Honeypots

Code can be found here: https://github.com/c2003-tamu/413

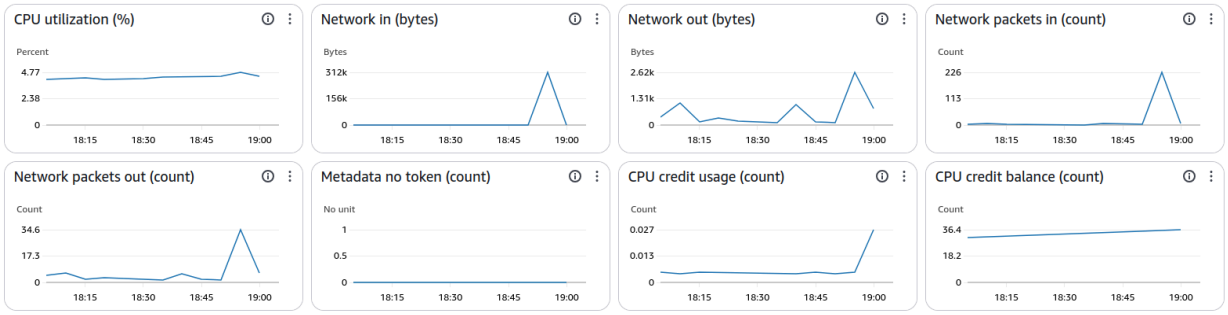
Environment Setup

- Provision EC2/other cloud instance with http and ssh traffic enabled
- SSH into instance
- Run command: sudo apt update && sudo apt upgrade
- Run command: git clone https://github.com/c2003-tamu/413
- Navigate to 413/honeypots directory
- Run command: python3 -m venv venv
- Run command: source venv/bin/activate
- Run command: pip install -r requirements.txt
- Run command: sudo ~/413/honeypots/venv/bin/python bank.py
- Bank application is now up, wait for ~1 hour

Outcome

I received a few requests from a couple of different IP addresses (seen below). It should be noted that the first 2 requests seen here were from my local machine to ensure that the application was accessible.

```
165.91.13.163 - - [13/Feb/2025 17:52:42] "GET / HTTP/1.1" 404 -
165.91.13.163 - - [13/Feb/2025 17:52:43] "GET /favicon.ico HTTP/1.1" 404 -
193.68.89.51 - - [13/Feb/2025 18:20:41] "GET / HTTP/1.1" 404 -
164.52.24.188 - - [13/Feb/2025 18:59:36] code 400, message Bad request version ("«Ò:ì_îïøAèèÉ#k|d+\x90\x00>\x13\x02\x13\x03\x13\x01Á,À0\x00\x9fÌeJ¨Ì³Á+Á/\x00\x9eÁŞÁ(\x00kÁ#Á'\x00gÁ")
164.52.24.188 - - [13/Feb/2025 18:59:36] "\x16\x03\x01\x02\x00\x01\x00\x01ü\x03\x03ºÊãeéÍÖ\x89n\x8eµ\x1a\x01ÂÉÉ?\x96L³°\x8e\x93¥€'®.Bö¾\x98  z%˜\x83ÂXtóÖ6'Ò «Ò:ì_îïøAèèÉ#k|d+\x90\x00>\x13\x02\x13\x03\x13\x01Á,À0\x00\x9fÌeJ¨Ì³Á+Á/\x00\x9eÁŞÁ(\x00kÁ#Á'\x00gÁ" 400 -
164.52.24.188 - - [13/Feb/2025 18:59:58] "GET / HTTP/1.1" 404 -
193.68.89.10 - - [13/Feb/2025 19:00:18] "GET / HTTP/1.1" 404 -
```



As can be seen above, the homepage (/ endpoint) was requested a few times by a few different IP addresses. What was really interesting was the request at 18:59:36, which appears to be trying to initiate a SSL/TLS handshake, which means that the client was trying to establish a HTTPS connection with the server. After that request, the same ip sends a plain http request that is handled correctly by the server.