CIS425 Final Project

James Driscoll

Professor Johnson

ECPI University

March 2022

**Scenario 1 Analysis**

You are a member of Acme Software Information Security Team. Over the last month, users have been reporting that they are being randomly locked out of their accounts. Devin Miles, the IT Administrator in charge of Active Directory cannot see any errors in the system logs or any signs of improperly functioning Domain Controllers. He asks for your assistance as he suspects that there may be something else more serious causing the frequent lock outs. He has provided you log files from Office365 to see if you help determine what is going on.

**Recommendations**

There are three recommendations that should be implemented immediately. First recommendation I would make is to adjust the password policy. Right now, it is a minimum of 7 characters using three of the four following characteristics (lowercase, uppercase, number, and special character). They are also set to expire every 180 days and can be reused. The adjustment I would suggest is to increase the length of passwords to a minimum of 12 characters, require all four of the characteristics, reduce the time to expire to 90 days, and prohibit reuse of passwords for 10 resets (Password Policy Best Practices for Strong Security in AD, n.d.).

Second recommendation I would make is to the Multifactor Authentication (MFA) policy. Enrolling employees to use MFA needs to be sped up. Right now, only 60% of employees are using it. The last 40% need to be enrolled by months end. Also, the company needs to ensure that they are not using SMS messaging for their one-time passcodes but using an authenticator such as Google or Microsoft. The reason for that is because SMS is the least secure as it is subject to being intercepted through a technique called sim jacking. This is where a threat actor notifies a phone company pretending to be their victim and has them transfer the information from the victims’ phone to the threat actors (What is SIM Jacking and How to Avoid it, 2020).

The third recommendation I would make is to set a finite number of login attempts. As seen in the log there some accounts that access was attempted multiple times from the same address. We can set the maximum number of logins attempted from any single IP address. Once that number is reached that IP address is banned. The key here is going to be to ban them for the maximum time allowed (Descalso, 2022).

**Incident Report**

During the past month, Acme Software has seen an increase in the number of cyber-attacks that involved an unknown threat actor or actors attempting to gain access to the network via brute forcing employee passwords. While these attacks have had minimal impact to both critical and non-critical services, several employees have had their accounts locked out resulting in requiring their passwords to be reset. Fortunately, the unknown threat actor or actors have not been successful in their attempts to gain access to the company’s network.

**Incident Information**

Things started when Devin Miles, the IT Administrator in charge of Active Directory notified the Software Information Security Team that he has been receiving complaints of random employees having their accounts locked out. He started investigating the complaints and did not see any issues in the logs and he says the Domain Controllers are operating as configured. Despite not seeing any issues with the network, Mr. Miles has a feeling that something sinister may be going on. I was tasked with conducting a deeper investigation into the situation and told Mr. Miles to forward all the logs so I can try to find out what the issue is.

**Action Plan**

Immediate remediation actions are to rest the passwords for the employee accounts that are locked out. Long term actions are to monitor and investigate unauthorized access attempts with the priority being those accounts that are mission critical and/or contain sensitive data.

**Conclusion/Recommendations**

To sum everything up. Acme Software has been the victim of a cyber-attack where the threat actor or actors tried to brute force their way onto the network. They were unsuccessful but in the process some employee accounts became locked out. A couple things that can be done immediately are to reset the passwords of the locked accounts and continue to monitor and investigate unauthorized access attempts.

There are three recommendations that need to be implemented moving forward. First, adjust the password policy. Increase the minimum number of characters from seven to 12. Also reduce the amount of time between resets from 180 days to 90. Then set a policy to where employees cannot reuse old passwords for at least 10 resets. Second, finish enrolling all employees to start using Multi-Factor Authentication (MFA). Third, set a limited number of logins attempts per IP address. Once that limit is reached, that IP address is blocked.

**References**

Descalso, A. (2022, January 11). *How to Prevent Brute Force Attacks in 8 Easy Steps*. Retrieved from Intelligent Technical Solutions: https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks

*Password Policy Best Practices for Strong Security in AD*. (n.d.). Retrieved from Netwrix: https://www.netwrix.com/password\_best\_practice.html

*What is SIM Jacking and How to Avoid it*. (2020, August 31). Retrieved from Kajeet: https://www.kajeet.net/iot-security-what-is-sim-jacking-and-how-to-avoid-it/

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Acme Software - Security Incident Report** | | | | |
| **Version 1.2 – Revised date – 12/8/2018**  **https://www.us-cert.gov/incident-notification-guidelines** | | | | |
| **Incident Detector’s Information** | | | | |
| **Date/Time of Report** | 19 March 2022 | | | |
| **First Name** | James | | | |
| **Last Name** | Driscoll | | | |
| **OPDIV (Operating Division)** | Information Systems/Information Security | | | |
| **Title/Position** | Acme Software Information Security Team | | | |
| **Work Email Address** | jdriscoll@acme.com | | | |
| **Contact Phone Numbers** | *777-777-7777* |  |  | *Other* |
| **Reported Incident Information** | | | | |
| **Reporting Person** | Devine Miles | | | |
| **Start Date/Time** | 19 March 2022 / 0433 | | | |
| **Incident Location** | IT office | | | |
| **Impact Description and Severity Levels**  **(Choose one severity level from each category)** | Functional Impact -Select all that apply   * No Impact * No Impact to Services * Minimal Impact to non-critical services * Minimal impact to critical services * Significant impact to non-critical services * Denial of non-critical services * Significant impact to critical services * Denial of critical services/Loss of control   Information Impact   * No Impact * Suspected but not identified * Privacy data breach * Proprietary information breach * Destruction of non-critical systems * Critical systems data breach * Core credential compromise * Destruction of critical systems   Recoverability   * Regular * Supplemented * Extended * Not recoverable | | | |
| **Priority Rating** | *Medium* | | | |
| **PII/PHI Compromise?** | *No* | | | |
| **Privacy Info?** | *No* | | | |
| **Attack Vector Taxonomy** | *Attrition – brute force to compromise, degrade or destroy* | | | |
| **Description of Incident** |  | | | |
| **Incident Attributes** | Location of observed activity   * Level 1 – Business DMZ * Level 2 – Business Network/non-core management systems * Level 3 – Business Network Management/Accounts/Trust stores * Level 4 – Critical System DMZ * Level 5 – Critical System Management * Level 6 – Critical Systems * Level 7 – Safety Systems * Unknown | | | |
| **Additional Support Action Requested** |  | | | |
| **Method Detected** | *Notification/IDS* | | | |
| **Number of Hosts Affected** | *1* | | | |
| **Information Sharing** | *Entities with which CMS and US-CERT can share incident data.* | | | |
| **System** | *Name of FISMA reported system (if known)* | | | |
| **Status** | *Ongoing.* | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Attacking Computer(s) Information** | | | | | |
| **IP Address / Range** | **Host Name** | | **Operating System** | **Ports Targeted** | **System Purpose** |
| **Unknown** | Unknown | | Unknown | Unknown | Unknown |
|  |  | |  |  |  |
| **Victims Computer(s) Information** | | | | | |
| **IP Address / Range** | **Host Name** | | **Operating System** | **Ports Targeted** | **System Purpose** |
| **Unknown** | Unknown | | Unknown | Unknown | Unknown |
|  |  | |  |  |  |
| **Action Plan** | | | | | |
| **Isolate affected system?** | | Remove affected systems from network - No | | | |
| **Backup affected system?** | | Verify previous backups for affected systems – **No** | | | |
| **Forensics performed** | | Name of persons performing forensics if required: | | | |
| **Vulnerability identification** | | Was the vulnerability identified, if so describe: No | | | |
| **Action Description** | | Reset passwords for the accounts that are locked out. Monitor and investigate unauthorized access attempts – with priority on those that are mission critical and/or contain sensitive data | | | |
| **Requestor** | |  | | | |
| **Assignee** | |  | | | |
| **Time Frame** | |  | | | |
| **Status** | |  | | | |
| **Conclusion / Summary** | | | | | |
| **Entities Notified** | | Director of Security | | | |
| **Resolution** | | *Passwords were reset for the accounts that were locked out.* | | | |
| **Lessons Learned** | | *What are we doing to mitigate future threats of this type? Going to configure system to limit the number of logins attempts from any single IP address. Configure IDS to alert when there are multiple attempts to login to a user’s account.* | | | |