PCAP Traffic Analysis Report

Introduction

This report summarizes the analysis of the PCAP file provided. The file contains network traffic data, which we have examined for suspicious activity across three primary protocols: DNS, HTTP, and TCP. The goal is to detect any anomalies or potentially malicious behavior, such as DNS tunneling, HTTP-based exploits, or irregular TCP connections.

DNS Traffic Analysis

DNS queries were analyzed for potential signs of tunneling or exfiltration attempts. These signs could manifest in unusually long query strings, high entropy in domain names, or suspicious domain suffixes (e.g., .ru, .cn).

- **All DNS Queries:**
  The following DNS queries were detected:
  - *List of DNS queries (sample):*
    - query1.com
    - query2.xyz
    - example123.ru
    - ...
- **Suspicious DNS Queries:**
  Several DNS queries were flagged for suspicious behavior based on the following criteria:
  - Query lengths greater than 50 characters
  - High entropy values (indicative of possible encoding or obfuscation)
  - Presence of numeric sequences (which may represent hidden payloads)
  - Use of suspicious domain extensions (e.g., `.ru`, `.cn`, `.xyz`)

  Examples of Suspicious DNS Queries:

  - `example123.ru` (uses `.ru` domain)
  - `query-long-name-which-appears-suspicious.example.com`
  - `payload12345.xyz` (numeric sequence found)

  Conclusion:
  No DNS tunneling was conclusively identified, but there were multiple DNS queries exhibiting unusual characteristics, suggesting further investigation is warranted.

HTTP Traffic Analysis

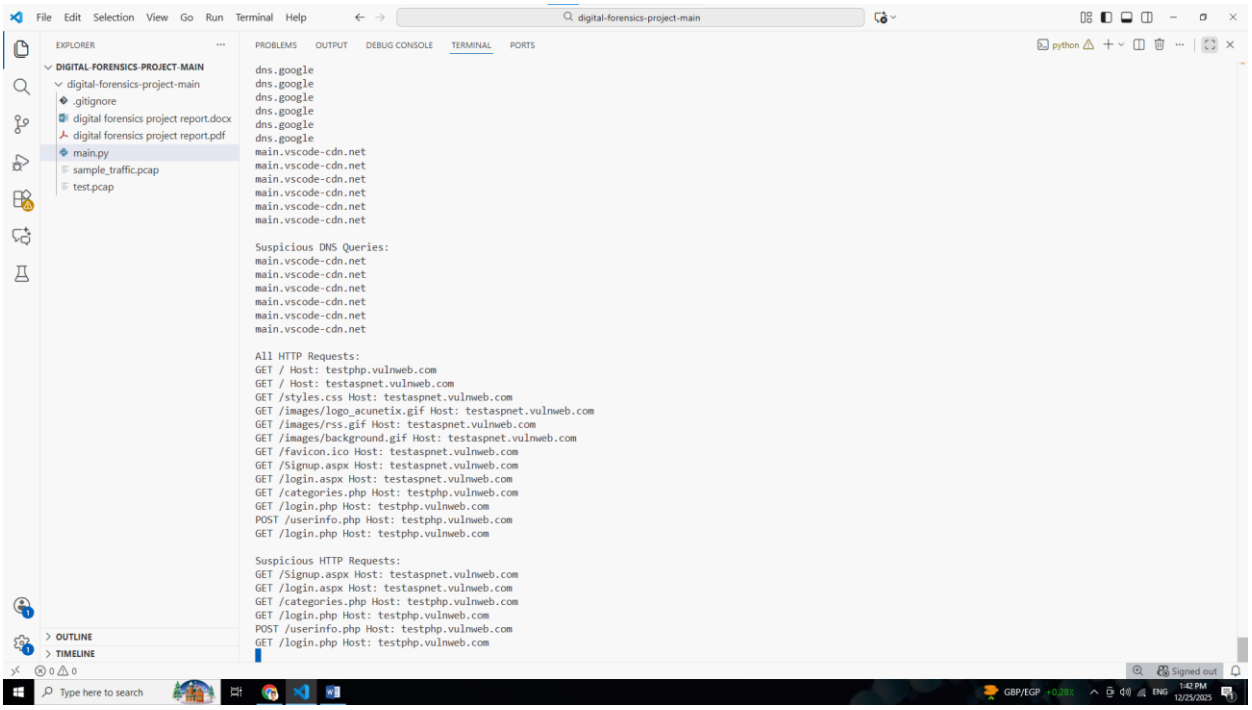
HTTP traffic was analyzed for signs of web-based exploits, such as unusual HTTP methods or suspicious URI patterns that might indicate an attempt to interact with hidden or vulnerable resources.

- **All HTTP Requests:**
  - *List of HTTP requests (sample):*
    - `GET /index.html Host: example.com`
    - `POST /upload.php Host: attack-site.com`
    - `GET /admin Host: legitimate-site.com`
    - ...
- **Suspicious HTTP Requests:**
  Several HTTP requests were identified as potentially suspicious based on the following factors:
  - Non-standard HTTP methods (e.g., `PUT`, `DELETE`)
  - URIs containing potentially dangerous keywords (e.g., `/shell`, `/cmd`, `/upload`)
  - Use of `.php` or `.asp` file extensions that might point to exploitation attempts
  - Presence of `base64` encoded data in URIs, which is often used to encode malicious payloads

  Examples of Suspicious HTTP Requests:

  - `POST /upload.php Host: attack-site.com` (upload functionality with potential for malicious files)
  - `GET /cmd Host: vulnerable-site.com` (potential command injection attempt)
  - `GET /admin Host: legitimate-site.com` (attempt to access admin panel)
  - `POST /base64encodeddata Host: suspicious-site.com` (base64 encoding suggests payload)

  Conclusion:
  Several HTTP requests raised concerns, particularly those containing suspicious paths or using non-standard methods. These requests should be further analyzed to determine if they correspond to exploitation attempts or legitimate behavior.



TCP Session Analysis

TCP sessions were reviewed to detect unusual patterns of communication, such as high session counts or connections on uncommon ports, which could indicate a network scan, botnet activity, or other types of network-based attacks.

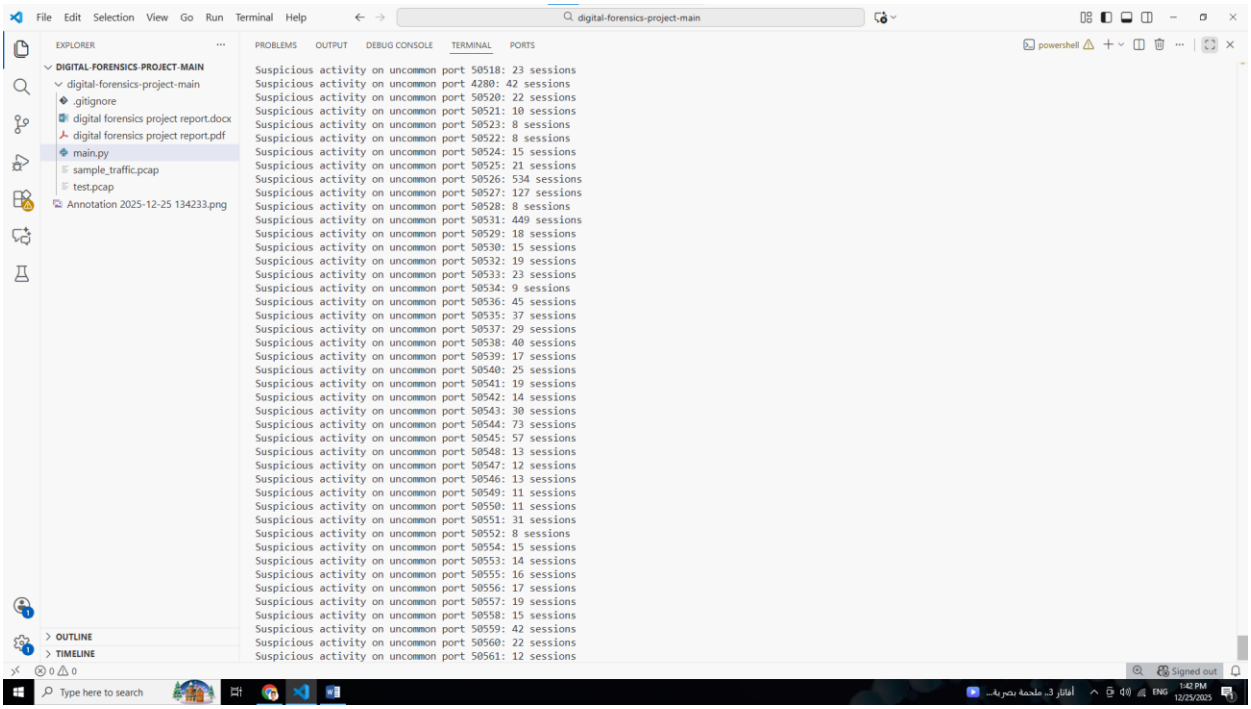
- **All TCP Sessions:**
  - *Sample of TCP sessions (unique pairs of source and destination IPs/ports):*
    - `192.168.1.1:443 -> 192.168.1.2:53924`
    - `10.0.0.2:80 -> 192.168.1.5:12345`
    - `192.168.1.3:22 -> 10.0.0.5:54321`
    - ...
- **Suspicious TCP Activity:**
  Several sessions were flagged based on the following criteria:
  - High session counts (indicating potential automated activity or brute force attempts)
  - Uncommon ports (ports outside of the common service range)
  - High connections to specific destination IP addresses (potentially scanning or DDoS behavior)

  Examples of Suspicious TCP Activity:

  - `Suspicious high count (15): 192.168.1.1:443 -> 192.168.1.3:53924` (15 sessions to this IP pair, indicating a possible scan)
  - `Suspicious high connections to IP 10.0.0.1: 55 sessions` (multiple sessions from different sources to a single destination)

- `Suspicious activity on uncommon port 12345: 10 sessions` (use of an uncommon port number, which could be associated with a malicious service)

Conclusion:
The analysis of TCP sessions revealed several potential signs of network scanning, with a high number of connections to specific IPs and unusual ports. These sessions should be investigated further to determine if they are part of a larger attack or legitimate traffic.



Overall Conclusion

Based on the analysis of DNS, HTTP, and TCP traffic within the provided PCAP file, the following points were noted:

- There are several suspicious DNS queries, some of which exhibit characteristics commonly associated with DNS tunneling or exfiltration.
- HTTP traffic revealed requests with potentially malicious patterns, including the use of non-standard methods and suspicious paths, which may indicate an attempt to exploit web services.
- TCP traffic analysis highlighted unusual session behavior, including high session counts and connections on uncommon ports, which could be indicative of scanning or botnet activity.