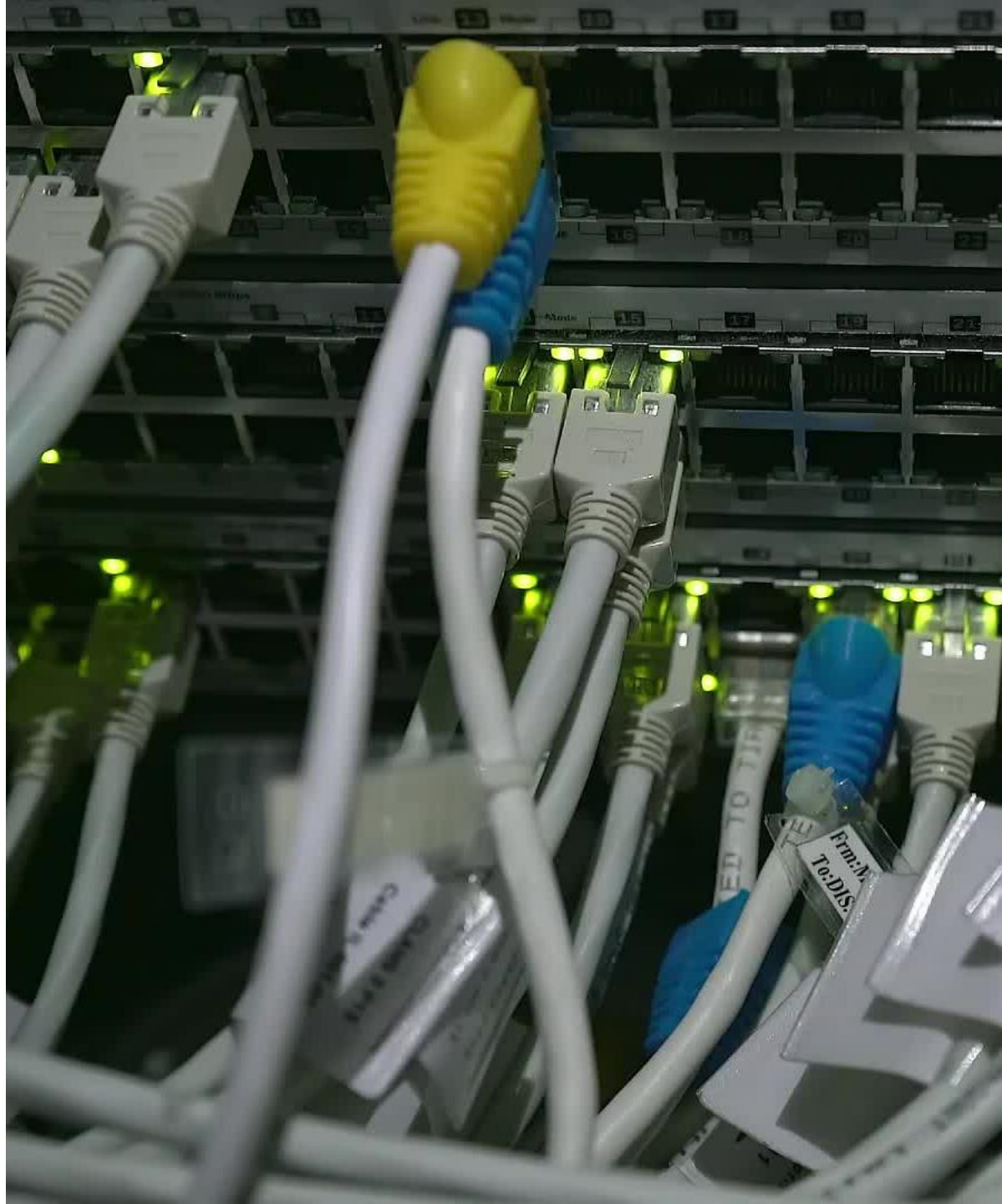
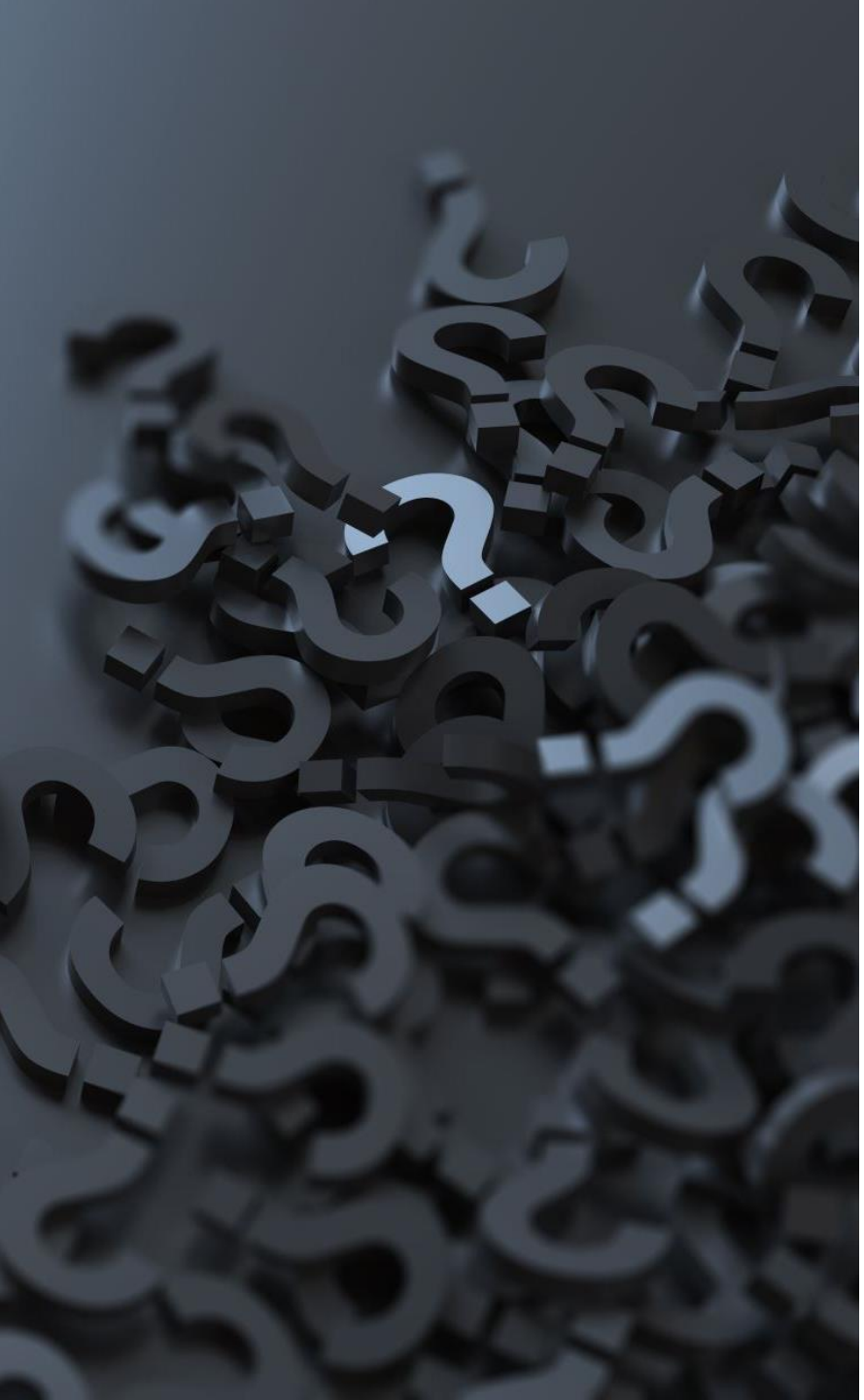
Etherjack

by nDepth Security

Physical pentest-assisting capability

Developed by: Raymond Nutting





BIO

- Bachelors' degree in Computer Information Systems, Minor in Information Security
- Hold multiple industry recognized certifications (CISSP-ISSEP, PenTest+, CEH, etc.)
- 23+ years IT and IA experience within public and private industry.
- Published author and co-author of three (3) McGraw-Hill All-in-One certification exam books:
  - CompTIA PenTest+ PT0-001
  - CompTIA PenTest+ PT0-002
  - GPEN GIAC Certified Pentester
- Founder and President / CEO of nDepth Security - https://ndepthsecurity.com

PROBLEM STATEMENT

- Physical pentesting helps validate organizational physical security controls.
- When physical protections can be compromised, pentesters will attempt exploitation of computer network devices using physical access to gain persistence to a target network.
- Pentesters will generally use specialized tools, such as USB-enabled devices to interface to a computer and attempt exploitation through execution of a malicious payload.
- In some cases, USB ports are either not available or inaccessible during the time of the pentest.
- Having additional complementary tools to support more use cases can ultimately improve a pentesters' chances of successfully gaining access to a target network.

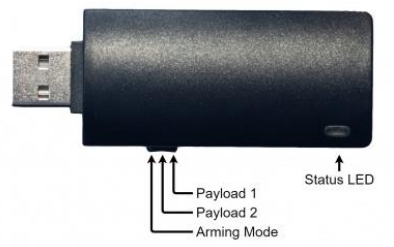
WHAT IS EHTERJACK?

- EtherJack or "EJ", is a "plug-and-pray" leave behind device that can be used to establish different levels of persistence on a target network through a series of software and hardware configurations.
- EJ was developed by and for pentesters to help support and aid in physical pentesting engagements by means of open/available RJ-45 Ethernet ports.
- EJ helps bring to light what a malicious actor can do when having physical access to an organization's network and how poor network security hygiene can lead to devastating consequences.
- EJ offers a complimentary solution to existing physical pentest-assisting capabilities and allows offensive security practitioners to expand their toolkits used during physical pentests and offers an additional leave-behind component that can accommodate most physical constraints and user requirements.
- As pentesters, ***we should leave no port untested!***

CAPABILITIES WITH SIMILAR INTERESTS

1

2



4

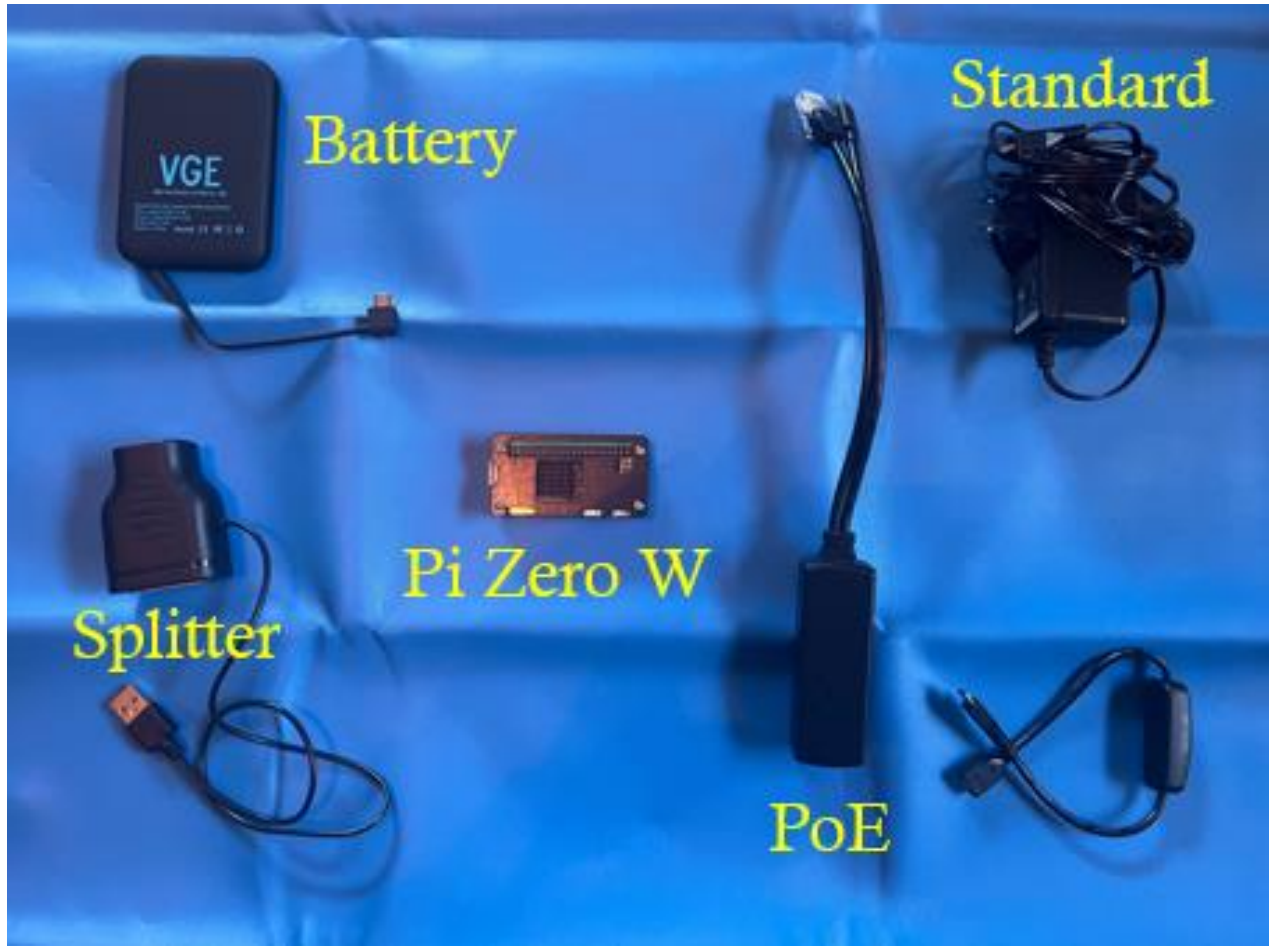
3

1. Hak5 USB Rubber Ducky
2. BashBunny
3. LAN Turtle
4. P4wnP1 A.L.O.A (A Little Offensive Application)

**All these capabilities attach to a USB port on a target host. What if a USB interface is not available?

HARDWARE

- **Raspberry Pi Zero W or Zero 2 W**.
- **microSD card** (64GB+ recommended).
- **Portable power bank** (micro-USB connection) or Pisugar Lithium Battery
- **Raspberry Pi Zero W** Basic Starter Kit provides assortment of necessary cables and accessories.
- **Micro USB Ethernet Adapter** for Raspberry Pi Zero
- **IEEE 802.3af Micro USB PoE Adapter** for Raspberry Pi for switches that support PoE.
- **USB-powered Ethernet Splitter** to share host network drop.
- **Ethernet cables** support network connectivity.
- **Raspberry Pi Zero Case kit** for protection and concealment (case will vary if Pisugar battery is used).
- **External Hard Drive Case** to store EtherJack hardware



IF YOU BUILD IT $HELLS WILL COME

~ $160

- Case - $15
- Splitter - $15
- Battery - $26
- PoE adapter - $15
- Pi Zero W - $25
- Pi Zero Case Kit - $13
- (2) Ethernet cables - $3
- RJ-45 adapter - $15
- Micro SD card - $25

Etherjack by nDepth Security

SOFTWARE

- Kali ARM (for Pi Zero W) .
- BASH scripting to carry out activities.
  - **Note**: EJ runs as a service
- C2 client with asynchronous communication.
  - **Example**: Bishop Fox's Sliver client in "beacon mode" that periodically checks in for tasking.
- Simple exploit to interact with EJ.
  - **Example**: Metasploit meterpreter payload.


```
#!/bin/bash
```

POWER MODES

- **Standard** - the most standard way to power EJ is using the 3.3v Pi power adapter that comes with the starter kit. The adapter terminates to a micro-USB interface that can be plugged into one of the two (2) available ports on the Pi Zero W.
- **PoE** - Power over Ethernet (PoE) can be achieved using the IEEE 802.3af Micro USB PoE Adapter and a network switch with an available PoE Ethernet port. This is the most optimal and convenient method you can use to power EJ since it requires less hardware and setup to obtain persistence. The PoE adapter provides power and Ethernet connectivity to the target network.
- **Battery** - When standard or PoE power methods are out of play, EJ can be powered using a portable battery bank which terminates to a micro-USB interface that can be plugged into an available USB port on the Pi. Mileage will vary on these portable components so time will be of the essence. When these power components are in play be sure to plan your remote activities accordingly.

CONFIGURATION MODES

- **LAN** - EJ operates passively in the background to blend and attach the ethernet interface to a RFC1918 compliant network using a sample of ARP packets collected on the network. The total number of ARP packets to sample/collect is defined in the **`EtherJack.conf`** file. Once the interface is configured, EJ will attempt to identify a gateway and execute a pre-defined payload to callhome and obtain persistent access on the network.
- **PRESET** - EJ configures the ethernet interface with user-provided settings (i.e., static IP or DHCP configuration). These settings are defined in the **`preset/preset.conf`** file. EJ will test/validate the preset settings and if testing is successful, EJ will execute the pre-defined payload to callhome and obtain persistent access on the network.
- **WIFI** - EJ operates as a rouge Wi-Fi access point using **`hostapd`** and **`dnsmasq`** for DHCP leasing. The **`wifi/wifi.conf`** file is used to configure the rouge Wi-Fi network address and IP address of wlan0. The **`wifi/hostapd.conf`** file defines the configuration settings for the wireless network.

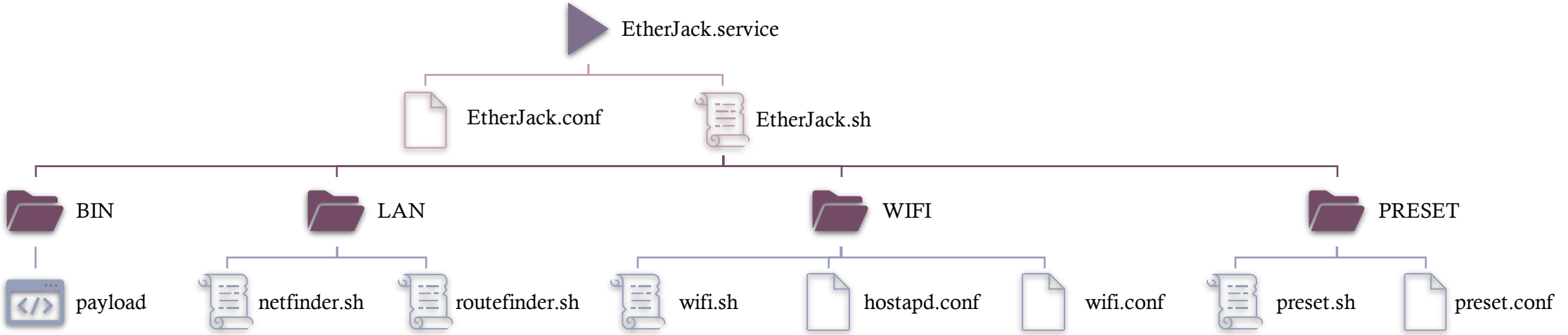
ETHERJACK INSTALLATION

- EJ is opensource and distributed under the GNU GPLv3 license.
- EJ can be installed from the nDepth Security GitHub repository:
  - https://github.com/ndepthsecurity/EtherJack

nDepth SECURITY

etherjack

ETHERJACK LAYOUT



ETHERJACK SETUP

- The `README.md` file provides details on how to install and configure EJ in all three (3) power and configuration modes:
  - Prerequisites
    1. Install Kali AM for Pi Zero W
    2. Update/upgrade Kali operating system
  - EtherJack Installation
    1. Git pull EtherJack repository in `/usr/local`.
    2. Install the EJ motd.
    3. Enable the `EtherJack.service`.
    4. Change the hostname to "etherjack"
    5. Disable some operating system services.
    6. Install packages (i.e., hostapd, dnsmasq)

- EtherJack Setup (EtherJack.conf)
  1. Set configuration mode (LAN, PRESET, WIFI) in EtherJack.conf file.

     ```
     sed -i 's/EJMODE=.*/EJMODE=LAN/' EtherJack.conf
     ```

  2. Define payload to execute.

     ```
     sed -i 's/EJEXE=.*/EJEXE=payload/' EtherJack.conf
     ```

  3. Define test IP and port for Internet checks (example.com).

     ```
     sed -i 's/TESTIP=.*/TESTIP=93.184.216.34/'
     EtherJack.conf
     sed -i 's/TESTPORT=.*/TESTPORT=80/' EtherJack.conf
     ```

SETTING UP LAN MODE

- There is very little to do as far as configuration in this mode.
- The only thing you may want to adjust is the sample size of ARP packets to collect. The default setting is five (5) packets.
- Depending on how active the network is will determine the amount of time required to collect the desired sample size defined in the EtherJack.conf file.
- Change as needed:

```
sed -i 's/PKTS=.*/PKTS=5/' EtherJack.conf
```

SETTING UP PRESET MODE

- Update the `preset/preset.conf` file and define if the target network uses DHCP:

```
sed –i 's/CONFIG=.*/CONFIG=DHCP/' preset/preset.conf
```

- Update the `preset/preset.conf` file with the appropriate STATIC configuration settings if the environment does NOT use DHCP:

```
# Example settings
sed -i 's/CONFIG=.*/CONFIG=STATIC/' preset/preset.conf
sed -i 's/IPADDR=.*/IPADDR=192.68.10.57/' preset/preset.conf
sed -i 's/NETMASK=.*/NETMASK=255.255.255.0/' preset/preset.conf
sed -i 's/GATEWAY=.*/GATEWAY=192.168.10.254/' preset/preset.conf
sed -i 's/NAMESERVER=.*/NAMESERVER=8.8.8.8/' preset/preset.conf
```

SETTING UP WIFI MODE

- WIFI mode enables users to have persistent access to the target environment without taking the risk of, or attempting to, connect to the Internet through the customer's network. It offers an out-of-band connection that users can interact with safely, within proximity of the EJ access point.
- After associating and authenticating to the EJ Wi-Fi access point, you can SSH to EJ using the kali user account and attempt further exploitation on to the target network using the eth0 interface.
- Update the `wifi/wifi.conf` file to define the network address, IP address for wlan0, and the netmask:

```
# Example settings
sed -i 's/WLANNET=.*/WLANNET=172.16.0/' wifi/wifi.conf
sed -i 's/WLANIP=.*/WLANIP=172.16.0.1/' wifi/wifi.conf
sed -i 's/MASK=.*/MASK=24/' wifi/wifi.conf
```

- Update the `hostapd.conf` file to define the hardware mode, Wi-Fi channel, SSID, and passphrase/password for the Wi-Fi network:

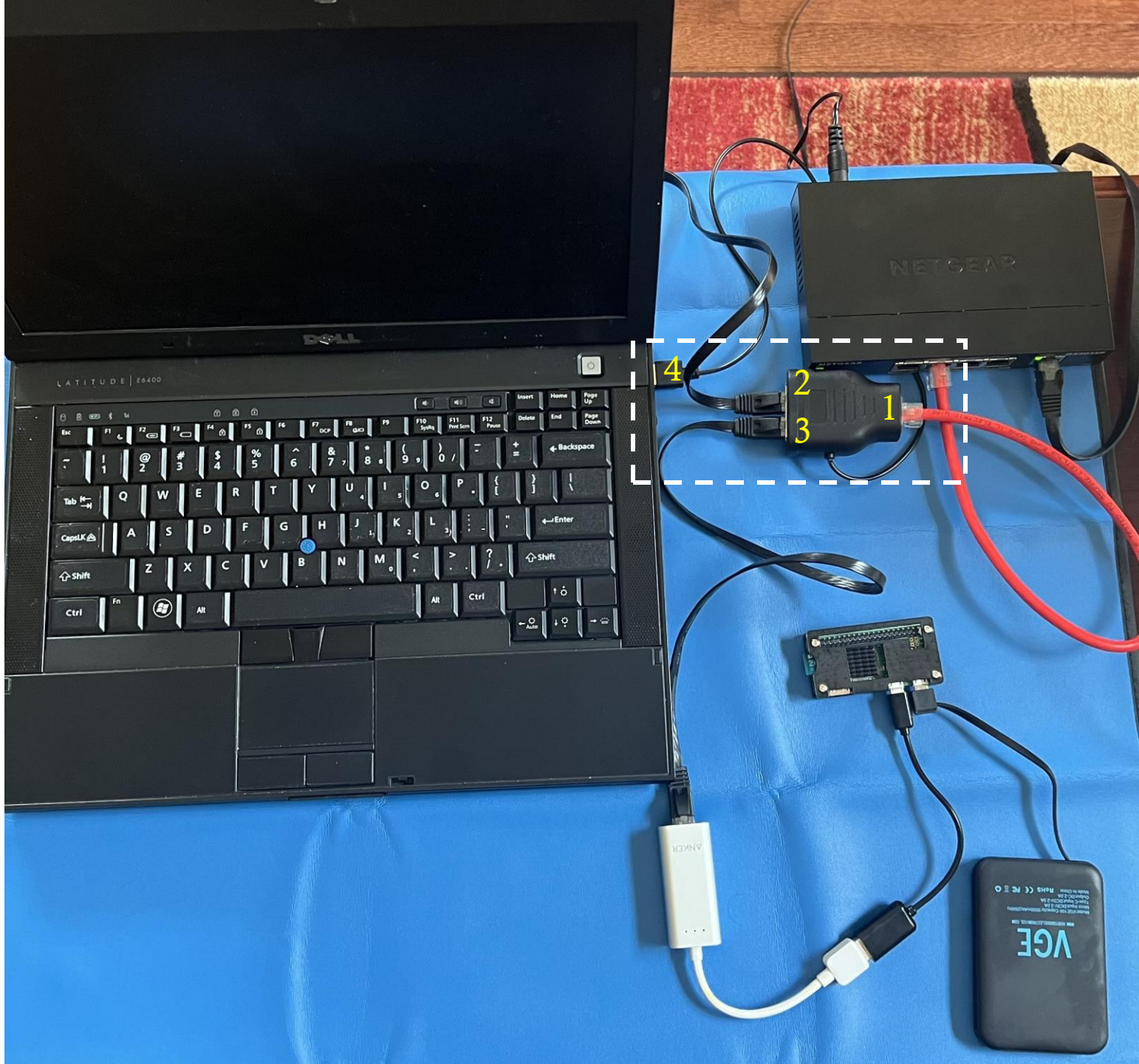
```
# Example settings
sed -i 's/hw_mode=.*/hw_mode=g/' wifi/hostapd.conf
sed -i 's/channel=.*/channel=11/' wifi/hostapd.conf
sed -i 's/ssid=.*/ssid=EJNET/' wifi/hostapd.conf
sed -i 's/wpa_passphrase=.*/wpa_passphrase=Pa22word/'
wifi/hostapd.conf
```

POE

- **PoE** – The Pi Zero utilizes a PoE dongle that connects to a PoE switch.

ETHERNET SPLITTER

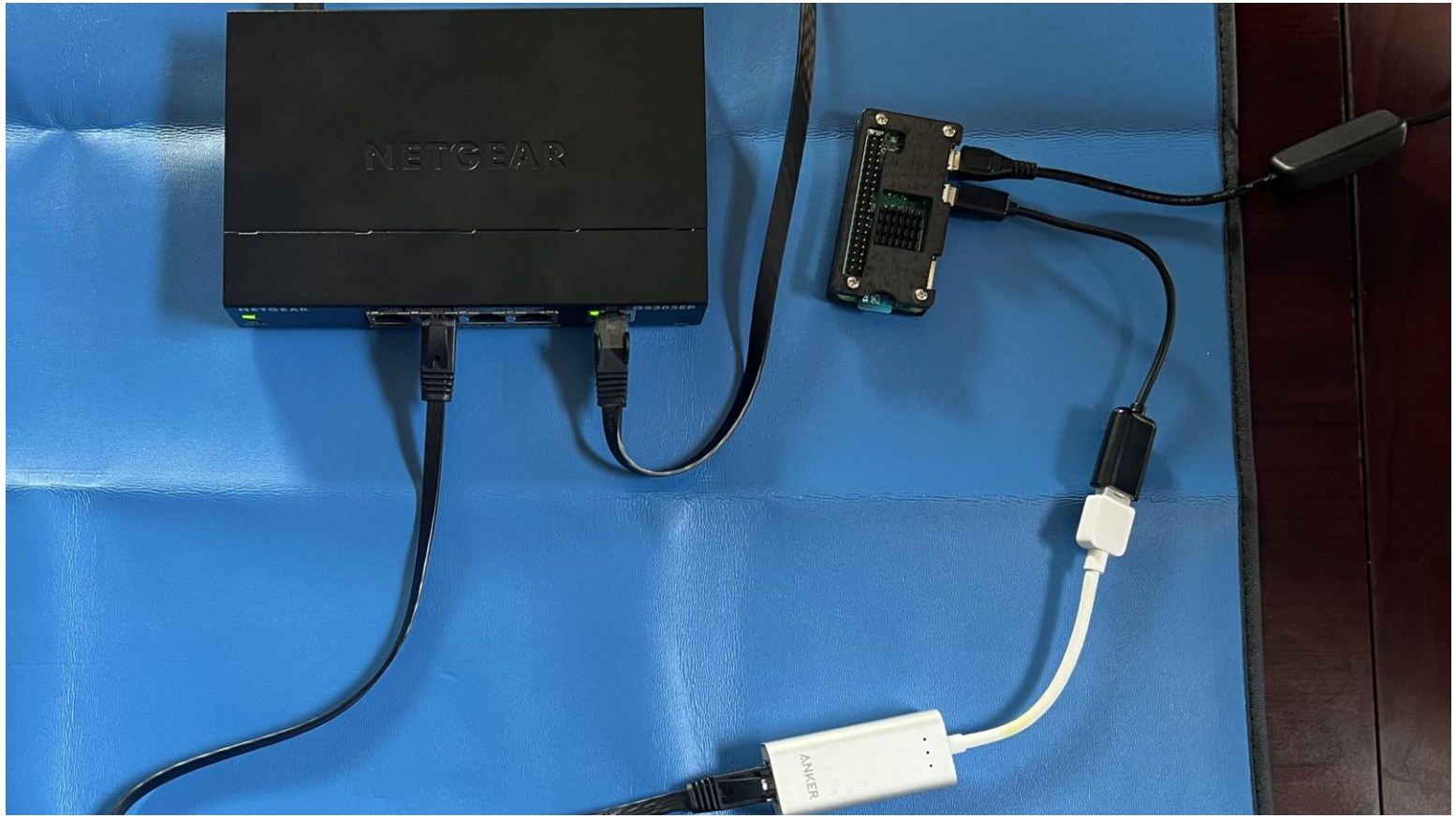
- **Splitter** – The Pi Zero plugs into a RJ-45 Ethernet splitter to share an existing network connection with an adjacent host.
  - 1 - Existing network connection
  - 2 - Ethernet going to computer
  - 3 - Ethernet going to EJ
  - 4 – Splitter draws power from computer over USB.
    - *Note: If USB is disabled on computer, use a USB wall charger.*



Etherjack

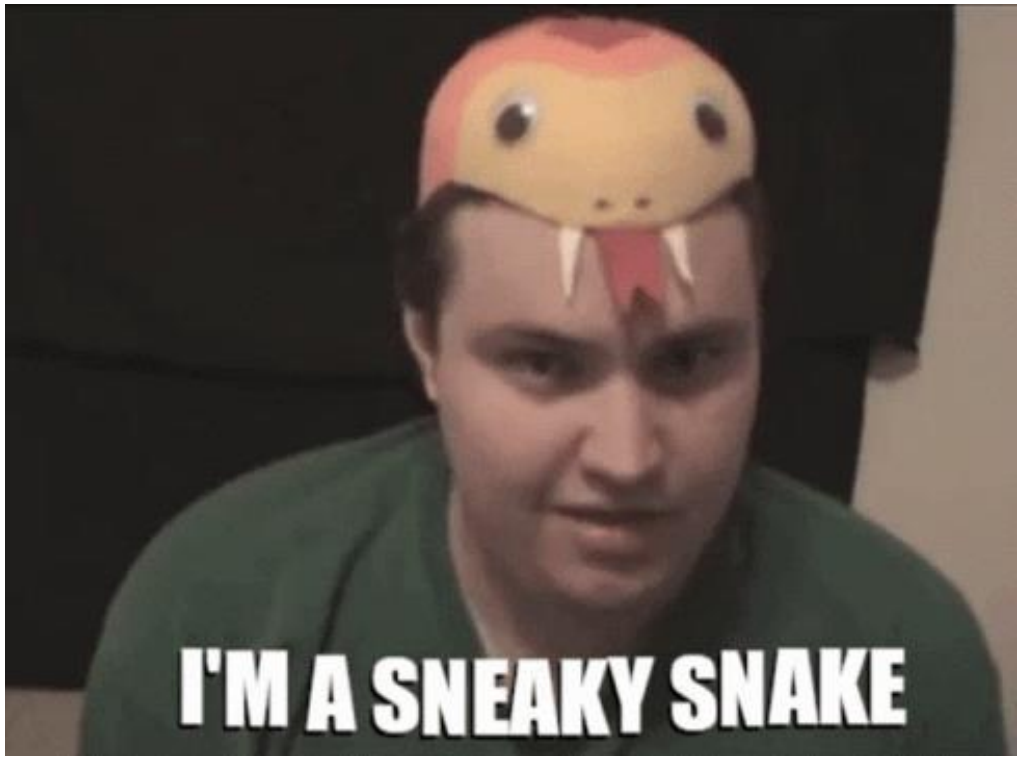
– NON-POE

Non-PoE – The Pi Zero plugs into a standard Layer-3 RJ-45 network port.



CONCLUSION

- EJ is a complimentary solution to existing physical pentest-assisting capabilities.
- EtherJack (EJ) is a capability that can be used to provide persistence on a target network during a physical pentest by utilizing an available RJ-45 Ethernet port.
- EJ supports multiple power and configuration modes to help accommodate most physical constraints.
- EJ demonstrates what a malicious actor can do when having physical access to an organization's network and how poor network security hygiene can lead to devastating consequences.
- EJ is hardware/software agnostic and can be customized to meet user requirements.



QUESTIONS ?

Raymond Nutting - EtherJack – A Plug-and-pray Leave Behind Device

3F81CE