

Açık Akademi Yayınevi “Ağ Güvenlik İpuçları”

<http://www.acikakademi.com/catalog/nethacks/>

İçindekiler

1. Bölüm: Unix İstemci Güvenliği

1. Bağlantı Noktalarınızın Güvenliğini Sağlayın
2. Suid ve Sgid Programları İçin Tarama Yapın
3. Herkes Tarafından ve Grup Tarafından Yazılabilir Dizinleri Arayın
4. POSIX ACL’ler ile Esnek İzin Hiyerarşileri Oluşturun
5. Günlük Dosyalarınızı Koruyun
6. Yönetici Yetkilerini Aktarın
7. Şifrelenmiş İmza Doğrulanmasını Otomatik Hale Getirin
8. Çalışan Servisleri Denetleyin
9. Servislerin Bir Ara yüze Bağlanarak Çalışmasını Engelleyin
10. Sandbox ile Servisleri Sınırlayın
11. Proftp’yi bir MySQL Kimlik Denetimi Merkezi ile Birlikte Kullanın
12. Stack-Smashing Saldırıları Engelleyin
13. Çekirdeğinizi grsecurity ile Kilitleyin
14. Yazılımları grsecurity ile Sınırlayın
15. Sistem Çağrılarını sysrtrace ile Sınırlayın
16. Otomatik sysrtrace Kural Oluşturulması
17. PAM ile Sisteme Girişleri Kontrol Edin
18. Sınırlandırılmış Kabul Ortamları
19. Kullanıcı ve Grup Kaynak Limitlerini Belirleyin
20. Sistem Güncellemelerini Otomatikleştirin

2. Bölüm: Windows İstemci Güvenliği

21. Sunucularda Yüklü Yamaların Kontrol Edilmesi
22. Açık Dosyaların ve Bunları Çalıştıran İşlemlerin Listelerinin Alınması
23. Çalışan Servis ve Açık Port’ların Listelenmesi
24. Denetlemenin Açılması
25. Günlük Dosyalarınızı Güvenlik Altına Alın
26. Maksimum Günlük Dosyası Büyüklüğünüzü Değiştirin
27. Ön tanımlı Paylaşımları Kapatın
28. Temp Dosyanızı Şifreleyin
29. Sayfalama Dosyanızı Sistem Kapanışında Temizleyin
30. Kullanıcıların Kullanımına Açık Programları Sınırlayın

3. Bölüm: Ağ Güvenliği

31. ARP Aldatmasını Tespit Edin
32. Statik ARP Tablosu Oluşturulması
33. Netfilter ile Güvenlik Duvarı
34. OpenBSD’nin PacketFilter’ı ile Güvenlik Duvarı
35. Kimlik Doğrulaması Özellikli bir Ağ Geçidi Yaratın
36. Windows ile Güvenlik Duvarı

37. Ağ Bilgilerinizi Ağ İçinde Tutun
38. Güvenlik Duvarınızı Test Edin
39. Netfilter ile MAC Filtreleme
40. İşletim Sistemi Parmak İzi (Fingerprinting) Saldırılarını Önleyin
41. Uzak İşletim Sistemi Saptama Yazılımlarını Yanıltın
42. Ağınızın Dökümünü Tutun
43. Ağınızdaki Açıkları Tarayın
44. Sunucu Saatlerinizi Eş Zamanlı Tutun
45. Kendi Sertifika Yetkilinizi Oluşturun
46. CA'nızı İstemcilerinize Dağıtın
47. IMAP ve POP Servislerini SSL İle Şifreleyin
48. TLS-Destekli SMTP Kurun
49. Ethernet Ağındaki Ağ Dinleyicilerini Uzaktan Tespit Edin.
50. Apache'yi SSL ve suEXEC ile Kurun
51. BIND Programı Güvenliği
52. MySQL Güvenliği
53. Unix Üzerinde Dosyalarınızı Güvenli Şekilde Paylaşın

4. Bölüm: Kayıt Tutma

54. Merkezi bir Syslog Sunucunun Çalıştırılması
55. Syslog İncelikleri
56. Windows Makineler ve Syslog
57. Kayıt Dosyalarının Otomatik Olarak Özetlerinin Alınması
58. Kayıtlarınızın Otomatik Olarak İncelenmesi
59. Uzak Ağlardan Gelen Kayıtların Birleştirilmesi
60. Süreç Hesaplaması ile Kullanıcı İşlemlerini Kayıt Altına Alma

5. Bölüm: Denetleme ve Sınıflandırma

61. Erişilebilirlik Denetlemesi
62. Sınıflandırma Grafikleri
63. Gerçek Zamanlı Ağ İstatistikleri için ntop
64. Ağ Trafik Denetimi
65. Güvenlik Duvarı Kayıtları ile İstatistikî Bilgileri Edinin
66. Başka Bir Ağın Trafiklerinin İncelenmesi

6. Bölüm: Güvenli Tünel Uygulamaları

67. Linux Altında IPsec Tünel Kurulumu
68. FreeBSD Altında IPSec Tünel Kurulumu
69. OpenBSD Altında IPSec Tünel Kurulumu
70. PPTP Tünel Uygulaması
71. Değişik FreeS/WAN Şifreleme Yöntemleri
72. SSH ile Tünel Kurulumu
73. SSH İstemci Anahtarları ile Sisteme Hızlı Giriş
74. SSH Üzerinden Squid Proxy
75. SSH Kullanılarak SOCKS Vekil Sunucusu
76. SSL ile Trafik Tünelleme ve Şifreleme
77. HTTP Üzerinden Tünelleme
78. Vtun ve SSH ile Tünel Uygulamaları
79. Otomatik vtun.conf Üretilmesi

- 80. Her Platformda Çalışacak VPN Çözümleri
- 81. PPP Tünelleri

7. Bölüm: Ağ Sızma Tespiti

- 82. Sızma İsteklerini Snort ile Tespit Edin
- 83. Uyarıların Takip Edilmesi
- 84. Gerçek Zamanlı İzleme
- 85. Algılayıcı Ağların Yönetimi
- 86. Kendi Snort Kurallarınızı Yazın
- 87. Snort inline ile Sızma İsteklerini Önleyin
- 88. SnortSam ile Otomatik Dinamik Güvenlik Duvarları
- 89. Normal Olmayan Davranışların Tespiti
- 90. Snort Kurallarını Otomatik Güncelleyin
- 91. Dağıtık ve Gizli Algılayıcı Ağlarının Oluşturulması
- 92. Yüksek Performanslı Ortamlarda Snort'un Barnyard ile Kullanımı
- 93. Web Uygulamaları Sızma İsteklerini Snort ile Takip Edin
- 94. Savunmasız Makinelerin Olduğu Bir Ağ Tasarlayın
- 95. Bal Çanağı Hareketlerini Kaydedin

8. Bölüm: Kurtarma ve Müdahale

- 96. Dosya Sistemlerinin İmajının Alınması
- 97. Dosya Bütünlüğünü Kontrol Edin ve Değiştirilen Dosyaları Bulun
- 98. RPM ile Değiştirilen Dosyaları Bulun
- 99. Sisteminizdeki rootkit'leri Bulun
- 100. Bir Ağın Sahibini Bulun.

İndeks