Duke | Code

Reprise: Developing and Prototyping Honeypots

Kal Behailu, Angel Huang, Luca Laureno, Anna Xu

Duke | Code

MEET THE TEAM

Kalkidan Behailu
MechE + CS ‘27

Angel Huang
CS ‘26

Luca Laureno
CS + Psych ‘27

Anna Xu
MechE + CS ‘27

Duke | Code

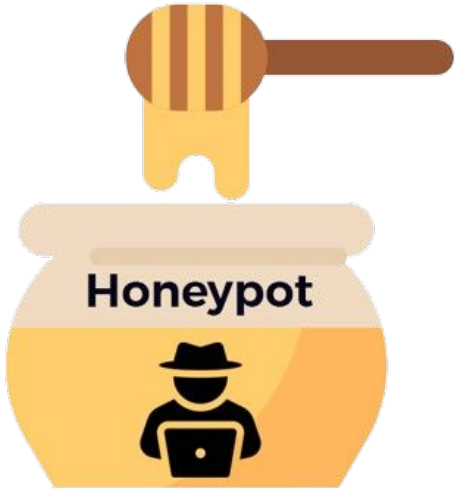
OUR GOAL

The goal of this project is to create a honeypot that emulates a virtual private network (VPN) server.

Duke | Code <+>

WHAT IS A HONEYPOT?

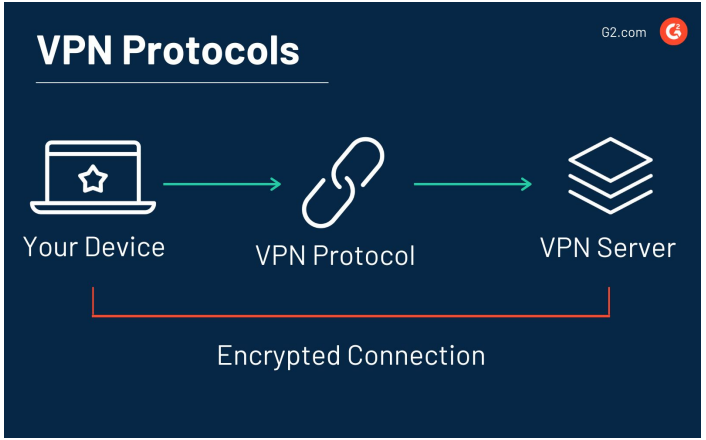
- ➔ Devices used to deceive cybercriminals/attackers
- ➔ Mimics services like VPNs, websites, etc.
- ➔ Collects data from the attacks



Duke | Code <+>

VPNs

- Provide secure, encrypted connections to users accessing the Internet
- Act as an intermediary between user's device and the Internet
- Different Protocols



Duke | Code <+>

STINGAR

- Our honeypot will be hosted on STINGAR
  - Shared Threat Intelligence for Network Gatekeeping and Automated Response
  - Honeypot platform owned by parent company Forewarned
  - Largest shared cyber threat platform in higher ed.
- Used by 80+ colleges nationwide

Duke | Code

HACKING TOOLS

Wireshark

- A type of packet sniffer
  - Used to capture + analyze network traffic
- Can detect suspicious activity and discover hacking attempts

Metasploit

- Tests network/device security by simulating attacks
  - Helps identify vulnerabilities before real hackers find them
- Often used with Nmap

Nmap

- Used to discover computers + services on a network
- Can help detect unauthorized devices/services
- Often used with Metasploit

Duke | Code

TECH STACK

Python

Docker

WireGuard

Ubuntu Linux

Fluent

strongSwan

Duke | Code <+>

BUILDING KALA

- Open-source framework on Github
  - Supports TCP + UDP, IKEv1/v2 + Wireguard
- Created honeypot Docker container
  - **First setback:** port usage conflict

Duke | Code

BUILDING KALA

- Testing honeypot connectivity – strongSwan and Wireguard
  - **Second setback:** WG port 9000 not accessible
    - Solution: add port to Dockerfile!
- Formatted WG logs to prevent flooding screen

Duke | Code

Level One

- Sender index
- Source IP
- Source port
- Dest IP
- Dest port

```
py-__init__[0497] | ======== WIREGUARD SETTING ========
honeypotvpn-1  | 2024-07-23 14:45:32,505 | INFO     | server.
py-__init__[0498] | PublicKey: kwcC05qapsVA28hoRI86ZUk6qlLM8s
c9mfeAaS8cuis=
honeypotvpn-1  | 2024-07-23 14:45:32,505 | INFO     | server.
py-__init__[0499] | ==================================
honeypotvpn-1  | 2024-07-23 14:45:32,505 | INFO     | server.
py-main[0618] | Serving on UDP :9000 (WIREGUARD)...
honeypotvpn-1  |
honeypotvpn-1  | ===LEVEL ONE LOGGING===
honeypotvpn-1  |
honeypotvpn-1  | 2024-07-23 14:45:40,040 | INFO     | server.
py-datagram_received[0547] | LOGIN FROM ('198.86.29.9', 42620
), SENDER INDEX 2007336512:
honeypotvpn-1  | ----------------------------------------
honeypotvpn-1  |
honeypotvpn-1  | =====INITIAL CONNECTION=====
honeypotvpn-1  |
honeypotvpn-1  | 2024-07-23 14:45:40,051 | INFO     | ip.py-h
andle_ipv4[0501] |
honeypotvpn-1  | TCP FROM 198.86.29.9:56551 -> 52.22.119.135:
443
honeypotvpn-1  |  DATA=b''
```

Duke | Code

```
honeypotvpn-1  |
honeypotvpn-1  | ===LEVEL TWO LOGGING===
honeypotvpn-1  |
honeypotvpn-1  | 2024-07-23 16:25:20,466 | INFO     | server.py-datagram_receiv
ed[0550] | LOGIN FROM ('198.86.29.9', 9724), SENDER INDEX 2940401074:
honeypotvpn-1  | ----------------------------------------
honeypotvpn-1  |
honeypotvpn-1  | =====INITIAL CONNECTION=====
honeypotvpn-1  |
honeypotvpn-1  | 2024-07-23 16:25:20,480 | INFO     | ip.py-handle_ipv4[0501] |

honeypotvpn-1  | TCP FROM 198.86.29.9:57612 -> 8.8.4.4:443
honeypotvpn-1  |  DATA=b''
honeypotvpn-1  | ----------------------------------------
honeypotvpn-1  |
honeypotvpn-1  | ===CREATING VPN SESSION===
honeypotvpn-1  |
honeypotvpn-1  | {'ip': '198.86.29.9', 'network': '198.86.24.0/21', 'version':
'IPv4', 'city': 'Durham', 'region': 'North Carolina', 'region_code': 'NC', 'cou
ntry': 'US', 'country_name': 'United States', 'country_code': 'US', 'country_co
de_iso3': 'USA', 'country_capital': 'Washington', 'country_tld': '.us', 'contin
ent_code': 'NA', 'in_eu': False, 'postal': '27705', 'latitude': 36.0229, 'longi
tude': -78.9464, 'timezone': 'America/New_York', 'utc_offset': '-0400', 'countr
y_calling_code': '+1', 'currency': 'USD', 'currency_name': 'Dollar', 'languages
': 'en-US,es-US,haw,fr', 'country_area': 9629091.0, 'country_population': 32716
7434, 'asn': 'AS13371', 'org': 'DUKE-INTERCHANGE'}
```

Level Two

- Level 1 logs
- VPN session
- Some requests
- More client info

Duke | Code <+>

Level Three

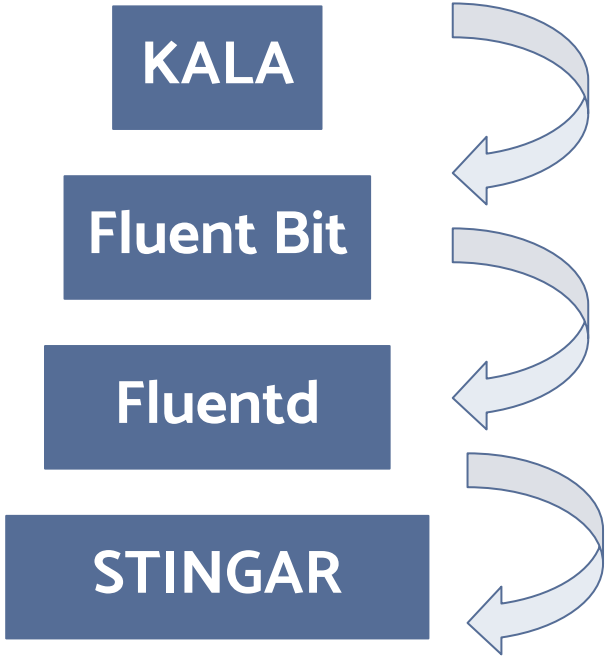
- Levels 1 and 2
- Every request/response
- All client info

```
GE'}, 'vpn_client_port': 56617, 'vpn_destination_ip': '142.25
1.179.188', 'vpn_destination_port': 5228, 'body_length': 0}
honeypotvpn-1  | ----------------------------------------
-
honeypotvpn-1  |
honeypotvpn-1  | =====UDP REQUEST=====
honeypotvpn-1  |
honeypotvpn-1  | {'ip': '239.255.255.250', 'error': True, 're
ason': 'Reserved IP Address', 'reserved': True, 'version': 'I
Pv4'}
honeypotvpn-1  | 2024-07-23 14:47:26,907 | INFO     | ip.py-h
andle_ipv4[0465] | Client Information:{'request_type': 'REQUE
ST', 'protocol': 'UDP', 'vpn_client_ip': IPv4Address('239.255
.255.250'), 'vpn_destination_ip': '198.86.29.9', 'vpn_destina
tion_port': 58436, 'body_length': 176}
honeypotvpn-1  | ----------------------------------------
--------
honeypotvpn-1  |
honeypotvpn-1  | =====UDP REQUEST=====
honeypotvpn-1  |
honeypotvpn-1  | 2024-07-23 14:47:27,683 | INFO     | ip.py-h
andle_ipv4[0465] | Client Information:{'request_type': 'REQUE
ST', 'protocol': 'UDP', 'vpn_client_ip': IPv4Address('239.255
.255.250'), 'vpn_destination_ip': '198.86.29.9', 'vpn_destina
tion_port': 58436, 'body_length': 176}
```

Duke | Code <+>

FINISHING TOUCHES

DATA FLOW

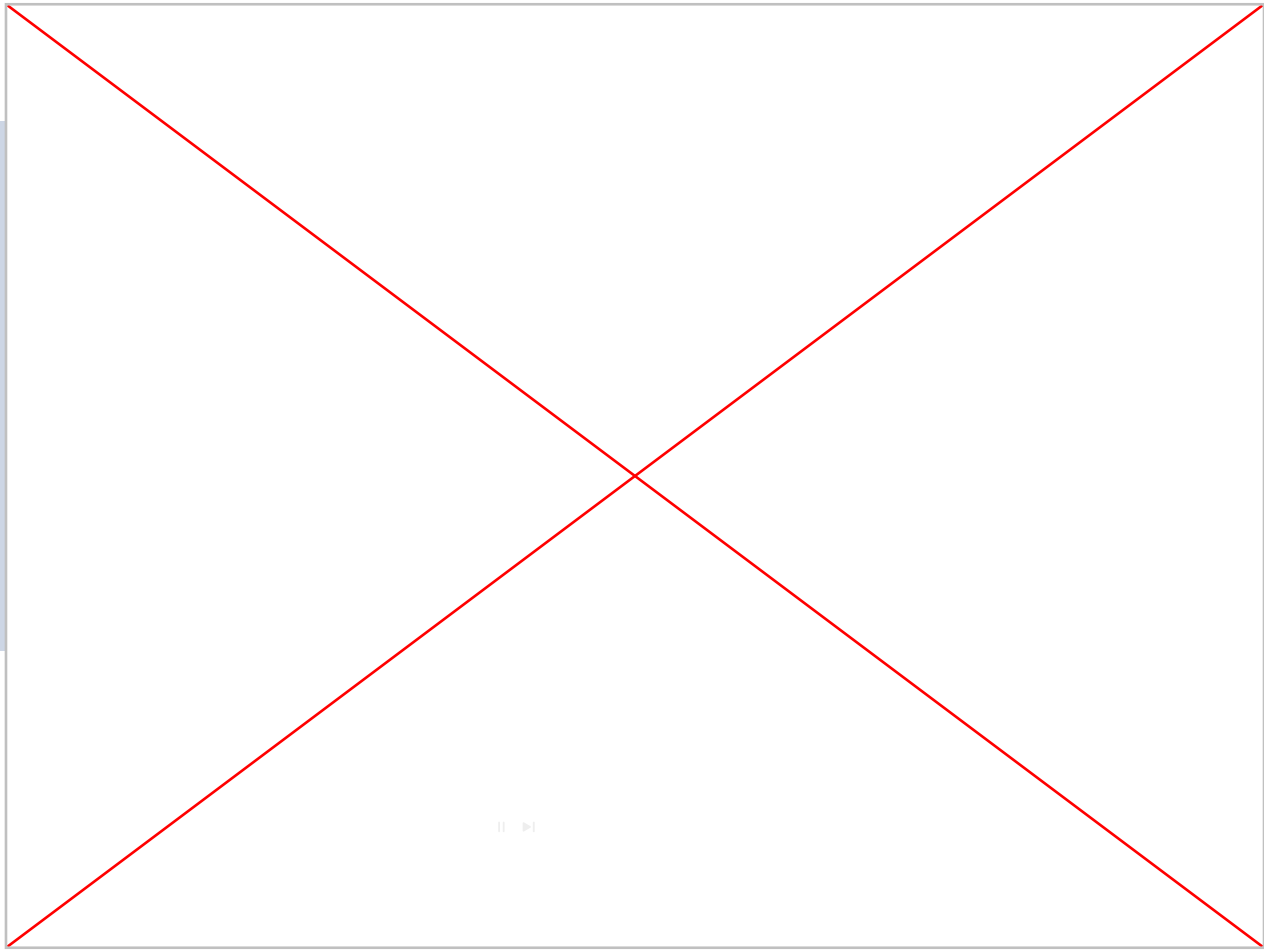


Future plans

- → Add other VPN protocols
- → Configure logging for IKE

Duke | Code <+>

PRODUCT DEMO!



Duke | Code <+>

Acknowledgements

Eric Hope
Team Lead

Hugh Thomas
Team Lead

Alex Merck
Mentor

Program Directors

Isabel Valls
Jen Vizas

CISCO

Project Sponsor

Program Facilitators

Jaelyn Cuellar
Mariam Gvenetadze

Duke | Code <+>

THANK YOU!

Any Questions?