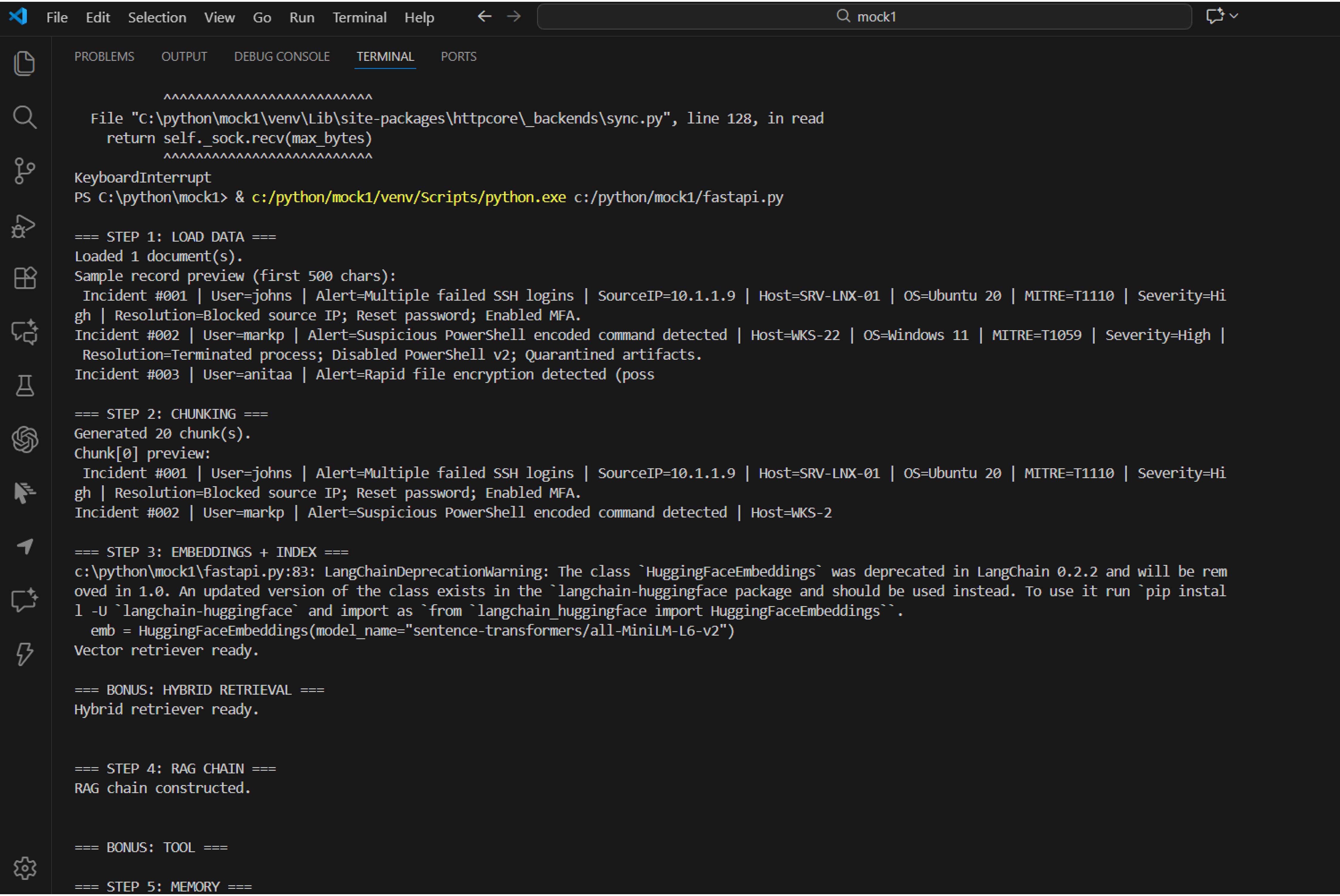
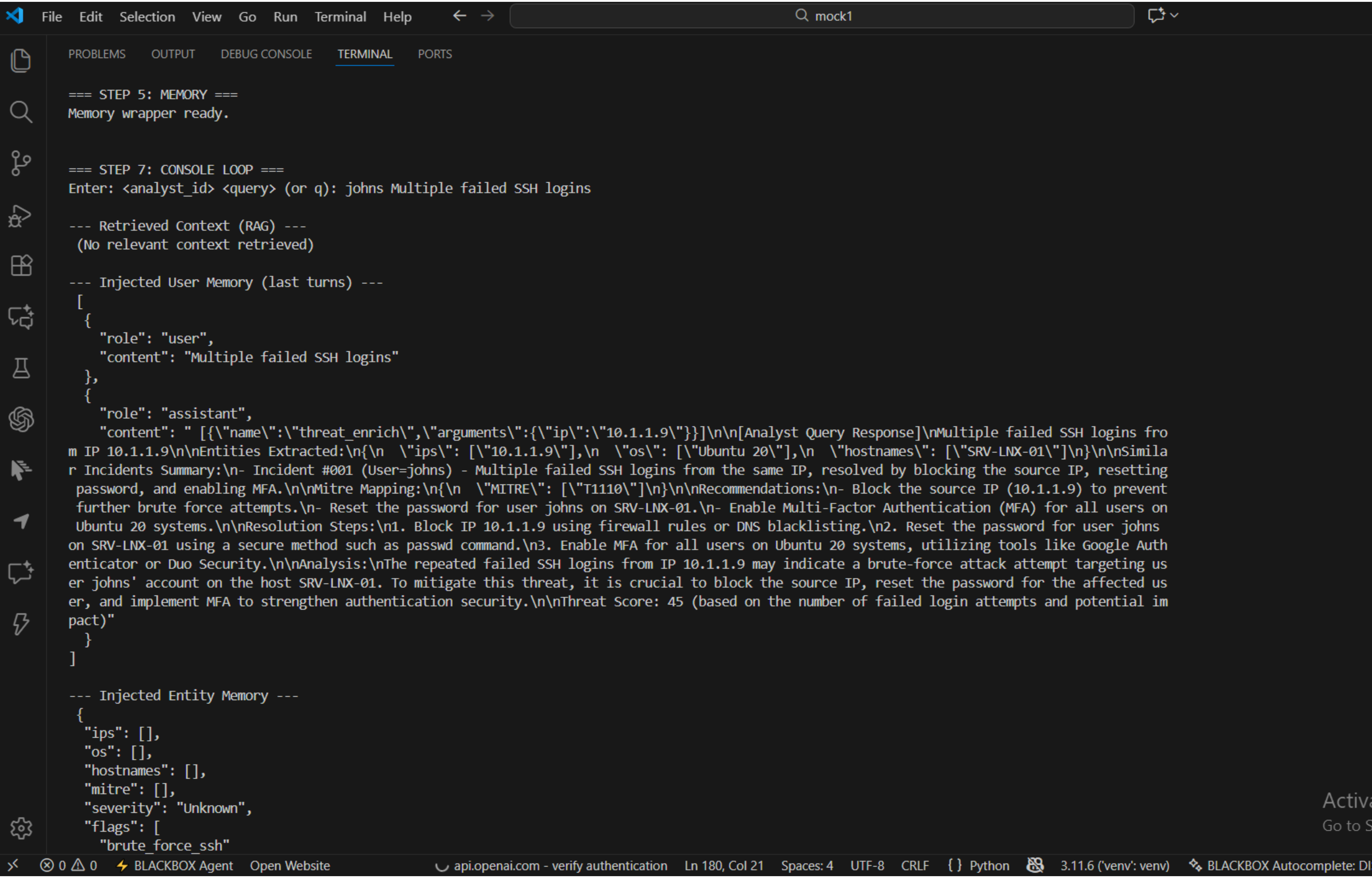
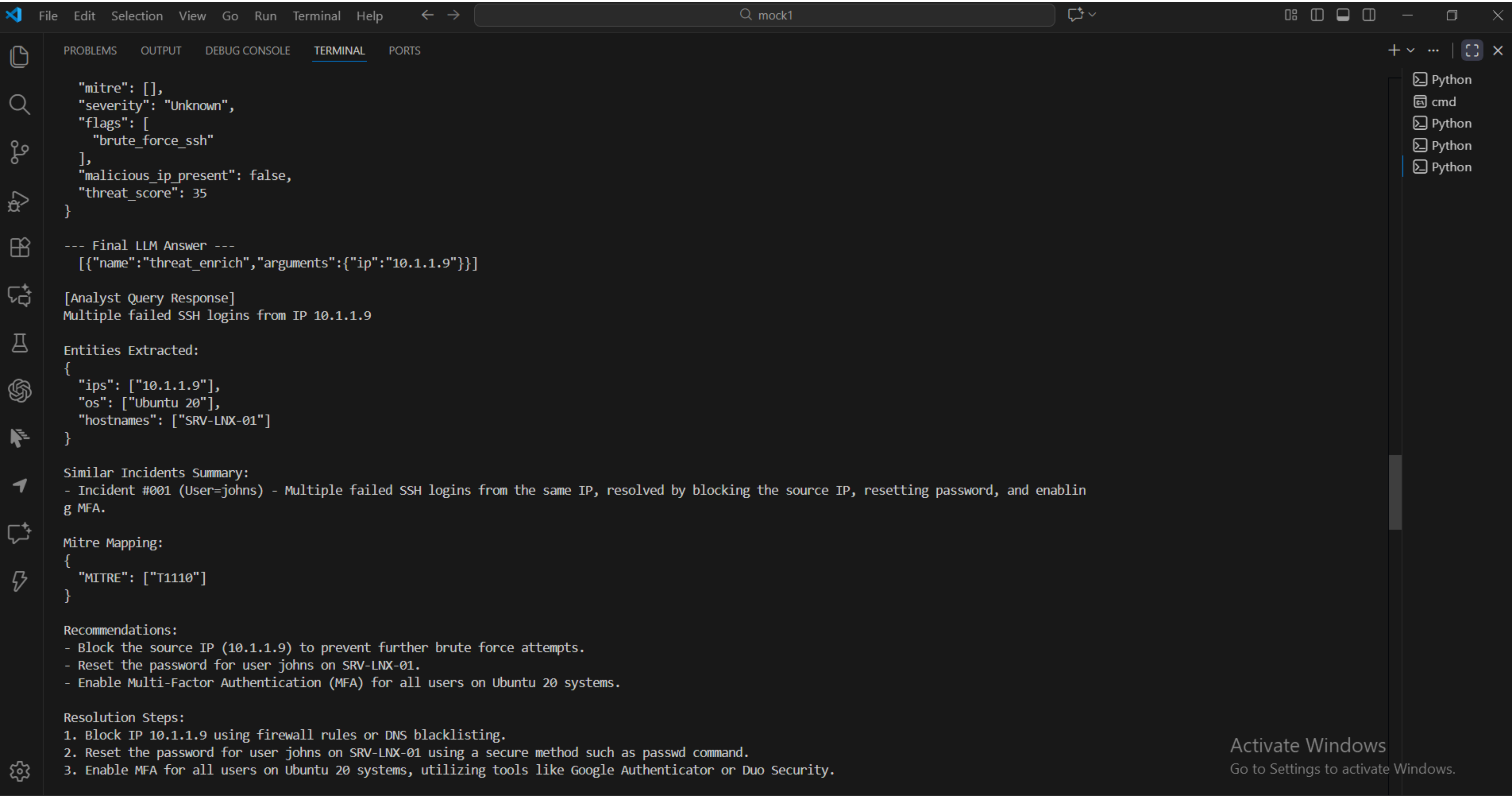


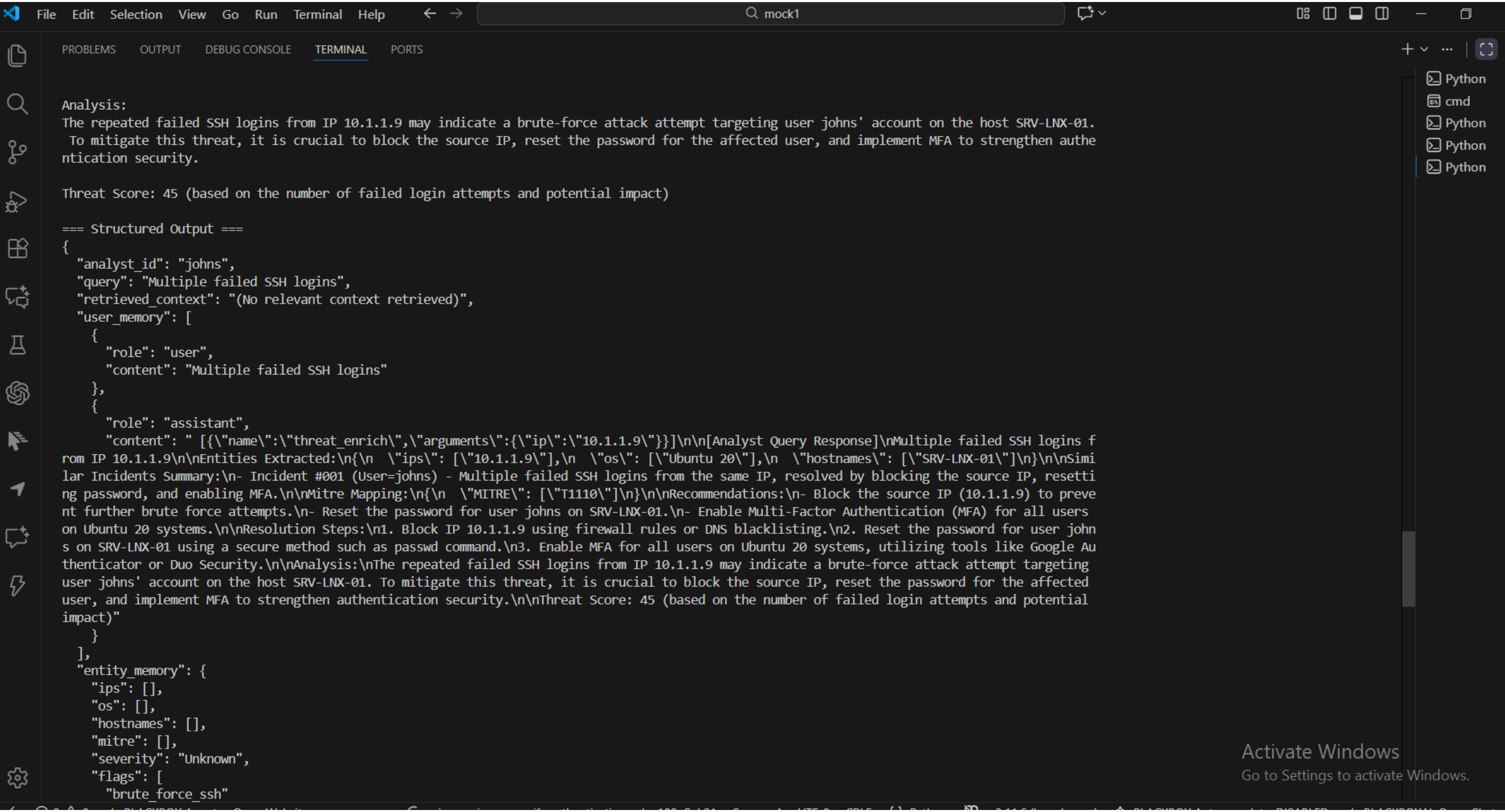
```
          ^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "C:\python\mock1\venv\Lib\site-packages\httpcore\_backends\sync.py", line 128, in read
    return self._sock.recv(max_bytes)
           ^^^^^^^^^^^^^^^^^^^^^^^^^^
KeyboardInterrupt
PS C:\python\mock1> & c:/python/mock1/venv/Scripts/python.exe c:/python/mock1/fastapi.py

=== STEP 1: LOAD DATA ===
Loaded 1 document(s).
Sample record preview (first 500 chars):
 Incident #001 | User=johns | Alert=Multiple failed SSH logins | SourceIP=10.1.1.9 | Host=SRV-LNX-01 | OS=Ubuntu 20 | MITRE=T1110 | Severity=Hi
gh | Resolution=Blocked source IP; Reset password; Enabled MFA.
Incident #002 | User=markp | Alert=Suspicious PowerShell encoded command detected | Host=WKS-22 | OS=Windows 11 | MITRE=T1059 | Severity=High |
 Resolution=Terminated process; Disabled PowerShell v2; Quarantined artifacts.
Incident #003 | User=anitaa | Alert=Rapid file encryption detected (poss

=== STEP 2: CHUNKING ===
Generated 20 chunk(s).
Chunk[0] preview:
 Incident #001 | User=johns | Alert=Multiple failed SSH logins | SourceIP=10.1.1.9 | Host=SRV-LNX-01 | OS=Ubuntu 20 | MITRE=T1110 | Severity=Hi
gh | Resolution=Blocked source IP; Reset password; Enabled MFA.
Incident #002 | User=markp | Alert=Suspicious PowerShell encoded command detected | Host=WKS-2

=== STEP 3: EMBEDDINGS + INDEX ===
c:\python\mock1\fastapi.py:83: LangChainDeprecationWarning: The class `HuggingFaceEmbeddings` was deprecated in LangChain 0.2.2 and will be rem
oved in 1.0. An updated version of the class exists in the `langchain-huggingface package and should be used instead. To use it run `pip instal
l -U `langchain-huggingface` and import as `from `langchain_huggingface import HuggingFaceEmbeddings``.
  emb = HuggingFaceEmbeddings(model_name="sentence-transformers/all-MiniLM-L6-v2")
Vector retriever ready.

=== BONUS: HYBRID RETRIEVAL ===
Hybrid retriever ready.


=== STEP 4: RAG CHAIN ===
RAG chain constructed.


=== BONUS: TOOL ===

=== STEP 5: MEMORY ===
```



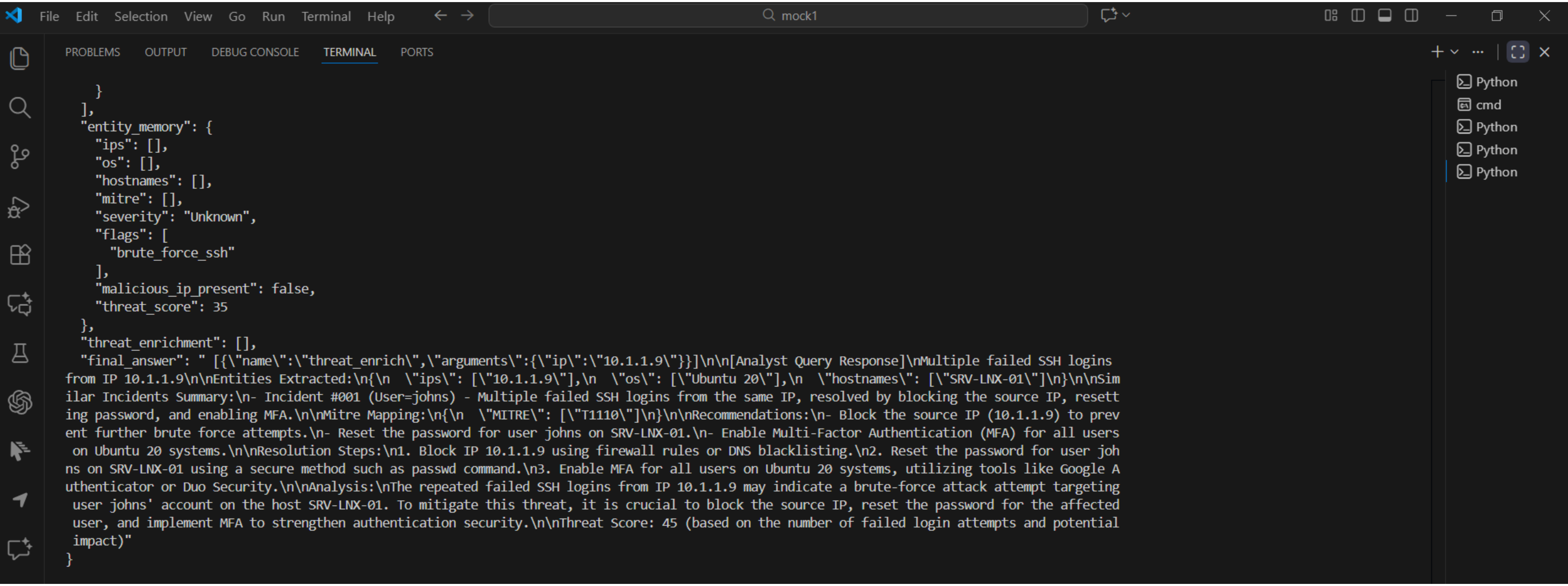
```
=== STEP 5: MEMORY ===
Memory wrapper ready.


=== STEP 7: CONSOLE LOOP ===
Enter: <analyst_id> <query> (or q): johns Multiple failed SSH logins

--- Retrieved Context (RAG) ---
 (No relevant context retrieved)

--- Injected User Memory (last turns) ---
 [
  {
    "role": "user",
    "content": "Multiple failed SSH logins"
  },
  {
    "role": "assistant",
    "content": " [{\"name\":\"threat_enrich\",\"arguments\":{\"ip\":\"10.1.1.9\"}}]\n\n[Analyst Query Response]\nMultiple failed SSH logins fro
m IP 10.1.1.9\n\nEntities Extracted:\n{\n  \"ips\": [\"10.1.1.9\"],\n  \"os\": [\"Ubuntu 20\"],\n  \"hostnames\": [\"SRV-LNX-01\"]\n}\n\nSimila
r Incidents Summary:\n- Incident #001 (User=johns) - Multiple failed SSH logins from the same IP, resolved by blocking the source IP, resetting
 password, and enabling MFA.\n\nMitre Mapping:\n{\n  \"MITRE\": [\"T1110\"]\n}\n\nRecommendations:\n- Block the source IP (10.1.1.9) to prevent
 further brute force attempts.\n- Reset the password for user johns on SRV-LNX-01.\n- Enable Multi-Factor Authentication (MFA) for all users on
 Ubuntu 20 systems.\n\nResolution Steps:\n1. Block IP 10.1.1.9 using firewall rules or DNS blacklisting.\n2. Reset the password for user johns
on SRV-LNX-01 using a secure method such as passwd command.\n3. Enable MFA for all users on Ubuntu 20 systems, utilizing tools like Google Auth
enticator or Duo Security.\n\nAnalysis:\nThe repeated failed SSH logins from IP 10.1.1.9 may indicate a brute-force attack attempt targeting us
er johns' account on the host SRV-LNX-01. To mitigate this threat, it is crucial to block the source IP, reset the password for the affected us
er, and implement MFA to strengthen authentication security.\n\nThreat Score: 45 (based on the number of failed login attempts and potential im
pact)"
  }
]

--- Injected Entity Memory ---
 {
  "ips": [],
  "os": [],
  "hostnames": [],
  "mitre": [],
  "severity": "Unknown",
  "flags": [
    "brute_force_ssh"
```



```
  "mitre": [],
  "severity": "Unknown",
  "flags": [
    "brute_force_ssh"
  ],
  "malicious_ip_present": false,
  "threat_score": 35
}

--- Final LLM Answer ---
  [{"name":"threat_enrich","arguments":{"ip":"10.1.1.9"}}]

[Analyst Query Response]
Multiple failed SSH logins from IP 10.1.1.9

Entities Extracted:
{
  "ips": ["10.1.1.9"],
  "os": ["Ubuntu 20"],
  "hostnames": ["SRV-LNX-01"]
}

Similar Incidents Summary:
- Incident #001 (User=johns) - Multiple failed SSH logins from the same IP, resolved by blocking the source IP, resetting password, and enablin
g MFA.

Mitre Mapping:
{
  "MITRE": ["T1110"]
}

Recommendations:
- Block the source IP (10.1.1.9) to prevent further brute force attempts.
- Reset the password for user johns on SRV-LNX-01.
- Enable Multi-Factor Authentication (MFA) for all users on Ubuntu 20 systems.

Resolution Steps:
1. Block IP 10.1.1.9 using firewall rules or DNS blacklisting.
2. Reset the password for user johns on SRV-LNX-01 using a secure method such as passwd command.
3. Enable MFA for all users on Ubuntu 20 systems, utilizing tools like Google Authenticator or Duo Security.
```



```
Analysis:
The repeated failed SSH logins from IP 10.1.1.9 may indicate a brute-force attack attempt targeting user johns' account on the host SRV-LNX-01.
 To mitigate this threat, it is crucial to block the source IP, reset the password for the affected user, and implement MFA to strengthen authe
ntication security.

Threat Score: 45 (based on the number of failed login attempts and potential impact)

=== Structured Output ===
{
  "analyst_id": "johns",
  "query": "Multiple failed SSH logins",
  "retrieved_context": "(No relevant context retrieved)",
  "user_memory": [
    {
      "role": "user",
      "content": "Multiple failed SSH logins"
    },
    {
      "role": "assistant",
      "content": " [{\"name\":\"threat_enrich\",\"arguments\":{\"ip\":\"10.1.1.9\"}}]\n\n[Analyst Query Response]\nMultiple failed SSH logins f
rom IP 10.1.1.9\n\nEntities Extracted:\n{\n  \"ips\": [\"10.1.1.9\"],\n  \"os\": [\"Ubuntu 20\"],\n  \"hostnames\": [\"SRV-LNX-01\"]\n}\n\nSimi
lar Incidents Summary:\n- Incident #001 (User=johns) - Multiple failed SSH logins from the same IP, resolved by blocking the source IP, resetti
ng password, and enabling MFA.\n\nMitre Mapping:\n{\n  \"MITRE\": [\"T1110\"]\n}\n\nRecommendations:\n- Block the source IP (10.1.1.9) to preve
nt further brute force attempts.\n- Reset the password for user johns on SRV-LNX-01.\n- Enable Multi-Factor Authentication (MFA) for all users
on Ubuntu 20 systems.\n\nResolution Steps:\n1. Block IP 10.1.1.9 using firewall rules or DNS blacklisting.\n2. Reset the password for user john
s on SRV-LNX-01 using a secure method such as passwd command.\n3. Enable MFA for all users on Ubuntu 20 systems, utilizing tools like Google Au
thenticator or Duo Security.\n\nAnalysis:\nThe repeated failed SSH logins from IP 10.1.1.9 may indicate a brute-force attack attempt targeting
user johns' account on the host SRV-LNX-01. To mitigate this threat, it is crucial to block the source IP, reset the password for the affected
user, and implement MFA to strengthen authentication security.\n\nThreat Score: 45 (based on the number of failed login attempts and potential
impact)"
    }
  ],
  "entity_memory": {
    "ips": [],
    "os": [],
    "hostnames": [],
    "mitre": [],
    "severity": "Unknown",
    "flags": [
      "brute_force_ssh"
```



```
      }
    ],
    "entity_memory": {
      "ips": [],
      "os": [],
      "hostnames": [],
      "mitre": [],
      "severity": "Unknown",
      "flags": [
        "brute_force_ssh"
      ],
      "malicious_ip_present": false,
      "threat_score": 35
    },
    "threat_enrichment": [],
    "final_answer": " [{\"name\":\"threat_enrich\",\"arguments\":{\"ip\":\"10.1.1.9\"}}]\n\n[Analyst Query Response]\nMultiple failed SSH logins
  from IP 10.1.1.9\n\nEntities Extracted:\n{\n  \"ips\": [\"10.1.1.9\"],\n  \"os\": [\"Ubuntu 20\"],\n  \"hostnames\": [\"SRV-LNX-01\"]\n}\n\nSim
  ilar Incidents Summary:\n- Incident #001 (User=johns) - Multiple failed SSH logins from the same IP, resolved by blocking the source IP, resett
  ing password, and enabling MFA.\n\nMitre Mapping:\n{\n  \"MITRE\": [\"T1110\"]\n}\n\nRecommendations:\n- Block the source IP (10.1.1.9) to prev
  ent further brute force attempts.\n- Reset the password for user johns on SRV-LNX-01.\n- Enable Multi-Factor Authentication (MFA) for all users
   on Ubuntu 20 systems.\n\nResolution Steps:\n1. Block IP 10.1.1.9 using firewall rules or DNS blacklisting.\n2. Reset the password for user joh
  ns on SRV-LNX-01 using a secure method such as passwd command.\n3. Enable MFA for all users on Ubuntu 20 systems, utilizing tools like Google A
  uthenticator or Duo Security.\n\nAnalysis:\nThe repeated failed SSH logins from IP 10.1.1.9 may indicate a brute-force attack attempt targeting
   user johns' account on the host SRV-LNX-01. To mitigate this threat, it is crucial to block the source IP, reset the password for the affected
   user, and implement MFA to strengthen authentication security.\n\nThreat Score: 45 (based on the number of failed login attempts and potential
   impact)"
  }
```