

First Output:

```
Users\User\Documents\RAG\Final_Rags>python milestone.py
LOAD DATA ===
cuments.

001 | User=johns | Alert=Multiple failed SSH logins | SourceIP=10.1.1.9 | Host=SRV-LNX-01 | OS=Ubuntu 20 | MITRE=T1110 | Severity=High | Resolution=Bl
e IP; Reset password; Enabled MFA.
002 | User=markp | Alert=Suspicious PowerShell encoded command detected | Host=WKS-2

CHUNKING ===
s: 24

EMBEDDINGS + INDEX ===

HYBRID RETRIEVAL ===
iever ready.

RAG CHAIN ===
onstructed.

TOOL ===
t_enrich added successfully

MEMORY ===
per ready.

CONSOLE LOOP ===

st ID (or 'exit'): T1053
/query: Malicious files on desktop
JSON-RESPONSE ---

id": "T1053",
"Malicious files on desktop",
": {
[
168.55.20"
```

Entities :

```
query : Malicious files on desktop
"entities": {
  "ips": [
    "192.168.55.20"
  ],
  "hostnames": [
    "WKS-81",
    "SRV-DB03",
    "WKS-64",
    ";",
    "WKS-11",
    "FIN12",
    ";",
    "WEB-03",
    "SRV-DB03",
    "WKS-55",
    "SRV-LNX-12",
    "SRV-APP2"
  ],
  "os": [
    "Windows",
    "Windows",
    "Windows",
    "Windows",
    "Debian",
    "Windows",
    "Ubuntu"
  ],
  "mitre": [
    "T1059",
    "T1078",
    "T1090",
    "T1091",
    "T1486",
    "T1059",
    "T1005",
    "T1021",
    "T1078",
    "T1041"
  ],
  "severity": [
```

Second Query -

```
Enter analyst ID (or 'exit'): T1053
Enter alert/query: brute force attacks
---BONUS : JSON-RESPONSE ---
{
  "analyst_id": "T1053",
  "query": "brute force attacks",
  "entities": {
    "ips": [
      "10.2.4.9",
      "192.168.55.20",
      "10.22.3.9"
    ],
    "hostnames": [
      "SRV-LNX-12",
      "SRV-FS01",
      "WEB-20",
      "WKS-72",
      "WKS-22",
      "WKS-81",
      "SRV-DB03",
      "SRV-LNX-12",
      "SRV-APP2",
      "WKS-77",
      "LAB-07",
      "WKS-98",
      "SRV-DB01"
    ],
    "os": [
      "Ubuntu",
      "Windows",
      "Debian",
      "Windows",
      "Windows",
      "Windows",
      "Ubuntu",
      "Windows",
      "Ubuntu",
      "Windows",
      "CentOS"
    ]
  },
  "os": [
    "Ubuntu",
    "Windows",
    "Debian",
    "Windows",
    "Windows",
    "Windows",
    "Ubuntu",
    "Windows",
    "Ubuntu",
    "Windows",
    "CentOS"
  ],
}
```

```
},
  "severity": [
    "High",
    "High",
    "High",
    "Medium",
    "Medium",
    "High",
    "Medium",
    "High",
    "Critical",
    "High",
    "Critical",
    "High",
    "High"
  ],
  "threat_score": 66,
  "response": " Based on the provided context, there have been multiple instances of brute-force attacks detected across various hosts in your #007, #029, and #037 for SSH, and #034 for SMB). In these cases, the resolution involved blocking the IP addresses from which the attacks originated (e.g., #007, #029, and #037 for SSH, and #034 for SMB). In these cases, the resolution involved blocking the IP addresses from which the attacks originated, implementing fail2ban or SMB throttling, resetting credentials, and conducting IOC scans.\n\nThreat indicators for brute-force attacks often include:\n1. Multiple authentication attempts within a short period of time.\n2. Unusual connections from IP addresses with known malicious activity.\n3. Attempts to access resources or services that typically require strong authentication.\n4. Login attempts using common or weak passwords.\n5. Rapid login attempts from multiple IP addresses.\n6. Attempts to access sensitive resources or services.\n7. Attempts to access services that are not typically accessible from the internet.\n8. Attempts to access services that are not typically accessible from the internet.\n9. Attempts to access services that are not typically accessible from the internet.\n10. Attempts to access services that are not typically accessible from the internet.\n\nTo mitigate the risk of brute-force attacks, it is recommended to:\n1. Implement strong password policies and enforce complexity requirements.\n2. Limit the number of failed authentication attempts before locking an account.\n3. Monitor network traffic for unusual activity and implement intrusion detection systems.\n4. Use multi-factor authentication (MFA) where possible to add an additional layer of security.\n5. Regularly update and patch vulnerable services and software.\n6. Implement access controls and restrict access to sensitive resources or services only to those who need it.\n7. Review system logs for signs of brute-force attacks.\n8. Educate users about the risks of using weak passwords and sharing credentials.\n\nIn the event of a brute-force attack, the following steps should be taken for resolution, if the analyst suspects a brute-force attack, it would be advisable to:\n1. Block the IP address from which the attack originated using a firewall or fail2ban or SMB throttling to prevent further attempts.\n2. Reset credentials for the affected user account(s).\n3. Review system logs for any signs of unauthorized access or authentication attempts.\n4. Investigate the source of the attack, if possible, by conducting an IOC scan or analyzing network traffic.\n5. Notify the incident response team and relevant stakeholders about the incident.\n6. Implement additional security measures to prevent future brute-force attacks, such as MFA or strengthening password policies."
}
-----

Tools, Entities, Score, Memory, Json Response Implemented

Enter analyst ID (or 'exit'): exit

(.rags C:\Users\User\Documents\RAG\Final_Rags>
```