INTERN CAREER
"WE SPEAK DATA"

TASK2

INCIDENT RESPONSE SIMULATION

Naoufal
GUENDOUZ

22 JUN 2024

Introduction

In today's rapidly evolving digital landscape, cybersecurity incidents have become increasingly sophisticated and frequent, posing significant threats to organizations across all sectors. Effective incident response is critical for mitigating the impact of these threats and ensuring the resilience of business operations. This report presents a detailed simulation of a cybersecurity incident, specifically a brute force attack.

This report is structured into five key sections: Scenario Creation, Incident Detection, Response Plan Execution, Forensic Analysis, and Post-Incident Assessment. Each section provides a step-by-step account of the incident simulation, from the initial detection of suspicious activities to the forensic analysis that uncovers the root cause and the final assessment of our response efforts. By meticulously documenting each phase, we not only enhance our preparedness for real-world cybersecurity threats but also identify areas for improvement and derive valuable lessons that will inform our future security strategies.

The simulated scenario involves a large car dealer company, "BMV" which experiences a surge in unusual login attempts across multiple staff accounts. Staff report being locked out of their accounts, and some have unauthorized transactions, raising suspicions of a coordinated brute force attack targeting the company's authentication systems. Through this scenario, we aim to train interns in detecting and responding to such attacks, improve our incident response procedures, and strengthen our overall cybersecurity posture.

Scenario creation

Context

A prominent car retailing company, "CMW inc" experiences unusual login attempts on employee accounts. Several employees report being locked out of their systems, and some accounts show signs of unauthorized access. The security team suspects a brute force attack targeting the company's internal authentication systems, potentially compromising sensitive operational data.

Objectives

The primary objective of this cybersecurity incident simulation is to train interns in detecting and responding to brute force attacks on employee accounts within a car retailing company, "CMW Inc." The exercise aims to enhance the interns' understanding of internal authentication security and monitoring. Additionally, it seeks to improve the company's incident response and forensic analysis capabilities, ensuring that the organization is better prepared to handle similar threats in the future.

Scope

The scope of the simulation encompasses several key phases: detection of unusual login attempts, containment of the attack, mitigation of its impact, and a thorough forensic analysis to uncover the root cause. The simulation will involve monitoring tools and logs to simulate the attack, assigning predefined roles to interns to execute the incident response plan, and conducting a post-incident assessment to identify gaps in the response and areas for improvement. Through this scenario, we aim to strengthen our incident response plan, implement stronger security measures, and ensure the resilience of our operational data against brute force attacks.

Incident detection

Roles

- **Incident Response Coordinator Intern**: Coordinates the response efforts and communicates with stakeholders.
- **Forensic Analyst Intern**: Analyzes logs and affected systems to determine the root cause.
- **Network Security Intern**: Monitors network traffic and identifies suspicious activities.
- **System Administrator Intern**: Manages the containment and recovery of affected systems.
- **Communications Officer**: Manages internal communication regarding the incident.

Incident Detection Simulation

The detection of the brute force attack starts with the Network Security Specialist, who monitors network traffic using security tools. During routine checks, the specialist notices an unusual increase in failed login attempts from various IP addresses targeting employee accounts. Recognizing the potential threat, the specialist immediately alerts the Incident Response Lead about the suspicious activity.

Upon receiving the alert, the Incident Response Lead confirms the potential threat and quickly contacts the Forensic Analyst and the System Administrator. The lead briefs them on the suspected brute force attack and the initial findings. At the same time, the Incident Response Lead informs the Communications Officer to prepare an internal communication plan to address the issue. The Communications Officer begins drafting a message to notify employees about the potential security threat and advises them on immediate precautions, such as avoiding login attempts.

The Forensic Analyst then conducts a detailed analysis of authentication logs to identify patterns in the failed login attempts, correlating them with specific IP addresses and timestamps. Meanwhile, the Network Security Specialist continues to monitor network traffic, identifying and tracking ongoing suspicious activities. This helps the specialist pinpoint specific IP addresses involved in the brute force attempts, providing essential data for containment.

In response, the System Administrator temporarily disables the affected employee accounts to prevent further unauthorized access. The administrator works closely with the Network Security Specialist to block the identified suspicious IP addresses, effectively isolating the threat. The Incident Response Lead ensures smooth coordination between the administrator and the specialist, keeping the Forensic Analyst informed about the containment measures for accurate analysis.

Response Plan Execution

Incident response plan

Incident Response Lead :

Upon receiving the alert from the Network Security Specialist, the Incident Response Lead confirms the incident. The lead immediately notifies the incident response team, which includes the Forensic Analyst Intern, Network Security Intern, System Administrator Intern, and Communications Officer. The lead formally initiates the incident response plan, outlining the initial steps and ensuring everyone understands their roles and responsibilities.

System Administrator:

The System Administrator's first task is to temporarily disable the affected employee accounts to prevent any further unauthorized access. This action helps to contain the breach and protect the integrity of the system. The System Administrator communicates with the Incident Response Lead to confirm which accounts have been disabled and ensures that this information is documented in the incident log.

Communications Officer:

The Communications Officer creates a group on Signal to safely communicate between the employees in case the system is affected and the hackers get alerted, he also prepares a comprehensive communication plan to inform employees and relevant departments about the incident. This plan includes a draft message that explains the nature of the threat, the immediate actions being taken.

Containment and Mitigation

Network Security Intern:

The Network Security Intern focuses on identifying and blocking the suspicious IP addresses involved in the brute force attempts. Using network monitoring tools, the specialist pinpoints the sources of the malicious traffic and implements IP blocks to prevent further intrusion attempts. The specialist maintains real-time monitoring to ensure no additional suspicious activities are occurring and reports back to the Incident Response Lead with updates.

System Administrator Intern:

Beyond disabling affected accounts, the System Administrator Intern enforces stricter account lockout policies and password complexity requirements across the organization. This includes setting policies that lock accounts after a certain number of failed login attempts and requiring all employees to update their passwords to meet higher complexity standards. These measures aim to mitigate the risk of future brute force attacks and enhance overall account security.

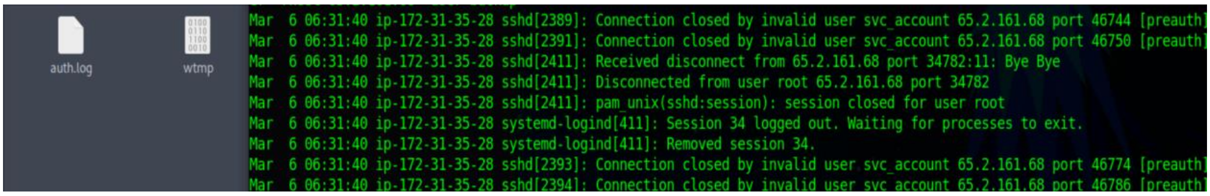
Forensic Analyst Intern:

The Forensic Analyst Intern begins a thorough forensic analysis of the authentication logs and other relevant data to trace the origin of the attack. The analyst examines patterns in the failed login attempts, correlates data with specific IP addresses, and identifies any compromised accounts. This analysis includes checking for any signs of data exfiltration or further system compromise. The Forensic Analyst prepares a detailed report on the findings and shares it with the Incident Response Coordinator Intern for review and further action.

Forensic Analysis

Log Analysis and Findings

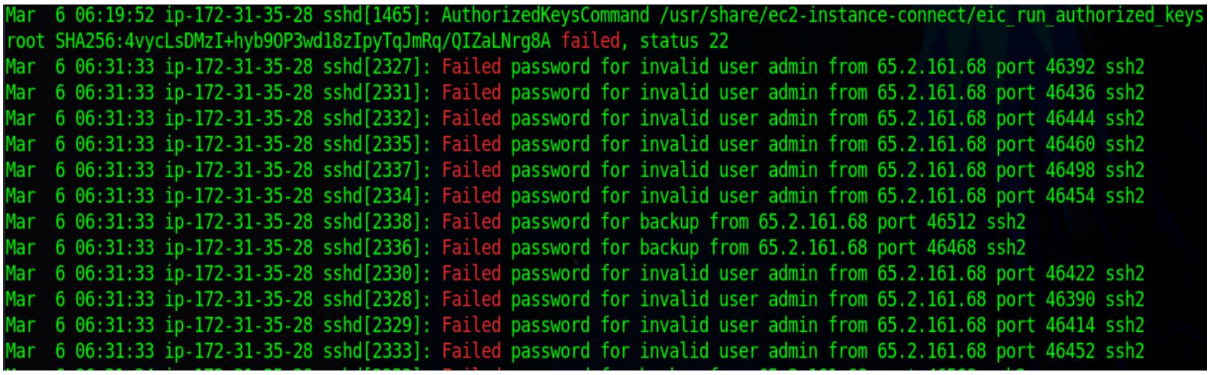
As part of our incident response process, the logs from the brute force attack were provided to the Forensic Analyst for detailed examination. The analysis of these logs has yielded critical insights into the nature and scope of the attack. Below is a summary of the key findings from the forensic analysis:



```
Mar  6 06:31:40 ip-172-31-35-28 sshd[2389]: Connection closed by invalid user svc_account 65.2.161.68 port 46744 [preauth]
Mar  6 06:31:40 ip-172-31-35-28 sshd[2391]: Connection closed by invalid user svc_account 65.2.161.68 port 46750 [preauth]
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Received disconnect from 65.2.161.68 port 34782:11: Bye Bye
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Disconnected from user root 65.2.161.68 port 34782
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session closed for user root
Mar  6 06:31:40 ip-172-31-35-28 systemd-logind[411]: Session 34 logged out. Waiting for processes to exit.
Mar  6 06:31:40 ip-172-31-35-28 systemd-logind[411]: Removed session 34.
Mar  6 06:31:40 ip-172-31-35-28 sshd[2393]: Connection closed by invalid user svc_account 65.2.161.68 port 46774 [preauth]
Mar  6 06:31:40 ip-172-31-35-28 sshd[2394]: Connection closed by invalid user svc_account 65.2.161.68 port 46786 [preauth]
```

Identification of Attack Patterns:

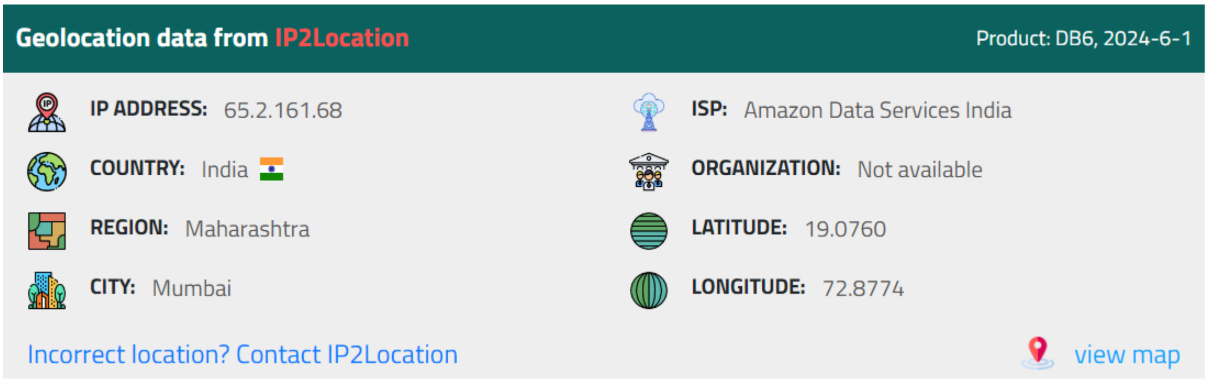
The logs revealed a significant number of failed login attempts originating from a specific IP address. These attempts were concentrated over a short period, indicating a coordinated brute force attack aimed at compromising employee accounts. The attack patterns included repetitive login requests with various username and password combinations, suggesting the use of automated tools by the attackers.



```
Mar  6 06:19:52 ip-172-31-35-28 sshd[1465]: AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys
root SHA256:4vycLsDMzI+hyb9OP3wd18zIpyTqJmRq/QIZaLNrg8A failed, status 22
Mar  6 06:31:33 ip-172-31-35-28 sshd[2327]: Failed password for invalid user admin from 65.2.161.68 port 46392 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2331]: Failed password for invalid user admin from 65.2.161.68 port 46436 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2332]: Failed password for invalid user admin from 65.2.161.68 port 46444 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2335]: Failed password for invalid user admin from 65.2.161.68 port 46460 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2337]: Failed password for invalid user admin from 65.2.161.68 port 46498 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2334]: Failed password for invalid user admin from 65.2.161.68 port 46454 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2338]: Failed password for backup from 65.2.161.68 port 46512 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2336]: Failed password for backup from 65.2.161.68 port 46468 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2330]: Failed password for invalid user admin from 65.2.161.68 port 46422 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2328]: Failed password for invalid user admin from 65.2.161.68 port 46390 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2329]: Failed password for invalid user admin from 65.2.161.68 port 46414 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2333]: Failed password for invalid user admin from 65.2.161.68 port 46452 ssh2
```

Source of the Attack:

Through IP address correlation, we identified suspicious IP addresses "65.2.161.68" as the primary sources of the attack. This IP address was traced back to India . Further investigation revealed that some of these IP addresses are associated with known malicious activities in security threat databases.



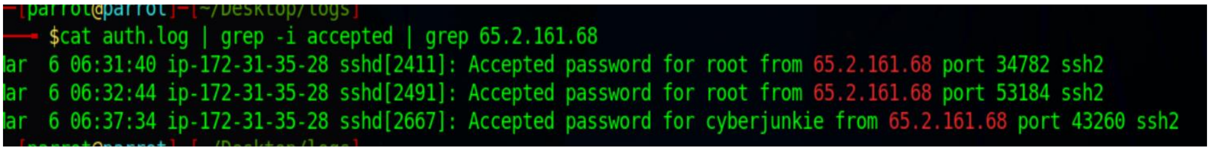
Geolocation data from IP2Location Product: DB6, 2024-6-1

IP ADDRESS: 65.2.161.68
ISP: Amazon Data Services India
COUNTRY: India
ORGANIZATION: Not available
REGION: Maharashtra
LATITUDE: 19.0760
CITY: Mumbai
LONGITUDE: 72.8774

Incorrect location? Contact IP2Location

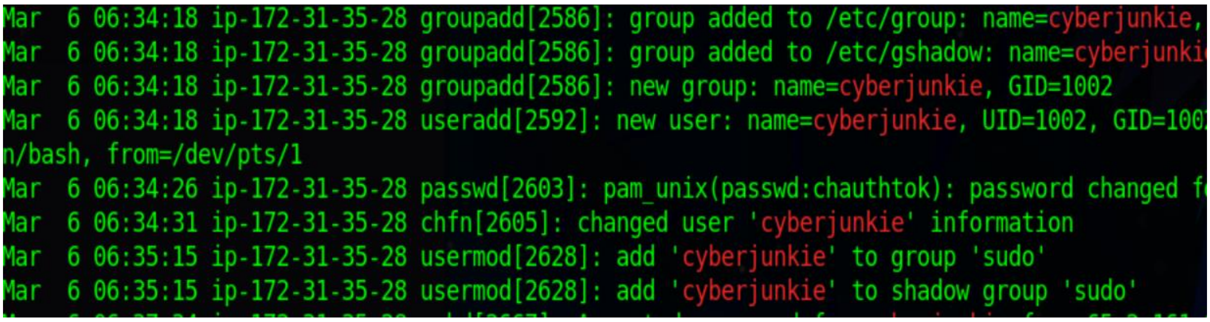
Compromised Accounts:

The forensic analysis identified a subset of accounts that experienced an unusually high number of failed login attempts (admin,backup,root). Among these, a few accounts showed successful logins following multiple failed attempts, suggesting that the attackers may have successfully guessed the credentials for these accounts.



```
─[parrot@parrot]─[~/Desktop/logs]
└──╼ $cat auth.log | grep -i accepted | grep 65.2.161.68
lar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Accepted password for root from 65.2.161.68 port 34782 ssh2
lar  6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
lar  6 06:37:34 ip-172-31-35-28 sshd[2667]: Accepted password for cyberjunkie from 65.2.161.68 port 43260 ssh2
```

The attackers also add a new user to the system to stay in the network

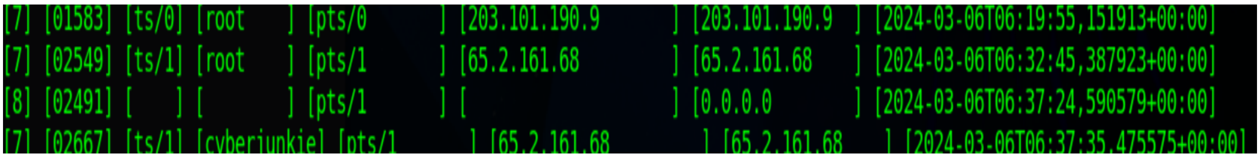


```
Mar  6 06:34:18 ip-172-31-35-28 groupadd[2586]: group added to /etc/group: name=cyberjunkie,
Mar  6 06:34:18 ip-172-31-35-28 groupadd[2586]: group added to /etc/gshadow: name=cyberjunki
Mar  6 06:34:18 ip-172-31-35-28 groupadd[2586]: new group: name=cyberjunkie, GID=1002
Mar  6 06:34:18 ip-172-31-35-28 useradd[2592]: new user: name=cyberjunkie, UID=1002, GID=100
n/bash, from=/dev/pts/1
Mar  6 06:34:26 ip-172-31-35-28 passwd[2603]: pam_unix(passwd:chauthtok): password changed f
Mar  6 06:34:31 ip-172-31-35-28 chfn[2605]: changed user 'cyberjunkie' information
Mar  6 06:35:15 ip-172-31-35-28 usermod[2628]: add 'cyberjunkie' to group 'sudo'
Mar  6 06:35:15 ip-172-31-35-28 usermod[2628]: add 'cyberjunkie' to shadow group 'sudo'
```

These accounts were immediately flagged for further investigation and remediation.

Attack Timeline:

The logs provided a detailed timeline of the attack, starting from the initial spike in failed login attempts to the eventual containment measures. This timeline helped us understand the progression of the attack and the effectiveness of our response actions. It was noted that the attack intensity peaked during non-business hours, possibly to evade detection.



```
[7] [01583] [ts/0] [root    ] [pts/0       ] [203.101.190.9        ] [203.101.190.9  ] [2024-03-06T06:19:55,151913+00:00]
[7] [02549] [ts/1] [root    ] [pts/1       ] [65.2.161.68          ] [65.2.161.68    ] [2024-03-06T06:32:45,387923+00:00]
[8] [02491] [    ] [        ] [pts/1       ] [                     ] [0.0.0.0        ] [2024-03-06T06:37:24,590579+00:00]
[7] [02667] [ts/1] [cyberjunkie] [pts/1       ] [65.2.161.68          ] [65.2.161.68    ] [2024-03-06T06:37:35,475575+00:00]
```

Post-Incident Assessment

Review Effectiveness

After the incident was contained, the Incident Response Coordinator Intern conducted a comprehensive debriefing session with the incident response team. During this session, the team reviewed all the actions taken to address the brute force attack, evaluating their effectiveness in mitigating the threat and restoring security. The Incident Response Lead also assessed the communication strategy implemented during the incident, particularly its impact on employees and other stakeholders. This evaluation helped determine whether the communication was clear, timely, and effective in informing and guiding employees through the incident.

Identify Areas for Improvement

The debriefing session highlighted several areas where the incident response plan could be improved. One significant gap identified was the need for enhanced monitoring and alerting mechanisms specifically designed to detect brute force attacks on internal accounts. The Incident Response Lead emphasized the importance of implementing multi-factor authentication for all employee accounts to add an extra layer of security against unauthorized access. Additionally, the review underscored the necessity of improving employee awareness regarding strong passwords and general security best practices. These improvements are essential to reduce the likelihood of similar incidents in the future and to better prepare the organization for swift and effective responses.

Lessons Learned

The incident response team documented the lessons learned from the incident, ensuring that the response plan was updated with these insights. The team recommended additional training and resources to strengthen the company's cybersecurity posture. This included regular security audits and penetration testing to proactively identify and address vulnerabilities. By incorporating these lessons and recommendations, the organization can enhance its preparedness and resilience against future cyber threats.

Conclusion

The response to the brute force attack on employee accounts at "VMW inc." demonstrated the importance of a well-coordinated incident response plan. Through effective teamwork and thorough analysis, the incident was contained, and valuable lessons were learned. The post-incident assessment revealed critical areas for improvement, including the need for enhanced monitoring, multi-factor authentication, and improved employee awareness. By addressing these gaps and implementing the recommended measures, "VMW inc." will significantly strengthen its cybersecurity defenses and be better equipped to handle future threats. The ongoing commitment to training and proactive security measures will ensure that the organization remains vigilant and prepared in an increasingly complex digital landscape.