

# Sistemde Bütünlük Denetim Uygulaması: Samhain

Deniz Özibrisim

Haziran, 2012

# İçindekiler

1	Giriş . . . . .	2
2	Bu güvenlik dediğimiz şey nereye kadar? Bana lazım mı? . . . . .	3
3	Kısaca dikkat edilmesi gerekenler . . . . .	4
4	Samhain . . . . .	5
5	Samhain Kurulumu . . . . .	6

# 1 Giriş

Bu ilk harflerle "Güvenlik" konusunda seri oluşturacak bir yazının temelini atmış bulunuyoruz.

Amacımız, güvenlik konusuna değinip önemini irdelemek ve bu yolda bize yardımcı olacak araçlar hakkında bilgi vermek olacak. Okuyacaklarınız asla sisteminizi %100 güvenli yapmayacaktır, imkânsız başarmak gibi bir gayemiz yok. :) Fakat, kesinlikle bu yolda size ışık tutacaktır.

Belirli zaman aralıkları ile sizlerle paylaşacağımız bu seri, şifre güvenliği ve kırılma noktası testlerini, şifre kırmak için kullanılan programları, bütünlük denetimini, saldırı engelleme sistemlerini, paket koklayıcılarını ve daha birçok güvenlik konusunu ele alacak. İleride kendi ağımıza fiziksel olarak bir saldırgan konumlandırıp (bu bizim), paket koklayıcılarla ağ trafiğinden geçen dosyalara bakacağız ve o adrese teslim giden dosyada değişiklik yapmaya çalışacağız. Fakat sizinle beraber yapacağımız kendi ağımızdaki gidip gelen şifreli paketler sayesinde bir saldırganın üzüntülü dakikalarına tanık olacağız.

Öncelikle anlamamız gereken, her zaman en 'zayıf' halkanın insan olduğudur. Fiziksel açıdan 'zayıf' olmak kulağa hoş gelse de bu durumda pek hoş karşılanmıyor. :) Bu yüzden daha bu konuya başlamadan sisteminizin (Linux ev kullanıcısı ya da sistem yöneticisi) güçlü şifreler ile oluşturulduğunu, bu şifreleri kimseyle paylaşmadığınızı ve bilgisayarınızın fiziksel olarak güvenli bir yerde olduğunu varsayıyorum.

## 2 Bu güvenlik dediğimiz şey nereye kadar? Bana lazım mı?

Güvenlik için, "Nereye kadar?" önemli bir sorudur. Çünkü bu işin sonu paranoyaya bağlanabilir. :)

Sistemimiz ne kadar fazla güvenli ise bir o kadar kısıtlı olacaktır, bu yüzden ileride anlatacağımız araçların hangilerini kullanacağınıza gerekliliği doğrultusunda siz karar vereceksiniz.

Bana lazım mı? Kime lazım değil ki? Elektronik Posta şifrelerinizin, sosyal ağ şifrelerinizin çalınmasını istemiyorsanız, sizin bilgisayarınızın sizden habersiz sağa sola saldırı yapmasını istemiyorsanız, özel dosya ve dokümanlarınızın başkalarının eline geçmesini istemiyorsanız evet size de lazım.

Daha büyük ağlarda ise bu durum zorunluluktur. Sadece dışarıdan içeriye gelecek tehditler için değil, içeriden dışarıya giden tehditlerden de siz sorumlusunuz. Güvenlik konusunun sadece bilgisayarınıza gelecek bir saldırı olmadığını, daha birçok güvenlik açığının sorun olabileceğini aşağıdaki örnekle belirtmek isterim.

Güzel Türkiye'min Bodrum kıyılarında başımdan geçen bir olayı aktarmak istiyorum.

Bu olay kayıt (log) tutmanın önemini vurgulayacaktır (Sistem yöneticisi arkadaşlara sesleniyorum :))

X firmasında çalışan bir şahıs, aynı firmada beraber çalıştığı X kişisi için sosyal ağlarda bir hesap oluşturup telefon bilgilerini verir (şirket bilgisayarından), bu doğrultuda X kişiye rahatsızlık veren telefonlardan, sosyal bir ortamda kişisel bilgilerinin bulunduğunu öğrenir ve savcılığa suç duyurusunda bulunur. Sonuç belli, siyah minibüsten inen, siyah takım elbiseli amcalar duruma el koymaya gelir. Siz aksini gösterene kadar suçlu olan sosyal ağa kaydın yapıldığı IP adresinin sahibidir. Bu şirkette Bilgi Teknolojileri Yöneticisi olarak görev yapıyorsanız, size iletilen tarihte ilgili hedefe girişi yapan kullanıcıyı tespit etmelisiniz, eğer bu düzende bir kayıt (log) tutmuyorsanız durum pek iç açıcı olmayacaktır.

Yukarıdaki örnek ile çok basit bir olayın başımıza ne işler açabileceğini anlatmak istedim.

Evet, güvenlik bana da lazım diyen arkadaşlar için devam ediyoruz :)

### **3 Kısaca dikkat edilmesi gerekenler**

Başta da belirttiğimiz gibi zayıf halka hep insan olduğu için, ne kadar güvenlik önlemi alırsanız alın eğer dikkatli davranmazsanız bu önlemler önem teşkil etmeyecektir. Bilgisayarınıza kurulmuş bir yazılım, kontrolsüz olarak sizden habersiz işler çevirebilir. Bunları en aza indirmek için, tanımadığınız kişilerden gelen elektronik postaları açmayınız, sohbet ettiğiniz kişiler ile dosya paylaşırken dikkatli olunuz, mümkünse tanımadığınız kişilerin gönderdiği dosyaları almayınız/kabul etmeyiniz. İçinde ne olduğunu bilmediğiniz o dosyalar, sorun çıkaracak afacan kodlarla dolu olabilir.

## 4 Samhain

Temiz bir sistem kurulumu yaptıktan sonra önemsemediğimiz araçların başında **Samhain, Tripwire** gibi araçlar geliyor.

Samhain bütünlük denetlemesi yapan bir programdır; ama işin bütün esprisi, mutlaka ve mutlaka temiz bir sisteme, mümkünse daha yeni kurulmuş ve hiç İnternet'e bağlanmamış bir sisteme kurulmasıdır. Yapısı gereği sonradan yapılan değişiklikleri gösterdiği için, kurulduğu sırada var olan sistem açığı ya da saldırganın yarattığı bir açık varsa zaten dosyada kurulumdan önce değişiklik yapıldığı için bunu algılamayacaktır.

Samhain kurulduktan sonra sistemi haritalar, imaj alır, bir bakış atar ya da resmini çeker diyebiliriz. :) Bu dosyaları md5 ile işaretler ve bir dahaki çalıştırmanızda karşılaştırma yaparak bütünlük denetimi yapar.

Sistemin herhangi bir açığının faydalanan saldırgan eğer sisteme sızarsa büyük ihtimalle ilerleyen zamanlarda daha rahat sisteme girip çıkmak için bir arka kapı (Backdoor) bırakacaktır. Eğer saldırganın değiştirdiği bir dosya var ise, sistem dosyasında değişiklik yapıldığını görürsünüz.

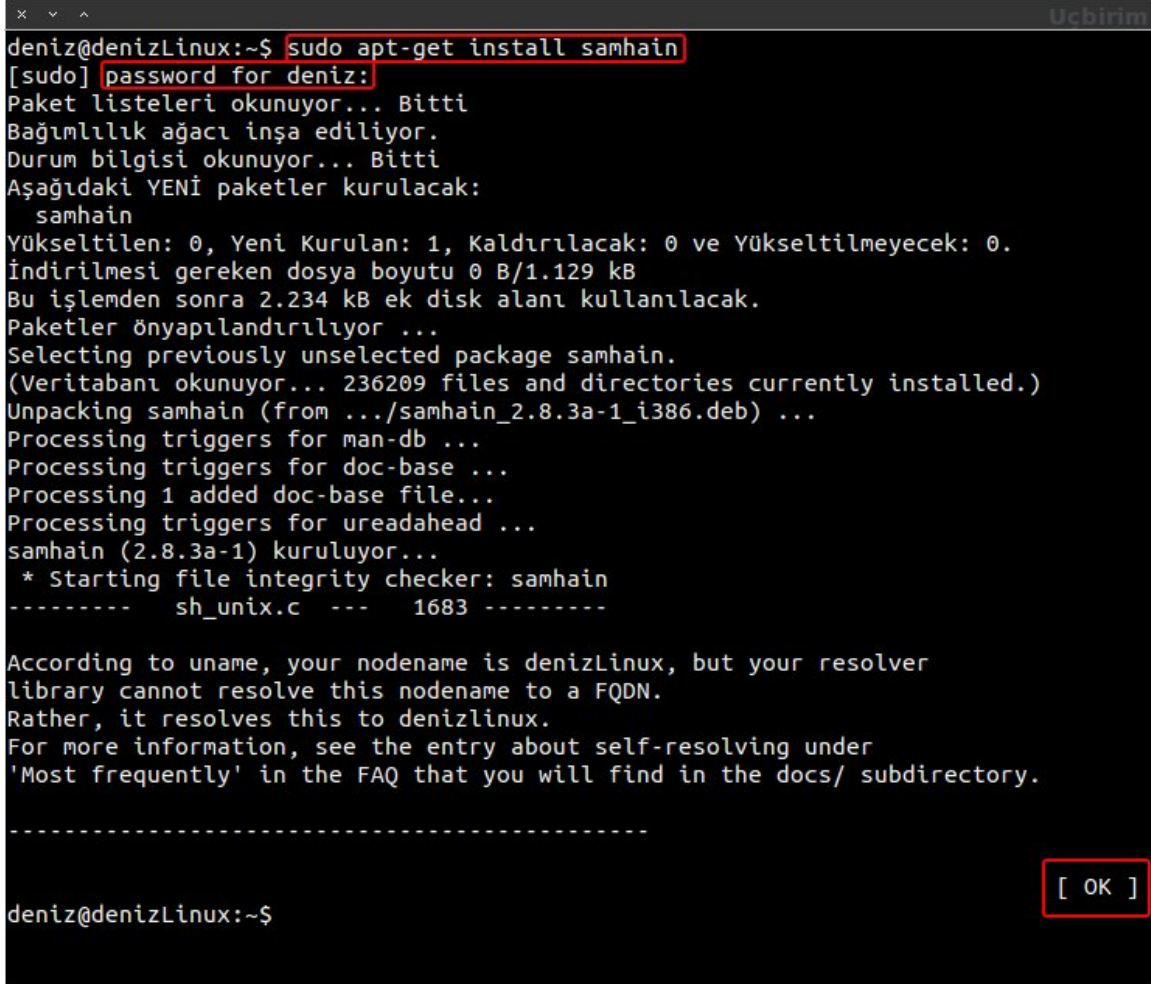
Programın veritabanının kurcalanmaması adına taşınabilir disk ya da başka bir ortamda tutmak daha mantıklı olabilir. Böylece sistemin ilk hâlinin değiştirilmeden durduğuna emin olursunuz. Samhain ayrıca dosya sistemi için "SUID check", "login" kontrol için "login check" ve "kernel rootkit"ler için de kontrol yapabilir. Bunları isteğe bağlı olarak aktif hâle nasıl getirdiğimizi yazımızın devamında göreceğiz.

(Tripwire ve benzer programlar aldıkları imajları veritabanına yazar. İlk yazdığı bilginin değişmemesini garantilemek için, taşınabilir disk ya da başka bir ortamda muhafaza edip kontrol sırasında takıp kullanmak daha güvenli olacaktır.)

## 5 Samhain Kurulumu

Ctrl+Alt+t tuş kombinasyonu ile Uçbirim penceremizi açıyoruz ve aşağıdaki komutu yazıyoruz, komutu yürütmek için yönetici şifremizi istiyor, şifremizi yazıp kurulumu devam ediyoruz.

```
1 sudo apt-get install samhain
```



```
deniz@denizLinux:~$ sudo apt-get install samhain
[sudo] password for deniz:
Paket listeleri okunuyor... Bitti
Bağımlılık ağacı inşa ediliyor.
Durum bilgisi okunuyor... Bitti
Aşağıdaki YENİ paketler kurulacak:
 samhain
Yükseltilen: 0, Yeni Kurulan: 1, Kaldırılacak: 0 ve Yükseltilmeyecek: 0.
İndirilmesi gereken dosya boyutu 0 B/1.129 kB
Bu işlemden sonra 2.234 kB ek disk alanı kullanılacak.
Paketler önyapılandırılıyor ...
Selecting previously unselected package samhain.
(Veritabanı okunuyor... 236209 files and directories currently installed.)
Unpacking samhain (from ../samhain_2.8.3a-1_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for doc-base ...
Processing 1 added doc-base file...
Processing triggers for ureadahead ...
samhain (2.8.3a-1) kuruluyor...
 * Starting file integrity checker: samhain
----- sh_unix.c --- 1683 -----

According to uname, your nodename is denizLinux, but your resolver
library cannot resolve this nodename to a FQDN.
Rather, it resolves this to denizlinux.
For more information, see the entry about self-resolving under
'Most frequently' in the FAQ that you will find in the docs/ subdirectory.

-----

deniz@denizLinux:~$ [ OK ]
```

Şekil 1:

Bilgi almak için,

```
1 man samhain
2 samhain --help
```

komutlarını kullanabilirsiniz.

Samhain yapılandırma dosyası /etc/samhain/ altında, "samhainrc" dosyasıdır. Dediğimiz gibi SuidCheck vb. özellikleri için dosyayı kendimize göre düzenlememiz gerekiyor. İsteddiğiniz herhangi bir editörle dosyayı açabilirsiniz.

```
1 sudo -H gedit /etc/samhain/samhainrc
```

Uçbirimden devam eden arkadaşlar aynı dosyayı "vi" ya da "nano" ile açıp gerekli değişiklikleri yapabilirler.

```

1 #####
2 #
3 # Optional modules
4 #
5 #####
6
7 [SuidCheck]
8 ##
9 ## — Check the filesystem for SUID/SGID binaries
10 ##
11
12 ## Switch on
13 #
14 SuidCheckActive = yes
15
16 ## Interval for check (seconds)
17 #
18 SuidCheckInterval = 7200
19
20 ## Alternative: crontab-like schedule
21 #
22 # SuidCheckSchedule = NULL
23
24 ## Directory to exclude
25 #
26 # SuidCheckExclude = NULL
27
28 ## Limit on files per second (0 == no limit)
29 #
30 # SuidCheckFps = 0
31
32 ## Alternative: yield after every file
33 #
34 # SuidCheckYield = no
35
36 ## Severity of a detection
37 #
38 SeveritySuidCheck = crit

```

[SuidCheck] , SuidCheckActive gibi satırların başındaki # işaretini kaldırdığınız zaman aktif olacaklar. SeveritySuidCheck, kritik (crit) olarak işaretli. Log dosyamızın içine, bir durum olduğu zaman kritik olarak yansıtacaktır. Log dosyamız da INFO ile bize bilgi verdiğini, WARN ile bizi uyardığını, CRIT ile de kritik bir durum olduğunu belirtmektedir.

Kernel ve LoginCheck için de aynı düzenlemeleri aşağıdaki gibi yapıyoruz:

```

1 [Kernel]
2 ##
3 ## — Check for loadable kernel module rootkits (Linux/FreeBSD only)
4 ##
5
6 ## Switch on/off
7 #
8 KernelCheckActive = True
9
10 ## Check interval (seconds); btw., the check is VERY fast
11 #
12 KernelCheckInterval = 300
13
14 ## Severity
15 #
16 SeverityKernel = crit
17
18
19 [Utmp]
20 ##

```



```

21 ## — Logging of login/logout events
22 ##
23
24 ## Switch on/off
25 #
26 LoginCheckActive = True
27
28 ## Severity for logins , multiple logins , logouts
29 #
30 SeverityLogin=info
31 SeverityLoginMulti=warn
32 SeverityLogout=info
33
34 ## Interval for login/logout checks
35 #
36 LoginCheckInterval = 300

```

Kurulumun ardından yapılandırma ayarlarınız bittiye artık şöyle bir göz atıp sistemimize bakması için start verme zamanı gelmiş demektir.

Aşağıdaki komut ile (samhain –help komutu ile, init, update, check komutlarını -t parametresi ile kullandığımızı göreceksiniz.) bütünlük denetlemesi yapabilmesi için gerekli veriyi yaratmasını sağlıyoruz.

```
1 sudo samhain -t init
```

Evet, sanırım kontrol etmek için bazı değişiklikler yapma zamanı geldi. :) Aklınızdan ne yaramazlıklar geçiyor bilmiyorum; ama ben bir iki mütevazî değişiklik yapmayı düşündüm, hep beraber sonuca bakalım.

/etc/tripwire /etc/conky/conky.conf ve /etc/passwd içine ekleme yaptım, şimdi sistemdeki değişikliklere bakalım, merakımızı giderelim.

Bütünlük denetimini yapması için,

```
1 sudo samhain -t check
```

Komutunu kullanmamız yeterli.

Kontrol sonucu için /var/log/samhain/samhain.log dosyasına bakıyoruz.

```

*samhain.log (/var/log/samhain) - gedit
Dosya Düzen Görünüm Ara Araçlar Belgeler Yardım
Aç Kaydet Geri Al
CRIT : [2012-06-06T15:34:21+0300] msg=<POLICY [ReadOnly] -----T->, path=</etc/tripwire>, ctline_old=<[2012-06-06T08:30:38]>,
ctline_new=<[2012-06-06T12:29:23]>, mtime_old=<[2012-06-06T08:30:38]>, mtime_new=<[2012-06-06T12:29:23]>,
E9359A696D9DBA0D463148DD9CB464F0A2D72D3A5007A648
CRIT : [2012-06-06T15:33:19+0300] msg=<POLICY [ReadOnly] --I---T->, path=</etc/conky/conky.conf>, inode_old=<1575965>,
inode_new=<1575897>, dev_old=<8,1>, dev_new=<8,1>, ctline_old=<[2012-06-05T14:26:11]>, ctline_new=<[2012-06-06T12:28:57]>,
[2012-06-05T14:26:11]>, mtime_new=<[2012-06-06T12:28:57]>,
7EED3D212D48C5E9EC5D2A85CBF68BE28C5A12FB661B1B11
CRIT : [2012-06-06T15:33:58+0300] msg=<POLICY [ReadOnly] --I---T->, path=</etc/passwd>, inode_old=<1587553>, inode_new=<1587586>,
dev_old=<8,1>, dev_new=<8,1>, ctline_old=<[2012-06-06T08:29:59]>, ctline_new=<[2012-06-06T12:29:45]>, mtime_old=<[2012-06-06T08:29:59]>,
mtime_new=<[2012-06-06T12:29:45]>,
F12F614A51B26E0B57485146AB368EAB5FAE547DF4386D50
INFO : [2012-06-06T15:33:28+0300] msg=<Checking>, path=</etc/python>
33FD0E2BA3B42F71DC0E4AC8CA7D0F926DFC0B06BCDA661
Düz Metin Sekme Genişliği: 8 Sat 326, Süt 49 ARY

```

Şekil 2:

Log dosyamızda gördüğümüz gibi ilk kutu içerisinde /etc/tripwire için kritik vermiş. Dosya yaratma ve değişiklik zamanı bilgileri vermiş.

İkinci ve üçüncü kutu, özellikle üçüncü kutu ciddi kritik ;), /etc/conky/conky.conf ve /etc/passwd için aynı durum söz konusu. Detaylarda dosyaların eski boyutunu ve yeni boyutunu, eski checksum değerini ve yeni checksum değerini de görebilirsiniz.

Dördüncü kutu kritik değil, sadece bilgi vermiş (INFO). /etc/python u kontrol ettiğini söylüyor.

Peki bu dosyalarda gerçekten biz değişiklik yaptık ve bunları Samhain'e bildirmek istiyoruz. Bu durumda aşağıda ki komutu kullanıyoruz:

```
1 sudo samhain -t update
```

Genelde check komutu ile kontrol yapıldıktan sonra bir sorun yoksa istenilen değişiklik yapılır ve update komutu ile bilgisi Samhain'e verilir.

İyi günlerde kullanın.

Monoton bir ortam yaratmamak için iptables, squid, dansguardian gibi konulara göz atacağımızın, VPN sunucu kurulumu ve ayarları konularını konuşacağımızın sözünü verelim şimdiden. :) Ardından VPN ile bağlanan kullanıcıların bütün ağımıza değil de sadece içeride bizim istediğimiz bilgisayarlara ulaşmalarını nasıl sağlarız, nasıl kısıtlama getiririz gibi konularla tekrar güvenlik kısmına da göz atmış oluruz.

Bir dahaki sayıda yeni güvenlik konularını konuşmak üzere hoşçakalın.