

Lpi.303-300-JPN.v2026-10-10.q77

試験コード : 303-300-JPN
試験名称 : LPIC Exam 303: Security, version 3.0 (303-300日本語版)
認証ベンダー : Lpi
無料問題の数 : 77
バージョン : v2026-10-10
ページの閲覧量 : 103
問題集の閲覧量 : 773

<https://www.jpnsiken.com/shiken/Lpi.303-300-JPN.v2026-10-10.q77.html>

質問: 1

対称キーとは何ですか？

- A. 暗号化と復号化の両方に使用されるランダムに生成されるキー
- B. 暗号化に使用されたキーとは異なる復号化に使用されるキー
- C. 暗号化と復号化に同じ鍵を使用する
- D. 暗号化に使用されるキーと復号化に使用されるキーが異なる

正解: ([正解を表示します](#))

質問: 2

次の DNS レコードのうち、IP アドレスをホスト名にマッピングするために使用されるものはどれですか？

- A. PTR
- B. A
- C. NS
- D. SOA

正解: ([正解を表示します](#))

質問: 3

pam_tally2モジュールまたはpam_faillockモジュールの目的は何ですか？

- A. パスワード有効期限ポリシーを適用する。
- B. ログイン失敗回数を追跡し、指定された回数の失敗後にアカウントをロックします。
- C. ユーザーセッションごとのリソース使用量を制限する。
- D. 多要素認証を要求する。

正解: ([正解を表示します](#))

The pam_faillock module (and its older counterpart, pam_tally2) tracks the number of consecutive failed authentication attempts for a user account and can automatically lock the account after a configured threshold is reached, helping to mitigate brute-force password guessing attacks.

Administrators can configure the number of allowed attempts, the lockout duration, and whether the lockout applies even to the root account. This differs from password expiration, which is handled by fields in /etc/shadow and related PAM modules.

質問: 4

次の式のうち、有効な AIDE ルールはどれですか？

(正しい答えを2つ選択してください。)

- A. /etc p+i+u+g
- B. append: /var/log/*
- C. /usr=all
- D. !/var/run/. *
- E. #/bin/

正解: ([正解を表示します](#))

質問: 5

中間者攻撃とは何ですか？

- A. 二者間の通信を傍受して情報を盗む攻撃
- B. 特定のユーザーまたは組織を標的とした攻撃
- C. 機密情報を盗むことを目的とした攻撃
- D. ネットワークやサーバーに大量のトラフィックを流して利用不能にする攻撃

正解: A ([コメントを发表する](#))

質問: 6

DNSSEC における DNSKEY レコードの目的は何ですか？

- A. DNSクエリの信頼性を検証する
- B. IPアドレスをホスト名にマッピングする
- C. DNSゾーンに署名する
- D. DNSサーバーに関する情報を提供する

正解: ([正解を表示します](#))

質問: 7

BIND に含まれるどのコマンドが DNSSEC キーを生成しますか？

(パスやパラメータなしでコマンドのみを指定します。)

解決策: dnssec-keygen

与えられた解決策が正しいかどうかを判断します。

- A. 正解
- B. 偽

正解: ([正解を表示します](#))

質問: 8

LUKS デバイスは、次のコマンドを使用してマップされました: cryptsetup

luksOpen/dev/sda1 crypt-vol このデバイスには 3 つの異なるキーがありますが、次のコマンドのうち最初のキーのみを削除するのはどれですか?

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

正解: ([正解を表示します](#))

質問: 9

ファイル afile に拡張属性が設定されていないときにコマンド getfattr afile を実行すると何が起こりますか?

- A. 出力は生成されず、getfattr は値 1 で終了します。
- B. 出力は生成されず、getfattr は値 0 で終了します。
- C. getfattr は警告を出力し、値 0 で終了します。
- D. getfattr は警告を出力し、値 1 で終了します。

正解: ([正解を表示します](#))

質問: 10

次のスタンザのうち、FreeRADIUS の有効なクライアント構成はどれですか?

- A. client private-network-1 {
ipaddr = 192.0.2.0/24
password = testing123-1
}
- B. client private-network-1 {
ip = 192.0.2.0/24
passwd = testing123-1
}
- C. client private-network-1 {
ip = 192.0.2.0/24
secret = testing123-1
}
- D. client private-network-1 {
ip = 192.0.2.0/24
password = testing123-1
}
- E. client private-network-1 {
ipaddr = 192.0.2.0/24
secret = testing123-1
}

正解: **E** ([コメントを发表する](#))

質問: **11**

ファイルに設定されている拡張属性を一覧表示するコマンドはどれですか？

- A. lsattr
- B. getfacl
- C. getfattr
- D. stat

正解: ([正解を表示します](#))

The getfattr command is used to display the extended attributes of a file, such as user-defined metadata or security-related attributes stored outside the standard inode fields. lsattr, in contrast, displays file attributes specific to certain filesystems (such as ext2/3/4), like the immutable or append-only flags. getfacl is used to display POSIX Access Control Lists, not extended attributes.

stat displays general file status information, such as size, permissions, and timestamps, but not extended attributes.

質問: **12**

ユーザー、発信元、サービスの組み合わせに基づいてログインアクセスを制限するために使用できるPAMモジュールはどれですか？

- A. pam_access
- B. pam_limits
- C. pam_nologin
- D. pam_selinux

正解: **A** ([コメントを发表する](#))

The pam_access module enforces login restrictions defined in the access.conf configuration file, which specifies rules based on combinations of users or groups, the origin (such as a hostname, IP address, or tty), and often the PAM service being used. This allows administrators to build fine-grained login policies, such as allowing a particular user to log in only from specific hosts.

pam_nologin instead simply prevents all non-root logins when the /etc/nologin file is present.

質問: **13**

以下のiptablesルールは何を実現するのでしょうか？

```
iptables -A INPUT -s !127.0.0.0/8 -p tcp -dport 111 -j DROP
```

- A. LANからポート111宛てのすべてのパケットを破棄します。
- B. ローカルマシンからのパケットでない限り、ポート 111 宛てのすべてのパケットを破棄します。
- C. ローカルマシンから発信され、ポート 111 宛てのすべてのパケットを破棄します。

D. ポート111宛てのパケットを除き、ローカルマシンから発信されたすべてのパケットを破棄します。

正解: ([正解を表示します](#))

質問: 14

シェルとその子プロセスの次のリソースのうち、Bash 組み込みコマンド ulimit によって制御できるものはどれですか。

(正しい答えを3つ選んでください。)

- A. 開いているファイル記述子の最大数
- B. 書き込まれるファイルの最大サイズ
- C. 新規に作成されるファイルの最大数
- D. 環境変数の最大数
- E. ユーザープロセスの最大数

正解: ([正解を表示します](#))

質問: 15

マウントされたファイルシステム上のバイナリの実行を防止するマウントオプションはどれですか？

- A. ノスイド
- B. ro
- C. noexec
- D. nodev

正解: ([正解を表示します](#))

質問: 16

Linux システムでホストスキャンを自動化するにはどうすればよいですか？

- A. cronの使用
- B. OpenSCAP の使用
- C. Linux監査システムの使用
- D. chkrootkit の使用

正解: A ([コメントを發表する](#))

有効的な**303-300-JPN**問題集はJPNTTest.com提供され、**303-300-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**303-300-JPN**試験問題集を提供します。JPNTTest.com 303-300-JPN試験問題集はもう更新されました。ここで**303-300-JPN**問題集のテストエンジンを手に入れます。最新版のアクセ

ス、<https://www.jpntest.com/shiken/303-300-JPN-mondaishu> 163問、30%ディスカウ
ント、特別な割引コード: **JPNshiken**」

質問: 17

ファイルのアクセス制御リストを表示するにはどのコマンドを使用しますか？

- A. 設定ファクル
- B. chmod
- C. 取得facl
- D. ls

正解: C ([コメントを発表する](#))

質問: 18

次の openssl コマンドのうち、ファイル private/keypair.pem に含まれる既存の秘密鍵を使用して証明書署名要求 (CSR) を生成するものはどれですか。

- A. openssl req - new -key private/keypair.pem -out req/csr.pem
- B. openssl gencsr -new- key private/keypair.pem -out req/csr.pem
- C. openssl req -key private/keypair.pem -out req/csr.pem
- D. openssl gencsr -key private/keypair.pem -out req/csr.pem

正解: ([正解を表示します](#))

質問: 19

サーバーが所有権情報を提供しない場合に、マウントされた CIFS 共有のファイルのローカル所有者として表示されるユーザーを指定するのは、mount.cifs のどのオプションですか？

(値やパラメータなしでオプション名のみを指定します。)

解決策: uid=arg

与えられた解決策が正しいかどうかを判断します。

- A. 正解
- B. 偽

正解: A ([コメントを発表する](#))

質問: 20

nftablesにおいて、「ベースチェーン」と「レギュラーチェーン」の違いは何ですか？

- A. ベースチェーンには、acceptルールのみを含めることができます。
- B. ベースチェーンは、入力や転送などのネットフィルタフックに直接接続され、カーネルからパケットを受信できるようにします。
- C. ベースチェーンはNATルールにのみ使用されます。
- D. ベース鎖と通常の鎖の間には機能的な違いはありません。

正解: ([正解を表示します](#))

A base chain in nftables is attached directly to one of the underlying netfilter hooks (such as prerouting, input, forward, output, or postrouting), which allows packets traversing the network stack at that point to be evaluated against the chain's rules. A regular chain, by contrast, is not attached to any hook and can only be reached when explicitly called (jumped or goto'd) from another chain, functioning similarly to a subroutine used for rule organization.

質問: 21

ルート CA の証明書に関して正しいのは次のうちどれですか？

(正しい答えを3つ選んでください。)

- A. 有効期間は無限で、期限が切れることはありません。
- B. X509v3 Authority 拡張を含める必要があります。
- C. CA の秘密鍵は含まれません。
- D. 自己署名証明書です。
- E. 共通名としてホスト名を含める必要があります。

正解: ([正解を表示します](#))

質問: 22

sysctl コマンドで変更できるデータはどのパスからアクセスできますか？

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

正解: ([正解を表示します](#))

質問: 23

rkhunter を構成するために使用されるファイルはどれですか？

- A. /etc/maldet.conf
- B. /etc/rkhunter.conf
- C. /etc/aide/aide.conf
- D. /etc/audit/auditd.conf

正解: B ([コメントを发表する](#))

質問: 24

Linux 拡張ファイル属性は名前空間に編成されています。次の名前のうち、既存の属性名前空間に対応するものはどれですか？(正しい回答を 3 つ選択してください。)

- A. 所有者
- B. 信頼できる
- C. システム
- D. デフォルト

E. ユーザー

正解: ([正解を表示します](#))

質問: 25

現在ロードされているSELinuxポリシーに従ってファイルのラベルを変更するには、どのコマンドを使用しますか？

- A. chcon
- B. restorecon
- C. semanage
- D. setsebool

正解: B ([コメントを发表する](#))

The restorecon command restores the default SELinux security context of one or more files based on the rules defined in the currently loaded policy's file contexts database. This is useful after files have been moved, copied, or had their context manually altered. chcon changes a file's context to an arbitrary value, but does not use policy-defined defaults and does not persist across a full relabel. semanage manages various aspects of SELinux policy, such as port and user mappings, while setsebool toggles SELinux boolean values.

質問: 26

次の DNS レコードのうち、DNS で X.509 証明書と証明機関情報を公開するために使用されるものはどれですか。

- A. DS
- B. A
- C. CAA
- D. NSEC

正解: ([正解を表示します](#))

質問: 27

平文とは何ですか？

- A. メッセージを暗号化するために使用されるキー
- B. メッセージを暗号化するために使用されるアルゴリズム
- C. 暗号化されたメッセージ
- D. 暗号化前の元のメッセージ

正解: D ([コメントを发表する](#))

質問: 28

次のコマンドのうち、ユーザー usera の自動パスワード有効期限を無効にするものはどれですか？

- A. chage --lastday 0 usera
- B. chage --maxdays -1 usera

- C. chage --maxdays 99 usera
- D. chage --lastday none usera
- E. chage --maxdays none usera

正解: **B** ([コメントを发表する](#))

質問: **29**

OpenSSLのどのコマンドを使えば、新しいRSA秘密鍵とそれに対応する証明書署名要求(CSR)を一度に生成できますか？

- A. openssl genpkey -algorithm RSA
- B. openssl req -new -newkey rsa:2048 -keyout key.pem -out req.csr
- C. openssl x509 -req -in key.pem
- D. openssl ca -in req.csr

正解: ([正解を表示します](#))

The command "openssl req -new -newkey rsa:2048 -keyout key.pem -out req.csr" generates a new 2048-bit RSA private key and simultaneously creates a Certificate Signing Request (CSR) containing the requested subject information, saving the private key and the CSR to the specified files. This CSR would then be submitted to a Certificate Authority for signing. "openssl genpkey" only generates a key without a CSR, while "openssl ca" is used by a CA to sign a submitted CSR, not to generate one.

質問: **30**

DoS 攻撃とは何ですか？

- A. 機密情報を盗むことを目的とした攻撃
- B. 特定のユーザーまたは組織を標的とした攻撃
- C. ネットワークやサーバーに大量のトラフィックを流して利用不能にする攻撃
- D. ソフトウェアの脆弱性を悪用する攻撃

正解: ([正解を表示します](#))

質問: **31**

DNS over TLS と DNS over HTTPS の目的は何ですか？

- A. DNSパフォーマンスを向上させるため
- B. DNSサーバーが互いに安全に通信できるようにする
- C. DNSクライアントとサーバー間の安全な通信を提供する
- D. DNSクエリ時間を短縮するため

正解: ([正解を表示します](#))

有効的な**303-300-JPN**問題集はJPNTest.com提供され、**303-300-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**303-300-JPN**試験問題集を提供します。JPNTest.com 303-300-JPN試験問題集はもう更新されました。ここで**303-300-JPN**

問題集のテストエンジンを手に入れます。最新版のアクセ

ス、<https://www.jpntest.com/shiken/303-300-JPN-mondaishu> 163問、30%ディスカウ
ント、特別な割引コード: **JPNshiken**」

質問: 32

次のアクセス制御モデルのうち、SELinux を使用して確立されるものはどれですか？

- A. ユーザー アクセス制御 (UAC)
- B. 強制アクセス制御 (MAC)
- C. セキュリティ アクセス制御 (SAC)
- D. 任意アクセス制御 (DAC)
- E. グループ アクセス制御 (GAC)

正解: B ([コメントを発表する](#))

質問: 33

SELinux コンテキストを変更するユーザーに対して新しいシェルを実行するために使用されるコマンドはどれですか？

(パスやパラメータなしでコマンドのみを指定します。)

解決策: newrole

与えられた解決策が正しいかどうかを判断します。

- A. 正解
- B. 偽

正解: ([正解を表示します](#))

質問: 34

次のコマンドは TCP パケットにどのような影響を与えますか？

iptables- A 入力 d 10.142.232.1 p tcp --dport 20:21 j 承認

- A. 10.142.232.1 からポート 20 または 21 宛てに送信されるすべての TCP トラフィックをドロップします。
- B. ポート20または21以外のすべてのTCPトラフィックをIPアドレス10.142.232.1に転送します。
- C. IP アドレス 10.142.232.1 のポート 20 と 21 のすべての TCP トラフィックを受け入れます。
- D. 10.142.232.1 からのポート 20 または 21 宛の TCP トラフィックのみを受け入れます。

正解: ([正解を表示します](#))

質問: 35

AppArmorプロファイルにおいて、「苛情」モードはどのような機能を持つのでしょうか？

- A. すべての制限された操作をブロックし、プロセスを終了します。
- B. SELinuxのパーミッシブモードと同様に、制限を強制することなくポリシー違反をログに記録します。

- C. その特定のプロファイルのみAppArmorを無効にします。
- D. 観察された行動に基づいて新しいプロファイルを自動的に生成します。

正解: B ([コメントを发表する](#))

When an AppArmor profile is placed into complain mode, actions that would violate the profile's rules are logged but not blocked, allowing an administrator to observe an application's actual behavior before switching the profile to enforce mode. This is conceptually similar to SELinux's permissive mode. The aa-genprof and aa-logprof tools can process these complain-mode logs to help build or refine a profile, but complain mode itself does not automatically generate profiles.

質問: 36

オンライン証明書ステータスプロトコル(OCSP)の主な目的は何ですか？

- A. クライアントとサーバー間で転送されるデータを暗号化します。
- B. クライアントが特定の X.509 証明書の失効状態をリアルタイムで確認できるようにする。
- C. 新しいX.509証明書を自動的に生成します。
- D. 証明書失効リスト全体をすべてのクライアントに配布します。

正解: B ([コメントを发表する](#))

The Online Certificate Status Protocol (OCSP) allows a client to query a certificate authority's OCSP responder to check the real-time revocation status of a specific certificate, rather than downloading and parsing an entire Certificate Revocation List (CRL). OCSP responses are typically much smaller and faster to process than CRLs, especially as the number of revoked certificates grows, though OCSP does introduce a dependency on the availability of the OCSP responder at validation time, which OCSP stapling helps address.

質問: 37

Linuxでファイルの所有者とグループを設定するには、どのコマンドを使用しますか？

- A. chmod
- B. chgrp
- C. setfacl
- D. chown

正解: D ([コメントを发表する](#))

質問: 38

認証局 (CA) の目的は何ですか？

- A. X.509証明書を発行し署名する
- B. X.509証明書を暗号化する
- C. X.509証明書を復号化する
- D. X.509証明書を保存する

正解: ([正解を表示します](#))

質問: 39

nftables コマンドのうち、現在アクティブなルールセット(すべてのテーブル、チェーン、ルールを含む)を表示するコマンドはどれですか？

- A. nft list ruleset
- B. nft show tables
- C. nft dump chains
- D. nft get rules

正解: A ([コメントを发表する](#))

The command "nft list ruleset" displays the complete, currently active nftables configuration, including all defined tables, chains, and the rules within them. This is the nftables equivalent of the older "iptables -L -v" command. nftables organizes rules hierarchically into tables (grouped by address family) and chains (which contain the actual rules), and this command provides a full view of that hierarchy exactly as it is loaded into the kernel.

質問: 40

暗号化されたLUKS形式のブロックデバイスを作成するために使用するコマンドはどれですか？

- A. cryptsetup luksFormat /dev/sdX
- B. mkfs.luks /dev/sdX
- C. cryptsetup open /dev/sdX
- D. dm-crypt --format /dev/sdX

正解: A ([コメントを发表する](#))

The command "cryptsetup luksFormat /dev/sdX" initializes a block device with the LUKS (Linux Unified Key Setup) header and format, prompting for a passphrase that will be used to protect the master encryption key. Once formatted, the device must be unlocked using "cryptsetup open" (or "luksOpen"), which creates a mapped device-mapper device that can then be formatted with a standard filesystem and mounted. There is no standard "mkfs.luks" command, since LUKS operates below the filesystem layer.

質問: 41

getcifsacl の出力に存在する可能性のあるプレフィックスは次のどれですか？

(正しい答えを3つ選んでください。)

- A. グループ
- B. SID
- C. 所有者
- D. ACL
- E. 許可

正解: ([正解を表示します](#))

質問: 42

どのSELinuxモードが、ポリシー違反をログに記録するものの、実際にポリシーを適用することはありませんか？

- A. 強制する
- B. 寛容
- C. 無効
- D. ターゲット

正解: B ([コメントを發表する](#))

In Permissive mode, SELinux evaluates access requests against the loaded policy and logs any actions that would have been denied, but it does not actually block them. This mode is useful for troubleshooting and policy development, allowing an administrator to review the audit log for potential AVC denials before switching to Enforcing mode, in which violations are actively blocked. Disabled mode turns SELinux off entirely, and Targeted is not a mode but rather a type of policy that only confines specific processes.

質問: 43

Linux におけるアクセス制御リストの目的は何ですか？

- A. ディスク容量を節約するためにファイルを圧縮する
- B. ユーザーとグループに対してきめ細かな権限を指定する
- C. ファイルを安全に転送するために暗号化する
- D. ファイルを実行可能としてマークする

正解: ([正解を表示します](#))

質問: 44

バッファオーバーフローとは何ですか？

- A. ウイルスの一種
- B. 正規のソフトウェアを装ったマルウェアの一種
- C. サービス拒否攻撃の一種
- D. ソフトウェアの脆弱性の一種

正解: D ([コメントを發表する](#))

質問: 45

Linux でファイルの権限を設定するために使用されるコマンドはどれですか？

- A. 設定ファクル
- B. グループチェンジ
- C. chmod
- D. チャウン

正解: C ([コメントを發表する](#))

質問: 46

セキュリティ評価の一環として、サービスやOSのフィンガープリンティングを含む包括的なネットワークポートスキャンを実行するために一般的に使用されるツールはどれですか？

- A. tcpdump
- B. nmap
- C. Wireshark
- D. netstat

正解: ([正解を表示します](#))

Nmap (Network Mapper) is a widely used tool for network discovery and security auditing, capable of performing port scans to identify open ports, service version detection (-sV) to identify the software and version listening on those ports, and OS fingerprinting (-O) to estimate the operating system of a target host based on characteristics of its TCP/IP stack responses.

tcpdump and Wireshark are packet capture and analysis tools rather than active scanners, and netstat displays local socket and connection information rather than scanning remote hosts.

有効的な**303-300-JPN**問題集はJPNTTest.com提供され、**303-300-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**303-300-JPN**試験問題集を提供します。JPNTTest.com 303-300-JPN試験問題集はもう更新されました。ここで**303-300-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/303-300-JPN-mondaishu> **163問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 47

openssl s_client の次のパラメータのうち、TLS サーバー名表示に使用するホスト名を指定するものはどれですか？

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

正解: ([正解を表示します](#))

質問: 48

コンテナランタイムやサンドボックスツールが攻撃対象領域を縮小するためによく使用する、プロセスによるシステムコールへのアクセスを制限するLinuxカーネル機能はどれですか？

- A. cgroups
- B. seccomp
- C. 名前空間
- D. 能力

正解: ([正解を表示します](#))

Secure Computing Mode (seccomp) is a Linux kernel feature that allows a process to restrict the set of system calls it is permitted to make, typically by loading a filter (often defined using BPF) that allows, denies, or traps specific syscalls. This significantly reduces a process's attack surface by preventing it from invoking syscalls it does not need, and is widely used by container runtimes like Docker and by sandboxing frameworks. cgroups control resource usage, namespaces provide isolated views of system resources, and capabilities divide root privileges into discrete units.

質問: 49

OCSP ステータスとは何ですか？

- A. サーバーが自身のIDの証明をクライアントに提供できるようにするメカニズム
- B. 特定の認証局によって発行されたすべての証明書の失効ステータスの証明をサーバーが提供できるようにするメカニズム
- C. サーバーがクライアントの身元の証明を他のサーバーに提供できるようにするメカニズム
- D. サーバーが自身のSSL/TLS証明書の失効ステータスの証明を提供できるメカニズム

正解: ([正解を表示します](#))

質問: 50

証明書失効リスト(CRL)の目的は何ですか？

- A. まだ発行されていない証明書の一覧です。
- B. 有効期限前に発行認証局によって失効された証明書の一覧です。
- C. クライアントが現在信頼している有効な証明書をすべて一覧表示します。
- D. 証明書の有効期限を気にする必要がなくなります。

正解: B ([コメントを發表する](#))

A Certificate Revocation List (CRL) is a signed list published by a Certificate Authority that identifies certificates which have been revoked before their scheduled expiration date, for reasons such as key compromise or the certificate no longer being needed. Clients can download and check a CRL to determine whether a certificate they are relying on is still valid, though this approach has largely been supplemented or replaced in many contexts by the more efficient real-time OCSP protocol.

質問: 51

SetUID ビットと SetGID ビットの違いは何ですか？

- A. SetUIDとSetGIDの間に違いはありません
- B. SetUID を使用すると、ユーザーはファイルの所有者を変更できます。一方、SetGID を使用すると、ユーザーはファイルのグループ所有者を変更できます。
- C. SetUID はファイル所有者の権限でファイルを実行できるようにしますが、SetGID はグループ所有者の権限でファイルを実行できるようにします。
- D. SetUIDはファイルに適用され、SetGIDはディレクトリに適用されます。

正解: ([正解を表示します](#))

質問: 52

通常、IPsec VPNの接続定義(ローカルおよびリモートのエンドポイント、認証方法など)を定義するstrongSwanの設定ファイルはどれですか？

- A. /etc/ipsec.conf
- B. /etc/ipsec.secrets
- C. /etc/strongswan.conf
- D. /etc/ipsec.d/certs

正解: ([正解を表示します](#))

The /etc/ipsec.conf file contains the connection definitions for strongSwan, including parameters such as the local and remote endpoints, authentication method, and the traffic selectors defining what should be protected by each connection. The /etc/ipsec.secrets file stores the actual authentication credentials, such as pre-shared keys or references to private key files, while /etc/strongswan.conf configures the general behavior of the strongSwan daemon itself, such as plugin loading and logging.

質問: 53

特定のバイナリファイルに現在割り当てられている機能を表示するコマンドはどれですか？

- A. getcap /path/to/binary
- B. setcap /path/to/binary
- C. capsh --print
- D. chmod +cap /path/to/binary

正解: A ([コメントを发表する](#))

The getcap command displays any file capabilities that have been assigned to a specific binary using setcap. This allows an administrator to audit which executables on a system have been granted elevated capabilities beyond the standard permission model. setcap, by contrast, is used to assign capabilities to a file, while capsh --print displays the capabilities of the current running shell process rather than those statically attached to a specific binary file.

質問: 54

トラストアンカーとは何ですか？

- A. 特定のCAによって信頼されている公開鍵のリスト
- B. 特定のCAによって生成された鍵ペア
- C. 特定のCAによって信頼されている秘密鍵のリスト
- D. 特定のCAによって信頼されているルート証明書

正解: ([正解を表示します](#))

質問: 55

すべてのサブコンポーネントを含む新しい FreeIPA サーバーをインストールおよび構成し、新しい FreeIPA ドメインを作成するコマンドはどれですか？

(特に、パスやパラメータのないコマンドのみ)。

解決策: ipa-server-install

与えられた解決策が正しいかどうかを判断します。

- A. 偽
- B. 正解

正解: ([正解を表示します](#))

質問: 56

次のどれが動作ベースの HID 技術の例ですか？

- A. ルールベースの検出
- B. ヒューリスティックベースの検出
- C. シグネチャベースの検出
- D. 異常ベースの検出

正解: D ([コメントを发表する](#))

質問: 57

DANE における TLSA レコードの目的は何ですか？

- A. TLSサーバーに関する情報を提供する
- B. ドメイン名をIPアドレスにマッピングする
- C. TLSサーバーの公開鍵に署名する
- D. DNSサーバーを認証する

正解: C ([コメントを发表する](#))

質問: 58

クライアントに代わって DNSSEC 検証を実行するために使用されるのは次のどれですか？

- A. プライマリネームサーバー
- B. 権威ネームサーバー

- C. 再帰ネームサーバー
- D. セカンダリネームサーバー

正解: [\(正解を表示します\)](#)

質問: 59

chroot 環境について正しい記述は次のどれですか？

- A. プログラムは関数呼び出しを使用してchrootパスを設定することはできません。コマンドchrootを使用する必要があります。
- B. chrootパス外のデータへのシンボリックリンクがたどられ、ファイルやディレクトリにアクセスできるようになります。
- C. chrootコマンドを使用する場合、開始されたコマンドは独自の名前空間で実行され、他のプロセスと通信できません。
- D. セキュリティを強化するため、chroot パス外のファイルへのハードリンクは追跡されません。
- E. chrootパスには、chroot環境で実行されるプログラムに必要なすべてのデータが含まれている必要があります。

正解: E ([コメントを发表する](#))

質問: 60

権限昇格とは何ですか？

- A. 脆弱性を悪用して権限を昇格させる攻撃
- B. 機密情報を盗むことを目的とした攻撃
- C. 特定のユーザーまたは組織を標的とした攻撃
- D. ネットワークやサーバーに大量のトラフィックを流して利用不能にする攻撃

正解: A ([コメントを发表する](#))

質問: 61

暗号化とは何ですか？

- A. 公的なメッセージを送信する技術
- B. 秘密のメッセージを送る技術
- C. メッセージを解読する技術
- D. 匿名メッセージを送信する技術

正解: B ([コメントを发表する](#))

有効的な**303-300-JPN**問題集はJPNTest.com提供され、**303-300-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**303-300-JPN**試験問題集を提供します。JPNTest.com 303-300-JPN試験問題集はもう更新されました。ここで**303-300-JPN**問題集のテストエンジンを手に入れます。最新版のアクセ

質問: 62

snort-stat プログラムの目的は何ですか？

- A. 設定されているすべてのネットワーク デバイスのステータスを返します。
- B. すべての Snort プロセスのステータスを表示します。
- C. 実行中の Snort プロセスの統計情報を表示します。
- D. Snort プロセスがまだ実行されており、パケットを処理しているかどうかを報告します。
- E. Snort 情報を含む syslog ファイルを読み取り、ポート スキャンの統計を生成します。

正解: ([正解を表示します](#))

質問: 63

次のどれが HID ツールの例ですか？

- A. 侵入防止システム (IPS)
- B. セキュリティ情報およびイベント管理 (SIEM) システム
- C. ウイルス対策ソフトウェア
- D. ファイアウォール

正解: ([正解を表示します](#))

質問: 64

トロイの木馬とは何ですか？

- A. ウイルスの一種
- B. サービス拒否攻撃の一種
- C. 正規のソフトウェアを装ったマルウェアの一種
- D. フィッシング詐欺の一種

正解: C ([コメントを发表する](#))

質問: 65

Linux 監査システムに含まれるどのコマンドが監査ログの検索とフィルタリングを提供しますか？

(パスやパラメータなしでコマンドのみを指定します。)

解決策: ausearch

与えられた解決策が正しいかどうかを判断します。

- A. 正解
- B. 偽

正解: ([正解を表示します](#))

質問: 66

DNSSEC における NSEC3 の目的は何ですか？

- A. DNSSEC鍵署名鍵に関する情報を提供する
- B. DNSサーバーを認証する
- C. DNSゾーンに署名する
- D. ゾーン列挙を防ぐため

正解: ([正解を表示します](#))

質問: 67

IP セットの目的は何ですか？

- A. 同じネットワーク インターフェイスに割り当てられた IP アドレスをグループ化します。
- B. /etc/hosts.allowから参照できるIPアドレスとユーザー名をグループ化し、拒否
- C. ネットワーク ルーティング テーブルで参照できる IP アドレスとネットワークをグループ化します。
- D. ローカル ネットワーク上のネイバーが使用する IP アドレスと MAC アドレスをグループ化します。
- E. netfilter ルールで参照できる IP アドレスをグループ化します。

正解: ([正解を表示します](#))

質問: 68

Linux 監査システム内で指定できるのは次のどのタイプですか？

(正しい答えを3つ選んでください。)

- A. システムコールルール
- B. コンソールルール
- C. ファイルシステムのルール
- D. ネットワーク接続ルール
- E. 制御ルール

正解: ([正解を表示します](#))

質問: 69

Fail2banの主な目的は何ですか？

- A. ディスクに保存されているログファイルを暗号化します。
- B. ログファイルを監視し、認証失敗の繰り返しを検出し、ファイアウォールルールを使用して問題のあるIPアドレスを動的にブロックします。
- C. ユーザーアカウント用の強力なランダムパスワードを生成します。
- D. ファイアウォールの必要性を完全に排除する。

正解: ([正解を表示します](#))

Fail2ban is a log-monitoring intrusion prevention tool that scans log files, such as those generated by SSH or web server authentication, for patterns indicating repeated failed login attempts. When a configured threshold of failures from a specific IP address is

reached within a defined time window, Fail2ban dynamically inserts a firewall rule (via iptables, nftables, or another supported backend) to temporarily block that IP address, helping to mitigate brute-force attacks without requiring permanent manual firewall configuration.

質問: 70

マウントされたファイルシステム上のバイナリの実行を防止するマウントオプションはどれですか？

- A. nosuid
- B. noexec
- C. nodev
- D. ro

正解: B ([コメントを发表する](#))

The noexec mount option prevents any binary or script located on that filesystem from being executed directly. This is commonly applied to filesystems such as /tmp or removable media to reduce the risk of malicious code execution. nosuid disables the effect of the setuid and setgid bits on that filesystem, nodev prevents device files from being interpreted as such, and ro mounts the filesystem as read-only, none of which specifically block execution of binaries.

質問: 71

AIDE を構成するために使用されるファイルはどれですか？

- A. /etc/maldet.conf
- B. /etc/audit/auditd.conf
- C. /etc/rkhunter.conf
- D. /etc/aide/aide.conf

正解: ([正解を表示します](#))

質問: 72

監視対象となるシステムコールやファイルを制御する監査ルールを定義するために使用されるauditd設定ファイルはどれですか？

- A. /etc/audit/auditd.conf
- B. /etc/audit/rules.d/audit.rules
- C. /etc/audit/auditd.conf
- D. /var/log/audit/audit.log

正解: ([正解を表示します](#))

Audit rules, which define which system calls, files, or directories should be monitored and under what conditions, are typically defined in files under /etc/audit/rules.d/ and compiled into

/etc/audit/audit.rules (or managed directly using the auditctl command for runtime changes). The

/etc/audit/auditd.conf file, by contrast, configures the behavior of the auditd daemon itself, such as log rotation and storage settings, while /var/log/audit/audit.log is where the resulting audit events are actually recorded.

質問: 73

Kerberos 構成ファイル krb5.conf 内で許可されるセクションは次のどれですか？

(正しい答えを3つ選んでください。)

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

正解: B,C,D ([コメントを发表する](#))

質問: 74

Linux監査フレームワークにおいて、`ausearch` コマンドの目的は何ですか？

- A. 実行中のカーネルに新しい監査ルールを追加します。
- B. キー、ユーザー、期間などの基準に基づいて、既存の監査ログエントリを検索およびフィルタリングします。
- C. 監査統計の要約レポートを作成する。
- D. auditdサービスを再起動します。

正解: ([正解を表示します](#))

The `ausearch` command is used to search through the audit log for specific events matching given criteria, such as a rule key (`-k`), a specific user (`-ua`), a time range (`-ts/-te`), or a system call.

This is particularly useful for investigating specific security events flagged by keyed audit rules.

`aureport`, in contrast, generates summarized, aggregate reports from audit data (such as counts of logins or file accesses), while `auditctl` is used to manage the rules themselves rather than search existing logs.

質問: 75

`rkhunter`の目的は何ですか？

- A. インストールされたパッケージを管理する
- B. ホストスキャンを自動化する
- C. システムログファイルを管理する
- D. ルートキットやその他のセキュリティ脅威を検出する

正解: D ([コメントを发表する](#))

質問: 76

非対称キーとは何ですか？

- A. 暗号化と復号化に同じ鍵を使用する
- B. 暗号化に使用されるキーと復号化に使用されるキーが異なる
- C. 暗号化に使用されたキーとは異なる復号化に使用されるキー
- D. 暗号化と復号化の両方に使用されるキーで、ペアで生成される

正解: ([正解を表示します](#))

有効的な**303-300-JPN**問題集はJPNTTest.com提供され、**303-300-JPN**試験に合格すること
に役に立ちます！JPNTTest.comは今最新**303-300-JPN**試験問題集を提供しま
す。JPNTTest.com 303-300-JPN試験問題集はもう更新されました。ここで**303-300-JPN**
問題集のテストエンジンを手に入れます。最新版のアクセ
ス、<https://www.jpntest.com/shiken/303-300-JPN-mondaishu> **163問、30%ディスカウ
ント**、特別な割引コード: **JPNshiken**」

質問: 77

eCryptfs に関して正しいのは次のうちどれですか？

- A. eCryptfs は、通常の Linux ユーザーのホーム ディレクトリであるディレクトリのみを暗号化するために使用することはできません。
- B. ユーザーがログイン パスワードを変更すると、eCryptfs ホーム ディレクトリの内容を新しいログイン パスワードを使用して再暗号化する必要があります。
- C. eCryptfs ディレクトリ内のすべてのファイルの内容は、パフォーマンスを向上させるために追加のインデックスが付いた tar ファイルに似たアーカイブ ファイルに保存されます。
- D. eCryptfs ディレクトリをアンマウントした後も、ディレクトリ階層と元のファイル名は表示されますが、ファイルの内容を表示することはできません。
- E. eCryptfs ディレクトリ内のすべてのファイルには、暗号化されたコンテンツを含む対応するファイルが存在します。

正解: ([正解を表示します](#))

有効的な**303-300-JPN**問題集はJPNTTest.com提供され、**303-300-JPN**試験に合格すること
に役に立ちます！JPNTTest.comは今最新**303-300-JPN**試験問題集を提供しま
す。JPNTTest.com 303-300-JPN試験問題集はもう更新されました。ここで**303-300-JPN**
問題集のテストエンジンを手に入れます。最新版のアクセ
ス、<https://www.jpntest.com/shiken/303-300-JPN-mondaishu> **163問、30%ディスカウ
ント**、特別な割引コード: **JPNshiken**」