# Reprise: Developing & Prototyping Honeypots

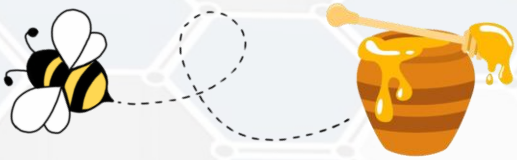
Anna Xu, Angel Huang, Kalkidan Behailu, Luca Laureno

## Introduction: What is a Honeypot?

A honeypot is like a mouse trap, set to **lure** in cyber-attackers to protect IT Infrastructure. The goal of our project is to develop a honeypot that mimics a VPN system that can be deployed on the networks of various universities.

The honeypot is a decoy system that mimics a real computer system or network but is designed to

1. **Detect**
2. **Deflect**
3. **Study**



hacking attempts!

When hackers attack the honeypot, their activities are **monitored and analyzed** to understand their techniques, tools, and goals. This information is then used to **improve security measures** for the real systems.

## VPN

VPN stands for Virtual Private Network, and it is a technology that creates a secure and encrypted connection over a less secure network, such as the internet.

## VPN Honeypot

Our VPN honeypot mimics a real VPN server that users connect to and use. Our VPN honeypot is programmed to log information when someone connects or even attempts to connect to the honeypot. These logs can then be seen in the STINGAR website.

Our honeypot logs:

- IP address
- Geolocation
- Date / Time

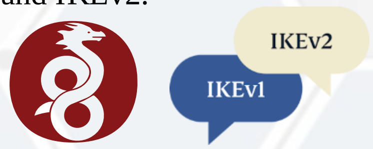
## Docker Containers

Our honeypot runs in a Docker container. A Docker container is like a small, lightweight package that holds everything an application needs to run: the code, libraries and settings

- This ensures the app **works the same everywhere**, whether it's on a developer's laptop, a testing environment, or a production server
- Containers are **isolated** from each other and the host system, which makes them **efficient and secure**.

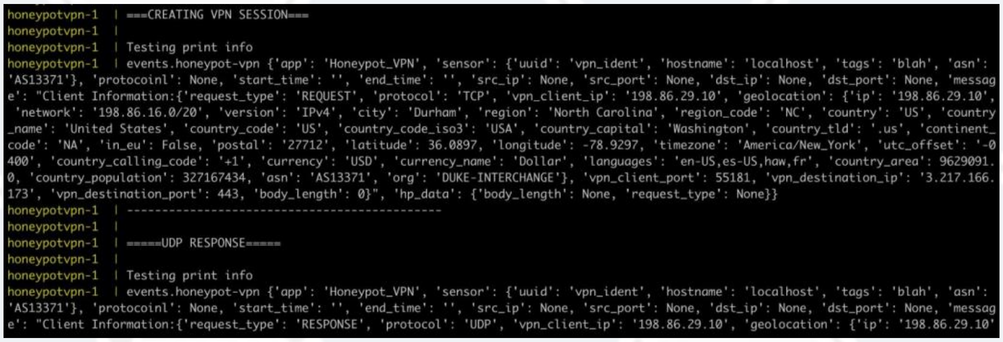
## Our Results

Our VPN honeypot currently supports WireGuard, IKEv1, and IKEv2.



Scan here for a video demo

Our honeypot has been successfully programmed to collect the IP address/port, date, time, geolocation and more of any user attempting to gain access to the VPN network. This allows Duke's IT Security Office (ITSO), Cisco, and 80 other universities across the country (like Stanford, Brown, Columbia, etc.) to gather threat intelligence by monitoring and analyzing the activities of these attackers. Below are some example logs that our honeypot was able to collect.



```
honeypotvpn-1  | ===CREATING VPN SESSION===
honeypotvpn-1  |
honeypotvpn-1  | Testing print info
honeypotvpn-1  | events.honeypot-vpn {'app': 'Honeypot_VPN', 'sensor': {'uuid': 'vpn_ident', 'hostname': 'localhost', 'tags': 'blah', 'asn':
'AS13371'}, 'protocoinl': None, 'start_time': '', 'end_time': '', 'src_ip': None, 'src_port': None, 'dst_ip': None, 'dst_port': None, 'messag
e': "Client Information:{'request_type': 'REQUEST', 'protocol': 'TCP', 'vpn_client_ip': '198.86.29.10', 'geolocation': {'ip': '198.86.29.10',
 'network': '198.86.16.0/20', 'version': 'IPv4', 'city': 'Durham', 'region': 'North Carolina', 'region_code': 'NC', 'country': 'US', 'country
_name': 'United States', 'country_code': 'US', 'country_code_iso3': 'USA', 'country_capital': 'Washington', 'country_tld': '.us', 'continent_
code': 'NA', 'in_eu': False, 'postal': '27712', 'latitude': 36.0897, 'longitude': -78.9297, 'timezone': 'America/New_York', 'utc_offset': '-0
400', 'country_calling_code': '+1', 'currency': 'USD', 'currency_name': 'Dollar', 'languages': 'en-US,es-US,haw,fr', 'country_area': 9629091.
0, 'country_population': 327167434, 'asn': 'AS13371', 'org': 'DUKE-INTERCHANGE'}, 'vpn_client_port': 55181, 'vpn_destination_ip': '3.217.166.
173', 'vpn_destination_port': 443, 'body_length': 0}", 'hp_data': {'body_length': None, 'request_type': None}}
honeypotvpn-1  | ---------------------------------------------
honeypotvpn-1  |
honeypotvpn-1  | =====UDP RESPONSE=====
honeypotvpn-1  |
honeypotvpn-1  | Testing print info
honeypotvpn-1  | events.honeypot-vpn {'app': 'Honeypot_VPN', 'sensor': {'uuid': 'vpn_ident', 'hostname': 'localhost', 'tags': 'blah', 'asn':
'AS13371'}, 'protocoinl': None, 'start_time': '', 'end_time': '', 'src_ip': None, 'src_port': None, 'dst_ip': None, 'dst_port': None, 'messag
e': "Client Information:{'request_type': 'RESPONSE', 'protocol': 'UDP', 'vpn_client_ip': '198.86.29.10', 'geolocation': {'ip': '198.86.29.10'
```