

İÇERİK

Donanım yazılımı (firmware) nedir ?

Neden analiz edilmelidir ?

Analiz yöntemleri ve araçları

Örnek analizler

Sonuç



BEN KİMİM?

Sızma Testi Uzmanı

Mesai saatlerinde

Zararlı Yazılım Analisti

Mesai saatlerinde ve boş zamanlarımda

Öğretim Görevlisi

**Bahçeşehir Üniversitesi
Siber Güvenlik Yüksek Lisans Programı**

Blog Yazarı

<https://www.mertsarica.com>

Güvenlik TV

<http://www.guvenliktv.org>

Sertifika Koleksiyoncusu

**CISSP , SSCP , OSCP , OPST , CREA,
CEREA**



MESLEĞİM

Finans sektörünün ihtiyaçlarına ve günün teknolojilerine uygun hizmetler sunan, ürünler meydana getiren, NBG Grup şirketlerinden **Finansbank**'ın Bilgi Teknolojileri iştiraki olan **IBTech** firmasında Kıdemli Sızma Testi Uzmanı olarak çalışmaktayım.

<http://www.finansbank.com.tr>

<http://www.ibtech.com.tr>



DONANIM YAZILIMI NEDİR VİKİ ?

Donanım yazılımı

Vikipedi, özgür ansiklopedi

Donanım yazılımı (veya **bellenim**) (İng: firmware), **sayısal veri** işleme yeteneği bulunan her tür **donanımın** kendisinden beklenen işlevleri yerine getirebilmesi için kullandığı **yazılımlara** verilen addır. **Elektronikte** ve **bilişimde** donanım yazılımı, kalıcı bellek, program kodu ve **veri deposudur**. Donanım yazılımının bulunduğu cihazlara tipik örnekler; (**beyaz eşya**, **elektronik saat**, trafik lambaları gibi) **gömülü sistemler**, bilgisayar çevre birimleri, **cep telefonu**, **dijital fotoğraf makinesi** verilebilir. Bu cihazlarda bulunan yazılım, cihazın kontrol **programını** barındırır. Donanım yazılımı ROM, EPROM, **flaş bellek** gibi kalıcı bellekte saklanır. Bir cihaz yazılımının değiştirilmesi, cihazın ömrü boyunca ya hiç yapılmaz ya da sadece birkaç kez yapılır. Bazı cihazların yazılımları üretim aşamasından sonra değiştirilemez. Donanım yazılımında güncelleştirme ya **yazılım hatası** ya da cihaza yeni bir özellik eklemek için yapılır. Bunun için **mikroçip** ROM'u değiştirilmesi gerekebilir veya flaş belleğin özel bir yöntemle tekrar **programlanması** gerekir. Bilgisayardaki BIOS yazılımı yalnızca, cihazın temel işlevlerini saklar, **işletim sistemi** gibi yüksek seviye yazılımlara ön ayak olur.

Donanım yazılımları genellikle kullanılan **mikroişlemcinin komut seti** ile yazılmış olan yazılımlardır. Bazı mikroişlemci kontrollü elektronik donanımların yazılımları; olası hata ve eksikliklerin giderilmesi veya güncel gereksinimlerin karşılanabilmesi gibi amaçlar ile yenilenebilir.



DONANIM YAZILIMLARI



NEDEN DONANIM YAZILIMI ANALİZİ ?

Güvenliğiniz için

Zafiyet araştırması için

Ödül programları (bug bounty) için

Merakınızı gidermek için



NEDEN DONANIM YAZILIMI ANALIZI ?

OCTOBER 14, 2013

Backdoor found in D-Link router firmware

Advisory (ICSA-14-073-01)

[More Advisories](#)

Siemens SIMATIC S7-1500 CPU Firmware Vulnerabilities

Original release date: March 14, 2014 | Last revised: March 17, 2014



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

redirect attacks as well as privilege escalation. The vulnerabilities could be exploited over the network without authentication.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.



ANALİZ YÖNTEMLERİ

Statik Analiz:

Şifreler, gizlenmiş sayfalar, arka kapılar vb. bulunabilir.

Binwalk, firmware-mod-kit, strings, file vb. araçlar ile donanım yazılımı statik olarak analiz edilebilir.

Dinamik Analiz:

Zafiyet analizi / doğrulaması yapılabilir.

JTAG ile donanım cihazı hata ayıklayıcı ile analiz edilebilir.

UART üzerinden işletim sistemine bağlantı kurulabilir.

QEMU ile OS üzerinde yer alan dosyaları analiz edilebilir.



ÖRNEK #1 - DİNAMİK ANALİZ

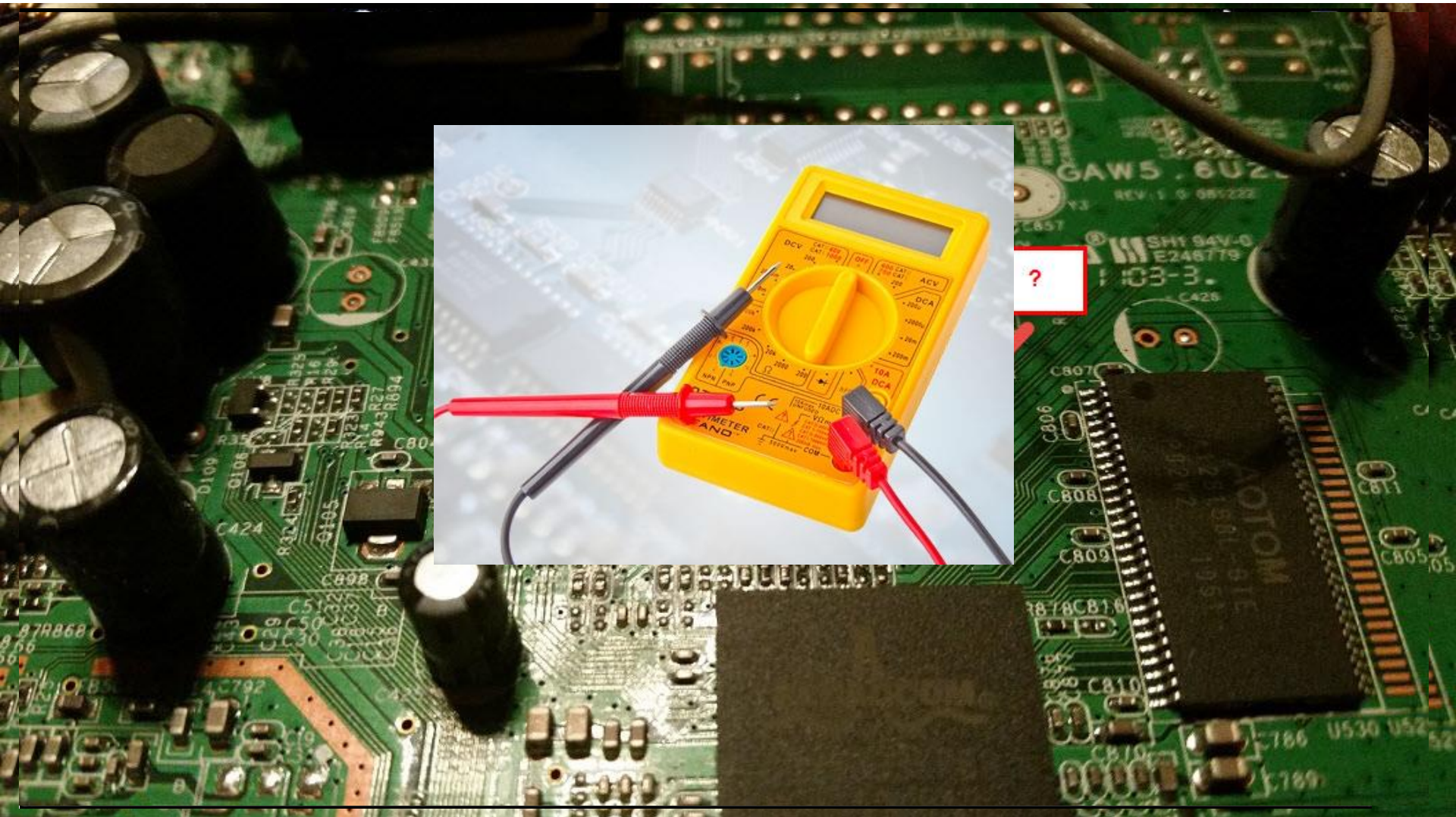
Evinizde kullandığınız modeminizin ne kadar güvenli olduğunu öğrenmek için güvenlik araştırması yapmaya karar verdiniz.

Telnet ile modeme bağlanıp, OS üzerindeki programlarda arka kapı arayacaksınız fakat telnet şifresini bilmiyorsunuz.

İhtiyaç listesi: Tornavida seti, ana kart üzerinde UART girişi, USB - TTL UART CP2104 çevirici, Putty veya SecureCRT, Dijital Avometre



ÖRNEK #1 - DİNAMİK ANALİZ



ÖRNEK #2 - STATİK ANALİZ

Evinizde kullandığınız modeminiz ile ISS'inizin, TR069 yönetim protokolü üzerinden haberleştiğini öğrendiniz.

Peki bu protokol üzerinden gelen/giden parametreler neler ?

İletişim, güvenli bir kanal üzerinden mi gerçekleşiyor?

Sorular, sorular aklınızdaki sorular ve yanıtları için;

İhtiyaç listesi: Charles veya Burp Suite Proxy, donanım yazılımı, binwalk, strings



ÖRNEK #2 - STATİK ANALİZ

Charles 3.9.2 - Session 1 *

File Edit View Proxy Tools Window Help

CWMP

Capturing from 3 interfaces [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr == 192.168.1.1 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
74	2014-06-20 16:08:53.068109000	192.168.1.1	192.168.1.34	SSDP	300	HTTP/1.1 200 OK
81	2014-06-20 16:08:56.283563000	192.168.1.1	192.168.1.34	TCP	60	iad1 > http [SYN] Seq=0 win=2800 Len=0 MSS=1400
82	2014-06-20 16:08:56.283971000	192.168.1.34	192.168.1.1	TCP	58	http > iad1 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1400
83	2014-06-20 16:08:56.285046000	192.168.1.1	192.168.1.34	TCP	60	iad1 > http [ACK] Seq=1 Ack=1 win=2800 Len=0
86	2014-06-20 16:08:56.383297000	192.168.1.1	192.168.1.34	TCP	240	[TCP segment of a reassembled PDU]
87	2014-06-20 16:08:56.582264000	192.168.1.34	192.168.1.1	TCP	54	http > iad1 [ACK] Seq=1 Ack=187 win=16800 Len=0
88	2014-06-20 16:08:56.584357000	192.168.1.1	192.168.1.34	TCP	1514	[TCP segment of a reassembled PDU]
93	2014-06-20 16:08:56.785027000	192.168.1.34	192.168.1.1	TCP	54	http > iad1 [ACK] Seq=1 Ack=1647 win=16800 Len=0
94	2014-06-20 16:08:56.786361000	192.168.1.1	192.168.1.34	TCP	1444	[TCP segment of a reassembled PDU]
95	2014-06-20 16:08:56.881494000	192.168.1.1	192.168.1.34	SSDP	360	HTTP/1.1 200 OK
98	2014-06-20 16:08:57.003451000	192.168.1.34	192.168.1.1	TCP	54	http > iad1 [ACK] Seq=1 Ack=3037 win=15410 Len=0
99	2014-06-20 16:08:57.004377000	192.168.1.1	192.168.1.34	HTTP/XML	189	POST /cwmpweb/CPemgt HTTP/1.1
104	2014-06-20 16:08:57.206218000	192.168.1.34	192.168.1.1	TCP	54	http > iad1 [ACK] Seq=1 Ack=3172 win=16800 Len=0
125	2014-06-20 16:08:57.535424000	192.168.1.34	192.168.1.1	HTTP	673	HTTP/1.1 401 Authorization Required (text/html)
128	2014-06-20 16:08:57.536558000	192.168.1.1	192.168.1.34	TCP	60	iad1 > http [ACK] Seq=3172 Ack=620 win=2181 Len=0
129	2014-06-20 16:08:57.537136000	192.168.1.1	192.168.1.34	TCP	60	iad1 > http [FIN, ACK] Seq=3172 Ack=620 win=2800 Len=0
130	2014-06-20 16:08:57.537160000	192.168.1.34	192.168.1.1	TCP	54	http > iad1 [ACK] Seq=620 Ack=3173 win=16800 Len=0
132	2014-06-20 16:08:57.538145000	192.168.1.34	192.168.1.1	TCP	54	http > iad1 [FIN, ACK] Seq=620 Ack=3173 win=16800 Len=0
133	2014-06-20 16:08:57.538897000	192.168.1.1	192.168.1.34	TCP	60	iad1 > http [ACK] Seq=3173 Ack=621 win=2800 Len=0

Size

Import Export OK Cancel Help

[root@kali: ~]



ÖRNEK #3 - STATİK & DİNAMİK ANALİZ

ISS'inizin hediye modem kampanyasından faydalanarak bir modem aldınız ve bu modem ön tanımlı ISS ayarları ile geldi.

Modemin ayarlarında zafiyete yol açan bir yapılandırma hatası veya eksikliği var mı ?

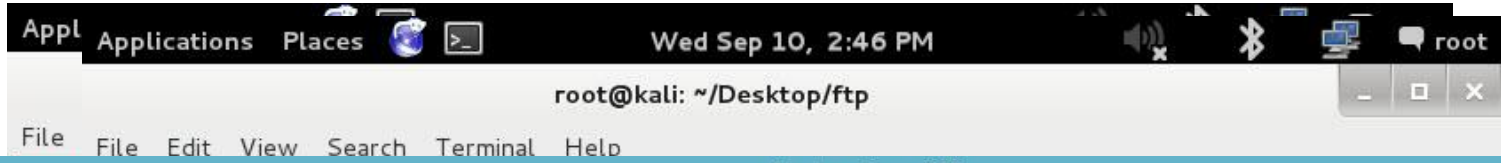
Modem donanım yazılım güncellemelerini üreticiden mi yoksa ISS'ten mi alıyor ?

Sorular, sorular aklınızdaki sorular ve yanıtları için;

İhtiyaç listesi: donanım yazılımı, binwalk, strings



ÖRNEK #3 - STATİK & DİNAMİK ANALİZ



Modem - SecureCRT
FTP - zyxeladmin@ftp.com.tr - FileZilla

Sunucu: Kullanıcı Adı: Parola: Kapı: Hızlı bağlantı

Durum: C:\Users\Mert\AppData\Local\Temp\{fz3temp-1}\empty_file_yq744zm karşıya yüklemesine başlanıyor
Komut: PASV
Yanıt: 227 Entering Passive Mode
Komut: STOR m.txt
Yanıt: 150 Connection accepted
Yanıt: 226 Transfer OK
Durum: Dosya aktarıldı, 0 bayt/1 saniye kadan aktarıldı

Yerel site: C:\Users\Mert\Desktop\ftp

Uzaktaki site:

Dosya Adı	Boyut	Tip	Son değişiklik	İzinler	Sahip/Grup
..					
.bin	18.984.768	BIN File	3.12.2013 00:48:47		
.rom	312.402	ROM File	3.12.2013 00:46:48		
m.txt	0	Text Docu...			
p.txt	0	Text Docu...	3.12.2013 00:50:28		
.bxt	0	Text Docu...	3.12.2013 00:51:35		

5 dosya. Toplam boyut: 19.297.170 bayt



ÖRNEK #4 - STATİK & DİNAMİK ANALİZ

Modemlerin yönetim sayfalarında kimi zaman zafiyetlerin kimi zaman ise arka kapıların olabileceğini biliyorsunuz.

Temmuz ayında TP-Link kullanıcılarının başına gelenleri gördükten sonra modeminizi incelemeye karar verdiniz.

**Modeminizde yer alan uygulamalarda ne tür zafiyetler var ?
Şüphelendiğiniz de nasıl doğrulayabilirsiniz ?**

(Disassemble && Debug)

İhtiyaç listesi: IDA Pro, Qemu, MIPS Assembly bilgisi, file, strings vb.



ÖRNEK #4 - STATİK & DİNAMİK ANALİZ

The screenshot shows the IDA Pro interface with the following components:

- Assembly View:**

```

00400EC8 loc_400EC8:
00400EC8 la $t9, unk_7679ECC0
00400ECC jalr $t9, getpid
00400ED0 nop
00400ED4 lw $gp, 0x1E8+var_1C8($sp)
00400ED8 move $a0, $s2
00400EDC la $a1, 0x400000
00400EE0 la $t9, CGIGetVariable
00400EE4 addiu $a1, (aUser - 0x400000) # "user"
00400EE8 move $s7, $v0
00400EEC jalr $t9, CGIGetVariable
00400EF0 move $s0, $t9
00400EF4 move $s1, $v0
00400EF8 beqz $v0, loc_400FB4
00400EFC lw $gp, 0x1E8+var_1C8($sp)

```
- Memory Dump (Hex View):**

```

$u0=MEMORY:00414040
00414040 .byte 0x60 # m
00414041 .byte 0x65 # e
00414042 .byte 0x72 # r
00414043 .byte 0x74 # t
00414044 .byte 0
00414045 .byte 0
00414046 .byte 0
00414047 .byte 0
00414048 .byte 0
00414049 .byte 0
0041404A .byte 0
0041404B .byte 0
0041404C .byte 0
0041404D .byte 0
0041404E .byte 0
0041404F .byte 0
00414050 .byte 0
00414051 .byte 0
00414052 .byte 0
00414053 .byte 0
00414054 .byte 0
00414055 .byte 0
00414056 .byte 0
00414057 .byte 0
00414058 .byte 0
00414059 .byte 0
0041405A .byte 0
0041405B .byte 0
0041405C .byte 0
0041405D .byte 0
0041405E .byte 0
0041405F .byte 0
00414060 .byte 0
00414061 .byte 0
00414062 .byte 0
00414063 .byte 0
00414064 .byte 0
00414065 .byte 0
00414066 .byte 0
00414067 .byte 0
00414068 .byte 0
00414069 .byte 0
0041406A .byte 0
0041406B .byte 0
0041406C .byte 0
0041406D .byte 0
0041406E .byte 0
0041406F .byte 0
00414070 .byte 0
00414071 .byte 0
00414072 .byte 0
00414073 .byte 0
00414074 .byte 0
00414075 .byte 0
00414076 .byte 0
00414077 .byte 0
00414078 .byte 0
00414079 .byte 0
0041407A .byte 0
0041407B .byte 0
0041407C .byte 0
0041407D .byte 0
0041407E .byte 0
0041407F .byte 0
00414080 .byte 0
00414081 .byte 0
00414082 .byte 0
00414083 .byte 0
00414084 .byte 0
00414085 .byte 0
00414086 .byte 0
00414087 .byte 0
00414088 .byte 0
00414089 .byte 0
0041408A .byte 0
0041408B .byte 0
0041408C .byte 0
0041408D .byte 0
0041408E .byte 0
0041408F .byte 0
00414090 .byte 0
00414091 .byte 0
00414092 .byte 0
00414093 .byte 0
00414094 .byte 0
00414095 .byte 0
00414096 .byte 0
00414097 .byte 0
00414098 .byte 0
00414099 .byte 0
0041409A .byte 0
0041409B .byte 0
0041409C .byte 0
0041409D .byte 0
0041409E .byte 0
0041409F .byte 0
004140A0 .byte 0
004140A1 .byte 0
004140A2 .byte 0
004140A3 .byte 0
004140A4 .byte 0
004140A5 .byte 0
004140A6 .byte 0
004140A7 .byte 0
004140A8 .byte 0
004140A9 .byte 0
004140AA .byte 0
004140AB .byte 0
004140AC .byte 0
004140AD .byte 0
004140AE .byte 0
004140AF .byte 0
004140B0 .byte 0
004140B1 .byte 0
004140B2 .byte 0
004140B3 .byte 0
004140B4 .byte 0
004140B5 .byte 0
004140B6 .byte 0
004140B7 .byte 0
004140B8 .byte 0
004140B9 .byte 0
004140BA .byte 0
004140BB .byte 0
004140BC .byte 0
004140BD .byte 0
004140BE .byte 0
004140BF .byte 0
004140C0 .byte 0
004140C1 .byte 0
004140C2 .byte 0
004140C3 .byte 0
004140C4 .byte 0
004140C5 .byte 0
004140C6 .byte 0
004140C7 .byte 0
004140C8 .byte 0
004140C9 .byte 0
004140CA .byte 0
004140CB .byte 0
004140CC .byte 0
004140CD .byte 0
004140CE .byte 0
004140CF .byte 0
004140D0 .byte 0
004140D1 .byte 0
004140D2 .byte 0
004140D3 .byte 0
004140D4 .byte 0
004140D5 .byte 0
004140D6 .byte 0
004140D7 .byte 0
004140D8 .byte 0
004140D9 .byte 0
004140DA .byte 0
004140DB .byte 0
004140DC .byte 0
004140DD .byte 0
004140DE .byte 0
004140DF .byte 0
004140E0 .byte 0
004140E1 .byte 0
004140E2 .byte 0
004140E3 .byte 0
004140E4 .byte 0
004140E5 .byte 0
004140E6 .byte 0
004140E7 .byte 0
004140E8 .byte 0
004140E9 .byte 0
004140EA .byte 0
004140EB .byte 0
004140EC .byte 0
004140ED .byte 0
004140EE .byte 0
004140EF .byte 0
004140F0 .byte 0
004140F1 .byte 0
004140F2 .byte 0
004140F3 .byte 0
004140F4 .byte 0
004140F5 .byte 0
004140F6 .byte 0
004140F7 .byte 0
004140F8 .byte 0
004140F9 .byte 0
004140FA .byte 0
004140FB .byte 0
004140FC .byte 0
004140FD .byte 0
004140FE .byte 0
004140FF .byte 0

```
- General registers:**
 - ZERO 00000000 MEMORY:dword_0
 - AT FFFFFFFF8
 - U0 00414040 MEMORY:00414040
 - U1 00414044 MEMORY:00414044
 - A0 00414043 MEMORY:00414043
 - A1 00000000 MEMORY:dword_0
 - A2 00414045 MEMORY:00414045
- Exports:**

```

00400F1C beqz $v0, loc_400FA4
00400F20 lw $gp, 0x1E8+var_1C8($sp)

```
- Dialog Box:**

Save network settings as default

OK Cancel Help



ÖRNEK #5 - DÜNYADAN

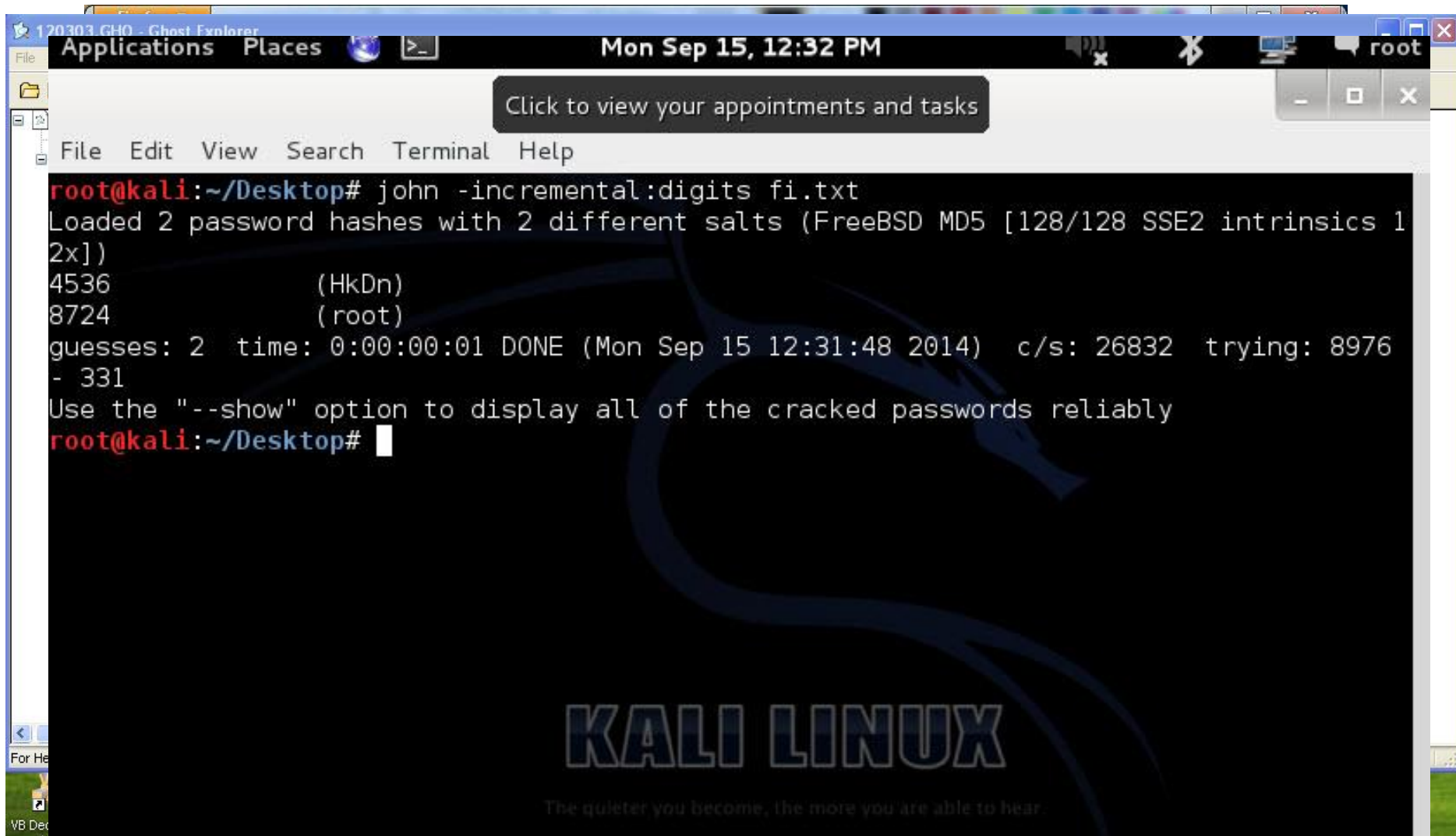
Donanım yazılımınızın peşinde rakipleriniz, dolandırıcılar, casuslar olabilir.

Donanım yazılımınızı internette paylaşım açmadan önce mutlaka sıkılaştırmanız gerekmektedir.

Aksi halde zafiyetlerin keşfedilmesi ve kötüye kullanılması düşündüğünüzden daha da kısa (Retweet) sürebilir.



ÖRNEK #5 - DÜNYADAN



```
120303.GHO - Ghost Explorer
Applications Places >_ Mon Sep 15, 12:32 PM root
Click to view your appointments and tasks
File Edit View Search Terminal Help
root@kali:~/Desktop# john -incremental:digits fi.txt
Loaded 2 password hashes with 2 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 1
2x])
4536          (HkDn)
8724          (root)
guesses: 2   time: 0:00:00:01 DONE (Mon Sep 15 12:31:48 2014)  c/s: 26832  trying: 8976
- 331
Use the "--show" option to display all of the cracked passwords reliably
root@kali:~/Desktop#
```

KALI LINUX
The quieter you become, the more you are able to hear.

DONANIM YAZILIMI MANİPÜLASYONU

Donanım yazılımını yamamak (patch) için **firmware-mod-kit** aracından faydalanabilirsiniz.

./extract-firmware ile donanım yazılımını açabilirsiniz.

fmk klasöründe bulunan donanım yazılımına ait olan dosyaları değiştirdikten sonra **./build-firmware.sh** ile paketleyebilirsiniz.



DONANIM YAZILIMI MANİPÜLASYONU

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# /opt/firmware-mod-kit/extract-firmware.sh /opt/firmware-mod-kit/
FW_1.2.0.36.bin
Firmware Mod Kit (extract) 0.99, (c)2011-2013 Craig Heffner, Jeremy Collake

Scanning firmware...

Scan Time:      2014-09-15 15:38:13
Signatures:     193
Target File:    /opt/firmware-mod-kit/..._1.2.0.36.bin
MD5 Checksum:  832f413b5cd21111cfdbcalc8bc17908

DECIMAL      HEX      DESCRIPTION
-----
168          0xA8     uImage header, header size: 64 bytes, header CRC
: 0x969D559A, created: Thu Dec 29 11:15:04 2011, image size: 2727936 bytes, Data
Address: 0x0, Entry Point: 0x0, data CRC: 0xE8484B9A, OS: Linux, CPU: MIPS, ima
ge type: Filesystem Image, compression type: lzma, image name: "RT-206v4TT RootF
S"
232          0xE8     Squashfs filesystem, big endian, lzma signature,
version 3.0, size: 2725690 bytes, 470 inodes, blocksize: 65536 bytes, created:
Thu Dec 29 11:15:04 2011
2728168     0x29A0E8 uImage header, header size: 64 bytes, header CRC
: 0xD039D69, created: Wed Dec 21 11:59:33 2011, image size: 758140 bytes, Data A
Address: 0x80010000, Entry Point: 0x80228000, data CRC: 0x160F6F4A, OS: Linux, CP
U: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux
root@kali:~#
  
```

SONUÇ

Donanımlar kapalı kutudan ibaret değildir, donanım yazılımına ulaşmak ve içeriğini görüntülemek oldukça kolay olabilir.

Donanım yazılımlarında tespit edilen bir zafiyetin kötüye kullanımının etkisi çok yüksek olabilir.

Donanımlarda kullanılan işletim sistemleri, modern işletim sistemleri kadar güvenli değildir.

Donanım yazılımları meraklı kişilerce açılabilir, değiştirilebilir ve tekrar paketlenir. (imza kontrolü)





SORULAR?



TEŞEKKÜRLER

mert.sarica@gmail.com

<https://www.mertsarica.com>

<https://twitter.com/mertsarica>

