Analyzing the CICIDS2017 Dataset: A Comprehensive Incident Response Approach

Presenter Names (Group 27):

Bratt Morejon
Amit Gupta
Alexander Nguyen

Project Overview

- Dataset: CICIDS2017 from the Canadian Institute of Cybersecurity.

- Objective: Analyze the dataset to identify and respond to cybersecurity incidents using professional playbooks and tools.

CICIDS2017 Dataset Overview

- Origin: Created by CIC to address IDS testing gaps.
- Data Type: Network traffic logs, .csv format.
- Technologies Targeted: Ubuntu servers, Windows OS, MAC, and Kali systems.
- Protocols: HTTP, HTTPS, FTP, SSH, Email.

What We Expect to Find?

- DDoS traffic volume may amplify with multiple attackers.
- NAT firewalls should integrate other devices for better security.
- Older OS like Win Vista require constant updates and service management.

CERT Societe Generale Playbook

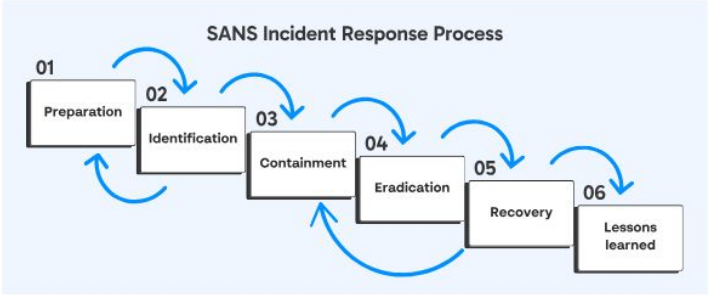
- Developed by CERT Societe Generale.
- Target Audience: SOC analysts, response teams, cybersecurity pros.
- Matches dataset assumptions but requires adaptation for specific attack types.

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

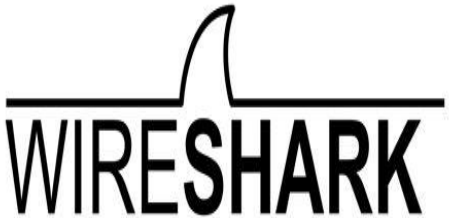
1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

SANS Incident Response Plan



Incident Response Tools

- **Wireshark**: Analyze network traffic.
- **Splunk**: Visualize and correlate data.
- **VirusTotal & AbuseIPDB**: Scan IP addresses.
- **Auditd**: Monitor file changes.

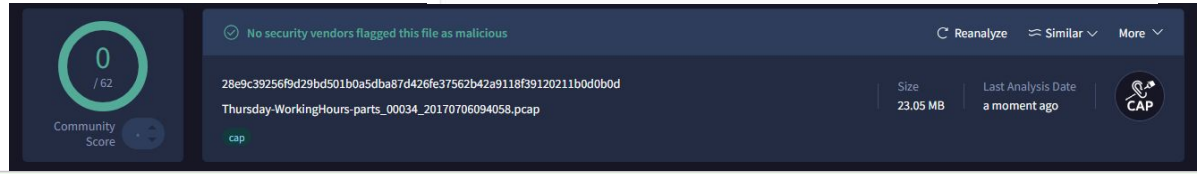


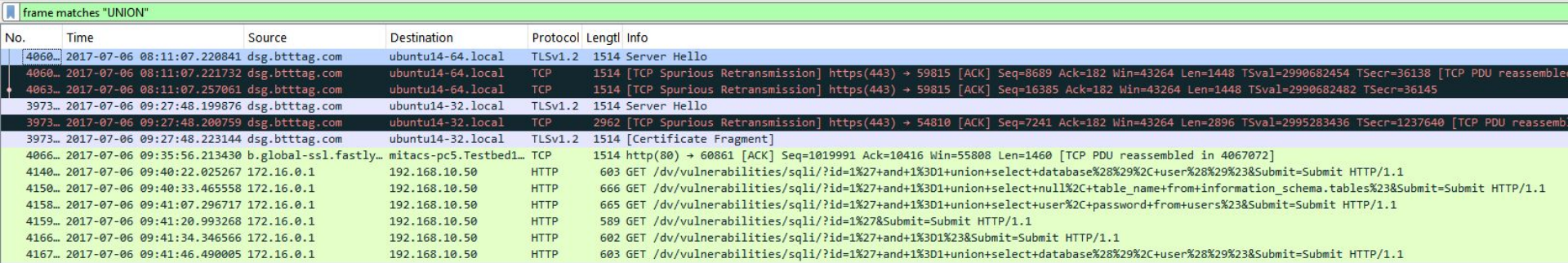
Monitoring the Dataset & Asset Identification

Identified unauthorized access and malware attacks :

- Brute Force, XSS, SQL Injection attacks.

- FTP-Patator and SSH-Patator attacks.





Conclusion:

Findings:
- The CICIDS2017 dataset revealed common attack patterns like SQL Injection, Brute Force, and DDoS attacks.
- Tools like Wireshark, Splunk, and VirusTotal were vital for traffic analysis and threat identification.
- The CERT Societe Generale Playbook provided a structured and effective incident response framework.

Key Lessons Learned:
- Realistic datasets improve IDS/IPS training and threat detection.
- Proactive measures like updates and robust firewall rules reduce vulnerabilities.
- Flexible playbooks are crucial for handling diverse attack scenarios.

Impact:
- Enhanced preparedness and actionable insights for minimizing downtime and data loss.
- Improved understanding of effective cybersecurity practices to tackle real-world threats.

Contact info

alexanderhonguyen19@gmail.com

amitgupta44347@gmail.com

bratmorejon@gmail.com

Source:

https://www.unb.ca/cic/datasets/ids-2017.html