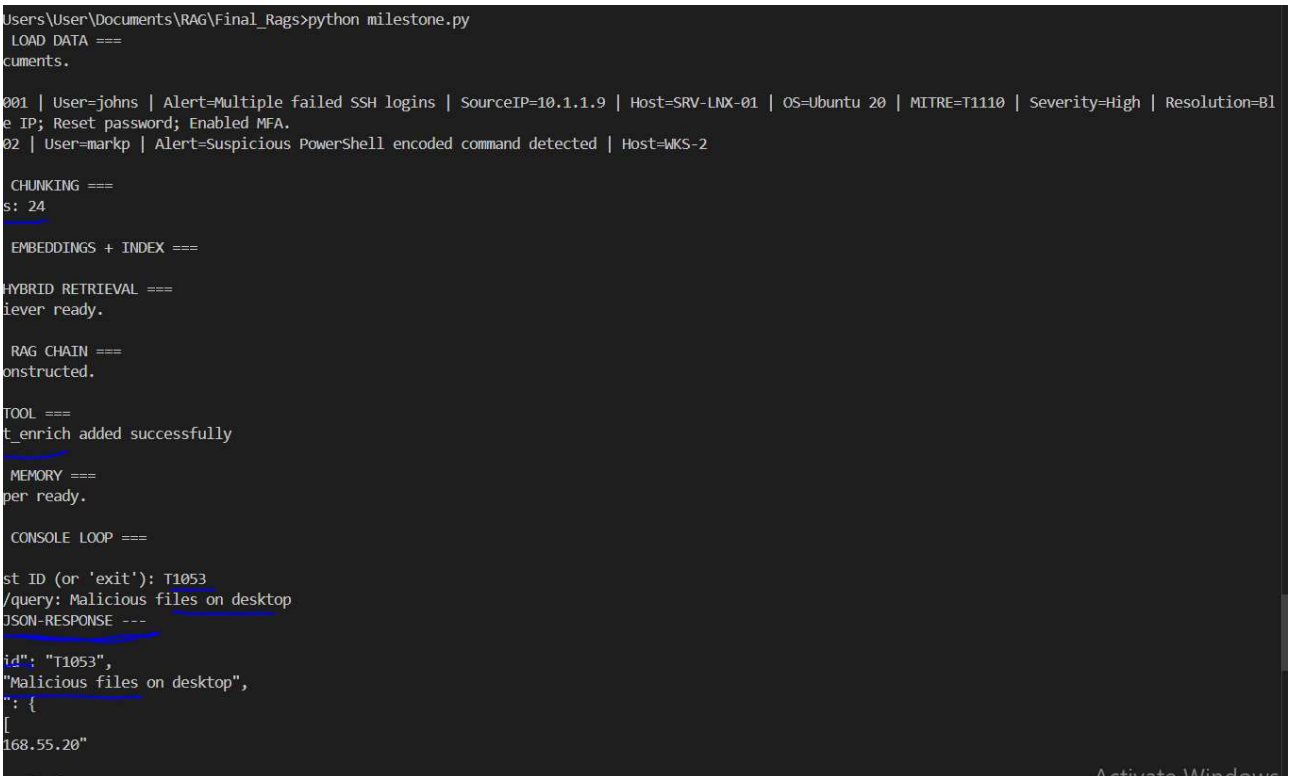
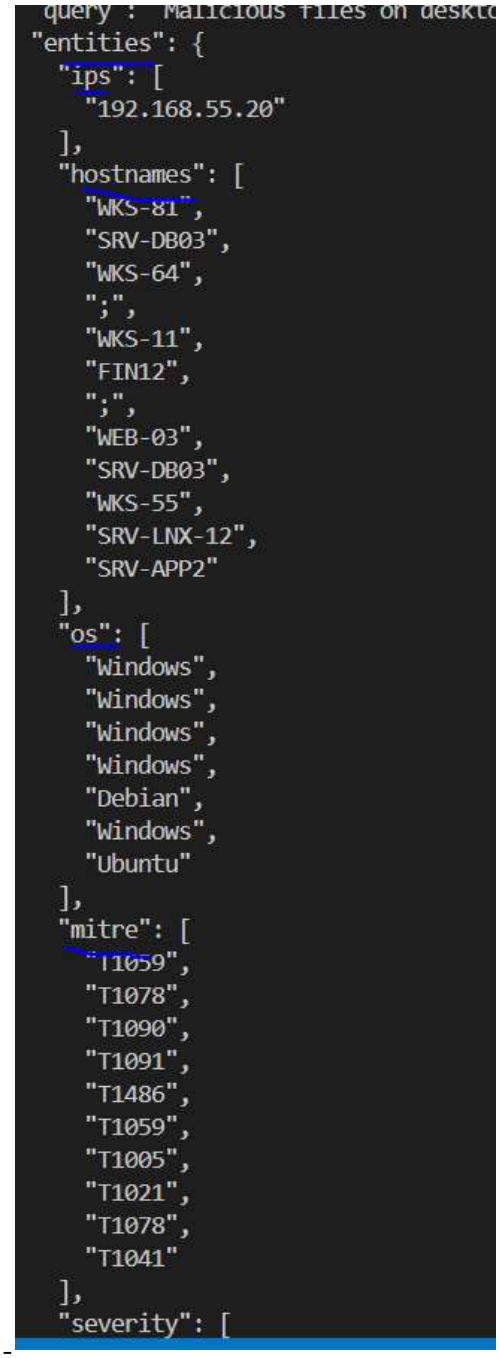
First Output:

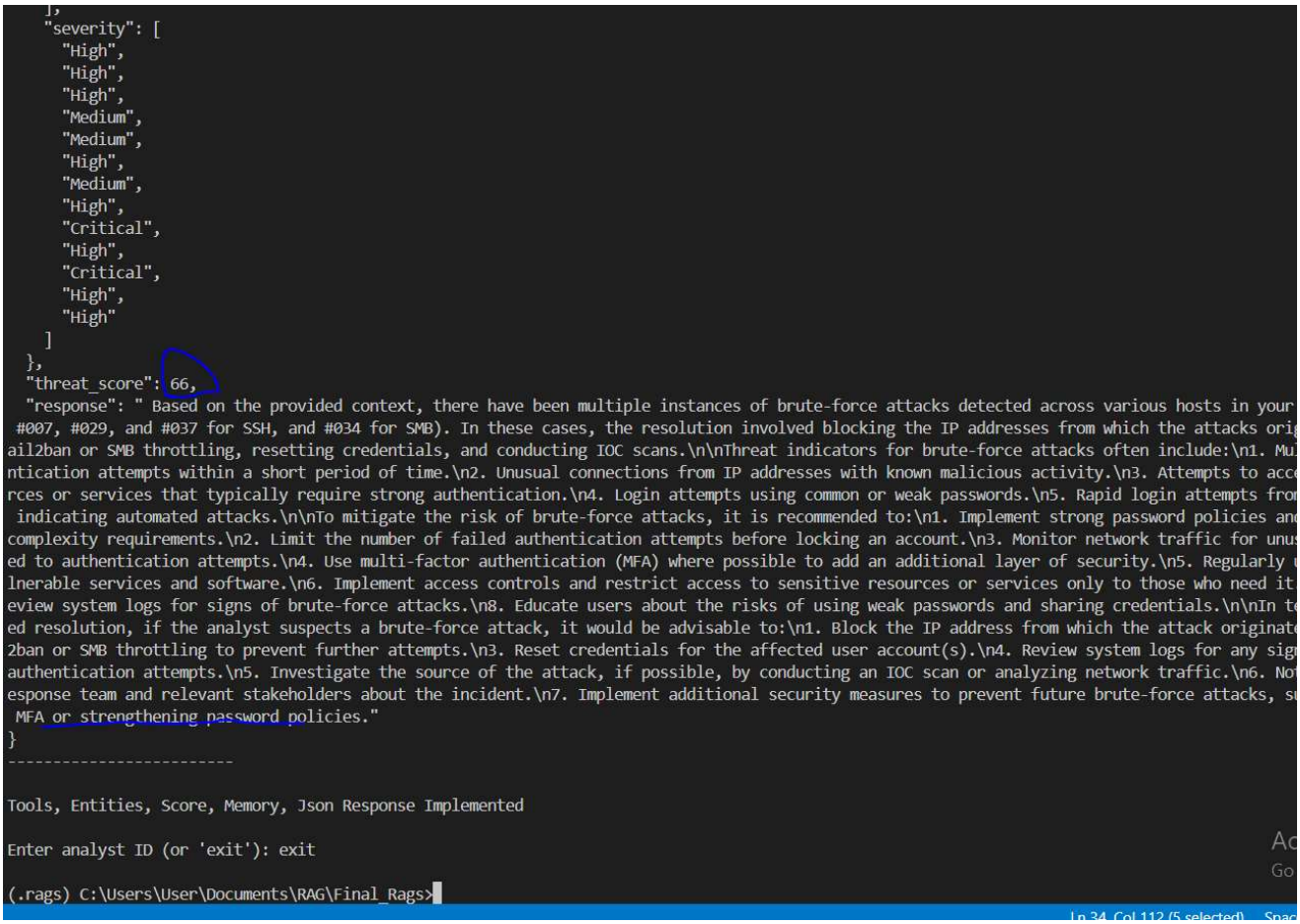


Entities :


"query": "Malicious files on deskto
"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 attackes
---BONUS : JSON-RESPONSE ---
{
  "analyst_id": "T1053",
  "query": "brute force attackes",
  "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"
    ],
```


],
"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 orig
ail2ban or SMB throttling, resetting credentials, and conducting IOC scans.\n\nThreat indicators for brute-force attacks often include:\n1. Mu
ntication attempts within a short period of time.\n2. Unusual connections from IP addresses with known malicious activity.\n3. Attempts to acc
rces or services that typically require strong authentication.\n4. Login attempts using common or weak passwords.\n5. Rapid login attempts fro
indicating automated attacks.\n\nTo mitigate the risk of brute-force attacks, it is recommended to:\n1. Implement strong password policies an
complexity requirements.\n2. Limit the number of failed authentication attempts before locking an account.\n3. Monitor network traffic for unus
ed to authentication attempts.\n4. Use multi-factor authentication (MFA) where possible to add an additional layer of security.\n5. Regularly
lnerable services and software.\n6. Implement access controls and restrict access to sensitive resources or services only to those who need it
eview system logs for signs of brute-force attacks.\n8. Educate users about the risks of using weak passwords and sharing credentials.\n\nIn t
ed resolution, if the analyst suspects a brute-force attack, it would be advisable to:\n1. Block the IP address from which the attack originat
2ban or SMB throttling to prevent further attempts.\n3. Reset credentials for the affected user account(s).\n4. Review system logs for any sig
authentication attempts.\n5. Investigate the source of the attack, if possible, by conducting an IOC scan or analyzing network traffic.\n6. No
esponse team and relevant stakeholders about the incident.\n7. Implement additional security measures to prevent future brute-force attacks, s
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>