

This is Google's cache of <http://www.hackforums.net/archive/index.php/thread-2891506-9.html>. It is a snapshot of the page as it appeared on 21 Aug 2015 16:18:04 GMT.

The [current page](#) could have changed in the meantime. [Learn more](#)

Full version [Text-only version](#) [View source](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

Hack Forums

[Hack Forums](#) > [Hacks, Exploits, and Various Discussions](#) > [Wifi WPA WEP Bluetooth 4G LTE Wireless Hacking](#) > List of Default WPS PIN

Full Version: [List of Default WPS PIN](#)

You're currently viewing a stripped down version of our content. [View the full version](#) with proper formatting.

Pages: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)

aanarchyy

04-28-2015, 10:02 PM

(04-28-2015 07:28 PM)agentshield Wrote: [\[->\]](#) On Comcast/xfinity Router/Gateway the wps are calculated by coverting the last 6 values of the mac address from hex to dec. after converting you will get either a 7 or 8 digit answer. if u get 8 digit. drop the first value, then reaver it.

Proof

Pin cracked in 73 seconds

[+] WPS PIN: '23407282'

[+] WPA PSK: 'H21208270B275A94'

[+] AP SSID: 'HOME-B778'

[+] Nothing done,

Have found a few HOME-XXXX networks that held true to this, but so far not too many, also, would be helpfull if you gave the MAC address.

Example of one that doesn't work, Xfinity router.

BSSID: 0C:F8:93:B3:7E:80-81 LAN 0C:F8:93:B3:7E:82 WAN

ESSID: HOME-7E82

WPS: 56276053

Model: TG862G v5
Chipset: RT2860

Noticed something interesting, when an AP has the WPS button pushed, it will accept the WPS pin of 000000, or maybe even any pin...

af48

05-03-2015, 05:08 AM
Thanks bro for sharing :)

agentshield

05-05-2015, 06:52 PM
NETGEAR WN3000RPv2 (wifi extender)
Hardware Version WN3000RPv2
Firmware Version V1.0.0.36
GUI Language Version V1.0.0.25

bssid:E4:F4:C6:EE:05:A4
essid:NEW CHUNKUS
mac:

PKE:192
PKR:192
Authkey:32
E-Hash1:32
E-Hash2:32
E-Nonce:16

PIN: 21317804
WPA key

[+] Pin count advanced: 1. Max pin attempts: 11000

although autopixie cracked the pin in 1 attempt the router wps locked as a result

BSSID Channel RSSI WPS Version WPS Locked ESSID

CC:03:FA:81:4E:AC 1 -49 1.0 No HOME-4EAC
38:2C:4A:E5:DD:18 6 -39 1.0 Yes HOME 2G
E4:F4:C6:EE:05:A4 7 -19 1.0 Yes NEW CHUNKUS
AC:3A:7A:3B:87:29 7 -25 1.0 No (null)

4C:60:DE:36:D8:5E 11 -52 1.0 No Lacayo
44:32:C8:62:0B:24 1 -68 1.0 No Divina Misericordia
34:08:04:BC:7B:64 6 -67 1.0 No Terry
^C

#####

Press CTRL+C to stop scan and choose accesspoint
6 - -b: CC:03:FA:81:4E:AC -c: 1 Pwr -50 -e: HOME-4EAC
7 - -b: 38:2C:4A:E5:DD:18 -c: 6 Pwr -41 -e: HOME 2G
8 - -b: E4:F4:C6:EE:05:A4 -c: 7 Pwr -15 -e: NEW CHUNKUS
9 - -b: C4:39:3A:11:77:58 -c: 7 Pwr -52 -e: HOME-7758
10 - -b: 4C:60:DE:36:D8:5E -c: 11 Pwr -54 -e: Lacayo
11 - -b: 34:08:04:BC:7B:64 -c: 6 Pwr -66 -e: Terry

^C

ssid:HOME-7758
bssid:C4:39:3A:11:77:58
WPSpin: 11446644

for some reason i cannt access the router page default router login not working.

any info on 2wirexxx AP?

also when i try to increase the tx power of the SAbrent NT -wghu realtek 8187 the tx power never changes from 20dbm. can someone help me with this.

The Sabrent NT-WGHU Wireless 802.11g USB 2.0 Adapter gives you the flexibility to position your Desktop PC or MAC where you want, without the cost or inconvenience of running network cables. Maximize data transfer speeds of up to 54 Mbps from as far as 800 meters with the included 7" 6dbi antenna. Simply install the USB Adapter into an available USB port, and connect to an available Wireless Network. (Reverse compatible with 802.11b). If you already have an internal wireless card, you can use this USB 1000mW adapter by disabling your internal card in Device Manager.

here is some info , i hope it helps

E4:F4:C6:EE:05:A4 -29 152 25 0 7 54e. WPA2 CCMP PSK NEW CHUNKUS
NETGEAR
AC:3A:7A:3B:87:29 -28 39 0 0 7 54e WPA2 CCMP PSK <length: 22> Roku
38:2C:4A:E5:DD:18 -45 107 8 0 6 54e WPA2 CCMP PSK HOME 2G ASUSTek
COMPUTER INC.

CE:03:FA:81:4E:AD -48 72 0 0 1 54e. WPA2 CCMP PSK <length: 12> Unknown
CE:03:FA:81:4E:AE -52 70 0 0 1 54e. OPN xfinitywifi Unknown
CC:03:FA:81:4E:AC -48 70 2 0 1 54e WPA2 CCMP PSK HOME-4EAC Technicolor
CH USA
C4:39:3A:11:77:5A -54 78 0 0 7 54e WPA2 CCMP PSK <length: 0> SMC Networks
Inc
4C:60:DE:36:D8:5E -52 75 0 0 11 54e WPA2 CCMP PSK Lacayo NETGEAR
C4:39:3A:11:77:59 -53 71 0 0 7 54e WPA2 CCMP PSK <length: 0> SMC Networks
Inc
C4:39:3A:11:77:5B -52 76 0 0 7 54e WPA2 CCMP PSK <length: 0> SMC
Networks Inc
C4:39:3A:11:77:58 -57 70 4 0 7 54e WPA2 CCMP PSK HOME-7758 SMC
Networks Inc
1C:1B:68:CD:78:E0 -65 12 1 0 6 54e WPA2 CCMP PSK ATTNAcKhCI ARRIS
Group, Inc.
34:08:04:BC:7B:64 -67 8 0 0 6 54e WPA2 CCMP PSK Terry D-Link Corporation

Çdñî\$ Lŭpî\$

05-06-2015, 11:50 AM

I need to post a few in here. Should update later.

Malek Elliot™

05-16-2015, 11:31 PM

(05-06-2015 11:50 AM)Çdñî\$ Lŭpî\$ Wrote: [\[->\]](#) I need to post a few in here. Should update later.

I wish people could continue to contribute to this thread, i'm currently working on a personal project with 2 friends of mine to make something out of this. Were working on a database website to get all the PIN, Firmware and models all classed with easy access to add them if they're valid and approved. Black Hat

fratri

05-17-2015, 04:17 PM

There is a spread sheet, or lets create a new one.

I have 2 links with google sheets that can share but I am unable to post links. But they are very updated.

Malek Elliot™

05-17-2015, 07:25 PM

(05-17-2015 04:17 PM) *fracri* Wrote: [\[->\]](#) There is a spread sheet, or lets create a new one.

I have 2 links with google sheets that can share but I am unable to post links.

But they are very updated.

Well so far i've talked to pomwtin and TheGrayAviator about my school summer projects and i receive a lot of advice and tips from both of them and some useful source to PIN's, i'm currently parsing a 180 PIN/Model/Firmware/Brand sheets in python that i found with some basics dorks on google. and Pom gave me source as well i'll indeed check this out later as i have to register to the said forums ...

fracri

05-17-2015, 08:17 PM

On Comcast/xfinity Router/Gateway the wps are calculated by coverting the last 6 values of the mac address from hec to dec. after converting you will get either a 7 or 8 digit answer.

How do you do this ? :P

MirrorDude

05-17-2015, 08:33 PM

(05-17-2015 08:17 PM) *fracri* Wrote: [\[->\]](#) On Comcast/xfinity Router/Gateway the wps are calculated by coverting the last 6 values of the mac address from hec to dec. after converting you will get either a 7 or 8 digit answer.

How do you do this ? :P

<http://www.binaryhexconverter.com/hex-to...-converter>

This method rarely works though...

soxrok2212

05-17-2015, 08:56 PM

(05-17-2015 08:33 PM)MirrorDude Wrote: [\[-> /http://www.binaryhexconverter.com/hex-to...-converter](#)

This method rarely works though...

Yeah Ive seen the pin scrambled... And it only worked 1 out of... It worked once haha. Probably a false positive or something I dunno

Pages: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)

[Hack Forums](#) > [Hacks, Exploits, and Various Discussions](#) > [Wifi WPA WEP Bluetooth 4G LTE Wireless Hacking](#) > List of Default WPS PIN

Reference URL's

- **Hack Forums:** <http://www.hackforums.net/index.php>
- :

Powered By [MyBB](#), © 2002-2015 [MyBB Group](#)