowledge Areas:

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

Terms and Utilities:

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

210.3 LDAP client usage

Weight: 2

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

Key Knowledge Areas:

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

Terms and Utilities:

- ldapsearch
- ldappasswd
- ldapadd
- ldapdelete

210.4 Configuring an OpenLDAP server

Weight: 4

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

Key Knowledge Areas:

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

Terms and Utilities:

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

Topic 211: E-Mail Services

211.1 Using e-mail servers

Weight: 4

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

Key Knowledge Areas:

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

Terms and Utilities:

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

211.2 Managing E-Mail Delivery

Weight: 2

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

Key Knowledge Areas:

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

Terms and Utilities:

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

211.3 Managing Remote E-Mail Delivery

Weight: 2

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

Key Knowledge Areas:

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

Terms and Utilities:

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

Topic 212: System Security

212.1 Configuring a router

Weight: 3

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

Key Knowledge Areas:

- iptables and ip6tables configuration files, tools and utilities
- Tools, commands and utilities to manage routing tables.
- Private address ranges (IPv4) and Unique Local Addresses as well as Link Local Addresses (IPv6)
- Port redirection and IP forwarding

- List and write filtering and rules that accept or block IP packets based on source or destination protocol, port and address
- Save and reload filtering configurations

Terms and Utilities:

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

212.2 Securing FTP servers

Weight: 2

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

Key Knowledge Areas:

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

Terms and Utilities:

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

212.3 Secure shell (SSH)

Weight: 4

Description: Candidates should be able to configure and secure an SSH daemon. This objective includes managing keys and configuring SSH for

users. Candidates should also be able to forward an application protocol over SSH and manage the SSH login.

Key Knowledge Areas:

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

Terms and Utilities:

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

212.4 Security tasks

Weight: 3

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

Key Knowledge Areas:

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

Terms and Utilities:

- telnet
- nmap
- fail2ban
- nc
- iptables

212.5 OpenVPN

Weight: 2

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

Key Knowledge Areas:

- OpenVPN

Terms and Utilities:

- /etc/openvpn/
- openvpn