SİSTEMİNİZİ SHELL'LERDEN KORUMANİN YONTEMLERİ

Bir onceki konumda size “Bir Siteye Shell Atmanin 20 Temel Yontemi”nden bahsetmistim. Bu konuyu daha iyi anlamaniz icin once onu okumanizi tavsiye ederim. Simdi de size bir siteye shell atilmasini engellemenin yontemlerini ogretecegim. Anlatacagim adimlar birbirinden bagimsizdir. Bu sekilde istediklerinizi kendi sisteminizde uygulayabilirsiniz. Adimlarda kod olarak detaya inmedim. Zira her sistemin kodlamasi kendine ozgundur. Buradaki mantigi alip kendi sisteminize gore uyarlamalisiniz.

1. Yontem

Bircok sitede gerekli olmadigi halde upload formlarina rastlanir. Ornegin iletisim sayfalarina koyulan upload formlari ya da sitedeki kullanicilarin imza ve avatar gibi sisteme dosya yukleme yaptiklari ozellikler genellikle gereksizdir. Bunlarin yerine uzaktan resim linki girilerek ya da iletisim kutusuna farkli alanlar eklenerek bu upload formlari kaldirilabilir. Bu soylediklerime daha bircok ornek eklenebilir. Webmaster olarak yapmaniz gereken sey siteye koyacaginiz bir upload formunun yerine baska neler yapilabilecegini dusunmektir.

2. Yontem

Sitenizde bir upload formu kullanmaya karar verdiniz ve baska careniz yoksa ilk yapmaniz gereken sey upload edilen dosyanin uzantisi ne olursa olsun belli bir kritere gore otomatik degismesini saglamaktir. Ornegin, sitenize resim yukleme modulu koydunuz ve kullanicilar bu modul ile istedikleri resimleri yukleyebiliyorlar. Buraya ekleyeceginiz bir kod ile yuklenen resimlerin uzantilari derhal otomatik olarak .jpg’ye cevirilsin. Bu sekilde zararli uzantilar ile shell atilmasinin onune gecebilirsiniz.

3. Yontem

Upload dizinini normalin disinda bir isimle adlandirmak cok onemlidir. Saldirganlar sisteme shell atsalar bile bu shellin nerede oldugunu bulmak icin “Upload, dosya, files, dosyalar” gibi bilindik dizinleri arastirirlar. Siz bu dizinlerin adlarini anlamsiz harflerle degistirirseniz saldirganlar shell atsa bile bunu bulmalari oldukca zor olacaktir.

4. Yontem

Gunumuzde pek cok sitede SQL Injection zafiyeti bulunmaktadir. Ne yazik ki bu zafiyeti ile sadece veritabani bilgileri cekilmiyor. Eger veritabani kullanicisinin yazma izinleri var ise saldirgan yakaladigi bir SQL Injection zafiyeti ile sisteme shell sokabilir. Bunun onune gecmek icin mevcut veritabani kullanicilarinin izinleri mumkun oldugunca kisitlanmalidir.

5. Yontem

FTP girisi bir sistemin ana kapisidir. Bu kapiyi korumasiz birakmak ya da ufak bir kilit ile korumaya calismak sistemi buyuk tehlikeye sokar. Ilk is olarak varsa anonymous FTP girislerini kapatin. Bu sekilde disaridan bir kullanicinin sisteme mudehalesini engellersiniz. FTP sifrelerini asla anlamli kelimelerden secmeyin. ^iB.$9B^Lt_)b gibi bir sifrenin BruteForce yontemi ile kirilmasi imkansiza yakindir. Ayrica FTP portunu degistirmek ve FTP'ye erisebilen IP Adreslerini sinirlamak da guvenligi onemli olcude artiracaktir.

6. Yontem

Web siteniz tamamen guvenli olsa dahi icerisinde bulundugunuz sunucunun guvenligi zayif ise yaptiginiz hersey bosa gidebilir. Bunun onune gecmek icin alacaginiz sunucu hizmetini cok iyi dusunup secmelisiniz. Sunucudaki Antivirus korumalari basta olmak uzere sunucuya ait diger guvenlik onlemleri hakkinda arastirma yapmalisiniz. Sisteminizin buyuklugune gore mumkun oldugunca az kisi ile ayni sunucuyu paylasmaya ozen gosterin. Zira diger sitelerdeki bir zafiyet ile sunucuya girilip sizin sisteminiz zarar gorebilir.

7. Yontem

Upload dizinlerinde mutlaka bir .htaccess dosyasi ile uzanti kontrolu yapin. Ornegin sadece resimlerin bulunmasi gereken bir upload dizinine php dosyasi atilmamasi icin .htaccess dosyasi ile o dizine yuklenecek butun dosyalara .jpg gibi davranilmasini saglayin. Boylece farkli uzantilar sisteme yuklense bile o dizinde calismayacaktir.

8. Yontem

Bircok saldirgan sisteme saldirirken exec(), passthru(), shell_exec(), system() gibi komutlar kullanir. Bu tarz sisteme mudahale edebilecek komutlari php.ini dosyasi ile kisitlamaniz gerekir. Eger serverda yetki sahibi iseniz /etc/php.ini dosyasina asagidaki kodu ekleyin:

disable_functions=exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source

Daha sonra da /etc/init.d/httpd restart diyerek sistemi yeniden baslatin. Boylece serverinizda bu gibi komutlar calismayacak ve shell atilsa bile servera zarar verilemeyecektir.

9. Yontem

2. yontemde bahsettigim gibi sisteme yuklenecek dosya adlarinin da belli bir kritere gore degistirilmesi onemlidir. Upload dizinlerine atilacak olan dosyalarin adlarini otomatik olarak 3132hj1g21.jpg gibi rasgele bir alfanumerik isimle degistirilmesini saglayin.

10. Yontem

Windows sunuculardа guclu antivirus cozumleri bulundugundan dolayi bu islem daha kolay yapilmasina karsin Linux sistemlerde sunucuya shell yuklendigi zaman bunu fark etmek bazen cok zor olabiliyor. Linux sunuculardaki zararlilari tespit etmek icin cok guzel bir arac gelistirilmis. Bu araci sunucunuza kurup zararli yazilimlarin onune gecebilirsiniz.
http://www.rfxn.com/projects/linux-malware-detect/

11. Yontem

Shellerin cogunda belli encode'lama yontemleri kullanilir. Bu sekilde sisteme atilacak bir shell korumalara takilmadan calisabilir. Bu gibi encode edilmiş shelleri engellemek icin php.ini dosyaniza asagidaki gibi bir ozellik eklemeniz gereklidir:

disable_functions = eval, base64_decode, gzinflate

Bu sekilde <?php eval(base64_decode(“DQppZiAoIWZ1… seklinde baslayan shellerin onune gecebilirsiniz.

12. Yontem

Scriptinizi guncel aciklar icin duzenli olarak tarayin. Sisteme atilan shelllerin buyuk kismi kullanilan scriptlerdeki zaafiyetler yuzundendir. Acunetix ve Netsparker gibi programlar ile sisteminizdeki zafiyetleri tarayabilirsiniz. Eger sisteminiz hazir script ise surekli guncelleyin ve mumkun oldugunca az eklenti kullanin. Ozellikle Joomla sistemlerde eklenti edinmeden once kullanan kisi sayisina ve guvenilirligine bakin.

13. Yontem

Asla warez script kullanmayin. Warez olarak edindiginiz tema ve scriptlerde buyuk olasilikla shell bulunur. Eger shell bulunmazsa bile bazi dosyalarda bilincli olarak arka kapi birakilir. Ornegin indirdiginiz bir Joomla temasinin bir dosyasinda bilincli olarak koyulacak bir XSS, SQL Injection ya da RFI zaafiyeti ile sisteminiz buyuk tehlikeye girecektir.

14. Yontem

Guvenligin en zayif halkasi olarak insan faktorunu asla unutmayin. Size karsi yapilacak bir sosyal muhendislik ve Phishing saldirisi ile sisteme kendiniz shell sokabilirsiniz ya da sokulmasina izin verebilirsiniz. Ornegin bir Phishing saldirisi ya da sosyal muhendislik ile guveninizi kazanan birisi size yardim etmek icin sizden Admin ve FTP bilgilerini isteyebilir. Sanal ortamda bu gibi durumlar bir hayli fazla oldugundan kimseye guvenmemeniz gerekir. Sanal ortamda karsinizda konustugunuz kisi yillardir tanidiginiz dostunuz olsa dahi bu gibi bilgileri aktarmayin. Cunku o kisinin hesabi ele gecirilmis ve sizinle onun adina konusuluyor olabilir. Daha da uc nokta bir ornek verecek olursak bulundugunuz ag dinleniyor olabilir. Bu sekilde yazismalarinizdan cikartilacak sifreler ile sisteminiz ele gecirilebilir.

15. Yontem

Sisteminizde dosya düzenleme ve kontrol izinleri sadece sizde olsun. Eger ki sistem tek bir kisi ile kontrol edilemeyecek kadar büyükse gerekli izinler mümkün olduğunca az kişide olmalıdır. Bu kisilerin butun hareketleri onlarin ulasamayacaklari ve duzenleyemeyecekleri bir yerde surekli olarak kayit altina alınmalıdır. Boylece o kisilerin sisteme zarar vermeye calismasi durumunda zafiyetin kaynagini bulabilirsiniz.

16. Yontem

Kisisel guvenliginize onem verin. Bilgisayarinizda mutlaka guncel ve guclu bir antivirus programi bulunsun. Buna ek olarak Firewall ve anti-keylogger yazilimlari da calistirin. Aginizdaki olasi dinlemelere karsi alinacak guvenlik tedbirlerini arastirin. FTP yazilimlarini asla kendi sitesinden baska yerden indirmeyin. Gectigimiz aylarda unlu bir FTP yaziliminin icerisine logger koyulup farkli sitelerden servis edilerek binlerce sistem ele gecirilmisti.

Yukarida saydigim yontemleri mumkun oldugunca uygularsaniz sisteminizi o olcude korumus olursunuz. Benim dusunceme gore %100 guvenli bir sistem olamaz. Ancak siz siz olun %99 güvenli bir sistemi hedefiniz olarak belirleyin ve çabalayın.

http://mahmutesat.com/blog/bir-siteye-shell-atmanin-20-temel-yontemi.asp#!/sisteminizi-shelllerden-korumanin-yontemleri.asp