

Aircrack-ng 1.1 - (C) 2006, 2007, 2008, 2009 Thomas d'Otreppe
Original work: Christophe Devine
<http://www.aircrack-ng.org>

usage: aircrack-ng [options] [<.cap / .ivs file(s)>]

Common options:

- a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
- e <essid> : target selection: network identifier
- b <bssid> : target selection: access point's MAC
- p <nbcpu> : # of CPU to use (default: all CPUs)
- q : enable quiet mode (no status output)
- C <macs> : merge the
- l <file> : write key

Static WEP cracking options:

- c : search all
- t : search by
- h : search th
- d <mask> : use maski
- m <maddr> : MAC addre
- n <nbits> : WEP key l
- i <index> : WEP key index (1 to 4), default: any
- f <fudge> : bruteforce fudge factor, default: 2
- k <korek> : disable one attack method (1 to 17)
- x or -x0 : disable bruteforce for last keybytes
- x1 : last keybyte bruteforcing (default)
- x2 : enable last 2 keybytes bruteforcing
- X : disable bruteforce multithreading
- y : experimental single bruteforce mode
- K : use only old KoreK attacks (pre-PTW)
- s : show the key in ASCII while cracking
- M <num> : specify maximum number of IVs to use
- D : WEP decloak, skips broken keystreams
- P <num> : PTW debug: 1: disable Klein, 2: PTW
- 1 : run only 1 try to crack key with PTW

The “Art” of Hacking Ethically

Hansel Wei

root@kali: /whoami

CompTIA Certified IT Infrastructure Professional

49 Security Division Lab Assistant

UNC Charlotte Computer Science Peer Tutor

Full Stack **Software Developer**

AN **ETHICAL HACKER!**

hwei3@uncc.edu

[Linkedin.com/hanselwei](https://www.linkedin.com/hanselwei)

[GitHub.com/darkmastermindz](https://github.com/darkmastermindz)

[Twitter.com/darkmastermindz](https://twitter.com/darkmastermindz)

So, what exactly is an Ethical Hacker?



“...Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s)...”

— EC Council (CEH)

You may be a 'hacker.'

"Hacking is Progress..."

*# The essence of hacking is finding unintended or overlooked
uses for the laws and properties of a given situation and then
applying them in new and inventive ways to solve a
problem—whatever it may be.*

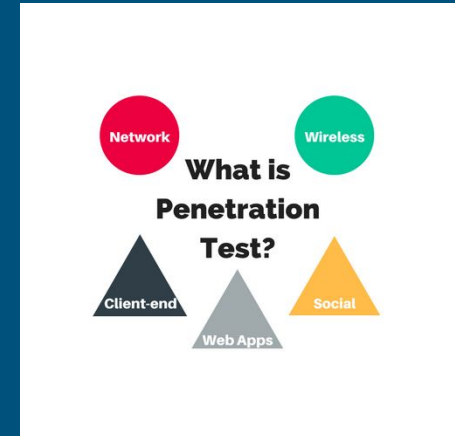
#

#

—Jon Erickson, THE ART OF EXPLOITATION

Penetration Testing

- **Pen testing** is the authorized practice of **testing** a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
- Specialized Operating Systems
 - [Kali Linux](#) (which replaced BackTrack in December 2012) based on Debian Linux
 - [BackBox](#) based on Ubuntu
 - [BlackArch](#) based on Arch Linux
 - [Pentoo](#) based on Gentoo Linux
 - [WHAX](#) based on Slackware Linux
- Types of Pen Testing
 - [Social Engineering](#)
 - Network Services
 - Client End
 - Web Apps
 - Wireless Security
 - Physical



Aircrack-ng 1.1 - (C) 2006, 2007, 2008, 2009 Thomas d'Otreppe
Original work: Christophe Devine
<http://www.aircrack-ng.org>

usage: aircrack-ng [options] <.cap / .ivs file(s)>

Common options:

```
-a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
-e <essid> : target selection: network identifier
-b <bssid> : target selection: access point's MAC
-p <nbcpu> : # of CPU to use (default: all CPUs)
-q        : enable quiet mode (no status output)
-C <macs> : merge the given Psk to a virtual Psk
-l <file>  : write key to file
```

Static WEP cracking options:

```
-c        : search alpha-numeric characters only
-t        : search binary coded decimal chr only
-h        : search the numeric key for Fritz!Box
-d <mask> : use masking of the key (A1:XX:CF:YY)
-m <maddr> : MAC address to filter usable packets
-n <nbits> : WEP key length : 64/128/152/256/512
-i <index> : WEP key index (1 to 4)
-f <fudge> : bruteforce fudge factor
-k <korek> : disable one attack method
-x or -x0 : disable bruteforce for
-x1       : last keybyte bruteforce
-x2       : enable last 2 keybytes bruteforce
-X        : disable bruteforce for
-y        : experimental single bruteforce
-K        : use only old KoreK attack
-s        : show the key in ASCII when found
-M <num>  : specify maximum number of IVs to use
-D        : WEP decloak, skips broken keystreams
-P <num>  : PTW debug: 1: disable Klein, 2: PTW
-1        : run only 1 try to crack key with PTW
```

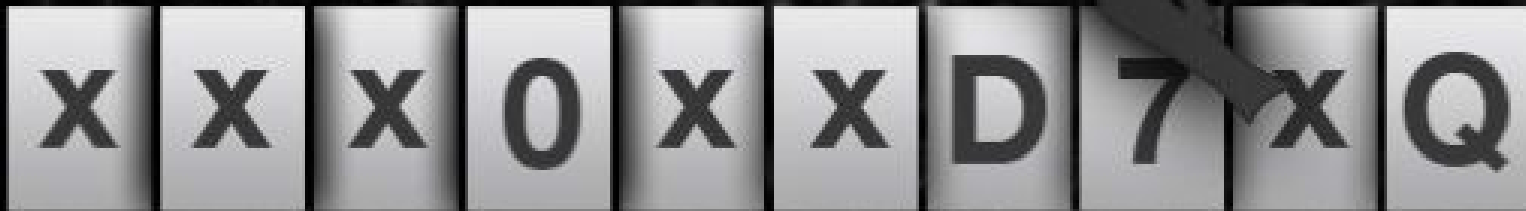
Wireless Exploitation Activity

Disclaimer: *"With great knowledge comes great responsibility; therefore, I am not responsible for your own actions; I am not a lawyer and can't help you if you don't, so please use this knowledge responsibly and only in an environment you own or educational environment with permission."*

WiFi Network Security

- Open
- WEP
- WPA/WPA-2
 - PSK
 - AES
 - Enterprise





- Very weak
- What is happening?

WEP Cracking

USB-Boot into Kali-Linux

"The quieter you are the more you can hear"

STOP: You may only use your personal device you own or receive prior permission from owner to do this activity.

Windows 10:

1. Search **Advanced Startup Options**
2. Click on **Use a Device**
3. **Select the USB**

Intel Based Mac:

1. **Turn off** computer
2. **Turn on and Hold** down the **Option** key,
3. **Use arrow keys to select USB**, press **Enter**

Other:

1. **Turn off** computer
 2. **Turn on & immediately Press the F? Key (Dell is F12)**
to select "boot from device"
 3. **Use arrow keys to select USB**, press **Enter**
Ask for help if needed
-

Username

Password

root

toor

Three Commands

Open up Terminal, we are going to use three commands to crack the WiFi

```
root@kali: airmon-ng
```

```
root@kali: airodump-ng
```

```
root@kali: aircrack-ng
```

- *airmon-ng*

- Show your available interfaces

- *airmon-ng start wlan1*

airmon-ng

- To begin monitoring in promiscuous mode

- You should get an error that tells you there's processes that may interfere

- *kill xxxx*

```
~# airmon-ng check kill
Killing these processes:
PID Name
870 dhclient
1115 wpa_supplicant
```

- Replace the x's with your process ID
 - NOTE: your PID **will** be different than mine

- *airmon-ng start wlan1*

- Yes, again, to begin monitoring in promiscuous mode

airodump-ng

- *airodump-ng wlan1mon*
 - Identify the nearby access points
- CTRL+SHIFT+T
 - To open up a new terminal tab
- *airodump-ng -c 6 -w wepcrack --bssid 00:1D:7E:6A:2E:4F wlan1mon*
 - Run airodump-ng on channel 6, writing the files wepcrack*, for the network with the bssid of the MAC address

aircrack-ng

- CTRL+SHIFT+T
 - Open a new terminal tab
- *aircrack-ng wepcrack-01.cap*
 - This will start cracking the capture file

Deeper Resources:

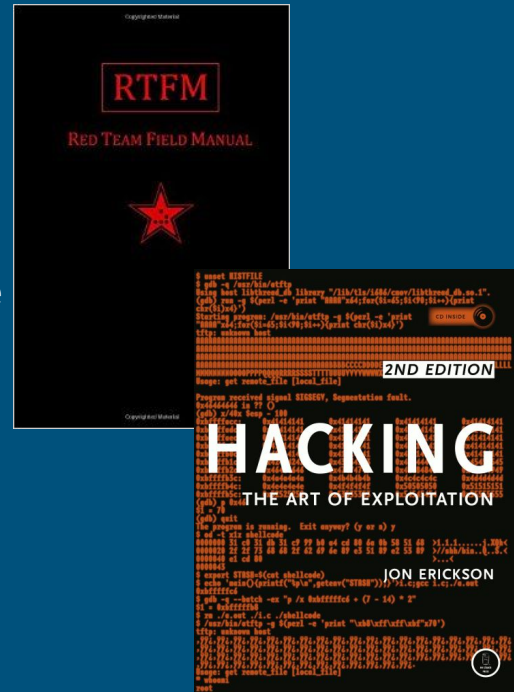
Get involved professionally:

- **Cybersecurity/Networking/IT Continuing Education Certifications:**
 - **CompTIA** - Computer Technology Association
 - CompTIA Security+ce
 - **CSA** CompTIA Security Analyst+ce
 - **CASP** - CompTIA Security Practitioner
 - **EC-Council**
 - **CEH** - Computer Ethical Hacker Certification
 - **Cisco / IC²** (CISSP) - Cisco Certified Information Security Professional

Deeper Resources:

Gain more raw knowledge. (Tools)

- **The Art of Exploitation** – Probably one of the best text books out there
 - io.hanselwei.me/hackingart
- **Red Team Field Manual / Blue Team Field Manual**
 - io.hanselwei.me/redteamfm
 - io.hanselwei.me/blueteamfm
- **Kali-Linux** - The Linux distribution with all pre-packaged hacking tools
 - Kalilinux.org



Deeper Resources:



Get involved in an ethical hacking community.

- **49th Security Division @ UNC Charlotte** – Free zero to hero Ethical Hacking Events, Friendly CTF Competitions, and Conferences 2-3 times a week to dive even deeper in ethical hacking and even in a secure lab environment.
 - To receive an interest form to join our Slack,
 - Email: 49securitydivision@gmail.com
 - Subject: **Winthrop GenCyber**
 - Our Website & Social Media
 - Website: <https://www.49sd.com/>
 - Twitter: [@49sd](https://twitter.com/49sd)



Contact me:

root@kali: /whoami

CompTIA Certified IT Infrastructure Professional

49 Security Division Lab Assistant

UNC Charlotte Computer Science Peer Tutor

Full Stack **Software Developer**

AN **ETHICAL HACKER!**

hwei3@uncc.edu

[Linkedin.com/hanselwei](https://www.linkedin.com/hanselwei)

[GitHub.com/darkmastermindz](https://github.com/darkmastermindz)

[Twitter.com/darkmastermindz](https://twitter.com/darkmastermindz)
