Contents

SCENARIO

Hashed Passwords Files: Back-up tapes with /etc/passwords and /etc/shadows files from a 2015 Linux database server were stolen, potentially affecting customer and order databases. The current password protection mechanism used then is unknown.

Incident Type

Hashed Passwords Files

1. Introduction

Scope:

This playbook outlines response steps to the theft of hashed passwords files from the back-up tapes containing /etc/passwords and /etc/shadows files stolen from a 2015 Linux database server of Viva la Vita Online, an online store that sells vitamins and food supplements. Since this playbook provides an approach to identify, contain, eradicate, and recover for this incident, it can also be used for similar incidents involving theft of sensitive data like credential compromise, data breaches, etc.

Assumptions:

- The stolen backup tapes contain sensitive data related to customers.
- The current password protection mechanism used in 2015 is unknown.
- The organization's Security Incident Response team is familiar with high level understanding of such incidents assuming the organization has a basic existing Incident Response playbook.
- An automated ticket/case gets raised in case of an incident.
- The company has an escalation matrix hierarchy.

Audience:

This document has been created for computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information security officers (CISOs), chief information officers (CIOs), computer security program managers, and others who are responsible for preparing for, or responding to, security incidents like Legal Advisors, and Management.

2. Incident Response Team

Roles and Responsibilities:

- Incident Response Manager: The primary point of contact who will coordinate the overall incident response plan, manages the team, and ensures all SLAs are met in the assigned deadline.
- IT Security Analyst: Responsible for conducting in-depth analysis of the incident, including investigating the stolen backup tapes and identifying the scope of the breach.
- Network and Systems Engineer: Responsible for containing the incident, restoring systems, and implementing security measures to prevent such incidents in the future.
- Application and E-commerce Specialist: Analyzes the security implications of the incident and recommends appropriate mitigation strategies for the online store and other connected systems.
- Legal and Compliance Advisor: Provides guidance on legal and compliance requirements, and coordinates with regulatory authorities if necessary.
- Communications and Public Relations Coordinator: Responsible for handling external communications and managing the organization's public image to third party vendors, customers during and after the incident.
- Human Resources Representative: Assists with any actions related to personnels, such as help in disabling compromised accounts or managing employee communications and informing other employees through proper communication channels.

3. Preparation

Tools and Resources:

- Network Controls
- Perimeter Firewall on the network egress points (**Fortinet FortiGate 7.4**)
- Intrusion Prevention Sensors on the internal network (**Suricata 6.0.15**)
- Email Gateway with Anti-malware Anti-Spam Protection (**Symantec Mail Security for Microsoft® Exchange 7.10**)
- Security Information and Event Management (**IBM QRadar 7.5**)
- Host Controls
- Anti-malware Endpoint Protection on all devices (**Symantec Endpoint Protection Client for Windows 14.3**)
- Full Disk Encryption on employee laptops (**Bitlocker for Windows 10 and 11 versions**)
- Other Controls
- Vulnerability Patching Management (**Tenable Nessus 10.6**)
- Backup and restoration tools
- Forensic analysis tools (e.g., EnCase, AccessData FTK, Autopsy)

The above tools and resources should be regularly reviewed and updated to address evolving threats and technologies.

Communication Channels:

- Establish secure and multiple communication channels for the Incident Response Team, such as encrypted email, secure messaging platforms, and dedicated conference lines to exchange reports.
- Open a conference bridge war room for the incident.
- Ensure that communication channels can be quickly adapted to the specific needs of the incident as adaptability will be needed in the situation.
- Use of Microsoft Teams, Skype, Outlook for communication between employees working on company premises and remotely.

4. Identification

Incident Detection Methods:

- With the help of Symantec Endpoint Protection Client, the implementation of file integrity monitoring to detect changes to critical system and database files, including /etc/passwords and /etc/shadows.
- To prevent accidentally blacklisting company's own domains, create and maintain list of all the domains owned by Viva la Vita Online.
- Regular monitoring of servers, authorized access attempts, unusual login patterns, or anomalous database queries.
- Monitor Internet search engines and public forums to detect information leakage.
- Protection of the physical location of the database servers by implementing access control to concerned employees only to avoid physical thefts.

Incident Reporting Mechanism:

- Confirm an automated ticket/case has been raised for the incident. If not, manually raise one.
- Gather and analyze information gained through internal communications like dedicated email groups, hotlines, or the incident reporting portal for such incidents.
- Establish clear procedures and report information about the incident by following the escalation matrix.

Initial Assessment Procedure:

- Gather and analyze available information about the incident, including the date of the backup tape theft, the affected systems, and the potential impact on customer and order data.

- Determine the scope of the incident and the potential risk to the company and notify relevant stakeholders.
- Assess the immediate actions required to contain the incident and prevent further damage.
- Find traces in the local file system, check logs wherever necessary.

5. Containment

Short-term Containment Strategies:

- Isolate affected systems: Immediately disconnect the affected systems from the network to prevent the spread of the incident, using the network segmentation capabilities of the Fortinet FortiGate firewall. Also, isolate the computing system in order to perform a forensics analysis later.
- Disable compromised accounts: Disable all accounts associated with the stolen backup tapes, including any accounts that may have had access to the affected systems, in coordination with the HR and legal team.
- Implement temporary security measures: Implement temporary security controls, such as increased logging, network segmentation, and enhanced monitoring using the Suricata IPS and IBM QRadar SIEM, to mitigate the immediate risks.
- Monitor for further suspicious activity: Closely monitor the company's systems and networks for any additional signs of compromise or suspicious activity using the existing security tools and controls.

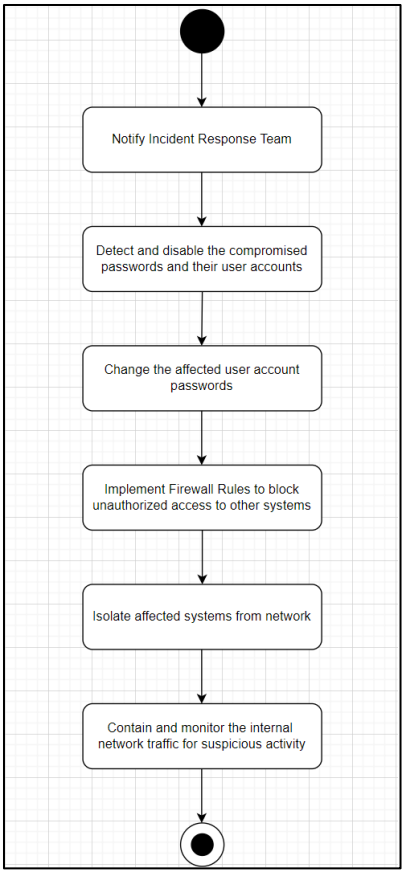

Figure : Short Term Containment Strategy

Long-term Containment Measures:

- Conduct a comprehensive risk assessment to identify and address any vulnerabilities that may have contributed to the incident, using the Tenable Nessus vulnerability management tool.
- Implement stronger password policies, such as password complexity requirements, regular password changes, and the use of multi-factor authentication, in coordination with the Application and E-commerce Specialist.
- Review and update backup and restoration procedures to ensure the security of sensitive data, leveraging the existing backup and encryption tools (Bitlocker).
- Regularly review and update the organization's incident response plan and playbooks to address evolving threats and lessons learned.

6. Eradication

Root Cause Analysis:

- Determine the extent of the compromise and the impact on customers and their orders with the help of Security Analyst.

- Analyze the password protection mechanisms used in 2015 to understand the level of risk.
- Analyze the security and weaknesses around the perimeter of the physical location of the database servers.

Eradication Procedures:

- Consider the encryption of backup tapes so that even if they are stolen in future incidents, data is protected.
- Implement stronger password hashing algorithms and salting techniques to protect any remaining sensitive data.
- If possible, contact law enforcements to recover the stolen backup tapes and prevent further misuse of the data.

7. Recovery

System Restoration Process:

- Restore the affected systems from the most recent, secure and clean backup, using the existing backup and restoration tools.
- Verify the integrity and security of the restored systems before returning them to production, in coordination with the Network and Systems Engineer.
- Implement additional security controls, such as file integrity monitoring and network segmentation, to prevent future incidents.

Validation Checks:

- Verify that all remaining sensitive data has been properly secured and there are no other vulnerabilities in the servers.
- Conduct comprehensive testing and validation to ensure restored systems are fully functional and secure.

Ongoing Monitoring:

- Implement continuous monitoring and alerting mechanisms, using the Suricata IPS and IBM QRadar SIEM, to detect any suspicious activity.
- Review and update the company's security controls and incident response procedures on regular intervals to address evolving threats.

8. Post-Incident Activity

Lessons Learned Session:

- Conduct a comprehensive review of the incident response process, including an assessment of the team's performance, the effectiveness of the playbook, and any areas for improvement.
- Document the lessons learned and incorporate them into the organization's incident response plan and playbooks.
- Establish a timeline for regularly reviewing and updating the incident response playbook to ensure it remains relevant and effective.

Incident Report Writing:

An incident report should be written and made available to all the audience as mentioned earlier. The following topics can be considered as part of the structure of the incident report:

- Initial cause of the incident
- Actions and timelines of important events
- Incident impact
- Root cause analysis
- Actions taken
- Indicators of Compromise (IOCs)
- Lessons learned

9. Appendices

Legal and Compliance Guidelines:

- Review any applicable laws, regulations, and industry standards that may govern the organization's response to this type of incident, such as removal of backup tapes notification requirements, in coordination with the Legal and Compliance Advisor.
- Consult with legal counsel to ensure that the incident response process and any actions taken are in compliance with current laws and regulations.

Contact Information:		
IT Director		
IT Staff		
Extended Team		
Helpdesk		
IT Manager		
Legal and Compliance Advisor		