IRON CLOUD
SECURITY

Script Details

Sierra Maldonado

Email Alert

It imports the required modules: json for JSON serialization and deserialization, and boto3 for interacting with AWS services.
It defines the lambda_handler function, which is the entry point for the Lambda function when it is triggered.
Within the lambda_handler, it creates a client object for interacting with AWS GuardDuty service using boto3.client('guardduty').
It retrieves a list of findings from GuardDuty using the get_findings method of the GuardDuty client.
It loops through each finding ID in the response using for finding in response['FindingIDs']:.
For each finding, it retrieves the detailed information of the finding using the get_findings method of the GuardDuty client, passing the finding ID.
It checks if the severity of the finding is greater than 4.0 using if finding_details['Severity'] > 4.0:.
If the severity is higher than 4.0, it calls the take_action function, passing the finding details as an argument.
The take_action function creates an SNS (Simple Notification Service) client using boto3.client('sns').
It publishes a message to an SNS topic identified by its ARN (Amazon Resource Number) using the publish method of the SNS client. The message is the serialized JSON representation of the finding details obtained from GuardDuty.
The message is published with a subject "GuardDuty Findings".

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.