Networks and Cyber Security II

Roll number: K214753

Name: Vania Abbas

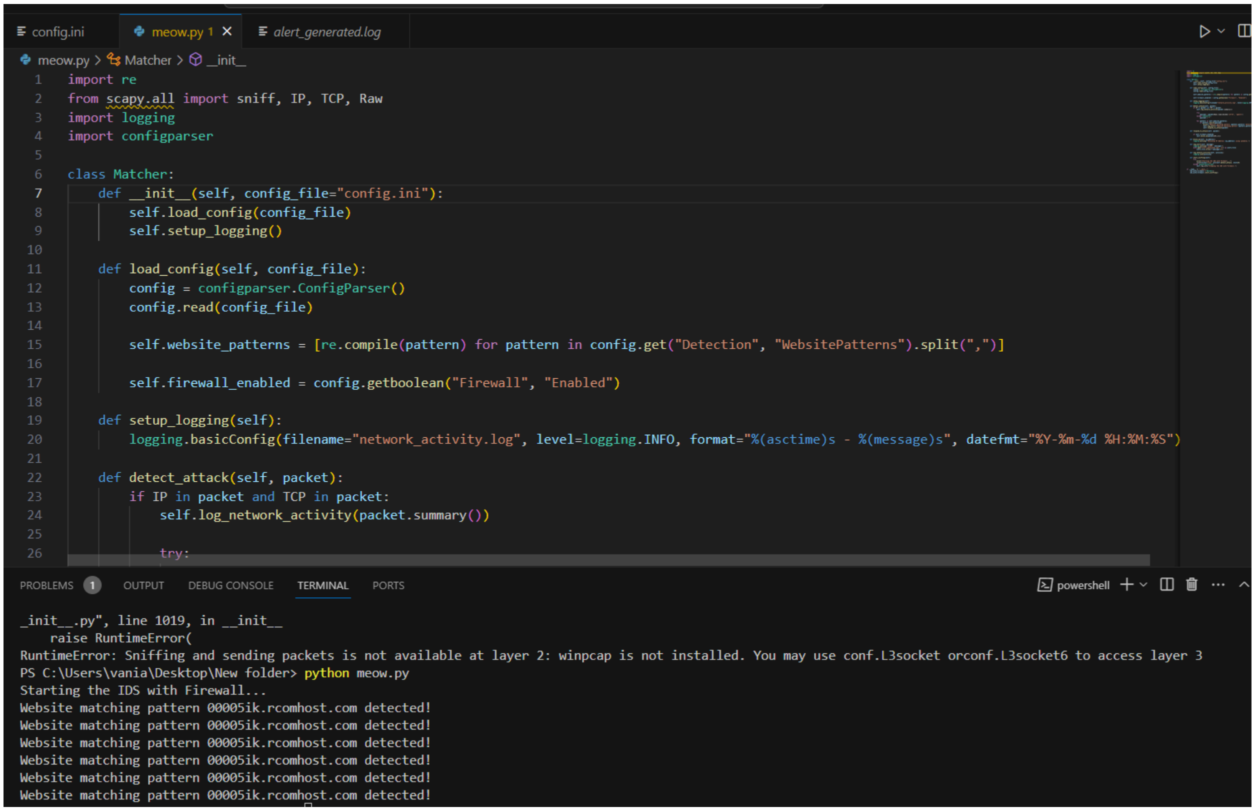
Section: BCY-6B

Design and implement a simple network security system that can identify and flag suspicious website access attempts.

This system should:

- Continuously monitor all network activity.
- Capture and analyze information.
- Compare this information against a list of predefined suspicious websites.
- Generate alerts for any website access that matches.

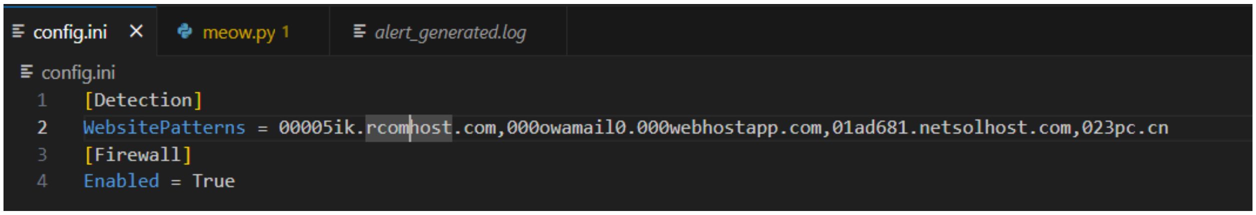
File 1. Detection



```python
import re
from scapy.all import sniff, IP, TCP, Raw
import logging
import configparser

class Matcher:
    def __init__(self, config_file="config.ini"):
        self.load_config(config_file)
        self.setup_logging()

    def load_config(self, config_file):
        config = configparser.ConfigParser()
        config.read(config_file)

        self.website_patterns = [re.compile(pattern) for pattern in config.get("Detection", "WebsitePatterns").split(",")]

        self.firewall_enabled = config.getboolean("Firewall", "Enabled")

    def setup_logging(self):
        logging.basicConfig(filename="network_activity.log", level=logging.INFO, format="%(asctime)s - %(message)s", datefmt="%Y-%m-%d %H:%M:%S")

    def detect_attack(self, packet):
        if IP in packet and TCP in packet:
            self.log_network_activity(packet.summary())

            try:
```

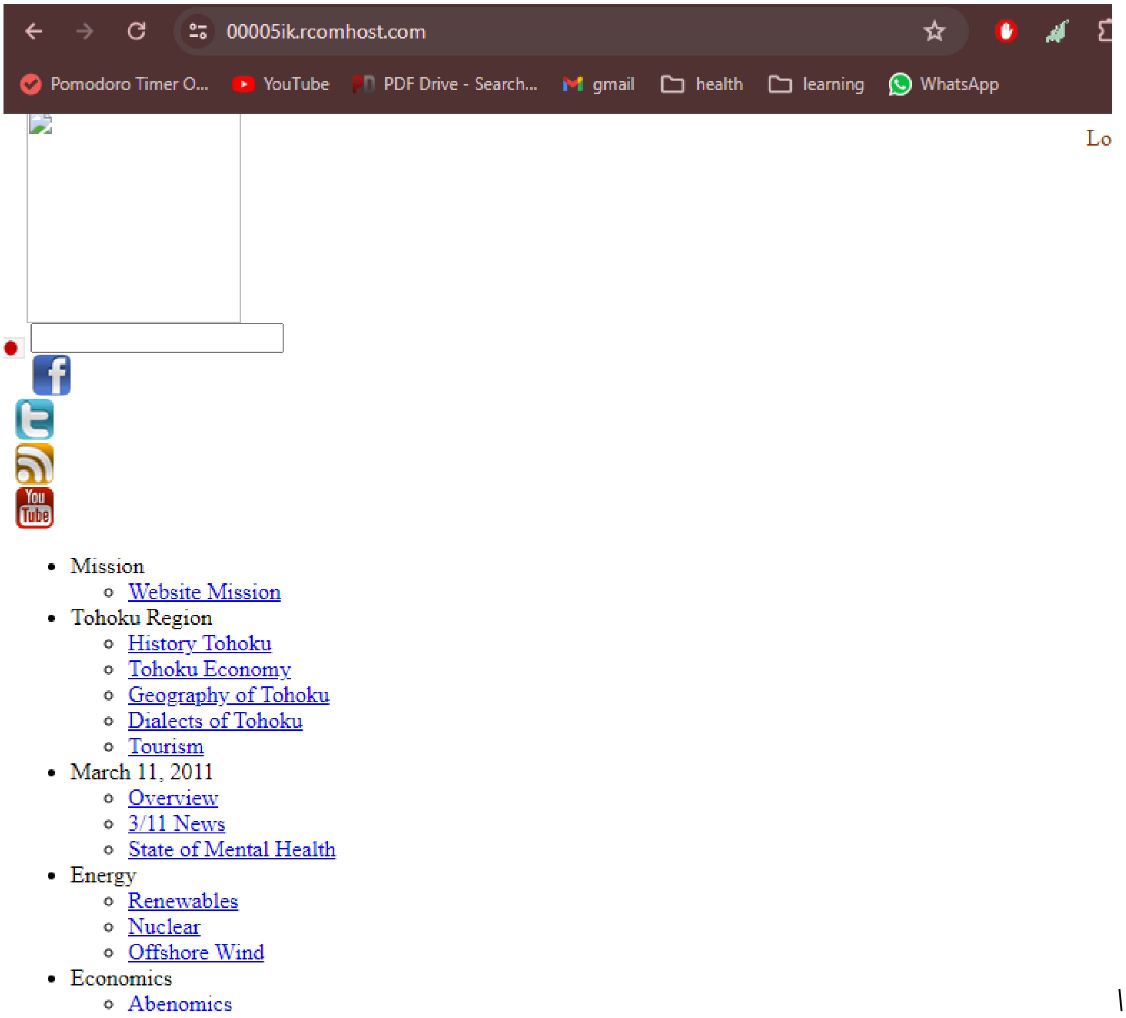
```
_init__.py", line 1019, in __init__
    raise RuntimeError(
RuntimeError: Sniffing and sending packets is not available at layer 2: winpcap is not installed. You may use conf.L3socket orconf.L3socket6 to access layer 3
PS C:\Users\vania\Desktop\New folder> python meow.py
Starting the IDS with Firewall...
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
```

File 2. Config.ini



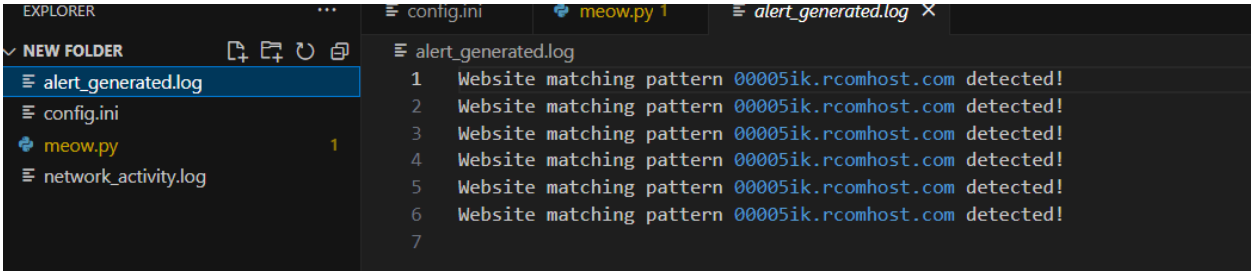
```ini
[Detection]
WebsitePatterns = 00005ik.rcomhost.com,000owamail0.000webhostapp.com,01ad681.netsolhost.com,023pc.cn
[Firewall]
Enabled = True
```

Image 1. When we visit the malicious website, https://00005ik.rcomhost.com/ , our system should generate a log as seen in image 2



- Mission
  - Website Mission
- Tohoku Region
  - History Tohoku
  - Tohoku Economy
  - Geography of Tohoku
  - Dialects of Tohoku
  - Tourism
- March 11, 2011
  - Overview
  - 3/11 News
  - State of Mental Health
- Energy
  - Renewables
  - Nuclear
  - Offshore Wind
- Economics
  - Abenomics

Image 2. Malicious website detected.



```
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
Website matching pattern 00005ik.rcomhost.com detected!
```

We can add as many malicious websites in our config.ini file. The link below will provide more malicious websites. As the files were too big, I added just a few websites in my config.ini file. Link:

https://github.com/mitchellkrogza/The-Big-List-of-Hacked-Malware-Web-Sites/blob/master/.dev-tools/_strip_domains/domains.txt