303-200.pass4sure

Number: 303-200
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

http://www.gratisexam.com/

LPI 303-200

LPIC-3 Exam 303: Security

Version 1.0

Exam A

QUESTION 1
SIMULATION
Which PAM module checks new passwords against dictionary words and enforces complexity? (Specially the module name only **without any path**.)

Correct Answer: pam_cracklib
Section: (none)
Explanation

Explanation/Reference:
http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html

QUESTION 2
SIMULATION
Which command installs and configures a new FreeIPA server, including all sub-components, and creates a new FreeIPA domain? (Specially **ONLY** the command without any path or parameters).

Correct Answer: ipa-server-install
Section: (none)
Explanation

Explanation/Reference:
https://www.freeipa.org/images/2/2b/Installation_and_Deployment_Guide.pdf

QUESTION 3
Which of the following sections are allowed within the Kerberos configuration file krb5.conf? (Choose **THREE** correct answers.)

A. [plugins]
B. [crypto]
C. [domain]
D. [capaths]
E. [realms]

Correct Answer: ADE

Section: (none)
Explanation

Explanation/Reference:
http://linux.die.net/man/5/krb5.conf

QUESTION 4
Which of the following components are part of FreeIPA? (Choose **THREE** correct answers.)

A. DHCP Server
B. Kerberos KDC
C. Intrusion Detection System
D. Public Key Infrastructure
E. Directory Server

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
https://www.freeipa.org/page/Documentation

QUESTION 5
Which of the following commands disables the automatic password expiry for the user usera?

A. chage --maxdays none usera
B. chage --maxdays 99 usera
C. chage --maxdays -1 usera
D. chage --lastday none usera
E. chage --lastday 0 usera

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
http://www.tutorialspoint.com/unix_commands/chage.htm

QUESTION 6
Given a proper network and name resolution setup, which of the following commands establishes a trust between a FreeIPA domain and an Active Directory domain?

A. ipa trust-add --type ad addom --admin Administrator --password
B. ipa-ad –add-trust --account ADDOM\Administrator--query-password
C. net ad ipajoin addom –U Administrator -p
D. trustmanager add –-domain ad: //addom --user Administrator –w
E. ipa ad join addom -U Administrator -w

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
https://www.freeipa.org/page/Active_Directory_trust_setup

QUESTION 7
In which path is the data, which can be altered by the sysctl command, accessible?

A. /dev/sys/
B. /sys/
C. /proc/sys/
D. /sysctl/

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
http://linux.about.com/library/cmd/blcmdl8_sysctl.htm

QUESTION 8
Which of the following statements is true about chroot environments?

A. Symbolic links to data outside the chroot path are followed, making files and directories accessible

B. Hard links to files outside the chroot path are not followed, to increase security
C. The chroot path needs to contain all data required by the programs running in the chroot environment
D. Programs are not able to set a chroot path by using a function call, they have to use the command chroot
E. When using the command chroot, the started command is running in its own namespace and cannot communicate with other processes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
http://www.computerhope.com/unix/chroot.htm
http://www.computerhope.com/jargon/c/chroot.htm

QUESTION 9
Which of the following commands adds a new user usera to FreeIPA?

A. useradd usera --directory ipa --gecos “User A”
B. idap- useradd –H ldaps://ipa-server CN=UserA --attribs
“Firstname: User: Lastname: A”
C. ipa-admin create user --account usera –-fname User --iname A
D. ipa user-add usera --first User --last A
E. ipa-user- add usera --name “User A”

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
https://docs.fedoraproject.org/en-US/Fedora/15/html/FreeIPA_Guide/adding-users.html

QUESTION 10
SIMULATION
Which command included in the Linux Audit system provides searching and filtering of the audit log? (Specify **ONLY** the command without any path or parameters.)

Correct Answer: ausearch
Section: (none)
Explanation

Explanation/Reference:
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Fixing_Problems-Searching_For_and_Viewing_Denials.html

QUESTION 11
Which of the following commands adds users using SSSD's local service?

A. sss_adduser
B. sss_useradd
C. sss_add
D. sss-addlocaluser
E. sss_local_adduser

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System-Level_Authentication_Guide/managing-sssd.html

QUESTION 12
Which of the following DNS record types can the command dnssec-signzone add to a zone? (Choose **THREE** correct answers.)

A. ASIG
B. NSEC
C. NSEC3
D. NSSIG
E. RRSIG

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
http://linux.die.net/man/8/dnssec-signzone

QUESTION 13
What effect does the configuration SSLStrictSNIVHostCheck on have on an Apache HTTPD virtual host?

A. The clients connecting to the virtual host must provide a client certificate that was issued by the same CA that issued the server's certificate.
B. The virtual host is served only to clients that support SNI.
C. All of the names of the virtual host must be within the same DNS zone.
D. The virtual host is used as a fallback default for all clients that do not support SNI.
E. Despite its configuration, the virtual host is served only on the common name and Subject Alternative Names of the server certificates.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
http://serverfault.com/questions/510132/apache-sni-namevhosts-always-route-to-first-virtualhost-entry

QUESTION 14
How does TSIG authenticate name servers in order to perform secured zone transfers?

A. Both servers mutually verify their X509 certificates.
B. Both servers use a secret key that is shared between the servers.
C. Both servers verify appropriate DANE records for the labels of the NS records used to delegate the transferred zone.
D. Both servers use DNSSEC to mutually verify that they are authoritative for the transferred zone.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
http://www.cyberciti.biz/faq/unix-linux-bind-named-configuring-tsig/

QUESTION 15
Which of the following statements are true regarding the certificate of a Root CA? (Choose **TWO** correct answers.)

A. It is a self-signed certificate.
B. It does not include the private key of the CA.
C. It must contain a host name as the common name.
D. It has an infinite lifetime and never expires.

E. It must contain an X509v3 Authority extension.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
https://en.wikipedia.org/wiki/Root_certificate

QUESTION 16
Which of the following parameters to openssl s_client specifies the host name to use for TLS Server Name Indication?

A. -tlsname
B. -servername
C. -sniname
D. -vhost
E. -host

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
https://www.openssl.org/docs/manmaster/apps/s_client.html

QUESTION 17
An X509 certificate contains the following information:

```
X509v3 Basic Constraints: critical
  CA:TRUE, pathlen:0
```

Which of the following statements are true regarding the certificate? (Choose **THREE** correct answers.)

A. This certificate belongs to a certification authority.
B. This certificate may be used to sign certificates of subordinate certification authorities.
C. This certificate may never be used to sign any other certificates.
D. This certificate may be used to sign certificates that are not also a certification authority.
E. This certificate will not be accepted by programs that do not understand the listed extension.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
https://en.wikipedia.org/wiki/X.509

QUESTION 18
A LUKS device was mapped using the command:

cryptsetup luksOpen/dev/sdal crypt-vol

Given that this device has three different keys, which of the following commands deletes only the first key?

A. cryptsetup luksDelKey /dev/sda 1 0
B. cryptsetup luksDelkey /dev/sda 1 1
C. cryptsetup luksDelKey / dev /mapper/crypt- vol 1
D. cryptsetup luksDelKey / dev /mapper/crypt- vol 0

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
https://help.ubuntu.com/community/EncryptedFilesystemHowto3

QUESTION 19
Which of the following lines in an OpenSSL configuration adds an X 509v3 Subject Alternative Name extension for the host names example.org and www.example.org to a certificate?

A. subjectAltName = DNS: www.example.org, DNS:example.org
B. extension= SAN: www.example.org, SAN:example.org
C. subjectAltName: www.example.org, subjectAltName: example.org
D. commonName = subjectAltName= www.example.org,
subjectAltName = example.org
E. subject= CN= www.example.org, CN=example.org

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
https://www.openssl.org/docs/manmaster/apps/x509v3_config.html

QUESTION 20
SIMULATION
Which option in an Apache HTTPD configuration file enables OCSP stapling? (Specify **ONLY** the option name without any values or parameters.)

Correct Answer: httpd-ssl.conf
Section: (none)
Explanation

Explanation/Reference:
https://wiki.apache.org/httpd/OCSPStapling

QUESTION 21
Which of the following statements is true regarding eCryptfs?

A. For every file in an eCryptfs directory there exists a corresponding file that contains the encrypted content.
B. The content of all files in an eCryptfs directory is stored in an archive file similar to a tar file with an additional index to improve performance.
C. After unmounting an eCryptfs directory, the directory hierarchy and the original file names are still visible, although, it is not possible to view the contents of the files.
D. When a user changes his login password, the contents of his eCryptfs home directory has to be re-encrypted using his new login password.
E. eCryptfs cannot be used to encrypt only directories that are the home directory of a regular Linux user.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
https://help.ubuntu.com/lts/serverguide/ecryptfs.html

QUESTION 22
Which of the following keywords are built-in chairs for the iptables nat table? (Choose **THREE** correct answers.)

A. OUTPUT
B. MASQUERADE
C. PROCESSING
D. POSTROUTING
E. PREROUTING

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
http://linux.die.net/man/8/ebtables

QUESTION 23
Which of the following methods can be used to deactivate a rule in Snort? (Choose **TWO** correct answers.)

A. By placing a # in front of the rule and restarting Snort.
B. By placing a pass rule in local.rules and restarting Snort.
C. By deleting the rule and waiting for Snort to reload its rules files automatically.
D. By adding a pass rule to /etc/snort/rules.deactivated and waiting for Snort to reload its rules files automatically.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
What is the purpose of IP sets?

A. They group together IP addresses that are assigned to the same network interfaces.
B. They group together IP addresses and networks that can be referenced by the network routing table.
C. They group together IP addresses that can be referenced by netfilter rules.
D. They group together IP and MAC addresses used by the neighbors on the local network.
E. They group together IP addresses and user names that can be referenced from /etc/hosts.allow and /etc/hosts.deny

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
http://ipset.netfilter.org/

QUESTION 25
Which of the following statements describes the purpose of ndpmon?

A. It monitors the network for neighbor discovery messages from new IPv6 hosts and routers.
B. It monitors remote hosts by periodically sending echo requests to them.
C. It monitors the availability of a network link by querying network interfaces.
D. It monitors the network for IPv4 nodes that have not yet migrated to IPv6.
E. It monitors log files for failed login attempts in order to block traffic from offending network nodes.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
https://en.wikipedia.org/wiki/NDPMon

QUESTION 26
Which of the following terms refer to existing scan techniques with nmap? (Choose **TWO** correct answers.)

A. Xmas Scan
B. Zero Scan
C. FIN Scan
D. IP Scan
E. UDP SYN Scan

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
https://nmap.org/book/man-port-scanning-techniques.html

QUESTION 27
SIMULATION

Which directive is used in an OpenVPN server configuration in order to send network configuration information to the client? (Specify **ONLY** the option name without any values or parameters.)

Correct Answer: push
Section: (none)
Explanation

Explanation/Reference:
https://community.openvpn.net/openvpn/wiki/RoutedLans

QUESTION 28
Which of the following statements are valid wireshark capture filters? (Choose **TWO** correct answers.)

A. port range 10000:tcp-15000:tcp
B. port-range tcp 10000-15000
C. tcp portrange 10000-15000
D. portrange 10000/tcp-15000/tcp
E. portrange 10000-15000 and tcp

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
https://wiki.wireshark.org/CaptureFilters

QUESTION 29
Which option of the openvpn command should be used to ensure that ephemeral keys are not written to the swap space?

A. --mlock
B. --no-swap
C. --root-swap
D. --keys-no-swap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
https://openvpn.net/index.php/open-source/documentation/manuals/65-openvpn-20x-manpage.html