DDoS Attack Detection Script Documentation

Overview

This DDoS Attack Detection Script is a Bash script designed to monitor and detect potential Distributed Denial of Service (DDoS) attacks on web server logs. The script analyzes Apache web server logs for suspicious traffic patterns and alerts administrators when potential DDoS attacks are detected. It allows for customization of detection parameters and can perform an action, like notifying an external system, upon detecting an attack.

Script Components

check_logs() Function: The core function responsible for scanning Apache logs and identifying potential DDoS attacks. The function takes several parameters:

- **domain**: The domain name for which the logs will be analyzed.
- **log_file**: The path to the Apache access log file for the given domain.
- **timeframe**: The time window (in seconds) within which multiple requests from the same IP address are counted as part of a potential attack.
- **threshold**: The minimum number of requests from a single IP address within the timeframe to trigger a potential DDoS alert.
- **report_url**: The URL to be called if a potential DDoS attack is detected. This URL should have a query parameter domain to specify the affected domain in the alert.
- **total_threshold**: An optional additional threshold for the total number of requests from all IPs within the total_timeframe to trigger a potential DDoS alert.
- **total_timeframe**: An optional additional timeframe (in minutes) within which the total_threshold is checked for a potential DDoS attack.

Main Script:

1. Reads configuration parameters from an INI file (ddos_checker.ini).
2. Retrieves Apache logs path, excluded domains, timeframes, thresholds, attack URLs, and additional parameters from the INI file.
3. Obtains a list of virtual hosts (domains) from the Apache logs directory.
4. Checks each domain for DDoS attacks using the check_logs() function.
5. Skips domains that are excluded from DDoS detection based on the configuration.

Configuration

The script requires a configuration file named ddos_checker.ini located in the same directory as the script. The INI file contains the following configuration parameters:

apache_logs_path: The path to the directory containing Apache access logs.
excluded_domains: A list of domains (separated by commas) to be excluded from DDoS attack detection.
timeframe: The time window (in seconds) within which multiple requests from the same IP address are counted as part of a potential attack.
threshold: The minimum number of requests from a single IP address within the timeframe to trigger a potential DDoS alert.
report_url: The URL to be called if a potential DDoS attack is detected. This URL should have a query parameter domain to specify the affected domain in the alert.
total_threshold (your preferred option): An additional threshold for the total number of requests from all IPs within the additional_timeframe to trigger a potential DDoS alert.
total_timeframe (your preferred): An additional time frame (in minutes) within which the total_threshold is checked for a potential DDoS attack.