

Forum:[Hack Forums](#)

Thread: [Hak5](#)

luddwi - November 7, 2018, 8:16 am

Hey long time lurker here deciding to contribute to the community. Going to make this as simple and easy to understand as possible.

Rubber Ducky

Spoiler ([Click to View](#))

A rubber ducky is a usb device that a computer thinks is a keyboard. It injects strings of code called a payload into the computer. It looks just like a Ordinary USB Flash drive.

Where to get one

You can head over to the hak5 shop and purchase one for 45\$, but I recommend making my own for around 2\$ bucks a piece. You can find tutorials on how to make a rubber ducky on youtube.

Payloads

Here is a short list of the basic things a Rubber Ducky PDownload and execute files

Grab known wifi keys

Reverse Shell

Wifi Backdoor

+Many More

You can find many more with a quick google search.

Specs

60 MHz 32-bit CPU, convenient type-A USB connector, Micro SD expandable memory, programmable payload replay button, JTAG interface with GPIO and DFU bootloader

I will not be covering the Bash Bunny but it's essentially a rubber ducky and lan turtle combined but not as good as having both

Network Implants

Spoiler ([Click to View](#))

Lan Turtle

Main FeaturesCan scan with nmap and use meterpreter on metasploit

Extract packets

Access to entire Lan

Gather Pcap files

Out of band remote access (3G model only)

Packet Squirrel

Main FeaturesScripts

Switch (a button you can press to easily select from different payloads)

Stealthy

Can be used as a firewall and vpn

Can gather packets

Both of these are MitM attacks and are very deadly in the right hands, both 45\$ off the hak5 shop are very worth.

[b]Wifi Pineapple

Spoiler ([Click to View](#))

The WiFi Pineapple lets pentesters perform targeted man-in-the-middle attacks, advanced reconnaissance, credential harvesting, open source intelligence gathering and more – all from a clean, intuitive web interface.

copy/paste of its features since they explain it well

1. Perform advanced man-in-the-middle attacks by thoroughly mimicking preferred networks
2. Gather intelligence, including what other networks the targets have connected
3. Completely visualizes the WiFi landscape with continuous, live passive monitoring
4. Capture WPA and WPA Enterprise credentials in pcap, hashcat, JTR or plaintext formats
5. All without impacting out-of-scope neighbors from an easy, cross-platform web interface

it honestly blows my mind how good this hardware is tbh.

have fun :) I plan to later on make a full in-depth guide on the wifi-pineapple so stay tuned. I hope I went over everything well if anyone doesn't understand something Im here to help also let me know if I left anything out. peace

?Criminal - November 7, 2018, 11:03 am

I have an exploit on hak5.org to pull anyones info that ordered a rubber ducky thats the ironic part about this.

luddwi - November 7, 2018, 11:29 am

(Nov 7, 2018 12:03 PM)?Criminal Wrote: [\[CITE\]](#) I have an exploit on hak5.org to pull anyones info that ordered a rubber ducky thats the ironic part about this.

pm me

biggioturbomaster - November 7, 2018, 11:37 am

(Nov 7, 2018 12:03 PM)?Criminal Wrote: [\[CITE\]](#) I have an exploit on hak5.org to pull anyones info that ordered a rubber ducky thats the ironic part about this.

Probably disclose it to them and if its real maybe they'll be cool about it and send you some swag? I've met Mubix and if they're all as chill as him they probably will.

?Criminal - November 7, 2018, 11:47 am

(Nov 7, 2018 12:37 PM)biggioturbomaster Wrote: [\[CITE\]](#) Probably disclose it to them and if its real maybe they'll be cool about it and send you some swag? I've met Mubix and if they're all as chill as him they probably will.

doubt it's something they'll care about it's just order enumeration but maybe it's something they will fix unsure lol it effects more then just hak5.org it's a bug in a shopify community plugin they utilize

that about 3,000 stores use and I don't believe shopify themselves will care enough to payout or fix it, it's kind of complex to exploit and takes some time but discloses all info on any order.

luddwi - November 7, 2018, 11:53 am

(Nov 7, 2018 12:37 PM)biggioturbomaster Wrote: [\[CITE\]](#) Probably disclose it to them and if its real maybe they'll be cool about it and send you some swag? I've met Mubix and if they're all as chill as him they probably will.

yea you will most likely get more money from hak5 than from selling the exploit/database

?Criminal - November 7, 2018, 11:58 am

(Nov 7, 2018 12:53 PM)luddwi Wrote: [\[CITE\]](#) yea you will most likely get more money from hak5 than from selling the exploit/database

it's not a database and it's not really an "exploit" per say I consider it more of an implementation flaw in how the shopify plugin works and you can abuse intended functionality to disclose orders because theres no rate limit you can go through tons of order number combos without much trouble, the most hak5 can do is disable it since shopify is cloud hosted, I don't believe hak5 themselves can modify the plugin to add rate limits.

Elvira - November 7, 2018, 4:57 pm

i ordered a pineapple from them once. i decided to spam wifi AP's named "black people" for some reason. bricked it..... is a cool product when it works

luddwi - November 7, 2018, 5:06 pm

(Nov 7, 2018 05:57 PM)Elvira Wrote: [\[CITE\]](#) i ordered a pineapple from them once. i decided to spam wifi AP's named "black people" for some reason. bricked it..... is a cool product when it works
Unfortunate man ?