Wifi WPA Cracking Windows

Note: I tried my best to get Windows to sniff wireless...without success. This seems to be very difficult without buying a proprietary driver (AirPCap). This will only cover the actual cracking of an already captured WPA transaction.

First, we need to download our tools. The program “aircrack-ng” is used to run the actual cracking. The program “john” is short for “John the Ripper”. John is also a password cracking program, but we’re going to use it to generate passwords.

Note, aircrack-ng might show up as a “harmful site”.

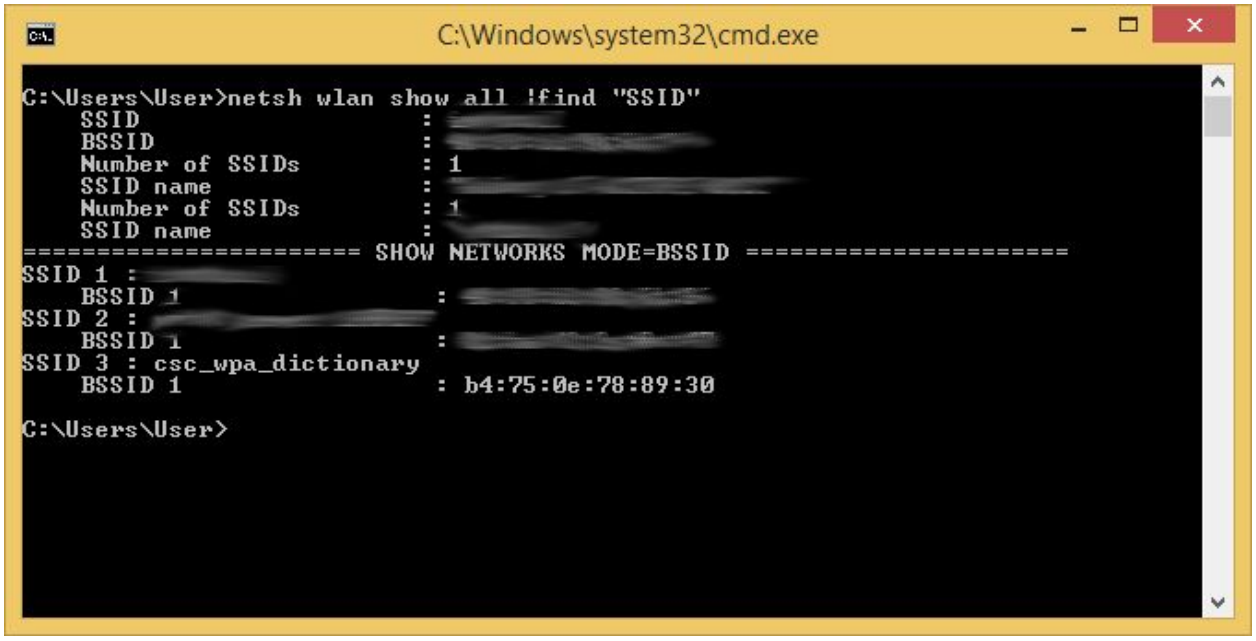
Project Pages:
http://www.aircrack-ng.org/
http://www.openwall.com/john/

Direct Download Links:
http://download.aircrack-ng.org/aircrack-ng-1.2-rc3-win.zip
http://www.openwall.com/john/h/john179w2.zip

Download these two zip files, and unzip them to your user folder (C:\Users\YOURNAME\).

Now we need a shell (a command line). Start one by hitting Window+R, and typing in “cmd”.

Once your shell opens, type “dir” and hit enter. The program “dir” shows all of the directories and files in your path (mine is C:\Users\User). Note that my home folder is a LOT cleaner than yours probably is. That’s ok, just make sure the two folder above are in here.



Although we can’t sniff any traffic, we can get a list of all the wireless access points in range of our wireless interface. We can do this with the “netsh” program. The “netsh” program is short for “network shell” (a command line utility for configuring networks). Anything you can do with the Windows network settings user interface you can do through the netsh command line utility.

So we run netsh, “wlan” means wireless local area networks, “show all” means show all interfaces. If you stop here, there’s a ton of information splatted onto the screen. To filter out the information we’re interested in, we can “pipe” the information through another command (“find” in this case).

The “|” character is called a “pipe”. A pipe passes the output from the preceding command to the second command. The program “find” takes a string and only prints lines with that string in them (note that every line has “SSID” somewhere in it).

From this information we can get the SSID (the name representation) and the BSSID (the number representation) of the access point.

```
C:\Windows\system32\cmd.exe

C:\Users\User>dir
 Volume in drive C has no label.
 Volume Serial Number is D2FE-8AD4

 Directory of C:\Users\User

01/23/2016  10:36 PM    <DIR>          .
01/23/2016  10:36 PM    <DIR>          ..
01/23/2016  10:36 PM             3,492 500.txt
01/23/2016  07:48 PM    <DIR>          aircrack-ng-1.2-rc3-win
01/23/2016  10:32 PM            72,068 dictionary.cap
01/23/2016  07:48 PM    <DIR>          john179
               2 File(s)         75,560 bytes
               4 Dir(s)  188,422,344,704 bytes free

C:\Users\User>_
```

Now that our tools are all setup, we need to copy over a capture file (provided separately). The capture file contains a single WPA handshake (you only need a single WPA handshake for this exploit to work). This is the “dictionary.cap” in the “dir” output above.

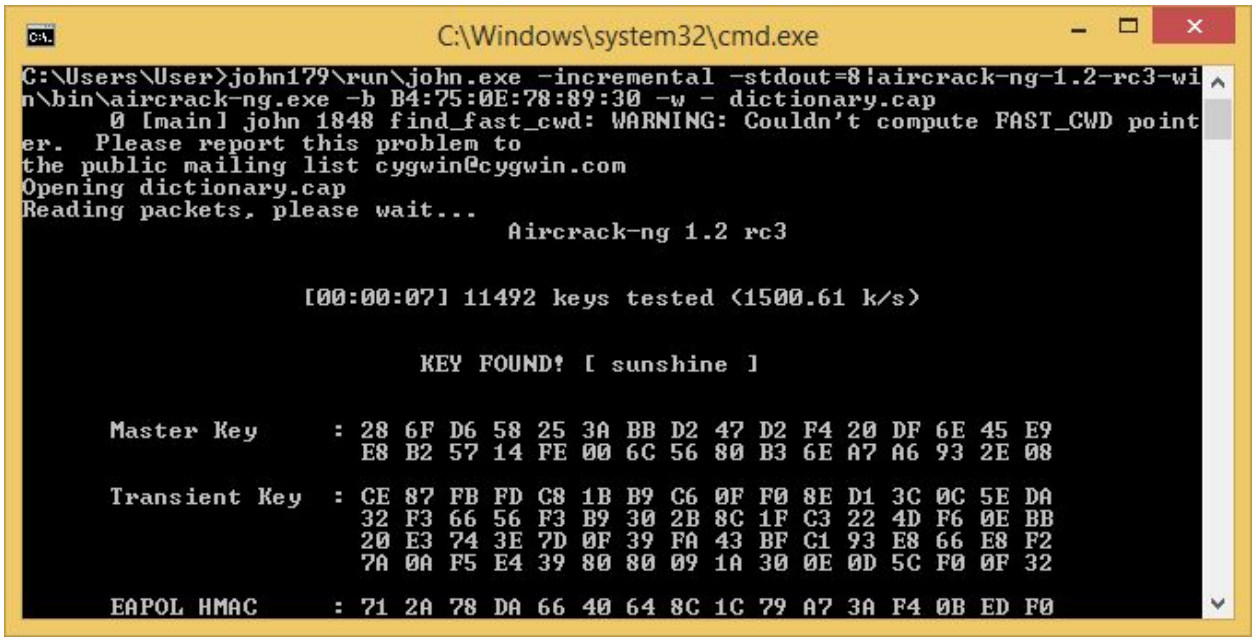
We will also need a dictionary (a dictionary is just a file full of words, one per line). The “500.txt” is a top 500 list of common passwords (it is also provided separately).

```
C:\Windows\system32\cmd.exe

C:\Users\User>aircrack-ng-1.2-rc3-win\bin\aircrack-ng.exe -b B4:75:0E:78:89:30 -
w 500.txt dictionary.cap
Opening dictionary.cap
Reading packets, please wait...
                                 Aircrack-ng 1.2 rc3

                    [00:00:00] 33 keys tested (534.44 k/s)

                           KEY FOUND! [ sunshine ]

      Master Key     : 28 6F D6 58 25 3A BB D2 47 D2 F4 20 DF 6E 45 E9
                       E8 B2 57 14 FE 00 6C 56 80 B3 6E A7 A6 93 2E 08

      Transient Key  : CE 87 FB FD C8 1B B9 C6 0F F0 8E D1 3C 0C 5E DA
                       32 F3 66 56 F3 B9 30 2B 8C 1F C3 22 4D F6 0E BB
                       20 E3 74 3E 7D 0F 39 FA 43 BF C1 93 E8 66 E8 F2
                       7A 0A F5 E4 39 80 80 09 1A 30 0E 0D 5C F0 0F 32

      EAPOL HMAC     : 71 2A 78 DA 66 40 64 8C 1C 79 A7 3A F4 0B ED F0

C:\Users\User>
```

Once we have the two files, we can run the cracking program (aircrack-ng.exe). The cracking program is located a couple directories deep in the aircrack-ng-1.2-rc3-win folder. There's probably a way to "install" aircrack-ng. But we can simple run the single program easy enough by just typing its "relative path" in the command line (this is where is is relative to where we are).

Next we have some arguments for it. First argument is the BSSID of the network we want to try and crack (B4:75:0E:78:89:30). Argument two is the dictionary file that we want to use (500.txt). Lastly, we need to tell it what file the capture is in (dictionary.cap).

If the password is in the dictionary, you'll get the above message showing that the key was found.



If the password is not in the dictionary, we can try and brute force it with john (brute force just means try every possible combination...this can take a while). Note that we're using the "relative path" to the john.exe program.

Now things really get complicated again. The command before the "|" character is generating all printable keys of length 8 (note, WPA passwords are 8-63 characters long).

The second command is the previous aircrack-ng command with one change, the "dictionary.cap" has been replaced with a "-". This is a special way of telling aircrack-ng to take information passed to it through a pipe as the dictionary file.

This should also crack the password.