1 reference
can you analyze my log file for cyber security threats and summarize the results.
1 reference

Summary of Cyber Security Threats in the Log File

1. Denial of Service (DoS) Attacks

The log file contains multiple entries indicating various types of DoS attacks, including:

- RST Scan
  - Example: `[DoS attack: RST Scan] from source 45.57.120.190, port 443 Friday, Mar 07, 2025 16:37:09`
- Fraggle Attack
  - Example: `[DoS attack: Fraggle Attack] from source 97.88.136.1, port 67 Friday, Mar 07, 2025 16:01:27`
- snmpQueryDrop
  - Example: `[DoS attack: snmpQueryDrop] from source 142.93.60.243, port 48890 Friday, Mar 07, 2025 15:12:32`
- TCP SYN Flood
  - Example: `[DoS attack: TCP SYN Flood] from source 18.118.100.31, port 41068 Thursday, Mar 06, 2025 23:43:28`
- ACK Scan
  - Example: `[DoS attack: ACK Scan] from source 52.123.128.14, port 443 Friday, Mar 07, 2025 10:33:45`

These entries suggest multiple attempts to disrupt network services by overwhelming the router with various types of malicious traffic.

2. Suspicious Admin Login Attempts

- Admin Login
  - Example: `[admin login] from source 192.168.1.36, Friday, Mar 07, 2025 16:43:59`

There is an entry indicating an admin login attempt. If this IP address is not recognized as an authorized admin source, it could indicate an unauthorized access attempt.

3. Too Many Bad Authentication Attempts

- Email Failed
  - Example: `[email failed] (#AUTH005) Too many bad auth attempts., Friday, Mar 07, 2025 17:03:47`

This entry indicates multiple failed authentication attempts, which could be a sign of a brute-force attack.

Recommendations

1. Implement Rate Limiting: To mitigate DoS attacks, implement rate limiting and traffic filtering on the router to block excessive traffic from suspicious IP addresses.
2. Monitor Admin Logins: Regularly review and monitor admin login attempts. Ensure that only authorized personnel have access and consider implementing multi-factor authentication (MFA).
3. Strengthen Authentication Mechanisms: Improve authentication mechanisms to prevent brute-force attacks, such as using complex passwords, enabling account lockout policies, and using MFA.
4. Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the network infrastructure.
5. Update Firewall Rules: Update firewall rules to block known malicious IP addresses and restrict traffic to essential services only.

By addressing these recommendations, you can enhance the security posture of your network and mitigate potential cyber threats.

can you cross reference the IP addresses in the log with a blacklist api?
1 reference

Summary of Cyber Security Threats and Blacklist Status

1. Denial of Service (DoS) Attacks

The log file contains multiple entries indicating various types of DoS attacks, including:

- RST Scan
  - Example: `[DoS attack: RST Scan] from source 45.57.120.190, port 443 Friday, Mar 07, 2025 16:37:09`
  - Example: `[DoS attack: RST Scan] from source 35.212.56.18, port 443 Friday, Mar 07, 2025 16:24:34`
- Fraggle Attack
  - Example: `[DoS attack: Fraggle Attack] from source 97.88.136.1, port 67 Friday, Mar 07, 2025 16:01:27`
- snmpQueryDrop
  - Example: `[DoS attack: snmpQueryDrop] from source 142.93.60.243, port 48890 Friday, Mar 07, 2025 15:12:32`
- ACK Scan
  - Example: `[DoS attack: ACK Scan] from source 52.123.128.14, port 443 Friday, Mar 07, 2025 10:33:45`

2. Suspicious Admin Login Attempts

- Admin Login
  - Example: `[admin login] from source 192.168.1.36, Friday, Mar 07, 2025 16:43:59`

There is an entry indicating an admin login attempt. If this IP address is not recognized as an authorized admin source, it could indicate an unauthorized access attempt.

3. Too Many Bad Authentication Attempts

- Email Failed
    - Example: `[email failed] (#AUTH005) Too many bad auth attempts., Friday, Mar 07, 2025 17:03:47`

This entry indicates multiple failed authentication attempts, which could be a sign of a brute-force attack.

Blacklist Status of IP Addresses

I performed a search to cross-reference the IP addresses involved in the DoS attacks with known blacklists. Here are the results:

1. 45.57.120.190
    - No specific blacklist information found.
2. 35.212.56.18
    - No specific blacklist information found.
3. 97.88.136.1
    - No specific blacklist information found.
4. 45.57.40.1
    - AbuseIPDB: 45.57.40.1: This IP address has been reported for abusive activity.
5. 142.93.60.243
    - No specific blacklist information found.
6. 141.98.11.88
    - No specific blacklist information found.
7. 154.213.200.14
    - AbuseIPDB: 154.213.200.14: WHOIS record available.
8. 205.210.31.229
    - AbuseIPDB: 205.210.31.229: Identified as part of Palo Alto Networks, potentially whitelisted.
9. 17.248.203.64
    - No specific blacklist information found.
10. 52.123.128.14
    - AbuseIPDB: 52.123.128.14: This IP address has been reported for abusive activity.

Recommendations

1. Implement Rate Limiting: To mitigate DoS attacks, implement rate limiting and traffic filtering on the router to block excessive traffic from suspicious IP addresses.
2. Monitor Admin Logins: Regularly review and monitor admin login attempts. Ensure that only authorized personnel have access and consider implementing multi-factor authentication (MFA).
3. Strengthen Authentication Mechanisms: Improve authentication mechanisms to prevent brute-force attacks, such as using complex passwords, enabling account lockout policies, and using MFA.
4. Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the network infrastructure.

5. Update Firewall Rules: Update firewall rules to block known malicious IP addresses and restrict traffic to essential services only.

By addressing these recommendations, you can enhance the security posture of your network and mitigate potential cyber threats.

can you make api Call for me to cross reference the IP addresses in the log with the results from the API call? you can use the following curl statement to make the call. The API key is the username and is provided in this link below:

```
curl https://api.blacklistchecker/ \
  -u key_ckcRSs82Sa9MaDRCQrmhyUQlB
```

I can create a script that you can run locally to cross-reference the IP addresses in the log file with the blacklist checker API. Here's a Python script that uses `requests` to make the API calls and check the blacklist status for each IP address.

Python

```python
import requests

API_KEY = 'key_ckcRSs82Sa9MaDRCQrmhyUQlB'

# List of IP addresses to check
ip_addresses = [
    '45.57.120.190',
    '35.212.56.18',
    '97.88.136.1',
    '45.57.40.1',
    '142.93.60.243',
    '141.98.11.88',
    '154.213.200.14',
    '205.210.31.229',
    '17.248.203.64',
    '52.123.128.14'
]

def check_blacklist(ip):
    url = f'https://api.blacklistchecker/{ip}'
    response = requests.get(url, auth=(API_KEY, ''))
    if response.status_code == 200:
        return response.json()
    else:
        return None

def main():
    results = {}
    for ip in ip_addresses:
        result = check_blacklist(ip)
        if result:
            results[ip] = result
        else:
            results[ip] = 'Error or not found'

    # Print results
    for ip, status in results.items():
        print(f'IP: {ip}, Status: {status}')

if __name__ == '__main__':
    main()
```

1 vulnerability detected

Save this script as `check_blacklist.py` and run it. This script will make API calls to the blacklist checker for each IP address in the list and print the results. Make sure you have the `requests` library installed. You can install it using `pip install requests`.

If you need any modifications or have any specific requirements, please let me know!