

Donanım Yazılımı Analizinin Önemi

written by Mert SARICA | 1 October 2015

Her siber güvenlik konferansında gerçekleştirdiğim sunumundan sonra olduğu gibi yine geleneği bozmayarak, 2014 yılında IstSec ve geçtiğimiz Eylül ayında Hacktrick siber güvenlik konferanslarında gerçekleştirdiğim donanım yazılımı (bellenim / firmware) analizi sunumundan sonra sunuma katılmayanlar için sunumu özetleyen bir blog yazısı yazmaya karar verdim.

Nesnelerin İnterneti (IoT) dediğimiz kavram hayatımıza girdi gireli, evimizde internete bağlanan birçok cihaz olduğunu görebiliyoruz. Bunlar arasında uydu alıcıları, ip kameraları, cep telefonlarını, raspberry pi gibi mini bilgisayarları en çok rastlanan nesnelere arasında sayabiliriz. Hacktrick sunumunda, evinde 7/24 çalışan Raspberry Pi, Beagle Bone gibi mini bilgisayarları olanlar el kaldırsın dediğimde, havaya kalkan ellerin sayısının beklediğimden fazla olduğunu söyleyebilirim. Durum böyle olunca da IoTler, akıllı cihazlar ve benzerleri, hayatımıza getirdikleri kolaylıkların yanında güvenlik risklerini de beraberinde getiriyorlar dersek pek yanılmayız.

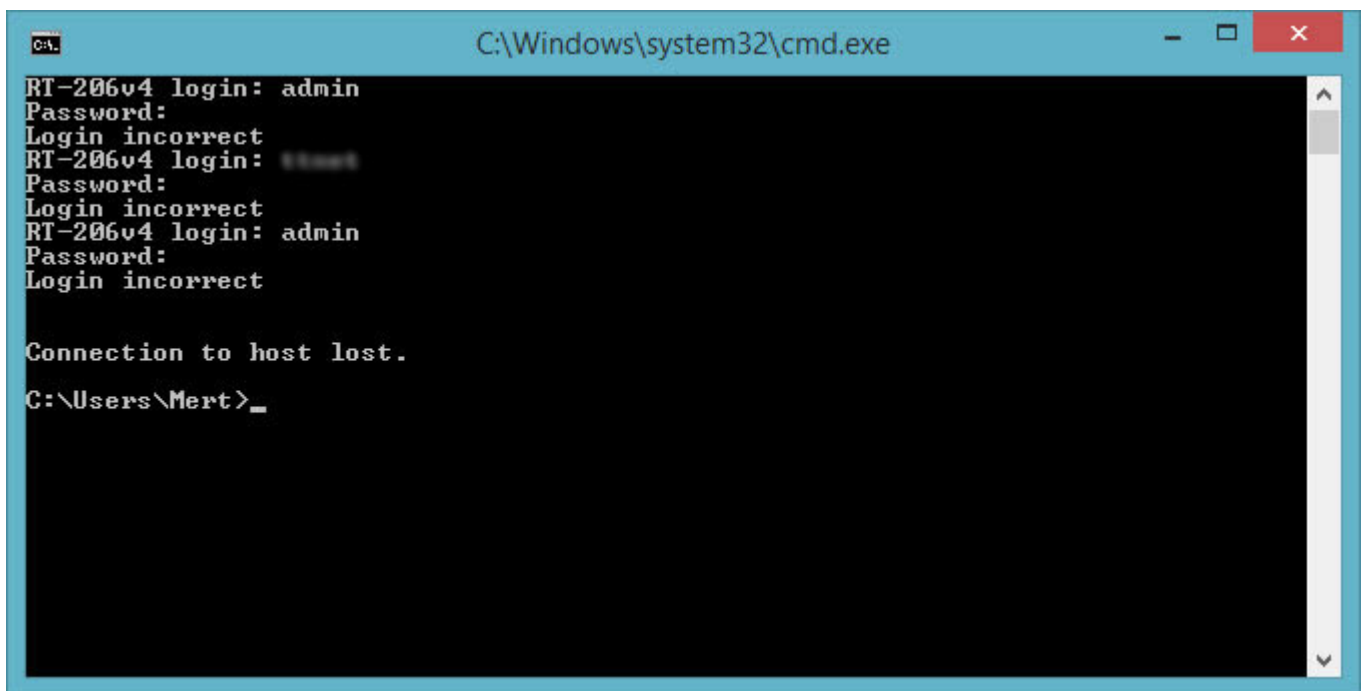
Aslında evlerimize soktuğumuz cihazlar akıllandıkça, casus olma potansiyeline de sahip olmaya başladılar. Hareketle kontrol edilen kameralı, akıllı televizyonunuz hacklendiğinde, başınıza gelebilecekleri bir düşünün, sevimsiz öyle değil mi ? :) Aslında haberlere baktığımızda bu söylediklerimin çok da uzak bir ihtimal olmadığını görüyoruz. Ağustos ayında Samsung'un akıllı buzdolabının hacklenerek Gmail kullanıcı adı ve şifre bilgilerinin çalınabildiği ortaya çıktı.

Bu tür cihazların hacklenebilmesi, modern işletim sistemlerine (Windows, Linux vs.) kıyasla daha kolay oluyor çünkü bu cihazlar çoğunlukla düşük donanımlarla çalışıyorlar. Düşük donanım dediğimizde de, ram, işlemci ve işletim sistemi açısından zayıf/kısıtlı olan bu cihazlar üzerinde örneğin Address Space Layout Randomization (ASLR), data execution prevention (DEP) gibi istismarı engelleyici kontroller bulunamayabiliyor. Donanım yazılımı geliştiricileri, modern işletim sistemi geliştiricileri gibi güvenliğe ön planda tutmadıkları için de çoğunlukla cihazlar üzerinde yer alan konfigürasyonlar örneğin modemlerde olduğu gibi zayıf ve istismara açık olabiliyor.

Bu cihazların güvenliđi istenilen seviyelerde olmadıđı srece, gvenlik uzmanları ve son kullanıcılar olarak, ev ađımızda yer alan bu cihazların donanım yazılımlarını analiz ederek gvenlik zafiyetlerini tespit etmek, hem merakımızı gidermek iin hem de bu cihazları gvenli bir Őekilde kullanmak isteyen bizler iin bir gereksinim haline gelebiliyor.

rneđin elimizde internet servis sađlayıcısı tarafından bize kampanya dahilinde hediye edilmiŐ bir modem var ve bu modeme ynetici arayznden bađlanıp, modem zerinde tanımlı kullanıcılar grntlemek istiyoruz. Neden bunu istiyoruz unk modemler zerinde kimi zaman varsayılan ynetici yetkisine sahip hesaplar olabiliyor veya internet servis sađlayıcısı uzaktan destek amacıyla kolay tahmin edilebilir parolaya sahip kullanıcı hesaplarını modemlere tanımlayabiliyorlar. Varsayılan hesaplar dıŐında modem ynetici arayzne giriŐ yaptığımızda gremediğimiz ancak ilgili sayfayı direk ađırdığımızda ulaŐabileceğimiz ve modem zerindeki zel ayarları (TR-069 ynetim protokol ayarları gibi) deđiŐtirmemizi sađlayan gizli sayfalar olup olmadığını da kontrol etmek istiyoruz. Bu sorulara yanıt bulmak iin modem ve modem donanım yazılımı zerinde eŐitli kontroller gerekleŐtirebiliriz.

Gizli ynetici hesaplarını bulmak iin yapacađımız ilk iŐ, modem telnet servisine bađlandıktan sonra cat /etc/passwd komutu yazarak mevcut hesapları kontrol etmek olabilir ancak iŐler her zaman dŐndgmz kadar kolay olmayabilir. Birincisi, ynetim paneline eriŐmek iin kullandıđımız kullanıcı adı ve Őifrenin telnet servisine eriŐmek iin yetkisi olmayabilir veya telnet servisi (telnetd) modem zerinde aık/ykl olmayabilir.

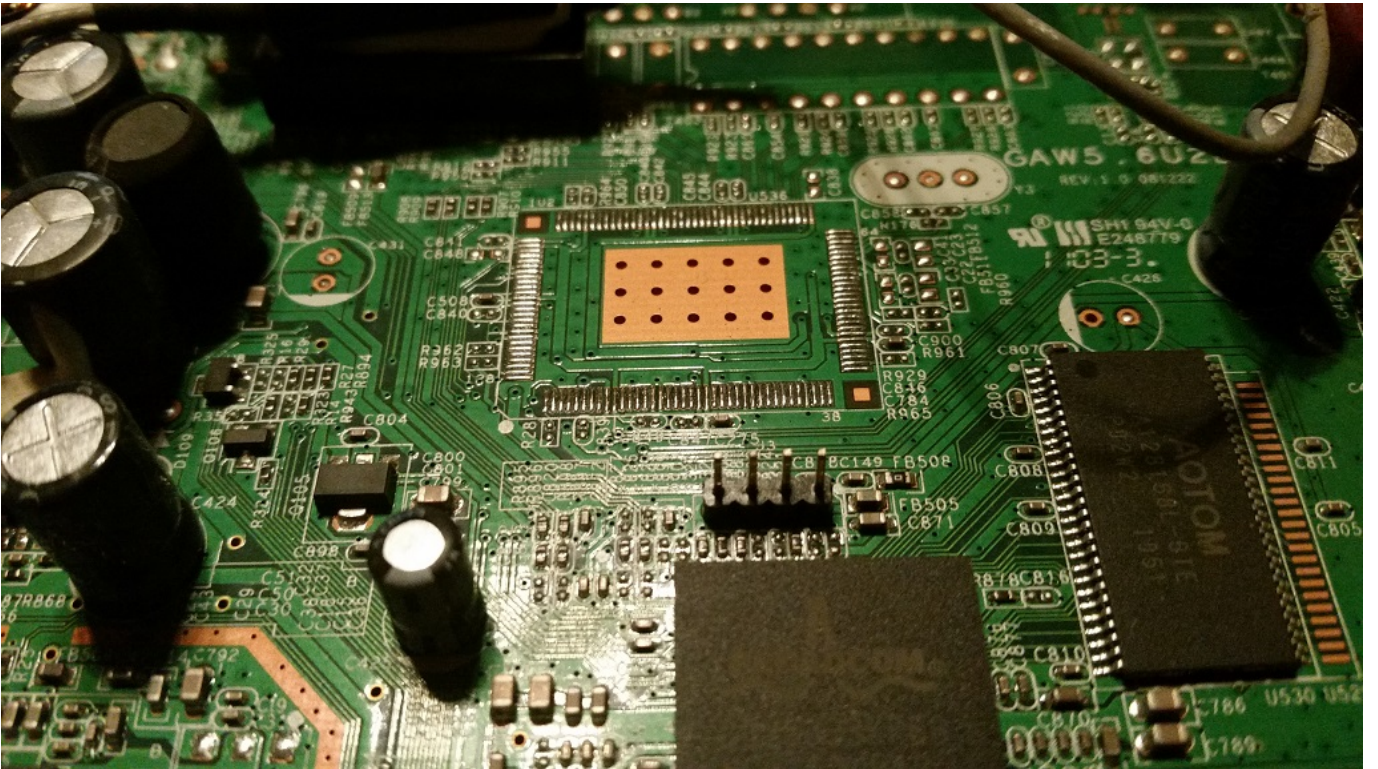


```
C:\Windows\system32\cmd.exe
RT-206v4 login: admin
Password:
Login incorrect
RT-206v4 login: *****
Password:
Login incorrect
RT-206v4 login: admin
Password:
Login incorrect

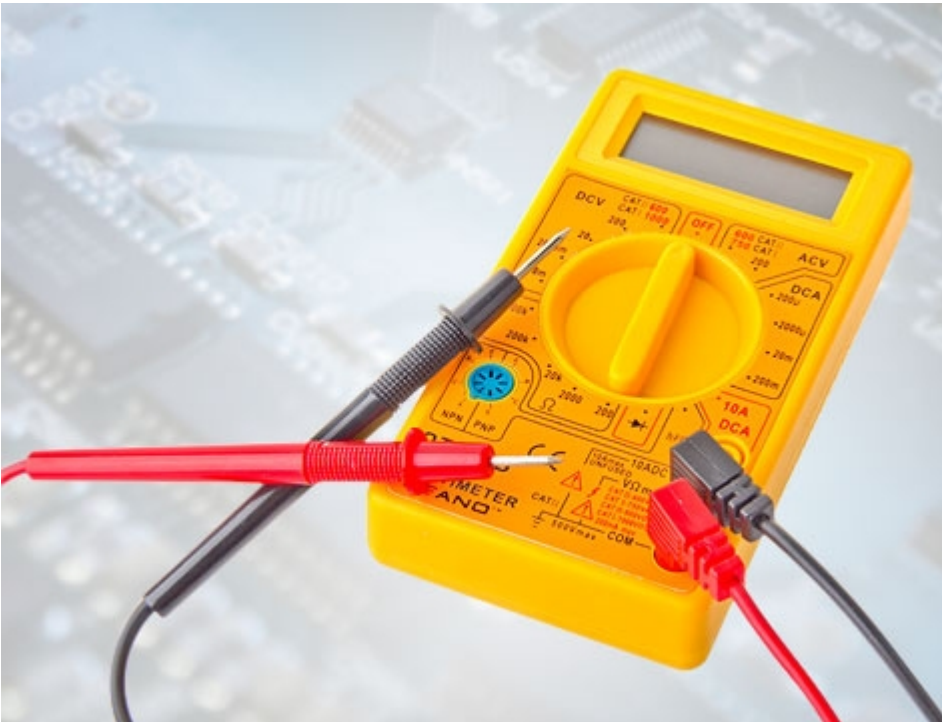
Connection to host lost.
C:\Users\Mert>_
```

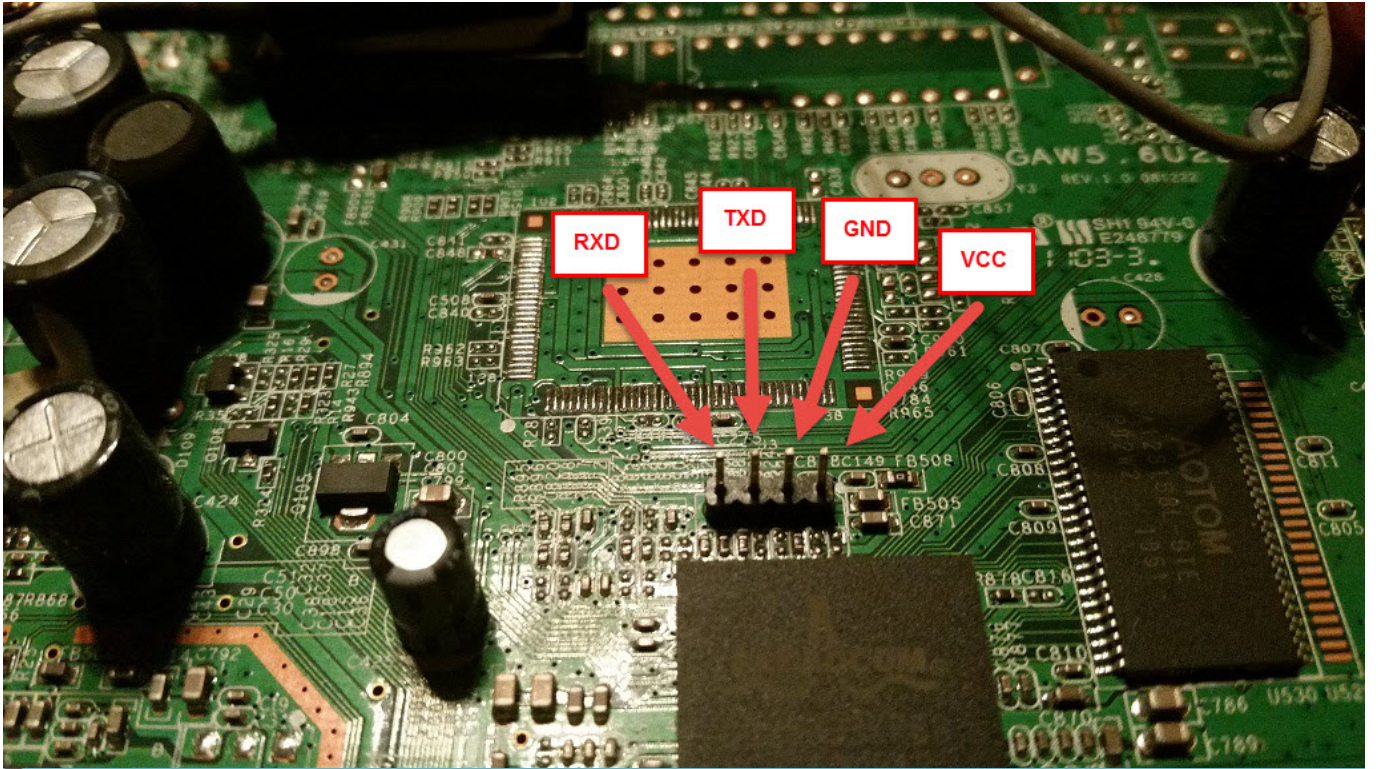


Böyle bir durumda yapmamız gereken bir tornavida seti olarak modemi açmak ve üzerinde UART seri bağlantı noktası aramak olabilir. Şanslıysak 4 PIN'den oluşan bu bağlantı noktasını çok geçmeden tespit edebiliriz.



Tabii bu seri bağlantı noktası üzerinden modem ile iletişim kurabilmek için USB – TTL UART CP2104 çevirici gibi bir ağıta ihtiya duyacağız. Ağıtı baėlamak iin ncelikle o drt pinden hangisi veri almak (RX), hangisi veri gndermek (TX) ve hangisi topraklama (GND) iin kullanılıyor onu bilmemiz gerekiyor. Srekli test sayesinde Dijital Avometre / Multimetre'de siyah ucu topraėa (iřaretli bir kutup), kırmızı ucu ise pinlere sırasıyla dokundurduğumuzda bir ses duyuyorsak o zaman bu pinin toprak (GND) pini olduėunu anlayabiliriz. Ardından RX, TX pinlerini ve baud oranını deneme yanılma yolu ile SecureCRT veya Putty ile tespit ederek komut satırına erişim sağlayabiliriz.





serial-com6 - SecureCRT

```
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
serial-com6 x
Copyright (C) 1998-2007 Erik Andersen, Rob Landley, Denys Vlasenko
and others. Licensed under GPLv2.
See source distribution for full notice.

Usage: busybox [function] [arguments]...
or: function [arguments]...

BusyBox is a multi-call binary that combines many common Unix
utilities into a single executable. Most people will create a
link to busybox for each function they wish to use and BusyBox
will act like whatever it was invoked as!

Currently defined functions:
l, [[, ash, cat, chmod, cp, date, dhcprelay, dmesg, echo,
false, free, halt, hostname, httpd, ifconfig, init, insmod,
kill, klogd, login, ls, lsmmod, mkdir, modprobe, mount,
pidof, ping, poweroff, ps, reboot, rm, rmdir, route, sh,
sleep, telnetd, test, tftp, true, udhcpd, umount,
vconfig, wget

# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.2.0 * 255.255.255.0 U 0 0 0 0 br0.1
127.0.0.0 * 255.0.0.0 U 0 0 0 0 lo

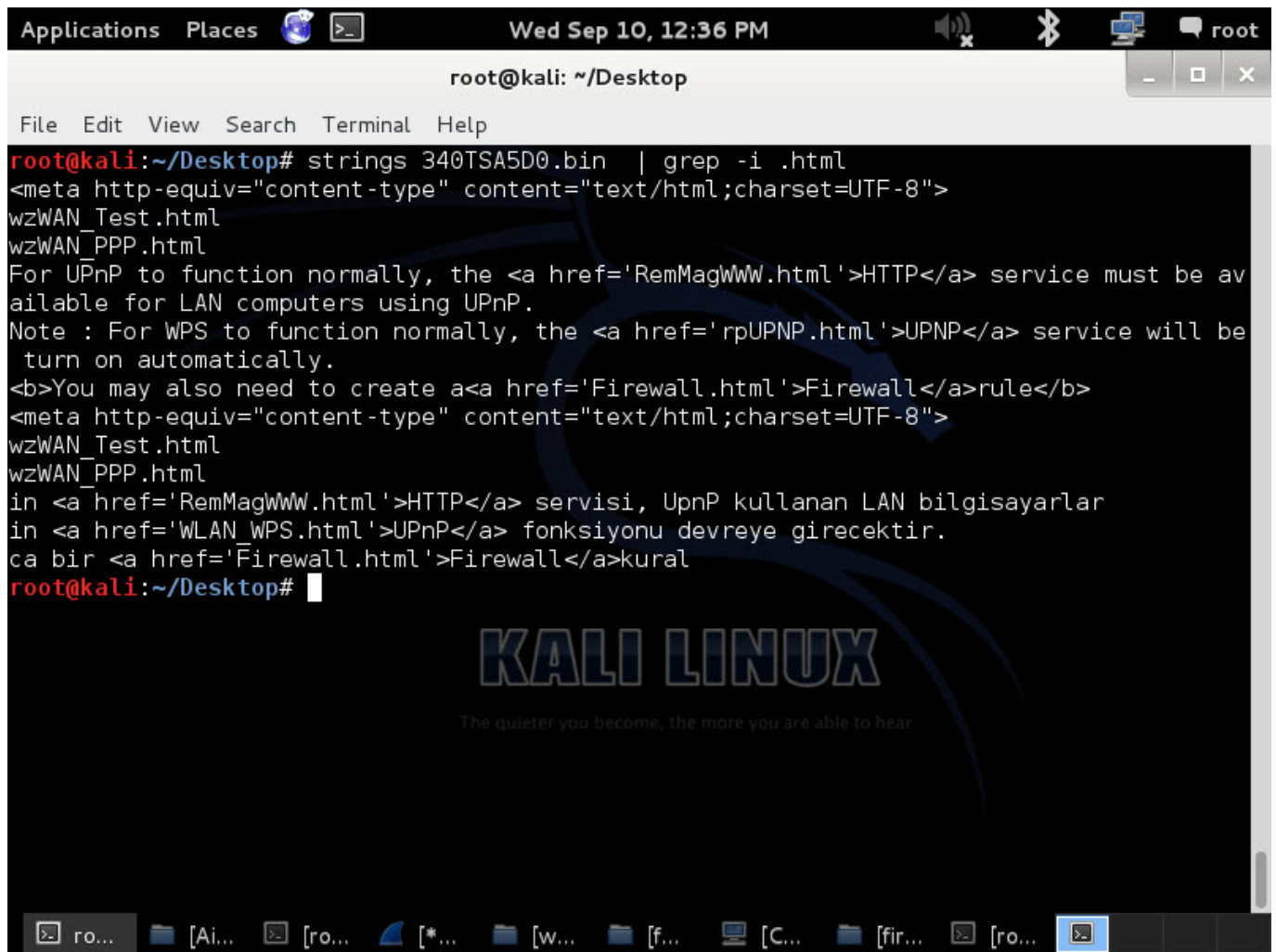
# ls -al
drwxr-xr-x 2 0 0 0 Jan 1 00:00 socks
drwxr-xr-x 2 0 0 0 Jan 1 00:00 tmp
drwxr-xr-x 3 0 0 0 Jan 1 00:01 run
drwxr-xr-x 3 0 0 0 Jan 1 00:00 lib
drwxr-xr-x 2 0 0 0 Jan 1 00:00 fyl
drwxr-xr-x 2 0 0 0 Jan 1 00:00 asd
drwxr-xr-x 2 0 0 0 Jan 1 00:00 cache
drwxr-xr-x 2 0 0 0 Jan 1 00:00 log
drwxr-xr-x 2 0 0 0 Jan 1 00:00 mnt
drwxr-xr-x 3 0 0 0 Jan 1 00:00 tr069
-rw-r--r-- 1 0 0 78 Jan 1 00:00 passwd
lrwxrwxrwx 1 0 0 29 Jan 1 00:00 ads1_phy.lnk -> /etc/ads1/ads1_phy_ANNEXA.bin
-rw-r--r-- 1 0 0 19798 Jan 1 00:00 config.xml
lrwxrwxrwx 1 0 0 21 Jan 1 00:00 lang.js -> /webs/lang/lang_tr.js
-rwxr-xr-x 1 0 0 7 Jan 1 00:00 dproxy.conf
-rw-r--r-- 1 0 0 20 Jan 1 00:00 resolv.conf
-rw-r--r-- 1 0 0 1524 Jan 1 00:00 wlan.conf
-rw-r--r-- 1 0 0 319 Jan 1 00:00 dnsmasq_dhcp.conf
-rw-r--r-- 1 0 0 316 Jan 1 00:00 hostapd.conf.wl0
-rwxr-xr-x 1 0 0 15 Jan 1 00:01 httpd.conf
-rw-r--r-- 1 0 0 115 Jan 1 00:01 invalid_host.html
-rw-r--r-- 1 0 0 12 Jan 1 00:01 dnsmasq.eco0146
drwxr-xr-x 13 0 0 141 Dec 29 2011 ..
drwxr-xr-x 12 0 0 0 Jan 1 00:01 .







# cat passwd
root:5Uu4Stto7E.IE:0:0:Admin:/tmp:/bin/sh
nobody::99:99:nobody:/tmp:/bin/false#
# █
```

Ready

Bir diğ er ö rnekte ise modem in yönetici arayüzündeki gizli sayfaları tespit

etmek istiyoruz. Bunun için ilk iş, donanım yazılımını (bellenim) üreticinin veya internet servis sağlayıcısının web sitesinden indirmek olacaktır. Ardından strings aracını bu donanım yazılımı üzerinde çalıştırabiliriz. Eğer aracın çıktısı aşağıdaki örnekte olduğu gibi sayıca az html sayfa adı veriyorsa ancak biz arayüzde çok daha fazla sayıda html sayfa olduğunu biliyorsak, binwalk gibi farklı bir araç ile analizi bir adım ileriye taşıyabiliriz.




```
Applications Places   Wed Sep 10, 12:36 PM     root

root@kali: ~/Desktop

File Edit View Search Terminal Help

root@kali:~/Desktop# strings 340TSA5D0.bin | grep -i .html
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
wzWAN_Test.html
wzWAN_PPP.html
For UPnP to function normally, the <a href='RemMagWWW.html'>HTTP</a> service must be available for LAN computers using UPnP.
Note : For WPS to function normally, the <a href='rpUPNP.html'>UPNP</a> service will be turn on automatically.
<b>You may also need to create a<a href='Firewall.html'>Firewall</a>rule</b>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
wzWAN_Test.html
wzWAN_PPP.html
in <a href='RemMagWWW.html'>HTTP</a> servisi, UpnP kullanan LAN bilgisayarlar
in <a href='WLAN_WPS.html'>UPnP</a> fonksiyonu devreye girecektir.
ca bir <a href='Firewall.html'>Firewall</a>kural
root@kali:~/Desktop#
```

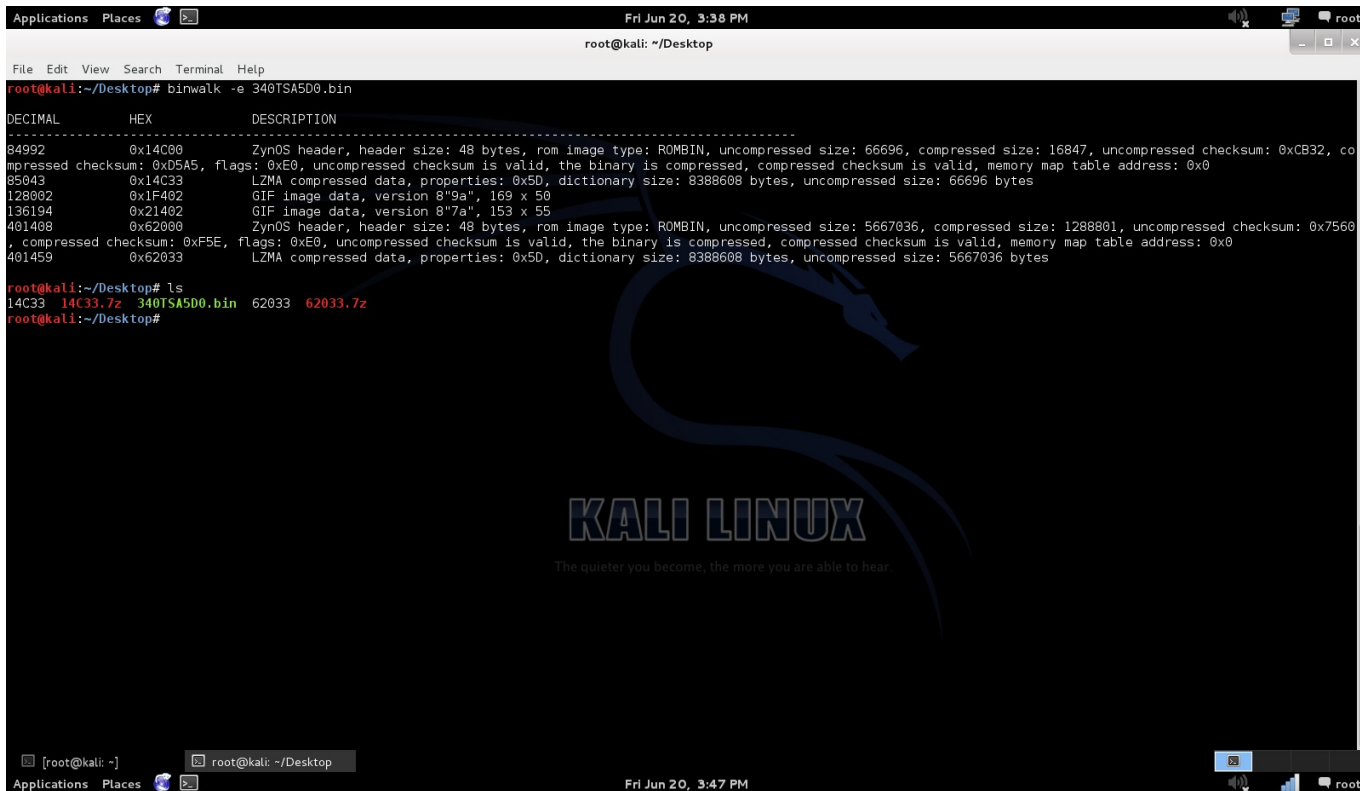
Donanım yazılımı analizi için biçilmiş kaftan olan binwalk aracı ile donanım yazılımını açtıktan (extract) sonra, çıkan dosyalar üzerinde strings komutunu çalıştırdığımızda çok daha fazla sayıda html dosya olduğunu görebiliriz.


```
Applications Places  Fri Jun 20, 3:38 PM
root@kali: ~/Desktop

File Edit View Search Terminal Help
root@kali:~/Desktop# binwalk -e 340TSA5D0.bin

DECIMAL      HEX          DESCRIPTION
-----
84992        0x14C00      ZynOS header, header size: 48 bytes, rom image type: ROMBIN, uncompressed size: 66696, compressed size: 16847, uncompressed checksum: 0xCB32, compressed checksum: 0xD5A5, flags: 0xE0, uncompressed checksum is valid, the binary is compressed, compressed checksum is valid, memory map table address: 0x0
85043        0x14C33      LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 66696 bytes
128002       0x1F402      GIF image data, version 8"9a", 169 x 50
136194       0x21402      GIF image data, version 8"7a", 153 x 55
401408       0x62000      ZynOS header, header size: 48 bytes, rom image type: ROMBIN, uncompressed size: 5667036, compressed size: 1288801, uncompressed checksum: 0x7560, compressed checksum: 0xF5E, flags: 0xE0, uncompressed checksum is valid, the binary is compressed, compressed checksum is valid, memory map table address: 0x0
401459       0x62033      LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 5667036 bytes

root@kali:~/Desktop# ls
14C33  14C33.7z  340TSA5D0.bin  62033  62033.7z
root@kali:~/Desktop#
```



```
Applications Places  Fri Jun 20, 3:47 PM
root@kali: ~/Desktop

File Edit View Search Terminal Help
root@kali:~/Desktop# strings 62033 | grep -i .html
/rpFWUpload.html
/RestoreCfg.html
<html>
</html>
Rphttp.c---[RpBuildReply]--case eRpRomUrl---fHtmlResponseLength =
Rphttp.c---[RpSendReplyBuffer]---fHtmlResponsePtr =
text/html
<html>
text/html
/rpDs1DisconnctWarn.html
">here</a></body></html>
<html>
text/html
/rpAutoFwupgrade! .html
">here</a></body></html>
"text/html; charset=
h_SysAdmin.html
h_Ethernet.html
h_NAT_Mode.html
h_wzOthers.html
h_TimeZone.html
h_wzStatus.html
h_NAT_RuleList.html
h_NAT_RuleEdit.html
h_DHCP.html
h_Diag.html
h_UPNP.html
h_NAT_ServerEdit.html
h_Filter.html
h_Status.html
h_wzNET.html
h_FirmUp.html
h_wzDiag.html
h_WLAN_Setup.html
h_FirstPage.html
h_DiagGeneral.html
h_DiagDSL.html
h_wzPPP.html
h_wzPPPOE.html
h_wzRFC.html
h_DyDNS.html
h_RManage.html
```

```
Applications Places Fri Jun 20, 3:48 PM root@kali: ~/Desktop
File Edit View Search Terminal Help
/Act_option.html
/rpSysAdmin.html
/rpTimeZone.html
/rpFWUpload.html
/FWUpSucc.html
/FWUpSuccPrev.html
/FwSuccess.html
/RestoreCfg.html
/MaintenanceUploadErr.html
/rpSysReboot.html
/RestoreSuccPrev.html
/RestoreSucc.html
/DefaultSucc.html
/DefaultSuccPrev.html
/RebootSuccPrev.html
/RebootSucc.html
/Success.html
<input type="button" value="Return" name="submit" onClick="window.location='rpFWUpload.html'">
<input type="button" value="Return" name="submit" onClick="window.location='RestoreCfg.html'">
/LAN_IP.html
/LAN_IPAlias.html
/LAN_Adv.html
/LAN_DHCPSetup.html
/LAN_ClientList.html
/GroupSetting.html
/PortSetting.html
/VlanSetup.html
/WAN.html
/WAN_Adv.html
/wanRemoteNode_Edit_Adv.html
/wanRemoteNode.html
/wanRemoteNode_Edit.html
/ViewLog.html
/rpCWMP.html
/rpAutoFwupgrade.html
/WLAN_General.html
/WLAN_Adv.html
/WLAN_APFilte Edit.html
/WLAN_MoreAP.html
/WLAN_MoreAP_Edit.html
/WLAN_MoreAPFilter_Edit.html
/WLAN_Scheduling.html
/WLAN_WPS.html
```

rpCWMP.html dosyasının adından da anlaşılacağı üzere TR-069 yönetim protokolü ile ilgili ayarların yapıldığı sayfa olduğunu hemen anlayabiliriz. Sayfayı çağırdığımız zaman gelen internet servis sağlayıcısının Auto Configuration Servers (ACS) adresini, Charles Proxy aracının sistem üzerinde dinlediği adresi ve bağlantı noktası (port) ile değiştirip, Charles'a gelen istekleri de internet servis sağlayıcısının ACS adresine yönlendirdiğimizde, bu gizli sayfa sayesinde başarıyla ACS ile modem arasında gerçekleşen trafiği izleyebiliriz.

192.168.1.1/rpCWMP.html


Most Visited Getting Started

CWMP

CWMP Setup

CWMP Activated Deactivated

Login ACS

URL 

User Name

Password

Connection Request

Path

Port

UserName

Password

Periodic Inform

Periodic Inform Activated Deactivated

Interval(s)

Apply Cancel

192.168.1.1/rpCWMP.html

Most Visited Getting Started

CWMP

CWMP Setup

CWMP Activated Deactivated

Login ACS

URL

User Name

Password

Connection Request

Path

Port

UserName

Password

Periodic Inform

Periodic Inform Activated Deactivated

Interval(s)

Apply Cancel

Charles 3.9.2 - Session 1*

File Edit View Proxy Tools Window Help

Structure Sequence

Overview Summary Chart

Name Value

Host socket://hdmacs-tr069. com.tr:7547

Path /

Notes

Request

Response

Content

Included

Failed

DN

Content

SSL

Timing

Status

End

Time

Request

Duration

DN

Content

SSL

Latency

Speed

Response

Size

Request

Response

Combined

Compression

Port Forwarding Settings

Forward local TCP and UDP ports to remote servers.

Enable Port Forwarding

Type	Start Port	End Port	Remote Host	Remote Port
<input checked="" type="checkbox"/> TCP	7547		hdmacs-tr069. com.tr	7547
<input checked="" type="checkbox"/> TCP	80		hdmacs-tr069. com.tr	80

Add Remove

Import Export OK Cancel Help

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 16:08:55.060109000	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	192.168.1.1	192.168.1.34	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	192.168.1.1	192.168.1.34	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	192.168.1.1	192.168.1.34	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	192.168.1.1	192.168.1.34	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 /cwpweb/CPemgt HTTP/1.1
104	2014-06-20 16:08:57.206218000	192.168.1.1	192.168.1.34	TCP	54	http > iad1 [ACK] Seq=1 Ack=3172 win=16800 Len=0
125	2014-06-20 16:08:57.535424000	192.168.1.1	192.168.1.34	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	192.168.1.1	192.168.1.34	TCP	54	http > iad1 [ACK] Seq=620 Ack=3173 win=16800 Len=0
132	2014-06-20 16:08:57.538145000	192.168.1.1	192.168.1.34	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

Peki donanım yazılımını analiz ettikten sonra Charlie Miller ile Chris Valasek'in Cherokee Jeep'i hacklerken yaptıkları gibi donanım yazılımını manipüle edip (patching) cihaza yüklemek istersek, donanım yazılımını tekrar paketlemek için faydalabileceğimiz Firmware Modification Kit (FMK) aracından da kısaca bahsetmek gerekir. İlgili donanım yazılımının dosya sisteminde yer alan dosyalarını, FMK'da yer alan extract-firmware.sh betiği ile diske açtıktan ve değişiklikler yaptıktan sonra yine aynı araçta yer alan build-firmware.sh betiği ile paketlememiz mümkün. Bu sayede hedef cihazın imza

kontrolü yapmadan donanım yazılımını güncellemeye izin verip vermediğini de kolaylıkla kontrol edebiliriz.

The screenshot shows a Kali Linux desktop environment. At the top, a web browser window is open to a PDF document titled "Remote%20Car%20Hacking.pdf". The document content includes a terminal command `iocupdate -c 4 -p usr/share/V850/cmcioc.bin`, a paragraph explaining the help text for 'iocupdate', a code block with usage instructions and examples, and a paragraph about reverse engineering the IOC application firmware. Below the browser, a terminal window is open, displaying the output of the `extract-firmware.sh` script. The terminal output shows the scan time, signatures, target file, MD5 checksum, and a table of firmware components.

illmatics.com/Remote Car x Mert

illmatics.com/Remote%20Car%20Hacking.pdf

```
iocupdate -c 4 -p usr/share/V850/cmcioc.bin
```

The help text for 'iocupdate' validates our initial analysis by describing that it is, indeed, used for sending a binary file to the IOC from the head unit.

```
%C: a utility to send a binary file from the host processor to the IOC
[options] <binary file name>
Options:
-c <n> Channel number of IPC to send file over (default is /dev/ipc/ch4)
-p Show progress
-r Reset when done
-s Simulate update
Examples:
/bin/someFile.bin (will default to using /dev/ipc/ch4)
-c7 -r /bin/someFile.bin (will reset when done)
-sp (simulate update with progress notification)
```

After we figured out how to reprogram the V850 package, we needed to reverse engineer and modify the IOC application firmware to add code to accept commands and forward them to the CAN bus. The

49

most important part was reverse engineering the IOC application firmware because we knew it would reveal the code necessary to send and receive CAN messages from the bus. Luckily, we see that the IOC can be re-flashed with firmware and that no cryptographic signatures are used to verify the firmware is legitimate.

Applications Places Mon Sep 15, 3:38 PM root

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/
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
ddress: 0x80010000, Entry Point: 0x80228000, data CRC: 0x160F6F4A, OS: Linux, CP
U: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux
```

Click to view your appointments and tasks

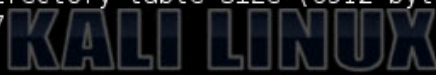
File Edit View Search Terminal Help

```
Extracting 232 bytes of header image at offset 0
Extracting squashfs file system at offset 232
Extracting 2704 byte footer from offset 3483684
Extracting squashfs files...
Firmware extraction successful!
Firmware parts can be found in '/root/fmk/'
root@kali:~#
root@kali:~# cd /opt/firmware-mod-kit/fmk
bash: cd: /opt/firmware-mod-kit/fmk: No such file or directory
root@kali:~# cd /root/fmk
root@kali:~/fmk# ls
image_parts  logs  rootfs
root@kali:~/fmk# cd rootfs
root@kali:~/fmk/rootfs# ls
bin  dev  etc  lib  mnt  proc  ramdisk  root  sbin  sys  tmp  usr  var  webs
root@kali:~/fmk/rootfs# ls webs
air.css      errors      js           menu frame.html  upnp
.            firewall   lan          nat              vlan
altmenu.css  homepage.html  lang        qos              wireless
atmenu.css   igmp       lang.js      report           wizard2.html
atmenu.js    images
cgi-bin      index.html  login.html   route
config.bin   internet   loginmain.html  tools
ddns        invalid_host.html  main.html    top.html
root@kali:~/fmk/rootfs# touch webs/mert.txt
root@kali:~/fmk/rootfs#
```




File Edit View Search Terminal Help

```
root@kali:~/fmk/rootfs# /opt/firmware-mod-kit/build-firmware.sh /root/fmk
Firmware Mod Kit (build) 0.99, (c)2011-2013 Craig Heffner, Jeremy Collake

Building new squashfs file system... (this may take several minutes!)
Squashfs block size is 64 Kb
Parallel mksquashfs: Using 1 processor
Creating big endian 3.0 filesystem on /root/fmk/new-filesystem.squashfs, block size 65536.
[=====] 345/345 100%
Exportable Big endian filesystem, data block size 65536, compressed data, compressed metadata, compressed fragments, duplicates are removed
Filesystem size 2661.86 Kbytes (2.60 Mbytes)
    29.02% of uncompressed filesystem size (9173.20 Kbytes)
Inode table size 3771 bytes (3.68 Kbytes)
    26.42% of uncompressed inode table size (14274 bytes)
Directory table size 4161 bytes (4.06 Kbytes)
    60.20% of uncompressed directory table size (6912 bytes)
Number of duplicate files found 7
Number of inodes 471
Number of files 255
Number of fragments 43
Number of symbolic links 83
Number of device nodes 70
Number of fifo nodes 0
Number of socket nodes 0
Number of directories 63
```



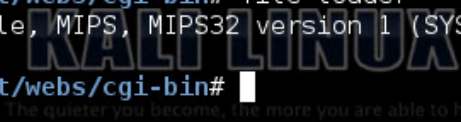
The quieter you become, the more you are able to hear

```
Applications Places   Mon Sep 15, 3:45 PM  root
root@kali: ~/fmk/rootfs
File Edit View Search Terminal Help
Inode table size 3771 bytes (3.68 Kbytes)
    26.42% of uncompressed inode table size (14274 bytes)
Directory table size 4161 bytes (4.06 Kbytes)
    60.20% of uncompressed directory table size (6912 bytes)
Number of duplicate files found 7
Number of inodes 471
Number of files 255
Number of fragments 43
Number of symbolic links 83
Number of device nodes 70
Number of fifo nodes 0
Number of socket nodes 0
Number of directories 63
Number of uids 1
    root (0)
Number of gids 0
Remaining free bytes in firmware image: 755516
Processing 2 header(s) from /root/fmk/new-firmware.bin...
Processing header at offset 168...checksum(s) updated OK.
Processing header at offset 2728168...sorry, this file type is not supported.
checksum update(s) failed!
CRC(s) updated successfully.

Finished!
New firmware image has been saved to: /root/fmk/new-firmware.bin
root@kali:~/fmk/rootfs#
```

Statik olarak değil de dinamik olarak donanım yazılımında yer alan programları teker teker analiz etmek istiyoruz dersek de o zaman, QEMU öykünücüsü (emulator) ve IDA Pro aracı sayesinde aşağıdaki ekran görüntülerinde yer aldığı şekilde programları (örnek: login) detaylı bir şekilde analiz edebiliriz.

```
root@kali:/squashfs-root/webs/cgi-bin# ls -al
total 176
drwxr-xr-x  2 root root  4096 Sep  7 07:08 .
drwxr-xr-x 21 root root  4096 Sep  7 07:08 ..
-rwxr-xr-x  1 root root    34 Sep  7 07:08 cert
-rwxr-xr-x  1 root root 44696 Sep  7 07:08 cert_load
-rwxr-xr-x  1 root root 53432 Sep  7 07:08 loader
-rwxr-xr-x  1 root root 15268 Sep  7 07:08 login
-rwxr-xr-x  1 root root 16940 Sep  7 07:08 restore_config
-rwxr-xr-x  1 root root 27280 Sep  7 07:08 webapp
root@kali:/squashfs-root/webs/cgi-bin# file login
login: ELF 32-bit MSB executable, MIPS, MIPS32 version 1 (SYSV), dynamically linked (uses shared libs), stripped
root@kali:/squashfs-root/webs/cgi-bin# file webapp
webapp: ELF 32-bit MSB executable, MIPS, MIPS32 version 1 (SYSV), dynamically linked (uses shared libs), stripped
root@kali:/squashfs-root/webs/cgi-bin# file loader
loader: ELF 32-bit MSB executable, MIPS, MIPS32 version 1 (SYSV), dynamically linked (uses shared libs), stripped
root@kali:/squashfs-root/webs/cgi-bin#
```



root@kali: /squashfs-root/webs/cgi-bin

File Edit View Search Terminal Help

```
root@kali: /squashfs-root/webs/cgi-bin# qemu-mips login
```

```
Content-type: text/html; Charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache
Expires: -1
```

```
<html>
<head>
  <meta http-equiv="Refresh" content="0; url=/login.html?ErrorCode=1">
</head>
<body>
</body>
</html>
```

```
root@kali: /squashfs-root/webs/cgi-bin# echo "redirect=&user=mert&password=mert&
gonder=TAMAM" | qemu-mips -E REQUEST_METHOD="POST" -E CONTENT_LENGTH=46 -E CONTENT_TYPE
="application/x-www-form-urlencoded" -g 1234 login
```

KALI LINUX

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

Select a debugger

Available debuggers

- No debugger
- Remote GDB debugger
- Trace replayer

Default debuggers (autoselected for new databases):
NONE

Set as default debugger

OK Cancel

Debug application setup: gdb

NOTE: all paths must be valid on the remote computer

Application: C:\Documents and Settings\Administrator\Desktop\login ...

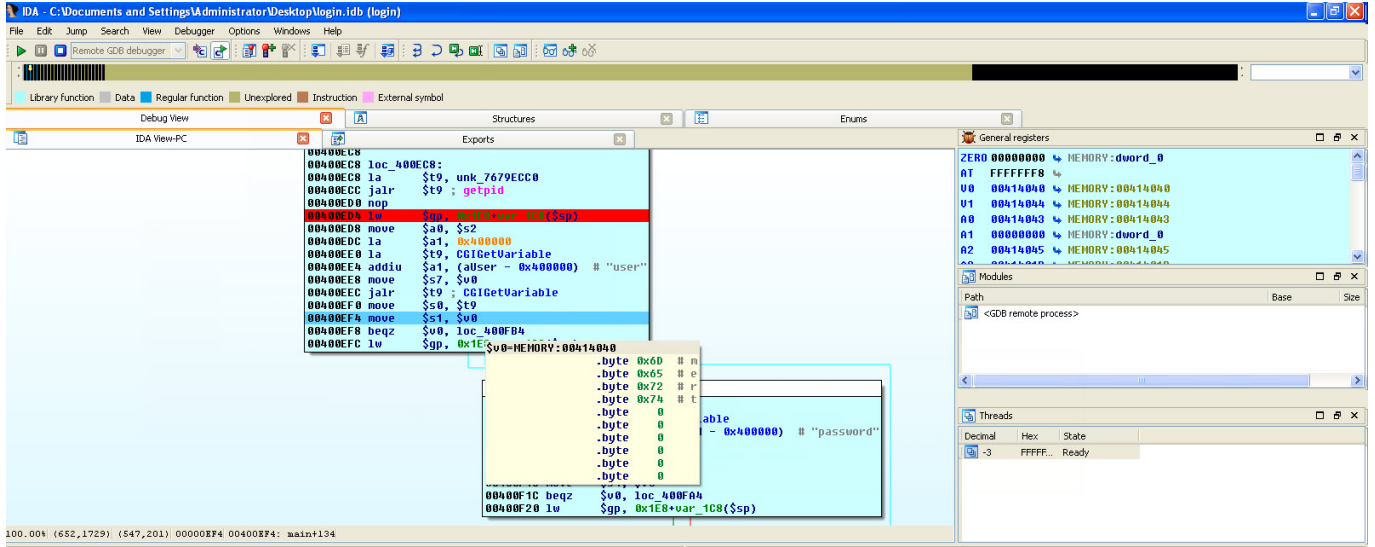
Input file: C:\Documents and Settings\Administrator\Desktop\login ...

Parameters: ...

Hostname: 192.168.114.253 Port: 1234

Save network settings as default

OK Cancel Help



Çok daha fazlasını öğrenmek ve uygulamak istiyorum diyenleriniz için ise Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts kitabına bir göz atmalarını tavsiye edebilirim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.