

GbdeileFreeBSDsunucularınıngüvenli ğininarttırılması

Yazılarımdadikkatedersenizdevamlı şekildeFreeBSD`ninnekadargüvenlibiri şletim sistemioldu ğundanbahsedipduruyorum.Hepimizoveyabu şekildegüvenlikduvarları, router`lar,switchlerlea ğımızıgeleceksaldırılarakar şısanalolarakkoruyoruz.Pekiya fizikselgüvenlik?Dola ştığımço ğusunucularındabugüvenlikçe şidininhiçmihiç dikkatealınmadı ğınıgördüm.Dı şarıülkelerde“Disasterrecovery”sözcü ğüilebirlikteanılan hırsızlıkgibiolaylarülkemizdendahaciddiyeealınmakta.Internetüz erindena ğımızagirmeyi başaramayanamasunucunuzdakibilgilerialmayıkafasınakoymu şolanbirki şi,istedi ği bilgilerinbulundu ğusunucularınızdanbirisiniaçıpsabitdiskiçıkartıyorvekayıplara karışıyor.”Yokdahaneler”,veya“Adamını şiyokgelipbenimsunucumdansabitdiskimi çalacak” şeklindedü şünenlerinizolabilir.Belkiufakölçeklifirmalardakimseninsizin diskinizleu ğraşmakistememesido ğruolabilirfakatiçindeyüzlerdeki şiselbilgivekredikartı numarasıgibide ğerlibilgilerinbulundu ğubirbankasunucusubuki şileriçin“A ğız sulandırıcı” şeklindetanımlandırılabilir.

Pekifizikselolaraksunucukapılarınıkapatılması,anahtarıngüvenl iyerlerdetutulmasıgibi bütünönemlerdı şındayapılabilecekbir şeyvarmi?

Bizyineoparanoyaksistemyöneticisitutumumuzudevamettirip,oldudabiris ibütün aldığımızönlemlerigeçipdiskimiziçaldıdiyelim. İşteozamanbumakaledesize bahsedeceğimyöntembizikoruyacak.

Güvenlikkonusundaparanoyakdenebilecekseviyedebirisiolarakdiskleri n şifrlenmesi konusundaara ştırmalarımsonundaFreeBSDelkitabındadabahsedilmi şolanbde programınıbaya ğıba şarılıbuldum.

Uygulama seviyesinde şifreleme

Bütür şifrelemeuzunyıllardanberidirPGPileuygulanılıpkullanılmakta. Tüm şifrelemeve şifrelerinaçılmasındansorumluolankullanıcıheri şlemba şında şifresiniġirerekkimli ğini doğrulamakzorundadır.

Dosya sistemi seviyesinde şifreleme

Çokfazlauygulanılmayaçalı şılanbiryöntemolmaklaberabermaliyetive"Sistem yöneticilerininproblemleriniarttırani şlemler"kategorisindekiyerinialmı ştır.

Heri şletimsistemininkendidosyasisteminikullanmasıvegenelgeçerdosyasi stemlerinin çokazolmasıyüzünden şirketbazında şifrelemeyegiri ş,sistemyöneticisiolaraksizeba şa ğrı katsayınızınıükselmesivedahafazlamesai şeklindegeridönecektir.

Di ğerbirsoruniseveritabanıgibiönemlibilgilerinbulundu ğudisklerin şifrlenmesindedir.Busistemleretest edilmeden yapılan şifrelemesonucundayanlı şgidenbir şeybüttündiskeula şımınızınengellemesianlamınagelebilir.

bilgiyi öğrenmeyeçalışı şankısımpolisisekullanıcıyıhiçkimseyehesapvermedenuzuncabir surehapistetutupondanbubilgiyenindesonundaalacaktır.

Dahakötüsükullanıcıbütün şifreleriversebildi ğitüm şifreleriverdi ğinigösterebilecek birmekanizmaStegfs'debulunmamaktadır.

Bukula ğaçokuzakgelsedeçokönemlikategorisine,örne ğindevletsırları,girenbilgiler hesabakatıldı ğındabusenaryonunhiçteokadaruzakolmadı ğıgörülebilir.

Hattabunagerçekhayattanbirörnekolarak1980`deIranba şkentiTehrankonsoloslu ğunda rehineolaraktutulmu şCIAajanlarınıverebiliriz.(1)

Buyüzdenkullanıcının tüm bilgileri yoketti ğinikanıtlayabilece ğivebu şekildekullanıcıyıda koruyabilenbir şifrelemesistemini seçilmesigerekmektedir.Budatabikigbde`niniçe rdiği özelliklerden biridir.Bununyanındaböyledurumlardagbdetarafındanyoke dilenanahtar şifrelerin enpahalıbrute-force yöntemleridedahil olmak üzerehiçbir şekildegeri kazanılabilmekonususözkonusude ğildir.

GBDE kısıtlamaları

Tabikiher şifrelemeyöntemindeoldu ğugibgde`nindekısıtlamalarıbulunmakta.

1.Gbdesadece"So ğukdisk"olarakadlandırdı ğımızvediskegiri şyapılmasınışa ğlamaya yarayan tümanahtarlarıdanarınmı şdisklerüzerindekibilgilerikorumakamacılıdizayn edilmiştir.örnekolaraksistemdençıkartılmı şdisklerverilebilir.

2.E ğergbdetarafından şifrelenmişbirayıtçalışı şanbirsistemeba ğlanılırsa,kendiüzerinde şifrelemeiçinkullanılmı şolananahtarlarıta şıyorolacaktır.Budatabikidiskeancaki şletim sistemininsunabildi ğigüvenli ğışa ğlayacaktır.Bunadaörnekolaraksistemeinteret'teiken girensaldırganınkullanıcısistemiaktifram`indetutulanbilgilerel aşarakbuanahhtarlarıelde etmeyeçalışı şmasıverilebiliyor.

GBDE nasıl çalışıyor?

Gbde'ninçalışı şmamantı ğınıkısacakullanıcıtarafındangirilen şifreninkullanıcıyaana şifreye girişizni vermesiveana şifreyeula şmaizniolankullanıcının tüm şifrelenmişsektör bilgilerineula şabilirli ğışa ğlanmasıolarakaçıklanabilinir.

FreeBSD altında GBDE

Bu şifrelemeyönteminikullanabilmekiçintek şartFreeBSD5.0veyadahayüksekbir versiyonunukullanıyolmanız.DahafazladetayagirmedenFreeBSD üzerindenasil kullanabilece ğimizebakalım:

1Tehran'dakiolayındetaylarınaula şmak için:

http://news.bbc.co.uk/onthisday/hi/dates/stories/april/25/newsid_2503000/2503899.stm

Her zamanki gibi süper kullanıcı oluyoruz. Ardından kernel' a eklemeye çalışmak için
/usr/src/sys/i386/conf dosyası içinde bulunana kernel dosyamızı girip:

```
options GEOM_BDE
```

Parametresini kernel'a ekliyoruz.

FreeBSD 5.0 versiyonu veya sonrasını bir versiyon kullanıyor olacağız. Bizim için "Yeni" şekilde kernelimizi derleyebiliriz:

```
quasar$ su
```

```
passwd:
```

```
quasar$ make buildkernel KERNCONF=quasar && make installkernel  
KERNCONF=quasar && reboot
```

Kernel derlenmesinden itibaren sistem tekrar başladıktan sonra artık yeni şifreleme yöntemiimizi uygulamaya sokabiliriz.

Gbde'nin bütün şifrelenmiş disk sektörlerine girebilmesi için bir kilit (lock) dosyasına ihtiyaç vardır. Her şifrelenmiş bölüm (partition) için ayrı bir kilit dosyası hazırlanır. Bunun yaratması için:

```
quasar$ mkdir /etc/gbde
```

Komutu ile bu klasörü oluşturuyoruz.

Kullanılmadan önce her bölümün gbde'ye gösterilmek üzere gbde'nin budosya bölümünü şifrelemesinin istendiğini belirtmek gerekir. Sadece bir defa yapılabilecek bu işlemi ise şu komutla verebiliriz:

```
quasar$ gbde init /dev/ad4s1c -i -L /etc/gbde/ad4s1c
```

Burada dikkate sadece gizli bölümün diskisimleridir. Ben kullandığım ikinci diskin şifrelenmesini istediğim için kendim diskime uygulağımı seçtim. Sisteminizdeki diskisimleri mount komutuyla görebilirsiniz.

Bu işlem sonrasındaki gbde size üzerindeki değişiklik yapabileceğiniz için bir menü sunacaktır. Burada yapılacak değişiklik sektör büyüklüğü (sector_size) parametresinde olabilir. 512 olarak gelen sektör büyüklüğüne, çok ufak kalıpla performans etkilemesini engellemek için 2048 olarak değiştireyim.

```
sector_size = 2048
```

Unutmayın budosyada değeri çok düşük olarak ayarlamak performans ve bozulmanın azalmasını sağlayacaktır. Ancak büyük kullanmak dosya sisteminizin çalmasıyla sonuçlanabilir.

Dahasın gbde size şifreleme için kullanılacak şifrenizi ikidefaya soracaktır. Tabii buradaki şifrenin 8 karakter veya daha büyük, küçük, rakam ve işaretlerden oluşması zaman zaman diskinizi güvenliğini artırıcı etkenlerin başında gelmektedir.

Buradadadikkatmenizgereken şeygbdekilitdosyanızhazırladıktan sonra hem bir yedeğininalınıpgüvenlibiryerdesaklanmasıdır. Unutmayın budosyanın silinmesi disk alan kısmını sistem girmesiyanında sizindeeri şiminizin engellenmesi anlamına gelmektedir.

Şimdide şifrelenmiş bölümü kernel'aba glayalım:

```
quasar$: gbde attach /dev/ad4s1c -l /etc/gbde/ad4s1c
```

Bölüm şifrelenmesi sırasında sizin belirlediğiniz şifre siz tekrar sorulacak ve bunun doğrulanması sonunda şifrelenmiş bölümünüz /dev/içinde.bde şeklinde bir dosya halinde gözükecektir.

```
quasar$: ls /dev/ad*
```

```
/dev/ad0          /dev/ad0s1b      /dev/ad0s1e      /dev/ad4s1
/dev/ad0s1        /dev/ad0s1c      /dev/ad0s1f      /dev/ad4s1c
/dev/ad0s1a       /dev/ad0s1d      /dev/ad4          /dev/ad4s1c.bde
```

Şifrelenmiş disk kernel'aba gladıktan sonra artık üzerinde yeni bir dosya sistemi oluşturabiliriz. Disk üzerinde yeni bir dosya sistemi oluşturmak için newfs komutunu kullanacağız:

```
quasar$: newfs -U /dev/ad4s1c.bde
```

Üzerine bilgi yazıp okuyabilmek için yeni diskimizi artıkmount edebiliriz:

```
quasar$: mkdir /mnt/sifreli
```

```
quasar$: mount /dev/ad4s1c.bde /mnt/sifreli/
```

Her şeyi ayarladığımız göre artık son bir testi yapabiliriz. Bakalım df ile diskimiz görüntüleniyor mu:

```
quasar$: df -H
```

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/ad0s1a	1037M	72M	883M	8%	/
/devfs	1.0K	1.0K	0B	100%	/dev
/dev/ad0s1f	8.1G	55K	7.5G	0%	/home
/dev/ad0s1e	1037M	1.1M	953M	0%	/tmp
/dev/ad0s1d	6.1G	1.9G	3.7G	35%	/usr
/dev/ad4s1c.bde	150G	4.1K	138G	0%	/mnt/sifreli

Gbde'nin kötü olaraklandırılabilen noktalarından biri ise her boot sonrasında şifrelenmiş bölümün tekrarı kernel'aba ınlanmasıyla ilgili olarak, Maalesef /etc/fstab dosyasında eklenmesi mümkün olmadığından tek çözüm bir script hazırlayıp bunların otomatik olarak çalıştırılmasıdır.

Bunu yazarken sizin belki de bana soracağınız soruyu kendim de sordum. Yazdığımız scriptte budo şifresini yazılması script üzerinde şifreyi okuyansaldırmanın hiçbir zorluğu olmadığına gerek kalmadan şifrelenmiş bölüme ulaşılmasına olanak vermeyecektir? Evet budo grubu yazdığı script yazmamızdaki şey aynacaktır.

Benim kullanma şeklimsiz kullanım amaçları ve alanlarınızı uygun olur mu bilmiyorum fakat sistem kapandıktan sonra yakınlardaki klonları bilgilendirilerek buraya aktarılacak ve bunları okuyacağımız zaman budo disk kernel'aba ınlayıp mount etme işlemlerini mantıklı olarak yapıyor.

Uyumluluk problemi açısından gbde hiç sorun yaşamamaktadır. Tek uyumsuzluk problemi sysinstall kullanımı sırasında ortaya çıkmaktadır. sysinstall kullanımı sırasında "Probing for devices" bölümünde diğer şifrelenmiş bölüm kernel'dan ayrılması durumunda ise sistemin hatı vermesi ve hata vermesi nedeniyle başlatılmasına sebep olabiliyor.. Bunu önlemek için kernel'aba ınladığımız bölümün gbde detach /dev/ad4s1c komutu ile kernel'dan ayrılması gerekmektedir.

Kolay gelsin.

Özgür Özdemirci

<http://www.enderunix.org>

<http://news.enderunix.org>

<http://haber.enderunix.org>

Sorularınızı için: dionypheles@gmx.net

Kaynaklar

GBDE–GEOM based disk encryption <http://phk.freebsd.dk/pubs/bsdcon-03.slides.geom-tutorial.pdf>

FreeBSD handbook http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/disks-encrypting.html