INTRUSION DETECTION

Authors:

Dennys Antunish: dantunish2@gmail.com

Angie Rivera: angiervr@gmail.com

Aliya Jones: alya.jones@macrlay.cuny.edu

Navruz Asatullaev: navruz.college@gmail.com

Evgeniia Yeroshkina: mironova.eug2016@gmail.com

INTRUSION DETECTION EVALUATION DATASET (CIC-IDS2017)

- Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick (UNB)
- To provide a realistic and modern dataset for evaluating Intrusion Detection Systems (IDS)
- Traffic Types:
  - Benign (normal) traffic
  - Attack traffic, including DoS / DDoS

HYPOTHESIS - WHAT WE EXPECTED TO FIND

- To find multiple victims on Friday, July 7th, 2017

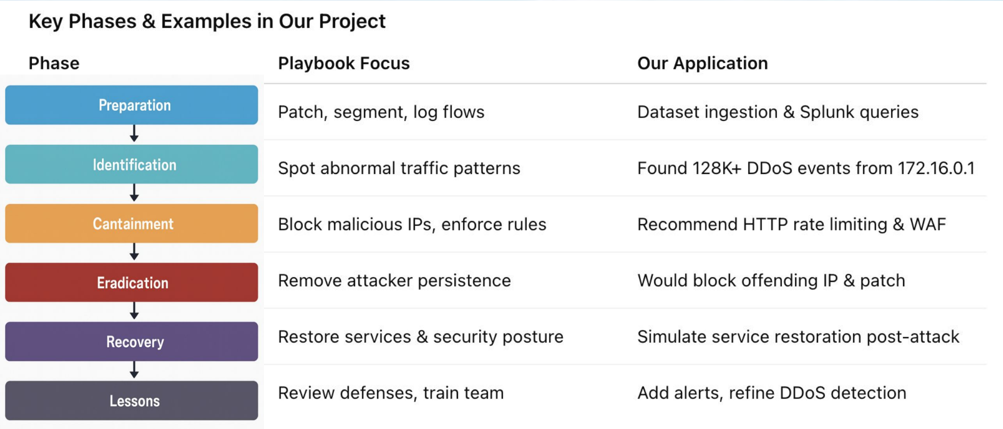
- To find a plethora of logs of an attempted attack at a company

- To find continuous use of the same IP address for multiple attacks

INCIDENT RESPONSE PLAYBOOK – GSPBC-1080

WHY DID WE CHOOSE THIS PLAYBOOK?

- ➔ Specifically addresses Dos/DDos attacks
- ➔ Aligns with our datasets focus on network traffic patterns
- ➔ Structured for Blue Team operations and SOC workflows
- ➔ Flexible – no assumption about tools or datasets



Key Phases & Examples in Our Project

Phase	Playbook Focus	Our Application
Preparation	Patch, segment, log flows	Dataset ingestion & Splunk queries
Identification	Spot abnormal traffic patterns	Found 128K+ DDoS events from 172.16.0.1
Cantainment	Block malicious IPs, enforce rules	Recommend HTTP rate limiting & WAF
Eradication	Remove attacker persistence	Would block offending IP & patch
Recovery	Restore services & security posture	Simulate service restoration post-attack
Lessons	Review defenses, train team	Add alerts, refine DDoS detection

Source: GuardSight CIRT Playbook Battle Cards, GSPBC-1080 – Network Denial of Service
Methodology: PICERL – *Preparation, Identification, Containment, Eradication, Recovery, Lessons*

MONITORING SOURCES

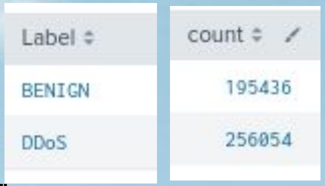
- What did we use to monitor and analyze?
  - Splunk to monitor network traffic patterns and identify potential threats.
- How did we use Splunk?
  - By filtering for events:
    - **Label and Destination IP*(we wanted to narrow down the logs to just DDoS and find the main IP that was been used for this attack)**
- Why it matters?
  - By starting with these two filers we were able to later detect high-volume traffic in these other fields **(Source;Destination IP, Destination Port, Protocol, Flow Duration , and Timestamps)**

MONITORING SOURCES

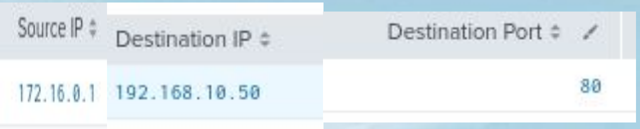
- Search by Label & Destination/ Source IP & Destination Port

  -
    ```
    index=main source="Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv" Label=*
    | stats count by Label
    ```

  -
    ```
    index=main source="Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv" Label="DDoS"
     | where isnotnull('Source IP') AND isnotnull('Destination IP') AND isnotnull('Destination Port')
    | stats count by "Source IP", "Destination IP", "Destination Port"
    | where count > 1
    ```



Label	count
BENIGN	195436
DDoS	256054

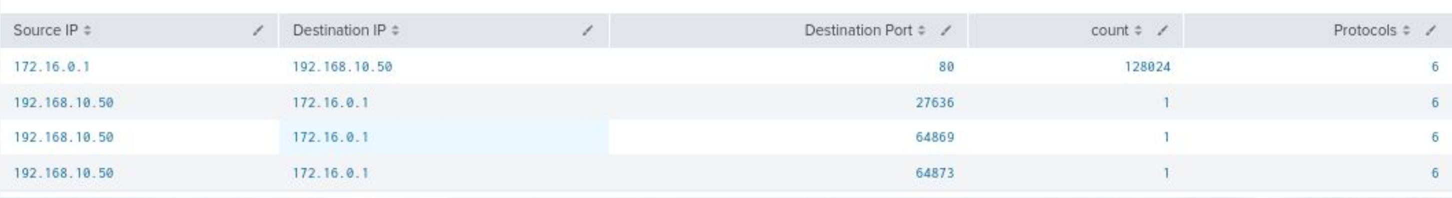


Source IP	Destination IP	Destination Port
172.16.0.1	192.168.10.50	80

- Including Protocol , Flow Duration & time

  -
    ```
    index=main source="Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv" Label="DDoS"
    | where isnotnull('Source IP') AND isnotnull('Destination IP') AND isnotnull('Destination Port')
    | stats count,
        values(Protocol) as Protocols,
        avg('Flow Duration') as Avg_Flow_Duration
      by "Source IP", "Destination IP", "Destination Port"
    | sort - count
    ```

  -
    ```
    index=main source="Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv" Label="DDoS"
    | where isnotnull('Source IP') AND isnotnull('Destination IP') AND isnotnull('Destination Port')
    | bucket _time span=1d
    | stats count, values(Protocol) as Protocols, avg('Flow Duration') as Avg_Flow_Duration
      by _time, "Source IP", "Destination IP", "Destination Port"
    | sort _time
    ```



Source IP	Destination IP	Destination Port	count	Protocols
172.16.0.1	192.168.10.50	80	128024	6
192.168.10.50	172.16.0.1	27636	1	6
192.168.10.50	172.16.0.1	64869	1	6
192.168.10.50	172.16.0.1	64873	1	6

IDENTIFIED ASSETS - VICTIM & ATTACKER

- What was identified while analyzing in Splunk?
  - The Attacker Asset **(Source IP**) and the Target Asset (**Destination IP**)
- What does this mean?
  - Understanding this gave insight into affected assets and where systems are the weakest/ vulnerable.

Target Asset (Destination IP):

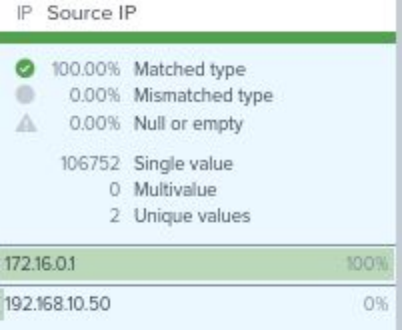
- **IP: 192.168.10.50**
- **Role: Internal server targeted on port 80 (HTTP)**
- **Impact: Likely runs a web app and was overwhelmed by traffic**

Attacker Asset (Source IP):

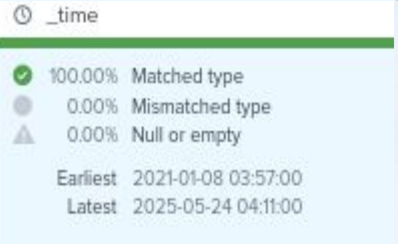
- **IP: 172.16.0.1**
- **Role: Primary source of malicious traffic**
- **Insight: Source of the traffic flood**

IDENTIFIED ASSETS-TRAFFIC DETAILS & IMPACT

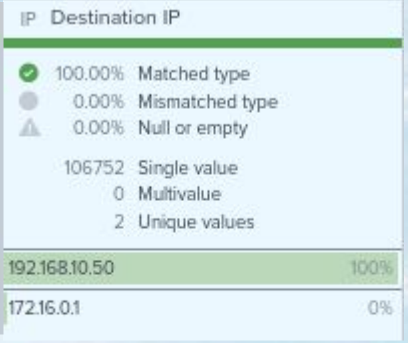
- **Network Protocols & Ports:**
  - **Protocol: TCP (Protocol 6)**
  - **Destination Port: 80**
  - **Impact: Attacker used normal web traffic (making it harder to detect but possibly revealing security gaps)**
- **Systems & Application Potentially Affected:**
  - **Web Apps IP: 192.168.10.50**
  - **Network Hardware : routers & switches**



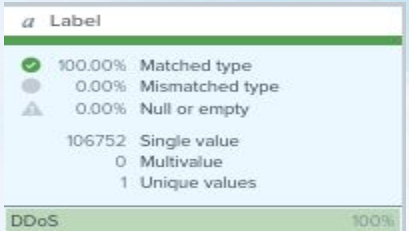
```
IP  Source IP

✓  100.00%  Matched type
●    0.00%  Mismatched type
⚠    0.00%  Null or empty

    106752  Single value
         0  Multivalue
         2  Unique values

172.16.0.1                    100%
192.168.10.50                   0%
```



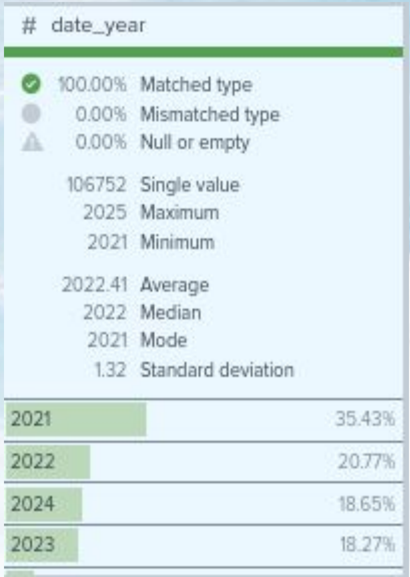
```
🕓  _time

✓  100.00%  Matched type
●    0.00%  Mismatched type
⚠    0.00%  Null or empty

  Earliest  2021-01-08 03:57:00
    Latest  2025-05-24 04:11:00
```



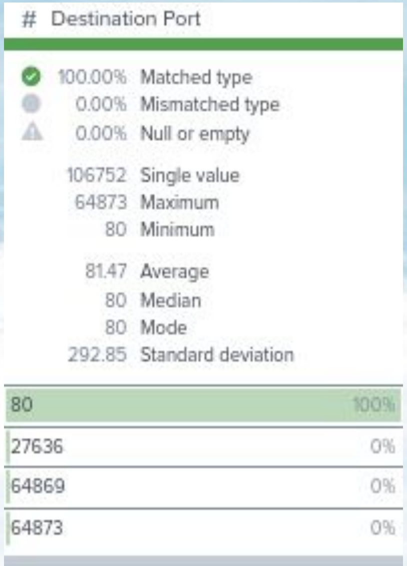
```
IP  Destination IP

✓  100.00%  Matched type
●    0.00%  Mismatched type
⚠    0.00%  Null or empty

    106752  Single value
         0  Multivalue
         2  Unique values

192.168.10.50                 100%
172.16.0.1                      0%
```



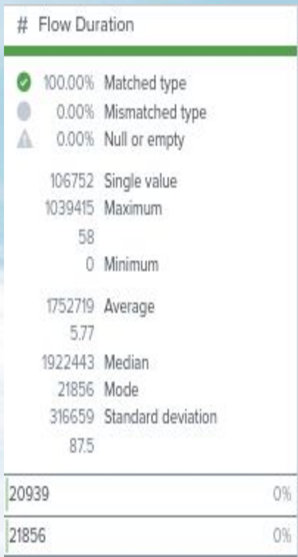
```
a  Label

✓  100.00%  Matched type
●    0.00%  Mismatched type
⚠    0.00%  Null or empty

    106752  Single value
         0  Multivalue
         1  Unique values

DDoS                          100%
```



```
#  date_year

✓  100.00%  Matched type
●    0.00%  Mismatched type
⚠    0.00%  Null or empty

    106752  Single value
      2025  Maximum
      2021  Minimum

   2022.41  Average
      2022  Median
      2021  Mode
      1.32  Standard deviation

2021                        35.43%
2022                        20.77%
2024                        18.65%
2023                        18.27%
```



```
#  Destination Port

✓  100.00%  Matched type
●    0.00%  Mismatched type
⚠    0.00%  Null or empty

    106752  Single value
     64873  Maximum
        80  Minimum

     81.47  Average
        80  Median
        80  Mode
    292.85  Standard deviation

80                            100%
27636                           0%
64869                           0%
64873                           0%
```



```
#  Flow Duration

✓  100.00%  Matched type
●    0.00%  Mismatched type
⚠    0.00%  Null or empty

    106752  Single value
   1039415  Maximum
        58
         0  Minimum

   1752719  Average
      5.77
   1922443  Median
     21856  Mode
    316659  Standard deviation
      87.5

20939                           0%
21856                           0%
```

IMPACT ANALYSIS AND TRIAGE

- Looking deep into the findings:
  - Impact Analysis
    - ~128,000 DDoS events → **High intensity**
    - **Single attacker**: `172.16.0.1`
    - **Critical ports** targeted (e.g., 80/443) → high business impact
    - **Conclusion**: **Severity = High | Priority**: Immediate mitigation
  - Triage
    - Goal: Confirm attack, asses spread, and identify attacker
    - Filtered on `Label=DDoS AND Dst IP=192.168.10.50`
    - **Attacker Identified**: `top Source IP` → `172.16.0.1`
    - **Timechart** showed **sustained spikes**
    - **Scope Check**: Only `192.168.10.50` affected
    - (Hypothetical) System log review for crash signs
    - Threat intel: Check if `172.16.0.1` is trusted or compromised

THREAT INTELLIGENCE

Type	Example	Why it matters
Source IP	`172.16.0.1`	Repeated source of attack traffic
Destination IP	`192.168.10.50`	Targeted internal server (likely hosting a web service)
Destination Port	`80`	HTTP — often abused in DDoS due to open access
Protocol	`6 (TCP)`	Used to mimic legitimate HTTP traffic
Flow patterns	High counts, short duration	Indicates flood behavior (common in DDoS attacks)

THREAT INTELLIGENCE

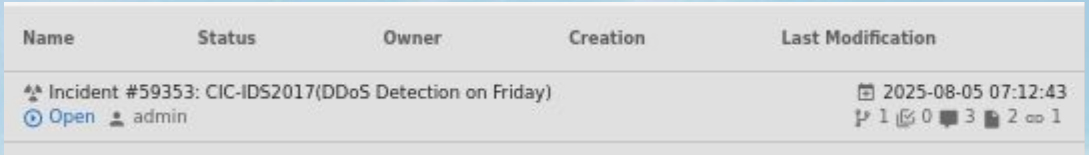
Tactic	Technique	Details from Dataset
Initial Access	External Remote Services (T1133)	Traffic flooded from external IP toward open HTTP port
Impact	Network Denial of Service (T1498.001)	Repeated, large-volume TCP traffic over port 80
Evasion	Abuse of Legitimate Protocol (T1071.001)	Using HTTP/TCP to disguise the attack as regular web traffic

RECOMMENDED REMEDIATION

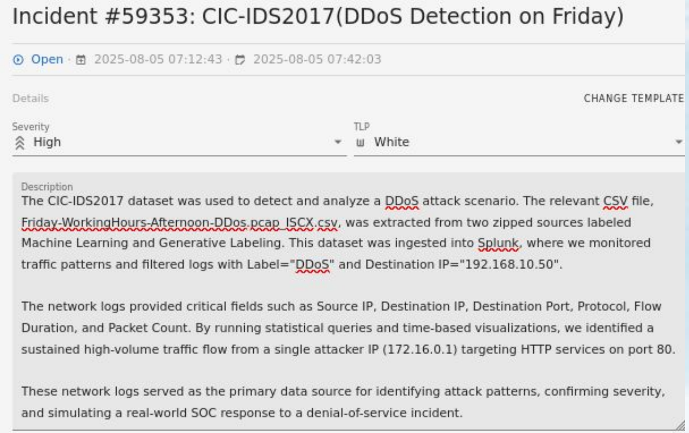
- Block attacker IP (172.16.0.1)
- Limit HTTP requests per IP
- Deploy Cloudflare WAF
- Set Splunk alerts for traffic spikes
- Enforce HTTPS and disable HTTP
- Update and secure all systems

CASE MANAGEMENT SYSTEM

- Catalyst was used for case management system to log and track each phase of the DDoS incident response.



Name	Status	Owner	Creation	Last Modification
Incident #59353: CIC-IDS2017(DDoS Detection on Friday)	Open	admin		2025-08-05 07:12:43 1 0 3 2 1



Incident #59353: CIC-IDS2017(DDoS Detection on Friday)

Open · 2025-08-05 07:12:43 · 2025-08-05 07:42:03

Severity: High

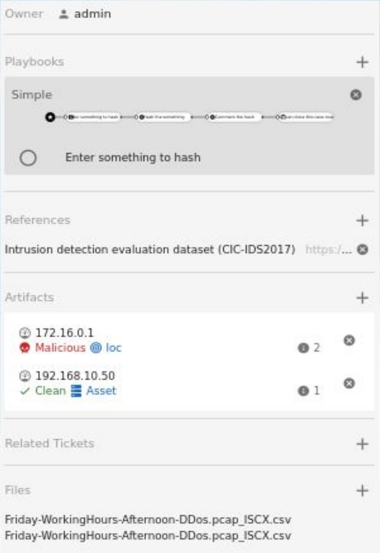
TLP: White

Description

The CIC-IDS2017 dataset was used to detect and analyze a DDoS attack scenario. The relevant CSV file, Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv, was extracted from two zipped sources labeled Machine Learning and Generative Labeling. This dataset was ingested into Splunk, where we monitored traffic patterns and filtered logs with Label="DDoS" and Destination IP="192.168.10.50".

The network logs provided critical fields such as Source IP, Destination IP, Destination Port, Protocol, Flow Duration, and Packet Count. By running statistical queries and time-based visualizations, we identified a sustained high-volume traffic flow from a single attacker IP (172.16.0.1) targeting HTTP services on port 80.

These network logs served as the primary data source for identifying attack patterns, confirming severity, and simulating a real-world SOC response to a denial-of-service incident.



Owner: admin

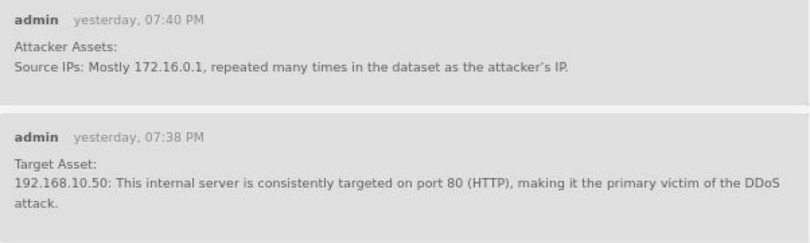
○ Enter something to hash

Intrusion detection evaluation dataset (CIC-IDS2017) https:/...

172.16.0.1
Malicious loc 2

192.168.10.50
✓ Clean Asset 1

Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv
Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv



admin yesterday, 07:40 PM

Attacker Assets:
Source IPs: Mostly 172.16.0.1, repeated many times in the dataset as the attacker's IP.

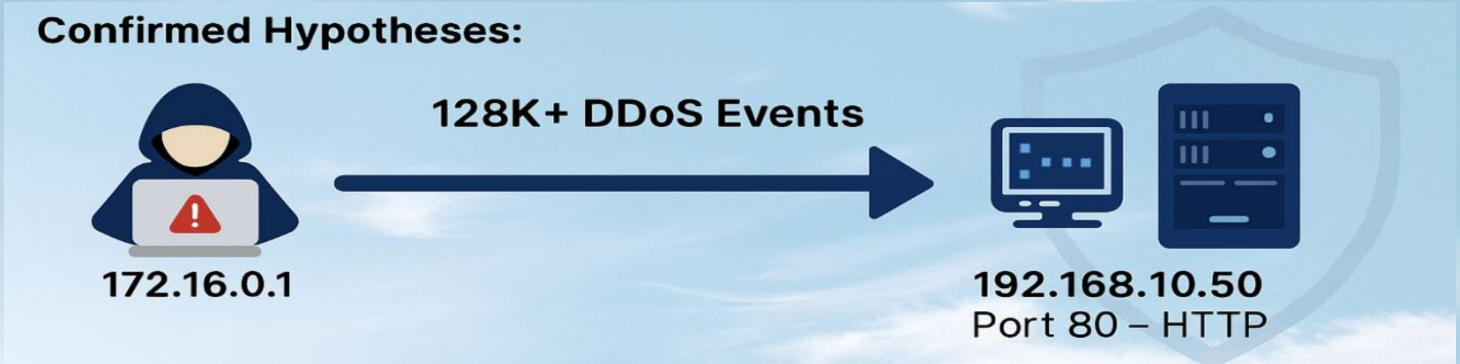
admin yesterday, 07:38 PM

Target Asset:
192.168.10.50: This internal server is consistently targeted on port 80 (HTTP), making it the primary victim of the DDoS attack.

LESSONS LEARNED

- Even one compromised internal IP can disrupt services if traffic is not monitored and restricted.
- Protocol abuse (e.g., HTTP flood) is a simple but effective evasion tactic if perimeter defenses aren’t deep-inspecting.
- Network flow logs are a powerful data source for identifying traffic-based attacks.
- Structured frameworks like MITRE ATT&CK help classify attacker behaviors and prepare mitigation playbooks.
- SOC tools like Splunk and Catalyst are vital not only for detection and response but also for documentation and improvement tracking.
-

CONCLUSION



Confirmed Hypotheses:

172.16.0.1

128K+ DDoS Events

192.168.10.50
Port 80 – HTTP

Lessons Learned:

- Importance of continuous monitoring & early detection
- Playbook-based response improves speed & effectiveness