Air6372SO Varsayılan Hesap Doğrulaması

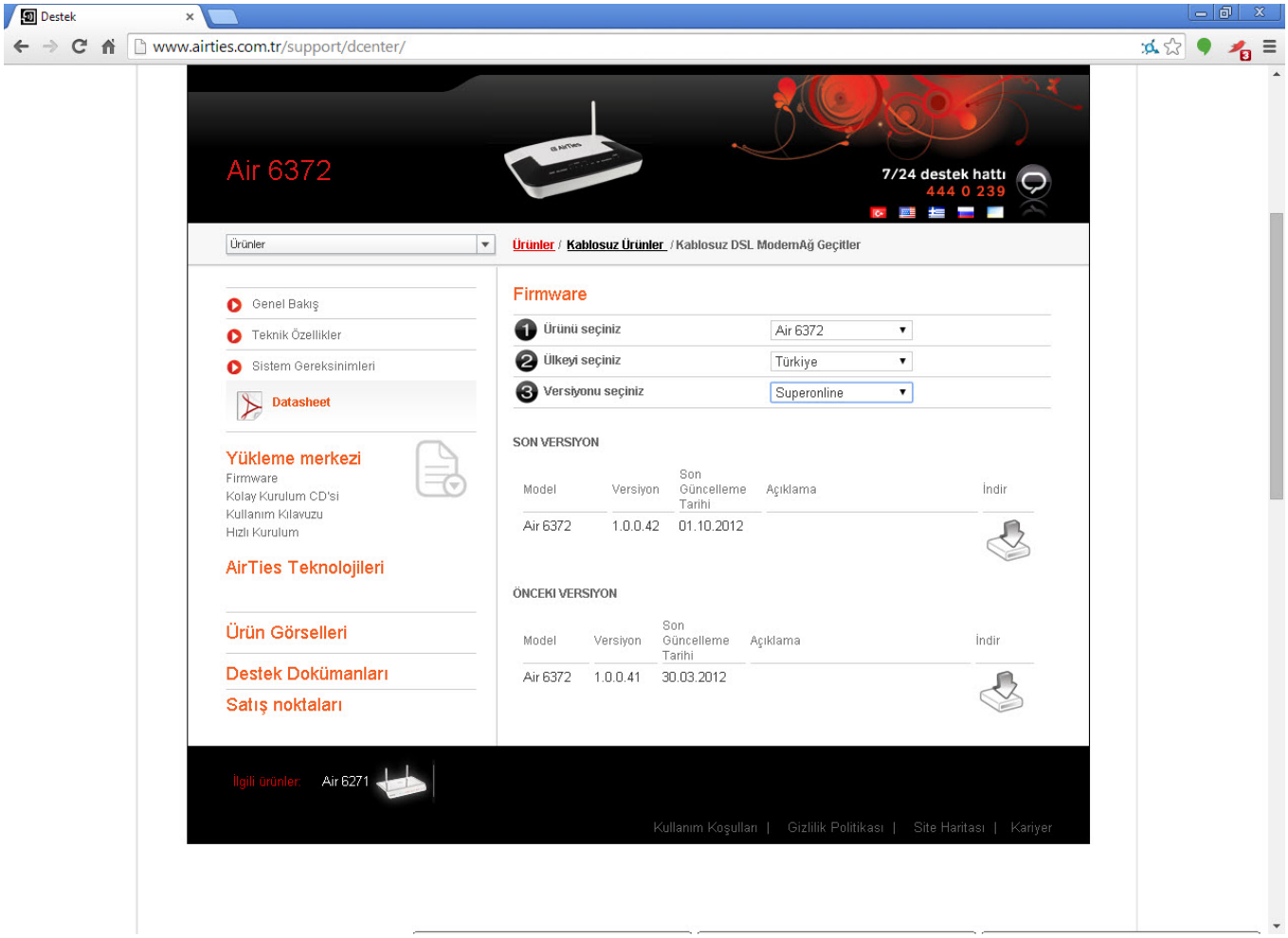
written by Mert SARICA | 1 December 2014

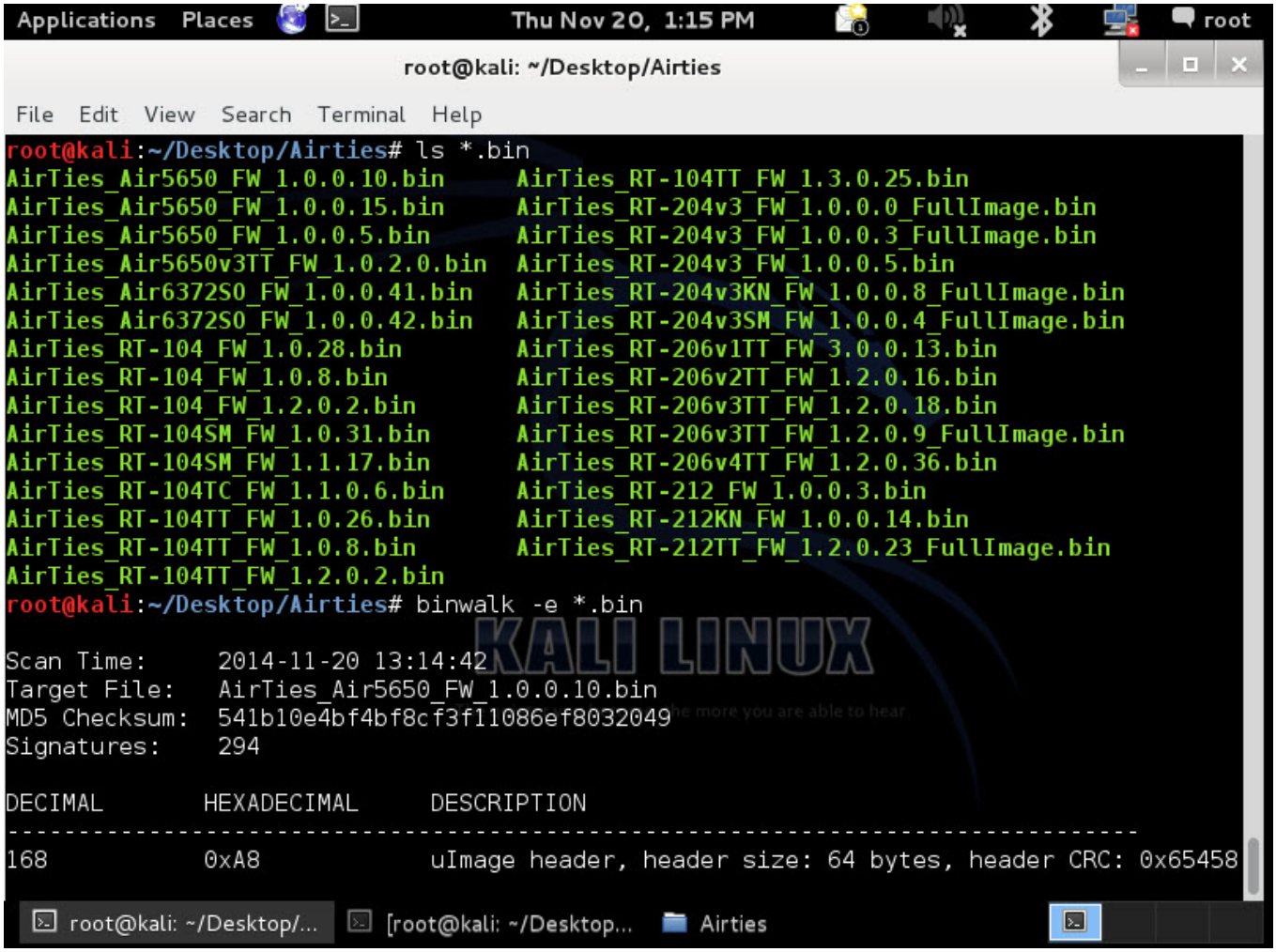
15 Kasım Cumartesi sabahı uykulu gözlerle gönderilen tweetlere bakarken Gökmen GÜREŞÇİ'nin "Airties arka kapısını doğrulayabilen oldu mu? Hangi modeller etkileniyor? Ben henüz doğrulayamadım " tweeti ile karşılaştım. Gökmen'e iddianın kaynağını sorduğumda bana Hacker Fantastic Twitter hesabından atılan aşağıdaki tweeti gösterdi.

Bu iddiayı doğrulamak için, IstSec konferansında yaptığım donanım yazılımı analizi sunumuna hazırlanmak için zamanında satın almış olduğum Airties RT-206v4 modeline hızlıca göz atmaya karar verdim. Nmap ile modemin bağlantı noktalarını (1-65535) kontrol ettiğimde, modemin 2323 bağlantı noktasını dinlemediğini gördüm. Bu durum, bahsedilen varsayılan hesabın sadece belli modellerde geçerli olduğunu ortaya koyuyordu. Elimde başka bir model olmadığı için donanım yazılımını statik olarak analiz etmek için işe koyuldum.

Airties'ın web sitesinde yer alan çoğu kablosuz modemin donanım yazılımını

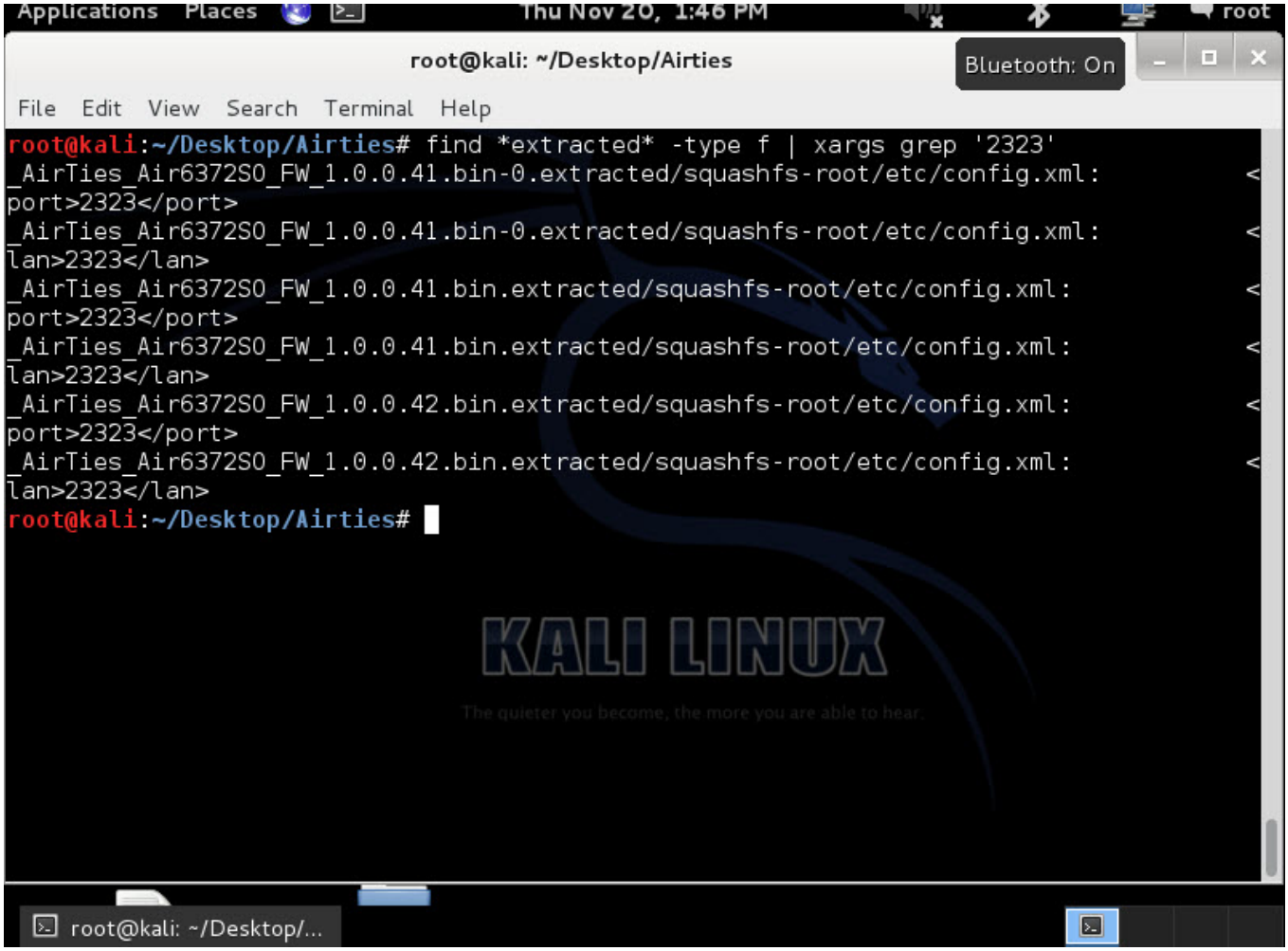
indirdikten sonra donanım yazılım analizi için biçilmiş kaftan olan ve Kali işletim sistemi ile gelen binwalk aracı ile donanım yazılımlarını bu araca toplu bir şekilde analiz ettirmeye başladım.





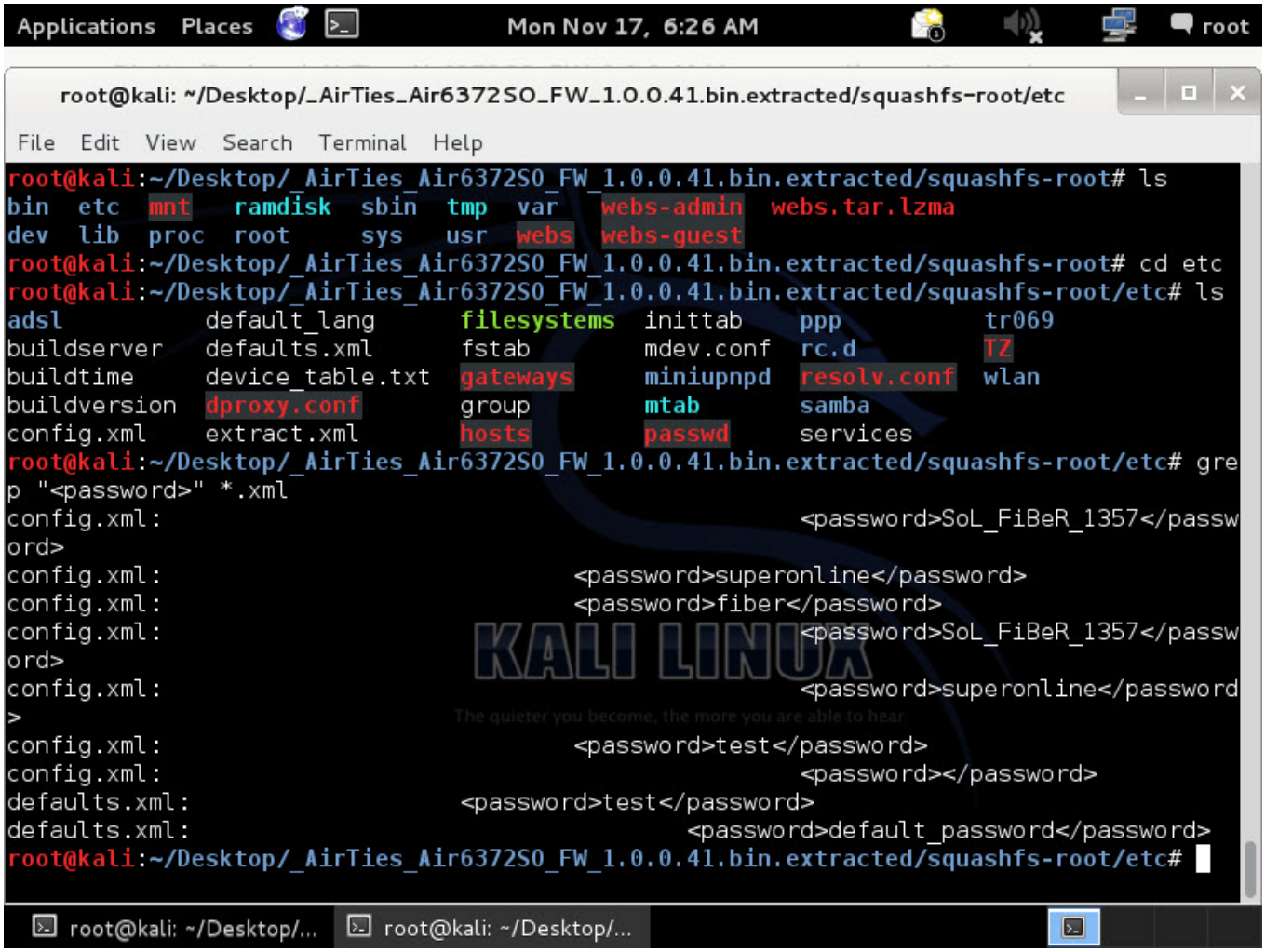
Bilmeyenler için binwalk aracından kısaca bahsetmek gerekirse, bu araç belirtilen donanım yazılımını otomatik olarak analiz ederek eğer sıkıştırılmış (compressed) ise öncelikle açarak içindeki dosyaları, dosya sistemi hiyerarşisine uygun olarak ilgili klasöre kopyalamaktadır. Siz de daha sonra kopyalanan bu dosyaları teker teker inceleyerek donanım yazılımı içinde yer alan yazılımlar, metin belgeleri hakkında fikir sahibi olabilir, konfigürasyon dosyalarını kolaylıkla inceleyebilirsiniz.

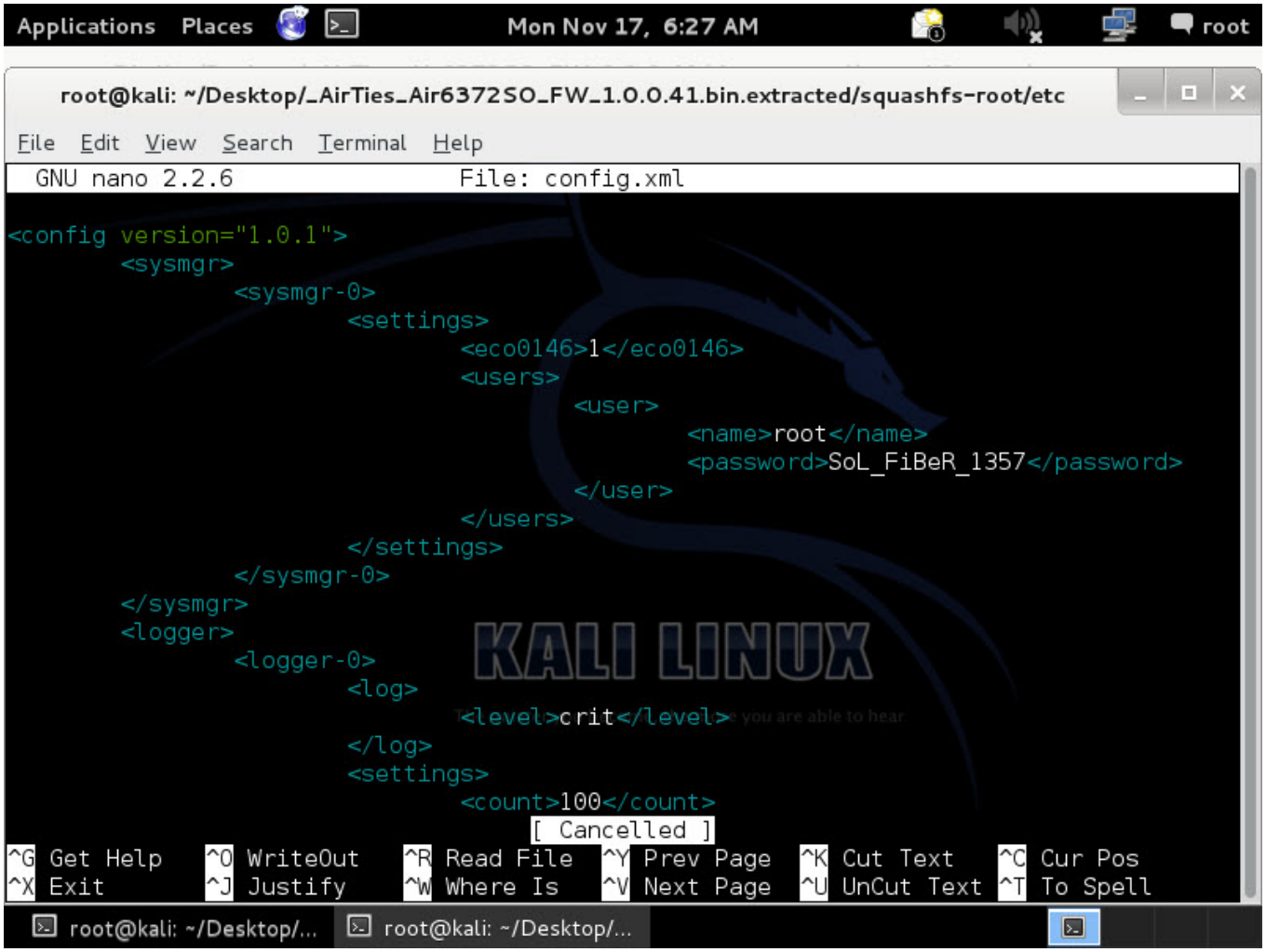
binkwalk aracına -e parametresi ile tüm donanim yazılımlarını (*.bin) analiz ettirdikten sonra teker teker her bir açılan klasörün içine bakmak yerine 2323 bağlantı noktasını tüm *extracted* geçen (binwalk açtığı donanım yazılımlarını bu şekilde isimlendiriyor) klasör isimleri içinde grep aracı ile aramaya başladım.

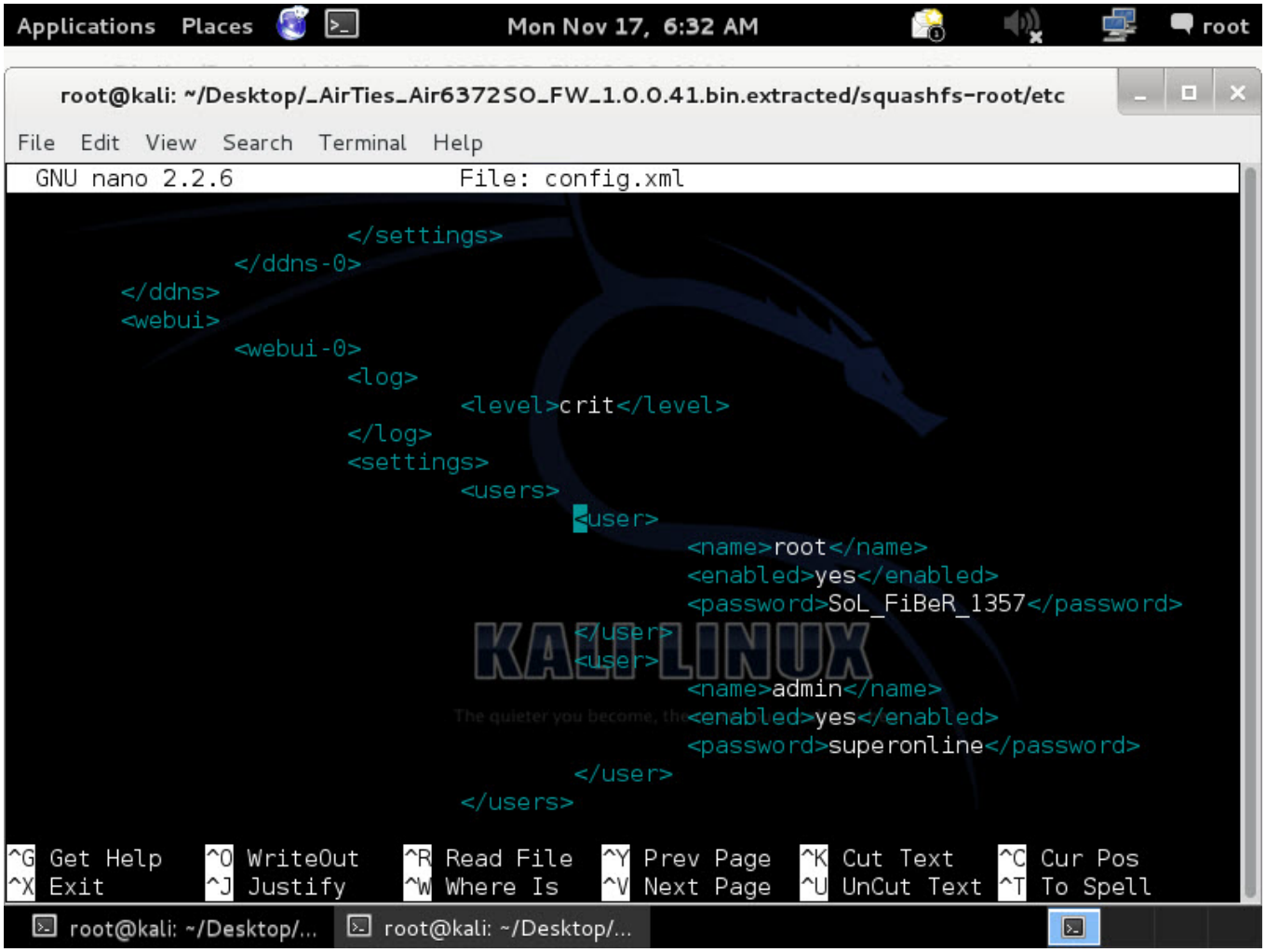


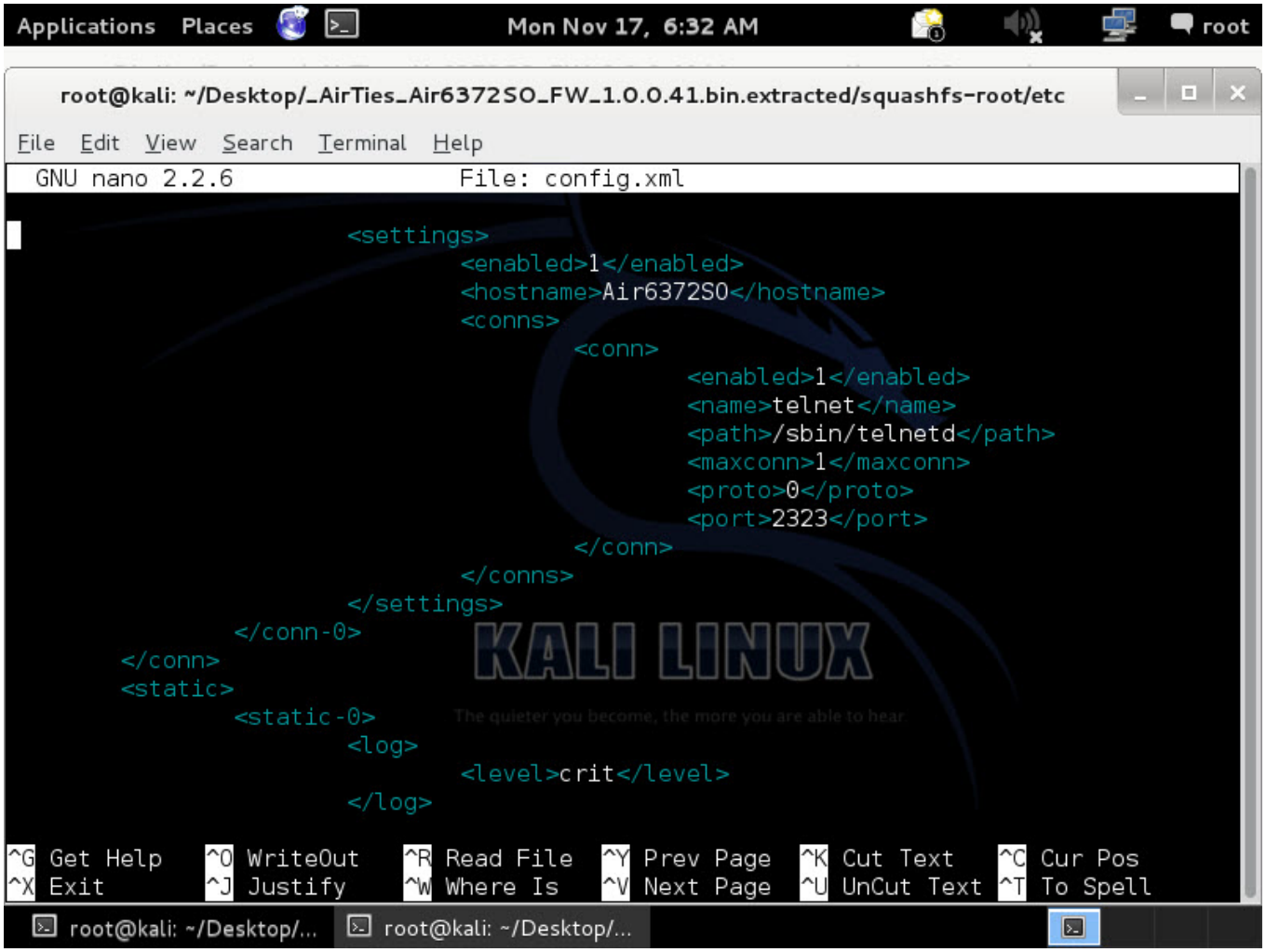
Grep aracının çıktısına göre bu varsayılan hesabın tek bir model için yani Air6372SO için geçerli olduğu olduğu görülüyordu.

config.xml dosyası içinde password kelimesini arattığımda ise iddia edilenden farklı olan SoL_FiBeR_1357 şifresi hemen dikkatimi çekti. Bu dosyaya metin editörü ile baktığımda ise bunun root şifresi olduğunu gördüm. (Airties'ın web sitesinde bu model için yer alan donanım yazılımı, Superonline için ayrıca geliştirildiği için muhtemelen şifre farklı)


Applications Places Mon Nov 17, 6:26 AM root
root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc
File Edit View Search Terminal Help
root@kali:~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root# ls
bin etc mnt ramdisk sbin tmp var webs-admin webs.tar.lzma
dev lib proc root sys usr webs webs-guest
root@kali:~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root# cd etc
root@kali:~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc# ls
adsl default_lang filesystems inittab ppp tr069
buildserver defaults.xml fstab mdev.conf rc.d TZ
buildtime device_table.txt gateways miniupnpd resolv.conf wlan
buildversion dproxy.conf group mtab samba
config.xml extract.xml hosts passwd services
root@kali:~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc# gre
p "<password>" *.xml
config.xml: <password>SoL_FiBeR_1357</passw
ord>
config.xml: <password>superonline</password>
config.xml: <password>fiber</password>
config.xml: <password>SoL_FiBeR_1357</passw
ord>
config.xml: <password>superonline</password
>
config.xml: <password>test</password>
config.xml: <password></password>
defaults.xml: <password>test</password>
defaults.xml: <password>default_password</password>
root@kali:~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc#
root@kali: ~/Desktop/... root@kali: ~/Desktop/...


Applications Places
Mon Nov 17, 6:27 AM
root
root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc
File Edit View Search Terminal Help
GNU nano 2.2.6 File: config.xml
<config version="1.0.1">
<sysmgr>
<sysmgr-0>
<settings>
<eco0146>1</eco0146>
<users>
<user>
<name>root</name>
<password>SoL_FiBeR_1357</password>
</user>
</users>
</settings>
</sysmgr-0>
</sysmgr>
<logger>
<logger-0>
<log>
<level>crit</level>
</log>
<settings>
<count>100</count>
[Cancelled]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
root@kali: ~/Desktop/...
root@kali: ~/Desktop/...


Applications Places Mon Nov 17, 6:32 AM root
root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc
File Edit View Search Terminal Help
GNU nano 2.2.6 File: config.xml
</settings>
</ddns-0>
</ddns>
<webui>
<webui-0>
<log>
<level>crit</level>
</log>
<settings>
<users>
<user>
<name>root</name>
<enabled>yes</enabled>
<password>SoL_FiBeR_1357</password>
</user>
<user>
<name>admin</name>
<enabled>yes</enabled>
<password>superonline</password>
</user>
</users>
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
root@kali: ~/Desktop/... root@kali: ~/Desktop/...



Tabii bende bu marka ve model modem olmadığı için bu kullanıcı adı ve şifrenin doğru olup olmadığını teyit etmek için hemen bir tweet göndererek takipçilerimden yardım istedim ve çok geçmeden hard_ress Twitter hesabından bu kullanıcı adı ve şifre ile modeme telnet üzerinden bağlanılabilindiği bilgisi geldi.

Aslında bunun gibi uzaktan destek amacıyla modemlere, ağ cihazlarına tanımlanan hesaplara ara ara rastlanmakta ve güvenlik araştırmacıları tarafından bunlar ortaya çıkarılmaktadır. Bunların ortaya çıkarılmasının kullanıcılar açısından en önemli kısmı ise, kötüye kullanılabilecek bu şifrelerin en kısa sürede değiştirilebilmesi veya hesapların devre dışı bırakılabilmesidir. Bende bunun için iki şifre ile ilgili olarak hemen Netsec e-posta listesine konu ile ilgili bir e-posta göndermeye karar verdim. E-postayı gönderdikten kısa bir süre sonra ise Necati ERSEN ŞİŞECİ'den gelen e-posta beni oldukça şaşırttı. Necati gönderdiği e-postada bu durumu Ocak 2014'de tespit ettiğini ve Superonline ile paylaştığını belirtiyordu (neden Airties değil de Superonline diye soracak olursanız bunun sebebi bu donanım yazılımının Airties firması tarafından Superonline için geliştirilmiş olması) fakat aradan geçen 9 ayda bu konu ile olarak ilgili donanım yazılımında hala

bir düzeltme yapılmamıştı.

N. Ersen SISECI via netsectr.org
to liste

10:34 PM (15 hours ago)

Turkish › English Translate message Turn off for: Turkish

Merhaba,

Her iki parolayı da 23 Ocak'da SüperOnline'a bildirmiştim. Uzaktan telnet ile veya root kullanıcı adı ve parolası ile web arayüzünden de girilebiliyor.

Ben bildirdiğim zaman 6372SO için 1.0.0.49 olan sürüm sahada kullanılıyordu. İlk parolayı kendi modemimin yedeğini alıp, içerisinden çıkartmıştım. İkinci parolayı ise, Firmware Mod Kit ile çıkartmıştım. Her iki yöntemi de SuperOnline'a detaylıca anlatan bir mail atmıştım.

SuperOnline, AirTies dan yeni firmware istemişti. AirTies, 1.0.0.52 sürümünü çıkardı ve bu sürümde, (base64 ile encode edilmiş yedekten root şifresi çıkartılamasın diye sanırım) yedek alma özelliği kapatıldı. Bu sürümde yedek alınamıyor. Bu sürüm ile sahadaki bir çok cihaz güncellendi ancak halen daha aynı parolalarla girilebiliyordu. Sanırım şu an hala en güncel sürüm 1.0.0.52.

Defalarca SüperOnline ile mailleştim ancak sonuç ortada. 9 ay oldu.

Umarım bir an önce sahadaki cihazları güncellerler.

Ek bilgi: root kullanıcısı ile web arayünden girildiğinde bile menü de olmayan ama TR069 menüsüne http://ModemIPAdresi/management/tr069.html adresinden ulaşılabilirsiniz.

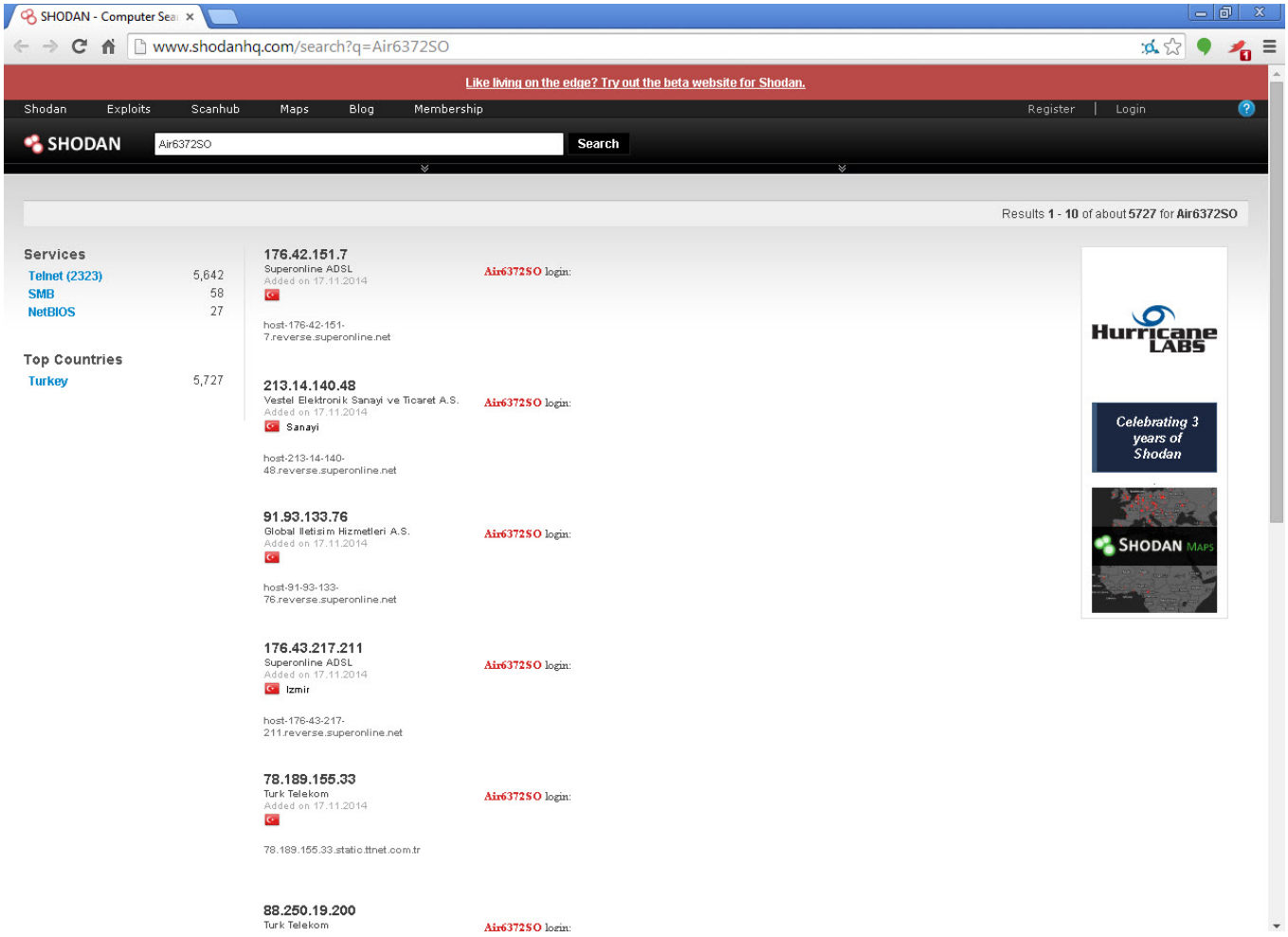
İyi geceler.

Necati Ersen ŞİŞECİ

16 Kasım 2014 17:53 tarihinde Mert SARICA <mert.sarica@gmail.com> yazdı:

Bu tür durumlarda art niyetli kişiler, modemlere uzaktan zararlı yazılım yükleme veya kullanıcıları zararlı sitelere yönlendirme girişiminde bulunabilirler dolayısıyla internet servis sağlayıcısı ve üretici firma tarafından bu tür zafiyetlerin en kısa sürede ortadan kaldırılması gerekmektedir.

Air6372SO modelini Shodan üzerinde arattığımda ise modem sayısının hiç de azımsanmayacak kadar çok olduğunu (10000+) gördüm.



Önlem olarak bu marka model modem kullanan kullanıcılara acil olarak port 2323 üzerinden bu şifreler ile modemlerine bağlanıp bağlanamadıklarını kontrol edip root şifrelerini değiştirmeleri gerekmektedir.

Bu hesabın internet servis sağlayıcısı ve üretici firma işbirliği ile en kısa sürede donanım yazılımlarından kaldırılması dileğiyle 2014 yılının bu son yazısı ile 2015 yılının herkese önce sağlık sonra mutluluk getirmesini dilerim.