SINAV HAZIRLIK REHBERI

Red Hat Certified System Administrator (RHCSA)

Ağ Güvenliği, Firewalld, SELinux ve SSH Konfigürasyon Soru Bankası & Analizi

📌 Doküman Hakkında

Bu doküman, Kurumsal Linux Yönetimi, Firewalld Bölge Mimarisi, SELinux Güvenlik Etiketleri, Kullanıcı İzinleri (umask) ve SSH Güvenliği başlıkları altında çözülen teknik deneme sınavı sorularını, detaylı açıklamalarını ve LinkedIn paylaşımı için hazırlanmış özel bir makale taslağını içerir.

1. Soru Bankası ve Detaylı Çözümler

Soru 1 (Soru 28): Which firewalld zone has the highest trust level, accepting all network connections?

A) public

B) home

C) trusted ✓ (Doğru Cevap)

D) internal

Çözüm / Açıklama:

`firewalld` mimarisinde **trusted** bölgesi en yüksek güven seviyesine sahiptir. Bu bölgeye atanan tüm ağ paketleri ve bağlantılar hiçbir kısıtlama veya engelleme olmadan kabul edilir.

Soru 2 (Soru 29): What does the command 'umask -S' display?

A) The umask in octal format.

B) The umask in a human-readable symbolic format. ✓ (Doğru Cevap)

C) The system's default umask value.

D) A summary of what the current umask will do.

Çözüm / Açıklama:

`umask` varsayılan olarak sekizlik (octal) formatta (örneğin `0022`) çıktı verir. `-S` parametresi eklendiğinde ise sembolik biçimde (örneğin `u=rwx,g=rx,o=rx`) insan tarafından okunabilir izin kısıtlamalarını gösterir.

Soru 3 (Soru 30): Which firewalld zone is designed for networks where you mostly trust other computers, such as a work or home environment?

A) public

B) dmz

C) work ✓ (Doğru Cevap)

D) drop

Çözüm / Açıklama:

work bölgesi, iş ortamı gibi ağdaki diğer cihazlara büyük oranda güvenilen yerler için tasarlanmıştır. Yalnızca kural olarak izin verilen servislerin geçişine izin verir.

Soru 4 (Soru 31): Which command provides a convenient way to save the entire current runtime firewall configuration to the permanent store?

A) firewall-cmd --permanent --reload

B) firewall-cmd --save

C) firewall-cmd --commit

D) firewall-cmd --runtime-to-permanent ✓ (Doğru Cevap)

Çözüm / Açıklama:

O anki aktif çalışma zamanında (runtime) yapılan geçici güvenlik duvarı kurallarını diske kalıcı olarak kaydetmek için `firewall-cmd --runtime-to-permanent` komutu kullanılır.

Soru 5 (Soru 32): What is the function of the `firewall-cmd --reload` command?

A) It restarts the firewalld service, dropping all existing connections.

B) It loads the permanent configuration into the live runtime environment without disrupting existing connections. ✓ (Doğru Cevap)

C) It saves the current runtime rules to the permanent configuration files.

D) It reloads the kernel's nftables module.

Çözüm / Açıklama:

`--reload` seçeneği, diski okuyarak kalıcı konfigürasyonu canlı çalışma ortamına aktarır. Bu sırada mevcut açık TCP/UDP bağlantıları koparılmaz ve kesinti yaşanmaz.

Soru 6 (Soru 33): Which `firewall-cmd` command would open TCP port 8080 in the `public` zone for the current session?

A) firewall-cmd --permanent --zone=public --add-port=8080/tcp

B) firewall-cmd --zone=public --add-port=8080/tcp ✓ (Doğru Cevap)

C) firewall-cmd --add-port=8080/tcp

D) firewall-cmd --permanent --add-port=8080/tcp

Çözüm / Açıklama:

Mevcut oturum (runtime) için `--permanent` kullanılmamalıdır. Ayrıca bölge açıkça `--zone=public` olarak belirtilerek `--add-port=8080/tcp` eklenmelidir.

Soru 7 (Soru 34): What is the default behavior of the `public` zone in firewalld?

A) All incoming connections are accepted.

B) All incoming connections are rejected with a message.

C) Only selected incoming connections are accepted. ✓ (Doğru Cevap)

D) All incoming packets are dropped with no reply.

Çözüm / Açıklama:

Varsayılan olan **public** bölgesinde gelen tüm istekler engellenir; sadece açıkça izin verilen servis veya portlara gelen bağlantılar kabul edilir.

Soru 8 (Soru 35): A `umask` of 002 is often used in collaborative environments for what reason?

A) It creates files with 664 permissions, allowing group members to modify each other's files. ✓ (Doğru Cevap)

B) It creates files with 644 permissions, making them read-only for the group.

C) It creates files with 775 permissions, making them executable by the group.

D) It prevents anyone other than the owner from accessing the files.

Çözüm / Açıklama:

Varsayılan dosya izni 666 - 002 = 664 (rw-rw-r--) olur. Bu sayede aynı gruptaki kullanıcılar dosyaları düzenleyebilir, böylece ortak çalışma kolaylaşır.

Soru 9 (Soru 36): What is a key benefit of using `ssh-copy-id` over manually installing a public key?

A) It uses a stronger encryption algorithm for the transfer.

B) It automatically sets the correct, restrictive file and directory permissions. ✓ (Doğru Cevap)

C) It does not require the user's password for the initial connection.

D) It allows multiple public keys to be copied at once.

Çözüm / Açıklama:

`ssh-copy-id` uzak sunucuda `~/.ssh` dizinini ve `authorized_keys` dosyasını oluştururken doğru izinleri (dizin için 700, dosya için 600) otomatik ayarlar.

Soru 10 (Soru 37): What is the purpose of the `PermitRootLogin no` directive in `sshd_config`?

A) To prevent all users from logging in.

B) To allow root to log in only with a key.

C) To prevent direct login as the root user, enhancing security. ✓ (Doğru Cevap)

D) To require the root user to use a password.

Çözüm / Açıklama:

Root kullanıcısının SSH ile doğrudan sisteme bağlanmasını engeller. Kullanıcıların standart hesapla bağlanıp `sudo` kullanmasını zorunlu kılarak izlenebilirliği artırır.

Soru 11 (Soru 38): In SSH key authentication, where is the public key placed?

A) In the ~/.ssh/private_keys file on the client.

B) In the /etc/ssh/sshd_config file on the server.

C) In the ~/.ssh/authorized_keys file of the user account on the remote server. ✓ (Doğru Cevap)

D) In the ~/.ssh/known_hosts file on the client.

Çözüm / Açıklama:

Public key, hedef uzak sunucudaki (remote server) kullanıcının `~/.ssh/authorized_keys` dosyası içine eklenmelidir.

Soru 12 (Soru 39): Which command is used to view the SELinux context of running processes?

A) ls -Z

B) ps -eZ ✓ (Doğru Cevap)

C) sestatus -p

D) getsebool -a

Çözüm / Açıklama:

Sistemde çalışan süreçlerin (processes) SELinux etiketlerini ve alanlarını (domain) görmek için `ps -eZ` veya `ps auxZ` kullanılır.

Soru 13 (Soru 40): Which command provides a simple, one-word output of the current SELinux mode, suitable for scripting?

A) sestatus

B) selinux-mode

C) getenforce ✓ (Doğru Cevap)

D) setenforce

Çözüm / Açıklama:

`getenforce` komutu sadece `Enforcing`, `Permissive` veya `Disabled` şeklinde tek kelimelik sade bir çıktı verir; betikler için idealdir.

Soru 14 (Soru 41): What is the most likely cause of an SELinux denial?

A) A bug in the SELinux policy.

B) A file or process having an incorrect context. ✓ (Doğru Cevap)

C) The system running out of memory.

D) A misconfigured firewall rule.

Çözüm / Açıklama:

SELinux reddetmelerinin (denial) en yaygın sebebi bir dosyanın veya sürecin yanlış etikete (context) sahip olmasıdır. `restorecon` ile düzeltilebilir.

Soru 15 (Soru 42): Which firewalld zone rejects incoming connections with an `icmp-host-prohibited` message?

A) drop

B) reject

C) block ✓ (Doğru Cevap)

D) public

Çözüm / Açıklama:

block bölgesi gelen tüm istekleri reddeder ve istemciye aktif olarak `icmp-host-prohibited` yanıtı döndürür. (drop bölgesi ise sessizce yok eder).

Soru 16 (Soru 43): In firewalld's order of precedence, which type of zone is checked first for a matching rule?

A) The zone associated with the incoming network interface.

B) The default zone.

C) A zone whose source IP address matches the packet. ✓ (Doğru Cevap)

D) The 'trusted' zone.

Çözüm / Açıklama:

`firewalld` öncelik sırasına göre ilk olarak paketin kaynak IP adresi ile eşleşen bir bölge (source zone) olup olmadığına bakar. Ardından arayüz (interface) bölgesine bakar.

Soru 17 (Soru 44): What is the correct two-step process for allowing a service to use a non-standard directory with SELinux?

A) 1. Use `chcon` to label the directory. 2. Use `setsebool` to allow the service.

B) 1. Use `semanage fcontext` to define a new rule. 2. Use `restorecon` to apply the label. ✓ (Doğru Cevap)

C) 1. Set SELinux to permissive. 2. Set SELinux back to enforcing.

D) 1. Use `restorecon` on the directory. 2. Use `semanage fcontext` to save the change.

Çözüm / Açıklama:

Standart dışı bir dizini SELinux ile kullanmak için önce `semanage fcontext` ile veritabanına kural eklenir, ardından `restorecon` ile etiket fiziksel olarak dizine uygulanır.

Soru 18 (Soru 45): Which command would you use to find the names of all predefined services that firewalld knows about?

A) firewall-cmd --list-all-services

B) firewall-cmd --get-services ✓ (Doğru Cevap)

C) firewall-cmd --info-service=*

D) firewall-cmd --list-services

Çözüm / Açıklama:

Sistemde önceden tanımlanmış tüm servis isimlerini listelemek için `firewall-cmd --get-services` kullanılır. (`--list-services` ise sadece o an bölgede aktif olanları listeler).

Soru 19 (Soru 46): After changing the SELINUX mode in `/etc/selinux/config`, what is required for the change to take effect?

A) Running `setenforce 1`.

B) Running `systemctl reload selinux`.

C) A reboot. ✓ (Doğru Cevap)

D) Logging out and logging back in.

Çözüm / Açıklama:

`/etc/selinux/config` dosyasındaki değişiklikler çekirdek (kernel) parametrelerini etkilediği için sistemin yeniden başlatılması (**reboot**) şarttır.

Soru 20 (Soru 47): What is the purpose of the 'httpd_enable_homedirs' SELinux boolean?

A) To allow the Apache web server to access user home directories. ✓ (Doğru Cevap)

B) To enable home directories for the 'httpd' user.

C) To force all web content to be stored in user home directories.

D) To disable SELinux protection for all home directories.

Çözüm / Açıklama:

`httpd_enable_homedirs` boolean anahtarı, Apache web sunucusunun kullanıcıların ev dizinlerindeki (`~/public_html`) web sayfalarına erişmesine izin verir.

Soru 21 (Soru 48): How is a firewalld 'service' defined?

A) As a systemd unit file.

B) As a human-readable identifier corresponding to specific ports and protocols in an XML file. ✓ (Doğru Cevap)

C) As a special type of rich rule.

D) As a kernel module that inspects traffic.

Çözüm / Açıklama:

`firewalld` servis tanımı, belirli port ve protokolleri XML formatında bir araya getiren ve insan tarafından okunabilir takma adlar sunan yapılandırma dosyalarıdır.

Soru 22 (Soru 49): Which `ssh-keygen` option is used to add a comment, typically your email address, to the key?

A) -C ✓ (Doğru Cevap)

B) -m

C) -i

D) (Diğer)

Çözüm / Açıklama:

`ssh-keygen` ile anahtar çifti oluşturulurken anahtarın sonuna açıklama metni veya e-posta eklemek için büyük `-C` parametresi kullanılır.

💼 LinkedIn Makale Taslağı

🚀 Red Hat Enterprise Linux (RHEL) Sistem Yönetiminde Kritik Güvenlik İpuçları ve RHCSA Notları

Sistem yöneticileri ve DevOps mühendisleri için Linux sunucu güvenliğini sağlarken en sık karşılaştığımız iki temel yapı taşı: Firewalld ve SELinux!

RHCSA (Red Hat Certified System Administrator) sınavına hazırlık sürecimde öne çıkan bazı kritik pratik bilgileri sizler için derledim:

🔥 Firewalld & Bölge Mimarisi:
1. Öncelik Sırası: Firewalld bir paketi işlerken ilk olarak Kaynak IP (Source IP) eşleşmesine bakar, ardından Ağ Arayüzü (Interface) bölgesini değerlendirir.
2. Geçici -> Kalıcı Kurallar: `firewall-cmd --runtime-to-permanent` komutu ile bellek üzerinde test ettiğiniz canlı kuralları tek hamlede konfigürasyon dosyalarına kaydedebilirsiniz.
3. Kesintisiz Yeniden Yükleme: `firewall-cmd --reload` komutu açık olan TCP bağlantılarını koparmadan kalıcı ayarları canlı sisteme uygular.

🛡️ SELinux ile Doğru Etiketleme:
1. En Yaygın Erişim Hatası: Sisteminizde bir 'SELinux Denial' (AVC) alıyorsanız sorun %90 ihtimalle hatalı dosya/süreç etiketidir (incorrect context).
2. Standart Dışı Dizin Ekleme: Web sunucunuza varsayılan dışı bir dizin tanımlıyorsanız 2 adımlı standart kuralı uygulayın:
👉 `semanage fcontext -a -t ...` (Kuralı veritabanına ekle)
👉 `restorecon -Rv ...` (Etiketi fiziksel olarak uygula)
3. Süreç Analizi: Çalışan servislerin SELinux alanlarını görmek için `ps -eZ` kullanabilirsiniz.

🔑 SSH Sertifika Güvenliği:
• Manuel anahtar kopyalamak yerine `ssh-copy-id` kullanın! Bu araç uzak sunucudaki `.ssh` ve `authorized_keys` izinlerini (700 ve 600) otomatik olarak en güvenli şekilde ayarlar.
• Root erişimlerini sınırlandırmak için `/etc/ssh/sshd_config` içinde `PermitRootLogin no` direktifini unutmayın.

Sistemlerinizin güvenli ve kesintisiz çalışması dileğiyle! 🐧💡

#Linux #RedHat #RHCSA #RHEL #SystemAdministration #Firewalld #SELinux #CyberSecurity #DevOps