Cat & Box Scenario

Playbook for Brute Force Attacks

Prepared by: Prinson D'silva
Date: January 13th, 2025
Revised: January 18th, 2025

Table of Contents

Executive Summary

This report is created for Box Manufacturing which specializes in producing cardboard boxes for cats and relies heavily on secure systems to protect sensitive business data. In order to protect their network against cyber threats such as Brute Force Attacks, a playbook has been developed in collaboration with Cat who is the consultant from their Managed Security Service Provider (MSSP) overseeing the security of their network systems.

According to Google Cloud, a brute force attack involves an attacker repeatedly attempting to log into a system using legitimate usernames and a list of potential passwords, often obtained through reverse engineering or the dark web.

The purpose of this report is to highlight the incident response workflow in the event of an attack and establish a clear incidence response protocol for Box Manufacturing to handle brute force attacks on their network while ensuring swift action is taken, preventing any compromise to the network and making sure that there is minimum impact to the business.

The Key Steps of Incident Response Process for this playbook was created as per the steps highlighted by CISA, are as follows:

1. Preparation
2. Detection & Analysis:
3. Containment
4. Eradication & Recovery
5. Post-Incident Activity
6. Coordination

There are a couple of key trigger items in the Incident Response Workflow which determine the next steps that need to be taken, including the escalation to key individuals involved in the process.

By outlining clear communication, escalation protocols, and detailed response actions, this report empowers Box to take immediate action and resolve any security incidents with minimal disruption to business operations. The close coordination between internal staff and the MSSP consultant (Cat) ensures that Box's systems are continuously monitored and protected against brute force attacks, allowing the company to focus on its core business of creating their well known cat boxes.

Scope of the project

This project follows an Incident response workflow which in our report is referred to as a 'Playbook."

A Playbook is a document that provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases, as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2 [CISA, 2021].

This playbook was developed by us as members of the security operations center (SOC) which according to IBM, is defined as a team of IT security professionals dedicated to monitoring an organization's entire IT infrastructure 24x7. [Scapicchio et al., 2024]
Our goal is to detect, analyze and respond to security incidents in real-time.

The scope of this playbook is to follow an incident response workflow in event of a brute force attack causing minimal business disruptions and which includes communication between internal and external staff, escalation protocols when required, and detailed response actions, with the help of a ticketing system.

Incident Response Team

The Incident Response Team includes members such as Internal staff of Box, the SOC, as well as the third party MSSP. They are listed depending on their Role and Tier (based on escalation).

There are also other members from the business which are not responsible for incident response procedures but are involved in the communication phase that are listed as well along with their shift details and criteria for escalation.

Internal Staff: Support

- Lucky - IT support specialist (lucky@box.cat Phone 269-5466)
- Dusty - Database specialist (dusty@box.cat Phone 462-8952)
- Ned - Network administrator (ned@box.cat Phone 877-4332)

SOC Team: Tier 1

- Prinson - SOC specialist (prinson@soc.cat)

External MSSP: Tier 2

- Cat - SOC Security Oversight (cat@soc.cat Phone 905-4616 or cell 902-4321)

Business Staff: Informed only when major impact and causing potential breach

- Misha - Shift/ Production Manager (mesha@box.cat Phone 902-9836)
    - Shift Coverage: 9AM to 5PM AST weekdays
- Minka - 2nd Production Manager (minka@box.cat Phone 562-7658)
    - Shift Coverage: 9AM to 5PM AST weekdays
- Percy F - CEO (percy@box.cat)
    - Informed only when escalated or urgent, or unresolved after 48 hours.

Incident Response Workflow (Playbook)

This playbook is designed to provide a systematic approach to handle brute force attacks on the Box Manufacturing network, ensuring proper notification and escalation procedures while addressing all security concerns. This playbook will guide the team in preparation, detection, containment, eradication, recovery, and post-incident activities.

1. Preparation

The goal in this step is to ensure that Box Manufacturing is fully prepared to handle a brute force attack by equipping the team with all necessary tools and protocols.

The following actions would be implemented based in this step:

- **Ensure proper logging and monitoring**:
    - Make sure that all systems (network devices, servers, workstations) have logging enabled - Lucky & Ned
    - Verify that logs are being sent to a central log on the server - Ned & Prinson
    - Ensure that the SOC is monitoring login attempts in real-time

- **Ensure that strong authentication mechanisms are in place**:
    - Multi-factor authentication (MFA) should be implemented on all critical systems
    - Password policies should be enforced (e.g., minimum length, complexity, expiration).
    - Implement account lockout mechanisms after a specified number of failed login attempts. i.e. 5+ failed login attempts within a 10-minute window which we consider suspected behaviour.

- **Staff Incident Response training**:
    - Making sure the ticketing system is working correctly and all necessary staff have access to it i.e. Lucky, Ned, Dusty.
    - Conduct briefings with all staff members and ensure they understand the importance of responding to network related anomalies.
    - Conduct exercises with internal support staff to simulate brute force attacks and evaluate their responses.

2. Detection & Analysis:

An attacker would conduct a Brute Force attack in order to gain access to an account or a set of accounts when passwords are unknown where the attacker may systematically guess the password using a repetitive or iterative mechanism. Based on MITRE's ATT&CK framework, the attack can be detected in the following ways:

- **Application log** - Monitor authentication logs for system and application login failures of Valid Accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.
- **Command** - Monitor executed commands and arguments that may use brute force techniques to gain access to accounts when passwords are unknown.
- **User Account** - Monitor for many failed authentication attempts across

various accounts that may result from password spraying attempts.

Once the mode of attack is detected and identified, a ticket would be created for this issue. This ticket would include all details based on the initial investigations. The next step would be to analyze the attack. For this, the Target IP and OS information needs to be acquired followed by the question:

- Is the source IP internal or external?
    - If internal: Tier 1 would search for any previous alerts raised on the entity (source IP). The machine could already be compromised. Considering it is compromised;
        - Scan the machine. If the scans are pointing to a malware alert, escalate the case to Tier 2.
        - Tier 2: Block the traffic from the source IP, disinfect the machine, verify the source of the malware and unblock the machine once no threats are found. The ticket can then be closed by Tier 2.
    - If external: Tier 1 would search the IP using IP reputation sites and act accordingly (continue the next steps of this playbook to gather information for Tier 2).
- Determine which data source was used to trigger the alert. Is the alert based on network logs or actual on-host login information?
    - Network based logs: Here we assume that the product triggering the alert cannot be sure about the traffic it monitors, as it might be encrypted. In this case, we only try to find out indicators of failure.
        - Find out which ports were used for the brute force.
        - Search the IP using IP reputation sites and act accordingly (continue the next steps of this playbook to gather information for Tier 2)
        - If the attack port does not match any listening service or any previously running service, mark the case as a 'false positive' as there is no chance of success without a service listening on the port.
          Even then, Escalate the source IP's information to Tier 2 for further hunting, as this is still considered an indication of a malicious presence trying its 'luck' around the network, and they would be equipped with better tools to continue the investigation.
    - Host-based logs (or logs from the last step of the previous section)
        - Search the logs for events indicating a 'failure to login' or 'user does not exist' (depends on the attacked service). If such logs exist, measure the time span during which they occurred. If the time span is very short, for example: a few seconds between attempts, escalate the case to Tier 2, an indication of a malicious presence trying its 'luck' around the network.
        - Search the logs for a successful login log entry. If such entry is found, escalate the case to Tier 2 for further investigation.

Communication:

- In the event of a lockout where the attacker was able to cause a denial of service (DoS) by locking out one or more essential accounts, send an email notification to Misha or Minka based on their availability.
- In case the investigation is escalated and/ or unresolved after 48 hours, send an email notification to Percy as well.

3. Containment:

The next step is containment where the attack is then contained to prevent further compromise and protect critical assets using the following actions:

- Find out all users that were used in the brute force attack. Look for any suspicious username from this list and search for other hosts that these usernames were used on. (Tier 1)
- Notify the owners of the legitimate accounts and the owners of the targeted machines that a brute force attempt was made on their assets. (Tier 1)
- Perform a more thorough investigation on the possibly affected hosts and act accordingly. (Tier 1)
    - If suspect of an Internal threat, disable the targeted account(s) temporarily.
    - If a suspected victim, revoke or reset any compromised user credentials immediately.
- If the attacker is an external IP, block it and ensure that the firewall is configured to prevent remote login attempts for the specific port in the case it was unnecessarily open to the public. (Tier 1)
- If the attacker is an internal IP, search for any malware infections and past malware alerts on the source host to see if the host is vulnerable. (Tier 1)

Communication:

- Notify Misha (if during her shift) or Minka (if after-hours/weekend) about the detected attack and the actions being taken.
- Cat (Tier 2) should be contacted to confirm the containment actions and provide additional recommendations or oversight.

Tier 2 Escalation:

- Cat will review the containment actions and suggest next steps for further analysis when escalated based on the following rationale: -
    - **Attack Severity:** Does the brute force attack appear to target critical systems?
        - If so, the attack will be escalated to Cat for immediate oversight and involvement.
    - **Attack Duration:** Does the attack continue for more than 24 hours or shows signs of evolving such as new IP ranges, new attack vectors (i.e. way for attacker to enter a network or system. examples: vulnerability exploits, insider threat, open ports)?
        - If so, additional resources will be involved.
    - **Business Impact:** Is the attack still causing a noticeable disruption in business operations?
        - If yes, it will be escalated to both Cat as well as Percy for higher-level intervention.

4. Eradication & Recovery:

The next step is to eradicate the attacker's presence in order to restore systems to normal functionality. Most tickets are usually closed in this step and the findings along with their resolutions are listed on the report.

Eradication:

- Ensure that all passwords have been reset and that no unauthorized access remains.
- Review and eliminate any malicious files, backdoors, or other tools that may have been left by the attacker.
- Verify that MFA is working and enforced on all critical systems.

Recovery:

- Once systems are cleaned, ensure that accounts are re-enabled with strong credentials and MFA.
- Test all affected systems and services to ensure that they are operational and secure.
- Monitor the systems for any signs of repeated brute force attempts.

5. Post-Incident Activity:

The goal of this step is to analyze the incident to prevent future attacks and improve the response process where the following actions would be implemented:

- Root Cause Analysis:
    - Conduct a detailed review of how the brute force attack bypassed security measures, if applicable.
    - Determine whether additional security measures need to be implemented, such as IP blacklisting, CAPTCHA to prevent automated attacks, or enhanced monitoring for future attack attempts. [Esheridan, 2025]

- Reporting:
    - Cat will provide a report summarizing the incident, impact, response, and recommendations for future improvements.
    - Share the incident report with Percy and Misha (if applicable), but only escalate to Percy if the incident remains unresolved after 48 hours.

- Preventative Measures:
    - Review and possibly update password policies, MFA implementation, and account lockout thresholds.
    - Educate employees about strong password practices and the risks of brute force attack.
    - For advanced users who want to protect their accounts from attack, give them the option to allow login only from certain IP addresses.
    - Assign unique login URLs to blocks of users so that not all users can access the site from the same URL. [Esheridan, 2025]

6. Coordination:

The final step where the goal is to ensure clear communication and coordination across all parties involved in response to the attack.

It is important to maintain regular status updates with the SOC and key internal personnel and this can be done by using secure channels (e.g., encrypted email) to share sensitive information.

Internal Coordination:

- Coordinate with key internal stakeholders, including IT support (Lucky), network administration (Ned), and the database specialist (Dusty), to ensure containment and recovery actions are aligned.
- Regular updates as highlighted in the previous steps to the management team (Percy and Misha/Minka) on the status of the attack and recovery.

External Coordination:

- Work closely with the third-party MSSP (Cat) to analyze and mitigate the attack.
- If the attack escalates or external assistance is needed, involve additional external resources (e.g., cybersecurity firms, law enforcement).

As mentioned in Step 2, an email notification will be sent on Detection of the attack to both the Client and Third Party Provider depending on the duration and impact of the attack.
Following are the examples of email notifications being sent:

- Internal: -

Subject: Potential Brute Force Attack Detected - Immediate Response Underway

Dear Percy & Misha/ Minka,

This is to inform you that our security systems have detected a series of failed login attempts, which we believe may indicate an attempted brute force attack on our systems. We have already taken steps to block the attack and prevent any unauthorized access.

We are working closely with our managed security service provider (Cat) to ensure that the situation is handled swiftly and effectively. You will be notified of any critical updates or changes to the situation. If the issue persists or worsens, we will escalate the matter as necessary.

Best regards,

Box Manufacturing Security Team

- External: -

Subject: Brute Force Attack Detected - Immediate Action Required

Dear Cat,

We have detected a potential brute force attack against our systems, originating from an IP address attempting to gain unauthorized access to several accounts. The incident is currently being analyzed, and we have taken initial containment actions by blocking the offending IP address.

Please review the logs and confirm the containment measures, and provide any additional recommendations to ensure that the attack does not escalate. We will continue to monitor the situation and provide you with updates as needed.

Thank you for your prompt attention to this matter.

Best regards,

Box Manufacturing Security Team

Conclusion & Recommendations

As the goal of this project was to highlight the incident response workflow in the event of an attack and establish a clear incidence response protocol for Box Manufacturing to handle brute force attacks on their network we can safely say that this playbook serves as a comprehensive guide to handling brute force attacks, with the flexibility to adapt to evolving threats while maintaining communication across all parties involved.

Of course, the field of cybersecurity is ever evolving but so are the attackers and all possible attack vectors that come with. Below are some recommendations as seen in the MITRE ATT&CK framework for mitigation of brute force by further enforcing Account use policies:

- Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out.
- Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.
- Consider blocking risky authentication requests, such as those originating from anonymizing services/proxies.

Since use of strong passwords are considered the best weapon against brute force attacks, here are a few ways by which users can strengthen passwords against brute force attacks [Kaspersky, 2025]:

- Longer passwords with varied character types - including more characters makes your password even harder to solve.
- Elaborate passphrases - passwords composed of multiple words or segments and should be sprinkled with extra characters and special character types.
- Create rules for building your passwords - consider using truncated words to create a string that is personalized and makes sense only to you (example: like replacing “good” with “gd”)
- Stay away from frequently used passwords - avoid using common passwords and change them frequently.
- Use unique passwords for every site you use - this way, you can keep other accounts from getting compromised in case one is breached.
- Use a password manager - these create and store extremely long and complex passwords for all the sites, although you have to remember the one primary password for access to these.

References

- Cybersecurity and Infrastructure Security Agency (2021, November) - *Cybersecurity Incident & Vulnerability Response Playbooks*. Retrieved from https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
- National Institute of Standards and Technology (2012) - *Computer security incident handling guide* : NIST Special Publication 800-61 Revision 2. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Google Cloud (2022) - *Top Security Playbooks*: White Paper Third Edition. Retrieved from https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C4/Top_Security_Playbooks_2022.pdf
- Scapicchio, M., Downie, A., & Finio, M. (2024, March 15). *What is a Security Operations Center (SOC)?*. IBM. Retrieved from https://www.ibm.com/think/topics/security-operations-center
- Alfredo Oliveira et. al (2017, May 31) - Techniques > Enterprise > *Brute Force.* MITRE ATT&CK. Retrieved from https://attack.mitre.org/techniques/T1110/
- Esheridan (Retrieved 2024, January) - *Blocking Brute Force Attacks.* OWASP. Retrieved from https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
- Kaspersky - *Brute Force Attack: Definition and Examples.* Retrieved from https://www.kaspersky.com/resource-center/definitions/brute-force-attack