

GCP-based SSH Brute-forcing Incident Response Playbook

Title	GCP-based SSH Brute-forcing Incident Response Playbook
Version	V1
Date issued	DD-MM-YYYY
Status	In progress
Document owner	Full Name
Creator name	Full Name
Creator organization name	<Organization Name>
Subject category	GCP Incident Response
Access constraints	NA
Review cycle	Annually

1. Introduction

1.1. Incident Overview

Attackers leverage the shared responsibilities, extensive Internet exposure, and complex network management of cloud environments to target organizations. The IH&R teams dealing with cloud networks face new threats and challenges every day. Therefore, they must be prepared with appropriate plans and procedures to determine such threats before they cause severe damage to the cloud environment.

Assume that an organization is using the Google Cloud Platform for its business operations. The organization's cloud platform was affected by an unexpected brute-force attack on SSH. This playbook describes different activities related to various stages of incident response for better implementation of incident response procedures in case of an SSH brute-force attack in the GCP environment.

1.2 Purpose of Playbook

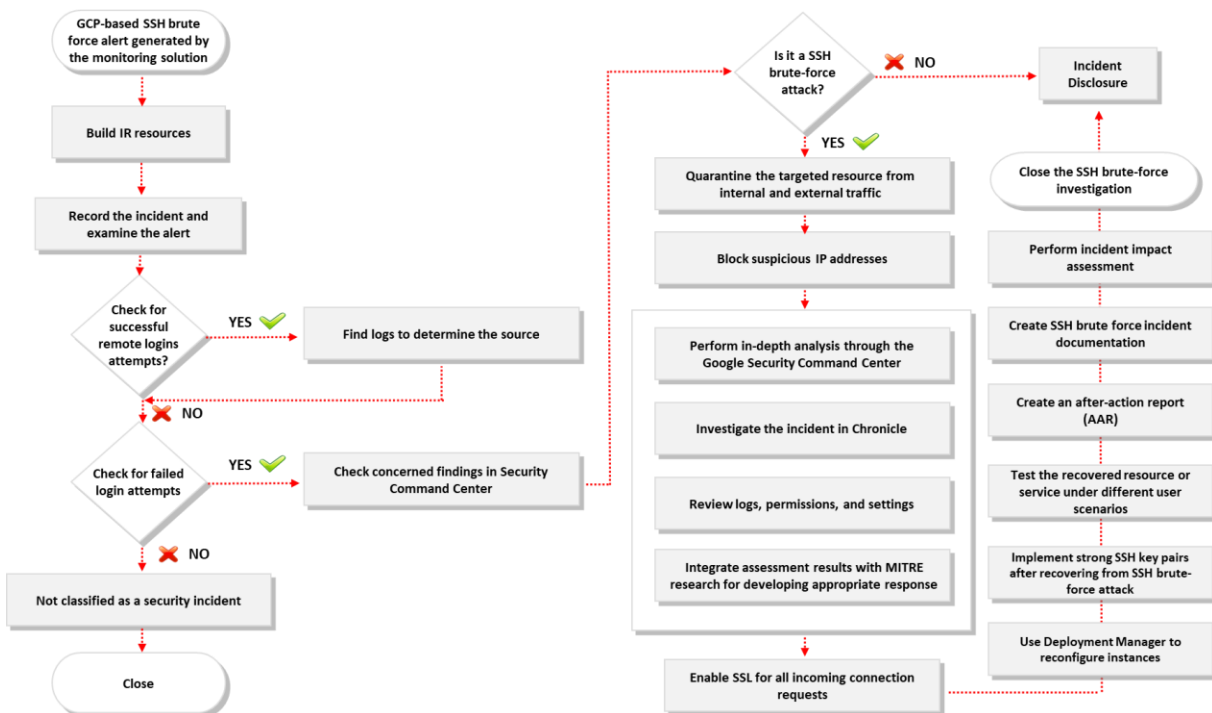
The main purpose of this playbook is to provide guidance for handling and responding to SSH brute force attacks in the GCP environment. This playbook includes step-wise guidance and procedures for the IH&R team to implement mitigative actions against SSH brute-force attempts.

1.3 Scope

This playbook is developed for the IH&R team to respond to SSH brute-force attacks in the GCP environment. Additionally, this document must be used alongside the incident response plan of organizations. The scope of this document is listed below (not limited to):

- Determine the total number of resources affected by an incident
- Understand and document various actions associated with SSH brute-force attack; for example:
 - Unusual API requests to GCP
 - Attempts to retrieve GCP IAM passwords
 - Unusual GCP configuration updates
- Identify any related activities by checking the following:
 - Suspicious GCP login attempts
 - Many login requests within a specific period
 - Unauthorized access to GCP from an unknown IP address and geolocation
 - Artifacts from Google VPC network traffic containing port scanning and connection requests to an anomalous port
 - Modification of privileged Google group accessibility to make it publicly available
 - Modification of Google Cloud services from an anonymous proxy IP address
 - Anonymous user agent accessing Google Cloud through an IAM service account
 - Unauthorized changes in two-factor authentication and Single Sign-on (SSO) settings
 - Alteration and misconfiguration of all access control policies in Google Cloud resources
- Analyze suspicious traffic
- Recover from the incident

1.4 Workflow Diagram



Workflow diagram for GCP-based SSH brute-force incident response

2. Preparation

2.1 Objectives

The main objective of the preparation phase involves preparing the organization or IH&R team to effectively respond to SSH brute forcing incidents. Another objective of this phase is to define the roles and responsibilities of the IH&R team to perform various activities during the response process.

2.2 Activities Involved

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Prepare for incident response:
 - Prepare, review, and practice the incident response procedures in accordance with the incident response plan
 - Prepare a team of experts for various specialized functions to efficiently manage the challenges of each incident
 - Accumulate industry best practices and guidelines before initiating the response process
 - Prepare the required tools and resources
 - Configure the GCP's automated and manual processes to get alerts for potential incidents

- Utilize machine learning functionalities to identify complex anomalies and unusual behaviors
- Establish and familiarize yourself with proper communication techniques such as IRC and phone bridge, which can be used during a security incident
- Customize incident alerts in different GCP services based on the requirement
- Develop some templates and a contact list that can be used to share information across teams during an incident
- Incorporate threat intelligence into the existing security capabilities to feed them with the latest risks, vulnerabilities, and common patterns
- Ensure that the team has the proper skillset with generic mitigation techniques such as rolling back changes and draining to minimize the time to mitigate (TTM)
- Create an effective dashboard layout such that responders can quickly pinpoint any changes or issues across the GCP
- Ensure that links to the concerned documents are available to be referred to by responders after being notified of an incident
 - Link 1:
 - Link 2:
 - Link 3:
- Conduct incident response drills to practice the skills of handling Google Cloud security incidents
- Implement a process maturity model to review the incident process
- Inform users:
 - Conduct regular training and awareness programs regarding the safe usage of GCP resources
 - Create a proper format for reporting and registering complaints
 - Ensure that training and awareness sessions are mandatory for employees handling critical data and systems of the organization
 - Provide proper contact information of personnel who can be contacted by users in case of GCP-based SSH brute-force attack

2.3 Stakeholders Involved/Communication

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Prepare for incident response <ul style="list-style-type: none"> ○ Create incident response processes and procedures ○ Define response mechanisms for incident response ○ Define security assertions ○ Incorporate threat intelligence ○ Subscribe to a continuous feed of current and relevant threats ○ Prepare related processes required for investigation ○ Generate notification alerts for unusual, malicious, or expensive activities 	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Service Desk	Email, Phone, Text Message
	Service Delivery Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Federal Agency	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
Inform users <ul style="list-style-type: none"> ○ Conduct training and awareness campaigns on the safe usage of cloud data 	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	HR Manager/Director	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

2.4 Additional Information (if any)

Note: Refer to the following templates and checklists to fill the necessary details:

- a. Preparation to Handle Cloud Security Incident.docx
- b. Cloud Security Incident Handling Toolkit.docx
- c. IH&R Plan Template.docx
- d. IH&R Plan Checklist.docx
- e. IH&R Policy and Procedure Template.docx

3. Detection and Notification

3.1 Objectives

The main objective of the detection phase is to perform initial investigation on the suspected GCP network and determine whether the brute-force attack on SSH caused damage to resources or compromised data.

3.2 Activities Involved

[Activities may differ based on organizational policies, but they are not limited to the following.]

- To detect unauthorized access to GCP through brute-force attack on SSH:
 - Check if the GCP was accessed from an unknown IP address or geolocation
 - Check for unusual remote access connection requests
 - Check for increased number of requests from the same source
 - Check for failed login attempts
 - Check for login attempts from unprivileged users
 - Check for unusual GCP configuration activities such as unknown instance creation or deletion
 - Check for unauthorized GCP IAM activities such as user creation and changes in user access privileges
 - Check for unauthorized changes in GCP IAM password policies
 - Check for unusual API requests to GCP
 - Check if artifacts from Google VPC network traffic contain port scanning and connection requests to an anomalous port
 - Check for modifications in Google Cloud services from an anonymous proxy IP address
 - Check for unauthorized changes in two-factor authentication and SSO settings

- Check for other alteration and misconfiguration of access control policies in Google Cloud resources
- Check for errors triggered from the Google Security Command Center (SCC) and its services
- Gather information from initial investigation:
 - Find logs related to the incident
 - Based on these logs, determine the type of incident
 - Note down who, how, and when the incident was reported
 - List the resources being targeted
 - List the number of resources affected
 - Determine the impact on business operations

3.3 Stakeholders Involved/Communication

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Detecting the incident <ul style="list-style-type: none"> ○ Monitor security solutions ○ Respond to manual and automated alerts ○ Escalate the incident via the ticketing system (if not escalated) 	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Initial investigation <ul style="list-style-type: none"> ○ Collect initial evidence data ○ Classify and prioritize the incident 	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message

	Head of IT	Email, Phone, Text Message
Notification of the incident ○ Follow the defined IH&R plan to notify the incident	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message

3.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- f. Cloud Security Incident Handling Toolkit.docx
- g. Incident Identification and Validation Template.docx
- h. Incident Priority Template.docx
- i. Incident Communication Logs Template.docx
- j. Incident Information Collection Form.docx
- k. Evidence Collection Template.docx

4. Containment

4.1 Objectives

The main objective of the containment phase is to identify the resources affected by SSH brute-force attacks and isolate them from the network while maintaining business operations.

4.2 Containment Steps/Activities

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Activities to contain GCP-based SSH brute-force incidents:
 - Block unauthorized access to the GCP
 - Quarantine the affected resources from internal and external traffic
 - Block suspicious IP addresses and disconnect any unused network services
 - Temporarily block password-based authentication
 - Temporarily block users with project-wide SSH keys using the following command:


```
gcloud compute instances add-metadata INSTANCE_NAME --  
metadata block-projectssh-keys=TRUE
```

- Disable root access to targeted resources
 - Filter and block suspicious traffic to SSH
 - Scan and disable exposed SSH services (if any)
 - Disable unused services
 - Disable unrestrictive firewall rules on port 22
 - Configure the SSH server on non-standard ports; by doing this, automated attacks on the default SSH port will be declined
 - Configure anti-brute-force tools to block request flooding from the same source
 - Create a snapshot of the virtual machine disk for forensic investigation after the workload is redeployed or deleted
 - Inspect the virtual machine while the workload is running to identify and contain emerging threats
 - Start a fresh copy of the container and delete the compromised container
 - Limit ongoing damage using cloud-integration tools and fix the underlying issue
 - Isolate compromised VMs and containers in the Google Cloud environment
 - Continuously manage access controls and enforce the principle of least privileges
 - Remove compromised cloud instances from the Google Cloud environment
 - Delete compromised cloud and user accounts
 - Update policies and anti-malware signatures
 - Use VPC Service Controls (VPC SCs) to stop data exfiltration attempts
 - Revoke and reissue credentials
 - Remove Google Cloud CLI credentials as an administrator
 - Remove Google Cloud CLI credentials as a user
 - Revoke application default credentials as an administrator
 - Revoke application default credentials as a user
 - Invalidate browser cookies as an administrator and user
 - Identify and delete all unauthorized access and resources by examining audit logs in the Google Cloud console
- Communicate the progress:

- Regularly inform the users and stakeholders about the status of the incident handling process

4.3 Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Containment activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

4.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- l. Containment of Cloud Security Incidents Checklist.docx
- m. Incident Containment Checklist.docx
- n. Incident Containment Template.docx

5. Analysis

5.1 Objectives

The main objective of this phase is to analyze the security incident and determine its scope. Another objective of this phase is to detect and report the incident impact to establish forensic investigation requirements and develop an effective mitigation strategy based on analysis results.

5.2 Activities Involved

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Analyze the scope of SSH brute-forcing attempt on the GCP:
 - Review cloud audit logs
 - Analyze the incident through Google Security Command Center
- Investigate the incident in Chronicle
- Review changes to permissions and settings
- Analyze VPC Flow Logs related to **srcIP**:

- `logName="projects/projectId/logs/syslog"`
- `labels."compute.googleapis.com/resource_name"="vmName"`
- Check the MITRE ATT&CK framework entry for the “Valid Accounts: Local Accounts” finding type
- Analyze IAM policies and security keys of the admin
- Analyze the port accepting requests for SSH
- Analyze the retention policies on log buckets
- Review SSH key management implemented on the GCP
- Analyze logs using tools such as DataDog

5.3 Stakeholders Involved

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Analyze the scope of incident	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Analyze the origin of requests and report potentially compromised resources	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Initiate evidence gathering and forensic analysis	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

5.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- o. Cloud Security Incident Report Template.docx
- p. Evidence Gathering and Forensic Analysis Form.docx
- q. Checklist for Handling the Forensic Evidence Properly.docx

6. Eradication

6.1 Objectives

The main objective of this phase is to take appropriate measures to eradicate the incident and prevent such incidents in future.

6.2 Eradication Steps/Activities

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Perform the following activities to eradicate access to the GCP through SSH brute-forcing:
 - Enforce strong passwords for SSH access
 - Restrict the number of login attempts
 - Enable SSL for all incoming connection requests
 - Activate multifactor authentication (MFA)
 - Assess the infected instance and block unknown IP addresses
 - Disable SSH access to the VM if necessary (strictly use SSH authentication with authorized keys for this operation)
 - Use the Google Cloud Armor solution or update firewall rules to block malicious IP addresses
 - Terminate all communications from suspected user accounts
 - Update all VMs and containers
 - Implement a defense-in-depth network strategy in the Google Cloud environment
 - Implement strong API key generation, storage, and management in the Google Cloud environment
 - Use VPC SCs to restrict unauthorized access
 - Implement the principle of least privileges and reset the password of all compromised resources
 - Deploy Google Cloud Armor to stop unusual traffic flow
 - Implement a zero-trust environment
 - Enforce WAF and granular security policies
 - Detach external IP addresses from the affected VM and use an intermediate VM to access them from another VM in the same network
 - If the security incident is not controlled, transfer the infected resource in a sandboxed environment

- Disable or limit access to Google Cloud Storage resources for all users
- Use Google Cloud data security tools to mitigate enterprise data loss and leakage
- Use `gcloud compute ssh` instead of plain SSH client to connect to Linux VMs

6.3 Stakeholders Involved/ Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Develop an eradication plan ○ Perform technical and business analyses and create a prioritized eradication plan ○ Establish a communication strategy based on the eradication plan	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Internal/External Communications Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Eradication activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

6.4 Additional Information (if any)

Note: Refer to the following document to fill the necessary details:

- r. Eradication of Cloud Security Checklist.docx
- s. Incident Eradication Template.docx
- t. Incident Eradication Checklist.docx

7. Recovery

7.1 Objectives

The main objective of this phase is to recover the affected systems, network, and other resources from the incident impact and maintain business continuity.

7.2 Recovery Steps/Activities

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Activities to recover from GCP-based brute-force attack on SSH:
 - Use Deployment Manager to reconfigure instances
 - Implement strong SSH key pairs after recovering from an SSH brute-force attack
 - Use the recent data backup in Google Cloud, used by the database server, to recover files
 - Test the recovered application or service with different user scenarios in a recovered environment
 - Take necessary snapshots to recreate disks in the event of zonal failure
 - Set up HTTP health checks to validate the functioning of GCP services
 - Implement MFA for all users under a tenant
 - Revoke refresh tokens or keys instantly after changing the credentials
 - If administrative rights have been removed by the attacker, remove trust relationships from the current servers
 - Limit administrative access by enforcing conditional access and privileged identity management
 - Restore the affected business-critical systems to normal parameters
 - Restore systems based on business impact analysis
 - File a complaint with the cybercrime department
 - Perform complete vulnerability analysis and patch the identified vulnerabilities
 - Restart any suspended services

7.3 Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Recovery activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

7.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- u. Recovery of Cloud Security Incidents Checklist.docx
- v. Incident Recovery Procedure Template.docx
- w. Incident Recovery Checklist.docx

8. Post-incident Activities

8.1 Objectives

The main objective of this phase is to create necessary reports such as incident documentation, lessons learned, and incident impact assessment. Another objective of this phase is to close GCP-based SSH brute-force investigation and disclose it to respective stakeholders.

8.2 Activities Involved

- Create a report describing the implementation of the incident response process (along with attacker vectors and their mitigation steps)
- Create an after-action report (AAR) that includes information such as what worked effectively, areas of improvement, and strategies for enhancing the response in case of similar unauthorized access incidents
- Review the document along with the concerned teams and subject matter experts
- Conduct meetings discussing the lessons learned to document the details of the GCP-based SSH brute-forcing incident. Ensure that the following questions are answered in these meetings:
 - When and how was the incident detected?
 - What happened exactly?
 - What were the motives behind brute-forcing the SSH?
 - Who was contacted first about the incident?
 - Did the team face any additional challenges during the response process?
 - Was the organization adequately prepared for the incident?
 - How was the incident contained?
 - How were the impacted resources?
 - What procedures were followed during recovery?
 - Were the documented procedures followed by the response team?
 - How well did the incident response team and management perform in resolving the incident?

- Is the incident response team capable enough to mitigate similar incidents in future?
- Were there any gaps in communicating the incident?
- Was the right amount of information shared with the right personnel?
- What tools and resources are required to detect, analyze, and prevent such incidents in future?
- Which tools were effective during the response process?
- Update the existing response process document with the newly identified threats and their response activities
- Create an incident impact assessment report to determine all types of losses due to the GCP-based SSH brute-forcing incident; this report must address the following, if required:
 - Any data loss incurred owing to the GCP-based SSH brute-forcing incident
 - Legal costs for investigating the case, lawyer's fees, etc.
 - Costs pertaining to analyzing the GCP-based SSH brute-forcing incident, recovering from it, and installing resources
 - Costs related to the damage of goodwill as well as loss of customer trust and reputation
- Close the GCP-based SSH brute-forcing incident investigation officially by informing the management and securely retain investigation reports considering the retention policy of the organization
- Disclose incident details to the respective stakeholders by consulting with the legal department of the organization

8.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Conduct lessons learned meeting	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create incident documentation	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create incident impact assessment report	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Close the investigation officially	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Senior Management	Email, Phone, Text Message
Disclose incident details to the respective stakeholders	Information Security Manager	Email, Phone, Text Message
	Manager - Information Governance	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	CISO	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Human Resource	Email, Phone, Text Message
	Media	Email, Phone, Text Message
	Vendors	Email, Phone, Text Message
	Customers & General Public	Email, Phone, Text Message
	Business Partners	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

8.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- x. Incident Documentation Template.docx
- y. Incident Impact Assessment Report Template.docx
- z. Incident Closure Letter.docx
- aa. Incident Disclosure Form.docx