

# Forum:[Hack Forums](#)

Thread: [./Dark Legion/The Dark Art of Phishing: Crafting a Wireless Honeypot](#)

**Dread.Reaper** - April 4, 2023, 7:28 am

@Genuine@

## The Dark Art of Phishing: Crafting a Wireless Honeypot

Written By: Dread.Reaper – Dark Legion

### Introduction:

In the realm of cyber deception, phishing remains a potent weapon. It relies on the exploitation of human vulnerability through social engineering to achieve its nefarious goals. This guide takes you on a journey through the technicalities of building a wireless honeypot, a tool designed to lure unsuspecting victims into the trap of phishing. You'll learn how to create a Wi-Fi hotspot under the guise of "Free Public Wifi," serving seemingly legitimate web content or files to attract and manipulate users.

### Design:

Spoiler ([Click to View](#))

### Prerequisites:

To follow this guide, you will need the following hardware and software:

#### Hardware:

- GL.iNet GL-B1300 (Convexa-B) router
- Raspberry Pi 4
- Wireless modem or Ethernet connection from a modem source with internet access

#### Software:

- DD-WRT custom firmware
- Raspberry Pi OS
- mitmproxy

### Setup:

First, flash the DD-WRT custom firmware onto the GL.iNet GL-B1300 router.

- Download the latest DD-WRT firmware for the GL-B1300 router from the DD-WRT website.
- Connect your computer to the router using an Ethernet cable.
- Open a web browser and navigate to the router's default IP address (usually 192.168.1.1).
- Log in to the router using the default username and password (usually "admin").
- Navigate to the "Administration" tab and select "Firmware Upgrade".
- Click the "Choose File" button and select the DD-WRT firmware file you downloaded earlier.
- Click the "Upload" button and wait for the firmware to install.
- After the firmware is installed, navigate to the "Setup" tab and configure the router with your preferred settings.

Connect the Raspberry Pi 4 to the router using an Ethernet cable.

Next we will install the Raspberry Pi OS and connect to it:

- Download the latest version of Raspberry Pi OS from the official Raspberry Pi website.
- Insert the microSD card into your computer.
- Use the Raspberry Pi Imager software to flash the Raspberry Pi OS image onto the microSD card.

You can download the Raspberry Pi Imager from the official Raspberry Pi website.

- Once the image is flashed onto the microSD card, insert it into the Raspberry Pi 4.
- Connect the Raspberry Pi 4 to your network using an Ethernet cable.
- Power on the Raspberry Pi 4.
- Use an SSH client to connect to the Raspberry Pi 4. You can use the Terminal app on macOS or Linux, or PuTTY on Windows.
- Open the SSH client and enter the following command to connect to the Raspberry Pi 4:  
`ssh pi@<ip-address>`
- Replace <ip-address> with the IP address of your Raspberry Pi 4. You can find the IP address by logging in to your router's admin interface or by using an IP scanner app.
- If prompted, enter the default password `raspberrypi`.
- Once connected, you can start configuring the Raspberry Pi 4 and installing the required software.

### Install and Configuration:

- Install mitmproxy using the following command:

```
sudo apt-get update
```

```
sudo apt-get install mitmproxy
```

- Create a new file called "mitm.py" on the Raspberry Pi 4 using the following command:

```
nano mitm.py
```

•

- Save and exit the "mitm.py" file.
- Start mitmproxy by running the following command:

```
mitmproxy -s mitm.py
```

- Connect to the honeypot WiFi network on a separate device and attempt to log in to a website.
- Check the output of the mitmproxy console for captured login credentials.

### Conclusion:

Crafting a wireless honeypot for phishing purposes is a complex endeavor, requiring a keen understanding of networking and web technologies. This guide serves as a starting point to develop these skills, but tread carefully. Deception, while fascinating, is a double-edged sword, and wielding it without caution can lead to unintended consequences. By exploring this dark art, we uncover the inner workings of phishing and better equip ourselves to recognize and counteract such threats in the digital landscape.

pe.

**WoodenHero** - April 5, 2023, 1:20 pm

Thank you for sharing this Tutorial for free, it is really simple and nice to start with

**Dread.Reaper** - April 5, 2023, 1:22 pm

(Apr 5, 2023 01:20 PM)WoodenHero Wrote: [\[CITE\]](#) Thank you for sharing this Tutorial for free, it is really simple and nice to start with

This really is not a very simple setup but I tried to make it as direct and straight forward as possible however.

Please let me know if you have any feedback or suggestions to improve design or functionality.

This is kinda theoretical concept at the moment stemmed from another thread I was in yesterday..

lots of room for improvement still I am sure.

Full article and PDF Download is here BTW: