Script Details

Sierra Maldonado

Email Alert

The Lambda function is triggered by log events from CloudWatch Logs. These log events are passed to the Lambda function as the event parameter.

The lambda_handler function processes the log events by iterating over each log event in the Records list.

For each log event, it extracts relevant information, such as the log message, source IP, and outcome, using the extract_source_ip and extract_outcome functions. In this example, the source IP is hardcoded as '3.142.131.22' for demonstration purposes, but in practice, you would extract it from the log message.

The increment_failed_attempts function keeps track of failed login attempts by storing them in a dictionary called failed_attempts_cache. It increments the count for an existing source IP or adds a new source IP with an initial count of 1.

The is_brute_force_attack function checks if the number of failed login attempts for a source IP exceeds a threshold (in this case, 3). If the threshold is exceeded, it returns True, indicating a potential brute force attack.

If a brute force attack is detected, the mitigate_brute_force_attack function takes action. In this example, it publishes a notification to an SNS topic using the boto3 AWS SDK. It constructs a message indicating the detected attack with the source IP and publishes it to the specified SNS topic. Additionally, it demonstrates an example of adding the detected IP address to a blocklist using AWS WAF (Web Application Firewall).

Attack Script:

Mode 1: Iterator
Asks for a file path to a dictionary (wordlist) file.
Reads the file line by line and prints each line (word) with a delay of 1 second between each word.
Mode 2: Password Check
Asks for a file path to a wordlist file.
Asks the user to enter a new password.
Checks if the new password is present in the wordlist file. If it is, it prints "Password is weak!" indicating that the password is not strong.
Mode 3: Brute Force SSH
Asks for a file path to a wordlist file.
Asks for an IP address to connect to and a username.
Attempts to establish an SSH connection to the provided IP address using each password from the wordlist file until a successful authentication occurs or the wordlist is exhausted.
Mode 4: Zipfiles
Asks for the path to a zip file and a password file.
Reads the passwords from the password file into a list.
Attempts to extract the files from the zip file using each password from the list until a successful extraction occurs or all passwords are tried.
Exit
Allows the user to exit the script.