WEB SUNUCU GÜVENLİĞİ:

Web Siteleri Neden Hacklenir?

Gereksiz yedek dosyaları
Default ayarlarla gelen konfigürasyon dosyaları
Yetkisi tam olarak verilmiş dosyalar ya da dosya izni kontrolü yapılmadan sunucuda barındırılan dosyalar

Örn:777 dosya izni
Default Kullanıcı ve Default şifreleri değiştirilmeyen kullanıcı hesapları

Örnek:Açık bırakılmış guest hesabı şifresi de guest'dir.

Yetkili bir ssl sağlayacısından alınmamış self-sign sertifikalar!
Yeni çıkan açıklıklara karşı güncellenmeyen ya da güncellemeye kapalı web sunucuları

Web Sunucu Güvenliğindeki Atak Vektörleri:

Kullanıcı hesaplarının ele geçirilmesi.
Web Sitelerinin İçeriklerinin Değiştirilmesi(Web Site Defacement)
Data Tampering
Data Theft:Veri Hırsızlığı
Root Access:Web sitesi tahrif edildikten sonra web sunucu kök dizinine erişme aynı ağda yer alıyorsa diğer sunuculara erişme ve zarar verme.

Yanlış Konfigüre Edilmiş Web Sunucusu:

- **Web sunucusundaki debug ve hata mesajlarının açık bırakılması**
- **Sunucuda yer alan web uygulama script dosyaları ve konfigürasyon dosyaları**
- **Anonymous yani herkesin erişebileceği hesapların açık bırakılması,default kullanıcı ve şifrelerinin açık unutulması**
- **Kullanılmadığı halde açık bırakılan servisler**
- **Sunucunun uzaktan yönetilmesine imkan veren ayarların açık bırakılması, aktif hale getirilmesi**

Web Sunucu Konfigürasyon hatası örnekleri:

Şekil 1:httpd.conf dosyasında yapılan ayarda sunucu durumu ve ayrıntıları görüntülenebilir.

Php.ini dosyasındaki söz konusu konfigürasyon doğru bir ayarlama biçimi değildir. display_error off yapılırsa php ile ilgili oluşan hatalar ekrana basılmaz.

Directory Traversal Saldırıları:

Directory traversal atağı saldırganın hassas dizinlere kadar girebilmesini sağlayan, web kök dizini dışından da komut çalıştırmasına imkan veren HTTP zaafiyetidir.

Web Sunucu Saldırı Metodolojisi:

Bilgi Toplama:
Örnek:netcraft.com üzerinden bilgi toplama.
Telnet ile banner grabbing yaparak bilgi toplama.
Website Mirroring:
Web sitesinin klasörlerini listelemek,dosya yapısını çıkarmak,harici linklerini listelemek için websitesinin offline bir kopyası oluşturulur.

Örnek:Teleport Pro, HTTrack

Web Sunucu açıklık taramaları:

Örnek:Nessus aracı ile tarama
Nikto aracı ile tarama

Oturum Çalma:

BurpSuite,Hamster,WebScarab,ParosProxy gibi araçlar kullanılarak oturum bilgileri elde edilebilir.

Şekil 2:Wfetch programı

Web sitesine gönderilen ham istek ve dönen cevabı görmek için Wfetch gibi araçlardan faydalanılır.

Protokol Bazlı Önlemler:

Gereksiz bütün portlar filtrelenmelidir.ICMP portu, netbios vb. kullanım gerekliliği olmayan protokoller kapatılmalıdır.

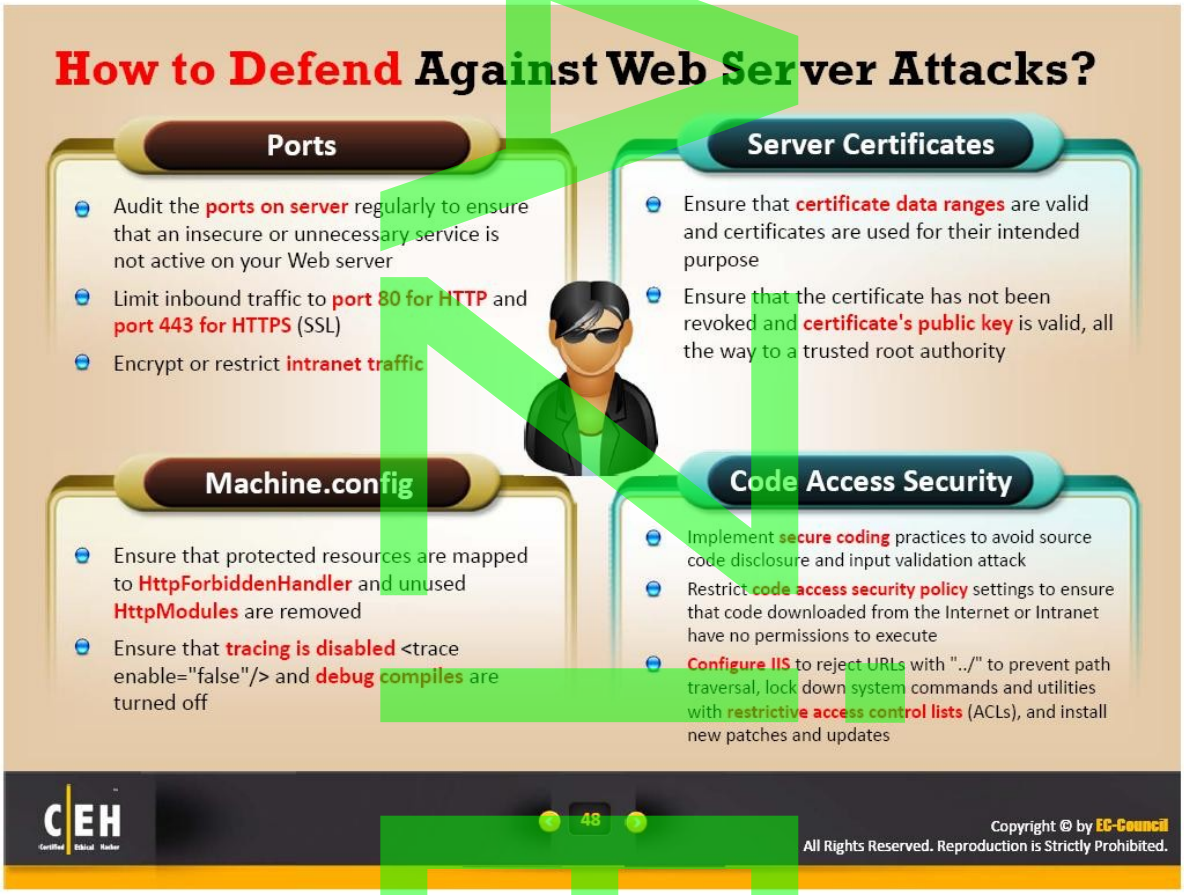
Uzaktan erişim yapılması şart ise vpn vb. Şifreli tünelleme yoluyla eirişim gerçekleştirilmelidir.

POP3,telnet,ftp,smtp protokolleri vb. Şifresiz protokoller kullanılıyorsa IPSec vb. Yetkilendirme ve şifreleme servisleri aktif hale getirilmelidir.

Dosya ve Klasör Bazlı Önlemler:

Arşiv dosyaları,yedek dosyaları,web script dosyaları vb. hassas bilgi içeren dosyaları internete açık klasörlerde unutmamak önemlidir!

Web sitesine yapılan giriş kayıtları, sql sunucu kayıtları gözlemlenmeli ve anomalilere karşı önlem alınmalıdır.



Patch Yönetim Aracı:MBSA(Microsoft Baseline Security Analyzer) programı ile güvenlik taraması gerçekleştirilmeli ve zayıflıklar tespit edilerek kapatılabilmektedir.

Zaafiyet Tespit Programları:Wikto windows için kullanılabilen web sunucu açıklık tarama programı.
Nikto linux için kullanabilecek zaafiyet tarama programı.

Web sunucu yama takibi ve yönetimi için diğer programlar