****

**Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı**

**LINUX SIKILAŞTIRMA(HARDENING) KONTROL LİSTESİ V.1.0**

**HAZIRLAYAN**

Cihan Mehmet DOĞAN

(Sızma Testi Uzmanı)

**18.12.2019**

**İçindekiler**

[ÖZET 2](#_Toc27560588)

[Linux Sıkılaştırma (Hardening) Kontrol Listesi 4](#_Toc27560589)

#

# ÖZET

Bu dokümanda Siber Olaylara Müdahale Ekibi tarafından hazırlanmış olan Linux işletim sistemine güvenli kontrol listesi yer almaktadır.

Linux işletim sistemi kurulumlarında ve kurulumdan sonra sistemin/sunucunun daha güvenlik olması için kontrol listesi yer almaktadır. Bu önlemler sisteminize gerçekleştirilebilecek dış ve iç saldırılara karşı korunmasında gereken en önemli bileşenlerden biri durumundadır.

## Linux Sıkılaştırma (Hardening) Kontrol Listesi

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Linux Sıkılaştırma (Hardening) Kontrol Listesi** | **Yapıldı** | **Yapılmadı** |
| **1** | Mümkün olan en güncel sürüm işletim sistemi ve kernel versiyonu kullanılmalıdır. |  |  |
| **2** | Güncellemeler belirli aralıklarla kontrol edilmelidir. |  |  |
| **3** | Güncellemelerin indirileceği listeler(/etc/apt/sourcelist) işletim sistemine ait otoritelerden yapılmalıdır. 3. parti siteler eklenmemelidir. |  |  |
| **4** | Minimal bir temel kurulum kullanmayı tercih edilmelidir. |  |  |
| **5** | /home /tmp /var /root /opt /usr /boot için ayrılmış dosya sistemleri oluşturulmalıdır. |  |  |
| **6** | Özellikle kritik veri bulunduran sunucularda/bilgisayarlarda mümkünse disk şifrelemesi kullanılmalıdır. |  |  |
| **7** | BIOS üzerinde parola korumalarını aktif edilmelidir. |  |  |
| **8** | Boot dizinini müdahalelere karşı kitlenmelidir. |  |  |
| **9** | GRUB bootloader üzerinde şifreleme uygulanmalıdır. |  |  |
| **10** | Sunucu üzerinde USB kullanımını devre dışı bırakılmalıdır |  |  |
| **11** | Genele açık dizinler için sticky bit kullanılmalıdır. |  |  |
| **12** | Suncuuda/Bilgisayarda dump alınabilmesinin önüne geçilmelidir. |  |  |
| **13** | Şifrelenmemiş kimlik doğrulama kullanan uygulamalardan devre dışı bırakılmalıdır. (FTP, telnet vb.) |  |  |
| **14** | Kullanılmayacak servisleri devre dışı bırakın (DNS, LDAP, DHCP, NFS vb) |  |  |
| **15** | Loglar için rsyslog kullanımına özen gösterin, bir kopyasını uzak sunucuda saklanmalıdır. |  |  |
| **16** | NTP kullanımına özen gösterilmelidir. |  |  |
| **17** | Cron ve servislerine kısıtlama getirin, kullanılmıyorsa kapatılmalıdır. |  |  |
| **18** | Servisler için root kullanıcısını kullanmayı bırakın mümkünse her bir servise ayrı ayrı kullanıcı oluşturulmalıdır. |  |  |
| **19** | Güçlü parola kullanımına özen gösterilmelidir. |  |  |
| **20** | root kullanıcı izinlerini kısıtlamak için sudo işlevselliğini kullanın(eğer sistemi birden fazla operatör kontrol ediyor ise) |  |  |
| **21** | Network bağlantılarını optimize edilmelidir. Gereksiz erişimler kısıtlanmalıdır. |  |  |
| **22** | IP yönlendirmelerini kalıcı olarak kernel üzerinden kapatılmalıdır. |  |  |
| **23** | SSH servislerinde mutlaka güncel sürümü ve güncel protokolleri kullanılmalıdır. |  |  |
| **24** | SSH servislerinde parolalı girişleri kapatın, mümkünse ssh key aracılığı ile girişe zorlanmalıdır. |  |  |
| **25** | SSH üzerinde asla root kullanıcısı kullanımına izin vermeyin. Yetkilendirilmiş normal kullanıcılar kullanılmalıdır. |  |  |
| **26** | Ağda IPS kullanımına özen gösterilmelidir. |  |  |
| **27** | Web sunucusu üzerinde root kullanıcısını kullanılmamalıdır. |  |  |
| **28** | Web sunucusunda mümkünse TLS kullanımına özen gösterilmelidir. |  |  |
| **29** | Web sunucuda HTTP Trace metodunu kalıcı olarak kapatılmalıdır. |  |  |
| **30** | Web sunucusunda kullanılmayan eklentileri kaldırılmalıdır. |  |  |
| **31** | Web sunucusu üzerinde halka açık dizinlerde 777 izinleri verilmemelidir. |  |  |
| **32** | Web sunucusunu bilgi sızdırmayacak şekilde yapılandırılmalıdır.(sürüm bilgilerinin gizlenmesi vb.) |  |  |
| **33** | SSH’dan giriş yapacak kullanıcılar için banner tanımlaması yapılarak üzerinde işlem yapılan sunucu hakkında kısaca bilgi verilmelidir. |  |  |
| **34** | Sunucu üzerinde açık olan portları kontrol edilmelidir. Kullanılmayan servisler kapatılmalıdır. |  |  |
| **35** | Iptables gibi güvenlik duvarı uygulamaları kullanmaya özen gösterilmelidir. |  |  |
| **36** | Sunucu üzerinde belirli aralıklarla malware taraması gerçekleştirilmelidir. (ClamAV, rootkit vb) |  |  |
| **37** | Sistemde kullanılmayan kullanıcı hesaplarını kalıcı olarak kaldırılmalıdır. |  |  |
| **38** | sysrq tuş kombinasyonunun kullanılmasına izin verilmemelidir. |  |  |
| **39** | Kullanılmayan yazılımlar kaldırılmalıdır. |  |  |
| **40** | Otomatik güncelleştirmeleri aktif edilmelidir. |  |  |
| **41** | Kernel güncelleştirmelerini mutlaka belirli aralıklarla yapılmalıdır. |  |  |
| **42** | Kullanıcıların sistemde kalıcı olarak oturum açmalarına izin vermeyin, timeout süreleri belirlenmelidir. |  |  |
| **43** | Güvensiz dosya paylaşımları yerine SFTP kullanımına özen gösterilmelidir. |  |  |
| **44** | Uygulamaların sıkılaştırma işlemleri için App Armor vb uygulamaları sisteminize dahil edilmelidir. |  |  |
| **45** | Sisteme zararlı yazılım bulaşma ihtimaline karşı mümkünse uygulamaları sandbox(izole ortam) olarak çalıştırılmalıdır. |  |  |
| **46** | Sunucunun kullanılan veri merkezi hakkında bilgileri paylaşılmamalıdır (mümkünse ip bilgilerini temizletin) |  |  |
| **47** | Sistemde kullanılan tüm komutları kayıt altına alınmalıdır. |  |  |
| **48** | Kullanılmıyorsa IPv6 kapatın (sadece IPv4 üzerinden iletişim sağlanacaksa) |  |  |
| **49** | Kullanılmıyorsa IPv4 kapatın (sadece IPv6 üzerinden iletişim sağlanacaksa) |  |  |
| **50** | Kullanıcı dizinlerini 3 ve 6 aylık aralıklar ile gözden geçirin, mümkünse virüs taraması yapılmalıdır. |  |  |
| **51** | Kullanılmayan desktop ekipmanlarını sunuculardan kalıcı olarak kaldırılmalıdır. |  |  |
| **52** | Uzaktan erişim için kullanılan uygulamaların servislerini kalıcı olarak kapatılmalıdır. (VNC, Teamviewer,Anydesk vb.) |  |  |
| **53** | Düzenli olarak yedeklerinizi alındığından emin olunmalıdır. |  |  |
| **54** | Yedeklerinizde bulunan kişisel verileri korumak için GPG şifrelemesi kullanımına özen gösterilmelidir. |  |  |
| **55** | Fiziksel sunucu güvenliğinizi mutlaka tamamlanmalıdır. (Kabin ve sistem odası güvenliği) |  |  |