

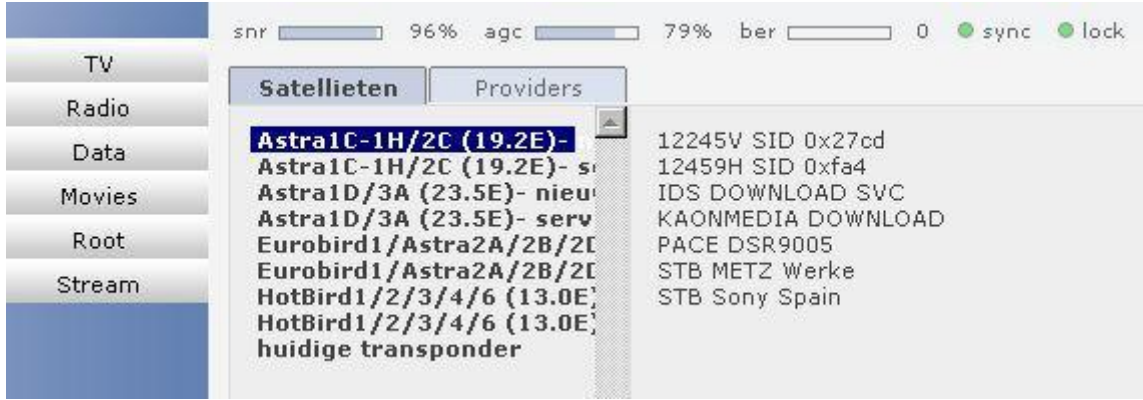
Yetersiz Şifre Politikasının Sonuçları

Bünyamin Demir, Aralık 2009, WGT E-Dergi 3. Sayı

Yazıya başlamadan önce değerli okura amacımı -iyi anlatmak- maksadıyla şu notları düşmek istiyorum;

- Aşağıda göreceğiniz ürün arayüzleri şahsi seçimim değildir. Denemeler sonucu karşıma çıkan arayüzlerdir.
- Yazıda ürün isimlerinden bahsetmedim. Fakat arayüzlerden tahminler olabilir. Yine de hatırlatmak gerekirse; amaç ürünleri kötülemek değil, bu tür açıklıkların internete çıkan ürünler de var olabildiğini göstermektedir.
- Bahsi geçen cihazlara ve bunları kullananlara kesinlikle zarar verilmemiştir. Lütfen sizler de testlerinizde kullanıcıların, yakınlarımızda olan arkadaşlarımız olabileceğini unutmayınız ve zarar vermeyiniz.

Bir kaç hafta önce bir tanıdığım uydu cihazları ile ilgili bana bir link gönderdi. Tabi kendisinin bulunduğu bir açıklığı içeriyordu. Kısaca açıklıktan bahsedecek olursak; bir uydu alıcısı cihazı alınmış ve bunun web arayüzü malesef internet ortamına açık bırakılmış. Tabi bu tür uydu alıcıları, kameralar v.s için internette birçok ipucu bulabilirsiniz. Arkadaşımın bu arayüze nasıl ulaştığı hakkında bilgim yok ama link aktif mi diye denediğimde ben de bahsi geçen arayüze ulaştım.



Tabi merakla içinde biraz gezinmeye başladım (zarar vermeden). İlk tıklamalar sonucu gördüklerim ilginçti.

```
bin/  
dev/  
etc/  
hdd/  
lib/  
mnt/  
tmp/  
sys/  
var/  
usr/  
boot/  
home/  
proc/  
sbin/  
media/  
share/
```

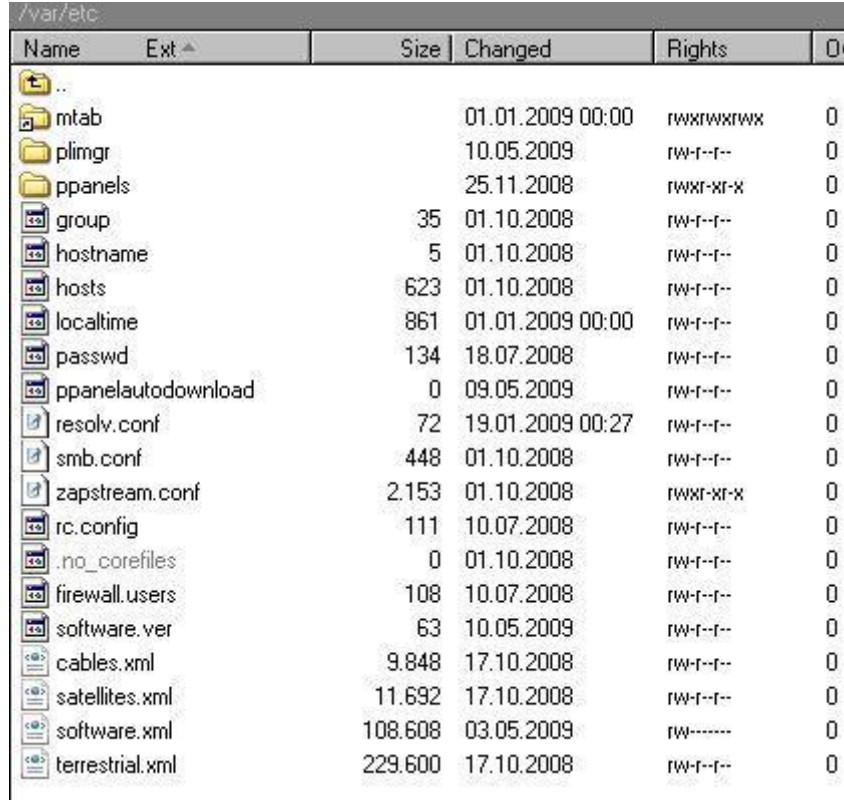
24 ANK.ARAC	BBC WORLD SERVIC	DMV
ABSAT	BFBS	DOGAN TV
ADMINISTRA.IT	BSS	DOGUS
AH-EDP	CINE 5	DU
AKSU TV	CTV	DUNA TELEVIZIO
AL JAZEERA	CYFRA +	DVL.TV
AL JAZEERA CHILDR	DEFAULT PROVIDER	EAS
ARABSAT	DEUTSCHE WELLE	ERTU
ARQIVA	DIGETTE	EUROSPORT
ARQIVA FRANCE	DIGGETE	EUTELSAT
ART	DIGITAL MEDIA CENT	FLASH TV
AVRASYA	DIGITAL PLATFORM	GCE
AVRUPA PLATFORM	DIGITAL PLATFROM	GCP
	DIGIT üRK	GLOBECAST

```
root: [REDACTED]/10:0:0:root:/home/root:/bin/sh  
daemon:*:1:1:daemon:/usr/sbin:/bin/sh  
bin:*:2:2:bin:/bin:/bin/sh  
sys:*:3:3:sys:/dev:/bin/sh  
sync:*:4:65534:sync:/bin:/bin/sync  
games:*:5:60:games:/usr/games:/bin/sh  
man:*:6:12:man:/var/cache/man:/bin/sh  
lp:*:7:7:lp:/var/spool/lpd:/bin/sh  
mail:*:8:8:mail:/var/mail:/bin/sh  
news:*:9:9:news:/var/spool/news:/bin/sh  
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh  
proxy:*:13:13:proxy:/bin:/bin/sh  
www-data:*:33:33:www-data:/var/www:/bin/sh  
backup:*:34:34:backup:/var/backups:/bin/sh  
list:*:38:38:Mailing List Manager:/var/list:/bin/sh  
irc:*:39:39:ircd:/var/run/ircd:/bin/sh  
gnats:*:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh  
nobody:*:65534:65534:nobody:/nonexistent:/bin/sh  
ftp:x:500:64002:Linux User,,,:/var/tmp/ftp:/bin/false
```

Fakat bundan sonrasını merak etmeye başladım. Acaba bu ürün için şu an açık kaç tane arayüz var?

Tabi Google Hacking sağolsun. **intitle:"XXXXX XXXX Interface"** v.s gibi keyword`ler ile aradığımda karşıma çıkan sonuçlar ilginç. Asıl anlamadığım, böyle bir ürün satıp, arayüzün internette erişilebilir olacağı varsayımı varsa neden arama motorlarının indekslenmesi engellenmez? Tabi sorun sadece arayüzünü verdiğim uydu alıcısı için değil, buna benzer diğer ürünlere bakılınca da malesef aynı durum geçerli. Biz neler yapılabiliyoruz kısmı ile devam edelim.

Daha sonra ürün hakkında biraz bilgi edindim. Bilmediğiniz bir programlama dilinde açıklık bulmak ne kadar zorsa, özelliklerini (kullanılan işletim sistemi, arayüzler, ön tanımlı ayarlar v.s) bilmediğiniz bir cihazı kurcalamakta okadar zor. Bilgiler edinip, Google yardımıyla bulduğum arayüzlere baktım. Ardından FTP erişimi olduğunu gördüm ve...



Name	Ext	Size	Changed	Rights	Own
..					
mtab			01.01.2009 00:00	rwxrwxrwx	0
plimgr			10.05.2009	rw-r--r--	0
ppanels			25.11.2008	rwxr-xr-x	0
group		35	01.10.2008	rw-r--r--	0
hostname		5	01.10.2008	rw-r--r--	0
hosts		623	01.10.2008	rw-r--r--	0
localtime		861	01.01.2009 00:00	rw-r--r--	0
passwd		134	18.07.2008	rw-r--r--	0
ppanelautodownload		0	09.05.2009	rw-r--r--	0
resolv.conf		72	19.01.2009 00:27	rw-r--r--	0
smb.conf		448	01.10.2008	rw-r--r--	0
zapstream.conf		2.153	01.10.2008	rwxr-xr-x	0
rc.config		111	10.07.2008	rw-r--r--	0
.no_corefiles		0	01.10.2008	rw-r--r--	0
firewall.users		108	10.07.2008	rw-r--r--	0
software.ver		63	10.05.2009	rw-r--r--	0
cables.xml		9.848	17.10.2008	rw-r--r--	0
satellites.xml		11.692	17.10.2008	rw-r--r--	0
software.xml		108.608	03.05.2009	rw-----	0
terrestrial.xml		229.600	17.10.2008	rw-r--r--	0

Dolayısıyla erişim sağlanacak noktalar bulup devam edilebilir. Fakat başka neler var derken, biraz daha meraktan sonra aşağıdaki arayüze ulaştım.

Home	Active Clients	Clients	Servers	Shares	Providers	Entitlements
------	----------------	---------	---------	--------	-----------	--------------

Connected clients: 7

7 ACTIVE CLIENTS IN LAST 20 SECONDS

Username	Host	Connected	Idle time	ECM	EMM
kemal		00d 05:48:34	00d 00:00:09	9267 (9265)	22589
ahmet		00d 04:59:31	00d 00:00:09	9778 (9778)	19458
hasret		00d 04:58:36	00d 00:00:04	2440 (2438)	2290 (
gunay		00d 04:54:00	00d 00:00:08	4742 (4723)	18652
ihsan		00d 04:49:54	00d 00:00:09	8421 (8420)	17142
ersan		00d 03:15:23	00d 00:00:05	8144 (8142)	11700
ibrahim		00d 01:34:42	00d 00:00:05	4756 (4753)	5610 (

Username	Shareinfo
kemal	local 0d00:000000 1362 (1362)
ahmet	local 0d00:000000 913 (913)
	remote 0d00:000000 904 (904)
hasret	local 0d00:000000 193 (193)
	remote 0d00:000000 22 (22)
gunay	local 0d00:000000 1585 (1571)
	remote 0d00:000000 255 (255)
ihsan	local 0d00:000000 1591 (1591)
ersan	local 0d00:000000 416 (416)
	remote 0d00:000000 701 (701)
ibrahim	local 0d00:000000 501 (501)
	remote 0d00:000000 71 (71)

Burada bulduğum "Host" adreslerini kullanmaya başladım ve karşıma aşağıdaki ekran geldi (başka şeylerde bulmak mümkün).

GİRİŞ

Şifre :

Hiç bir şey yapmadan "Tamam" a basınca da malesef aşağıdaki ekran geliyor.

Internet Bağlantısı:	Bağlantı var
ADSL Bağlantısı:	Bağlantı var
ADSL Hızı:	256 / 1024 kbps

Tabi artık bu uydu alıcısını kullanan kişinin modemine de hakim olmaya başladık. Bundan sonrasının teknik kısmını uzatmayıp, aslında değinmek istediğim konuya geçmek istiyorum.

Belki hepimiz bu tarz bir uydu alıcısına sahip olmasak da buna benzer kameralar veya en azından bir ADSL modem sahibiyizdir. Yukarıda verilen örnekler de görüldüğü gibi, karşımıza bazı güvenlik problemleri çıkıyor. Ön tanımlı şifreler veya şifre atanmamış arayüzler.

Peki bu bu probleme sebebi nedir?

- Ürünün sahibi olan firma yeteri kadar güvenlik politikası belirlememiş.
- Ürünü alıp, arayüze şifre koymayan veya ön tanımlı gelen şifreyi değiştirmeyen alıcı hatası.

Firmayı ele aldığımızı düşünelim. Bir kere bu şekilde internet ortamına açılacak bir ürün ise (özellikle ADSL modemler) muhakkak bir şifre koyması gerekiyor -ki su an bunu bir çok ürün de görebiliriz. Peki bu koydukları genel şifre (muhtemelen satılan her ADSL modem için geçerlidir), yeterli mi? Belki IT ile direk veya dolaylı olarak bağlantılı işlerde çalışan kişiler, bu ön tanımlı şifreleri değiştirmeyi bir güvenlik gerekliliği olduğunu biliyorlardır. Fakat bu konuda herhangi bir bilgisi olmayan ve sadece amacı internete çıkmak isteyen bir kullanıcı. Bu ön tanımlı şifreyi değiştirmesi gerektiğini nerden bilecek? Hemen kendi ADSL modem kitapçığını aldım ve baktım. Malesef bu şifrenin değiştirilmesi için herhangi bir ibare yok. Peki şu soruyu hemen soralım; ADSL modem satın alıp, internete çıkmak isteyen bir kişi, kendisinin artık bir kurban olduğunun farkında olsa ne yapar? Bunun hukuki boyutunu merak etmiyor değilim. Çünkü bundan doğacak zarar için elimde olan kitapçıkta birşey yazmıyor. Fakat bir an için firma gibi düşünmeye başlayalım. Sattığımız ürünün güvenliğini nasıl sağlarız? Her bir ürün için ayrı şifre üretsek. Bu bize her bir kitapçığa ayrı şifre yazmamızı ve buna ayrı bir yönetim kaynağı ayırmamız gerektirecektir. Takibi genel şifre vermekten zor olsa bile, çok masraflı olacağını düşünmüyorum. Fakat kitapçık kaybolursa ve kişi şifresini unutmuşsa ne olacak? Her modem için seri numarası üretilmiş olmalı. Bu seri numaralarına göre atanmış ön tanım şifreler firmada bulunmalı ve yine bir telefon numarası ile, seri numaranızı verip şifrelerinizi alabiliyor olmalısınız. Tabi bu iş için kişi istihdam edilmesi gerekecek ve yine maliyet artacak. Varsayalım ki bunu da yaptık. Ardından arayan kişinin gerçekten bizden modemi satın alan kişi olduğunu nerden bileceğiz? Ürünü satarken kimlik fotokopisi mi almamız lazım, emin değilim. Gerçekten Firma için de kolay bir konu değil. Yine de kitapçıkta bu ön tanımlı şifrenin değiştirilmesini önemli bir not olarak düşseler muhtemelen bu tür açıklıklar ciddi oranda azalacaktır. Parola seçimlerini de dikkate almakta fayda var. Karakter uzunlukları, içinde sayı veya ?!\$ v.s gibi karakterler geçip geçmeyeceği konularını da ele almak lazım.

Belki bundan sonrası için bu çalışmalar yapılabilir fakat geçmişte satılmış ürünler hala çok ciddi tehlikeler oluşturuyor. Cihaz üzerindeki uygulama güncellemelerine bu şifre politikaları

katılsa çok güzel olur, hatta auto update ile de çözülebilse ne güzel. En azından problemler biraz daha azalacaktır.

Toparlamak için önerilerimizi madde madde sıralarsak;

- İnternete açık ürünlerin arayüzlerinin sıkı bir şifre politikası olmalı
- Eğer internete açık olması gerekmiyorsa muhakkak sadece local erişimlere izin verilmeli.
- Üretici firma, ürünü alan kişilere güvenlik politikası için şifre değiştirmeyi hem not düşmeli (kullanma klavuzu) hem de zorunlu kılmalı. Tabi burda sıkı bir şifre politikasının önemi artmaktadır.
- Ürün internete açıksa ve bu tarz güvenlik problemlerini gidermek isteniyorsa muhakkak auto update ile zaman zaman kritik güvenlik problemleri güncellenmeli.
- Her ihtimale karşı internete açık ürünler arama motorları tarafından indekslenilmemeli.