|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Incident Response Lab (Core)  Otis Smith / Cybersecurity Professional / 10.20.23 |  |
|  |  |  |  |
| Pipette dropping liquid in a petri dish | | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
|  |  | TABLE OF CONTENTS |  |
|  |  | Summary …………………………..  Discovery……………………………  Vulnerability……………………….  Exploitation………………………..  References.………………………..  Mitigation…………………………… |  |



|  |  |  |
| --- | --- | --- |
| Summary |  | |
| This incident response report outlines the process of a simulated security incident involving the exploitation of a virtual machine named LazySysAdmin. The attacker successfully gained unauthorized access, escalated privileges, and accessed sensitive data, demonstrating vulnerabilities in the virtual machine's security configuration. The report concludes with the mitigation recommendations to enhance the security posture of the system.  A hand holding a glowing city  Description automatically generated | |  |

1. Download and Setup:
   * Identified the target VM (LazySysAdmin) on Google Drive and downloaded the VM Images.zip.

A black and red screen

Description automatically generated

* + Successfully imported and configured LazySysAdmin on VirtualBox.



* + Verified network settings on Kali Linux to ensure connectivity.

A screenshot of a computer

Description automatically generated

1. Network Scanning:
   * Conducted network scans using nmap to identify LazySysAdmin's IP address (10.0.2.6) and open ports (22, 80, 139, 445, 3306, 6667).

A screenshot of a computer program

Description automatically generated

1. Directory Traversal:
   * Utilized dirb to explore directories on LazySysAdmin, discovering potential areas of interest such as "wp" and "wordpress."
   * A screenshot of a computer

     Description automatically generated
   * A computer screen with text and numbers

     Description automatically generated
2. Credential Discovery:
   * Discovered a username ("togie") in the WordPress directory.

A screenshot of a computer

Description automatically generated

* + Explored open ports 139 and 445 to identify shared directories using smbclient.
  + A screenshot of a computer

    Description automatically generated

|  |  |  |
| --- | --- | --- |
| Vulnerability |  | |
| 1. Web Application Vulnerability:    * Identified a potential vulnerability in the WordPress directory, leading to the discovery of MySQL credentials in the wp-config.php file.    * A screenshot of a computer       Description automatically generated 2. Brute Force Attack:    * Used Hydra tool to perform a brute force attack on SSH with the username "togie" and the rockyou.txt wordlist.    * Successfully obtained the SSH login credentials: username "togie" and password.   A screenshot of a computer program  Description automatically generated | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exploitation | | |  | |
| 1. SSH Access:    * Logged in via SSH using the obtained credentials, gaining access to the LazySysAdmin machine.   A screenshot of a computer  Description automatically generated   1. Privilege Escalation:    * Reviewed system commands, logs, and directories to escalate privileges.    * Located the "proof.txt" file in the root directory, providing the final flag.   A computer screen with text and numbers  Description automatically generated | | | |  |
| References |  |  | |  |

1. Tools Used:
   * Google Drive
   * VirtualBox
   * Kali Linux
   * nmap
   * dirb
   * smbclient
   * Hydra
   * SSH
2. Online Resources:
   * Medium article walkthrough for LazySysAdmin VM.
3. Documentation:
   * Autopsy documentation for forensic analysis.

# Mitigation:

# 

1. Secure Configuration:
   * Follow best practices for secure VM configurations and regularly update system configurations.
2. Access Controls:
   * Implement strong access controls and enforce the principle of least privilege.
3. Network Security:
   * Monitor network traffic and employ intrusion detection and prevention systems.
4. Password Management:
   * Enforce strong password policies and implement account lockout mechanisms.
5. Software and Patch Management:
   * Keep all software up-to-date with the latest security patches.
6. File Integrity Monitoring:
   * Implement file integrity monitoring tools to detect unauthorized changes.
7. Incident Response Plan:
   * Develop and maintain an incident response plan with regular training.
8. Data Encryption:
   * Encrypt sensitive data to protect it from unauthorized access.
9. User Education:
   * Provide security awareness training to users.
10. Logging and Monitoring:
    * Set up comprehensive logging and monitoring mechanisms.
11. Forensic Analysis:
    * Conduct thorough forensic analysis in the event of a security incident.
12. Periodic Vulnerability Assessments:
    * Conduct regular vulnerability assessments to identify and remediate weaknesses.

The mitigation strategies aim to enhance overall security, prevent unauthorized access, and strengthen the system against potential vulnerabilities. Regular updates, strong access controls, and proactive monitoring contribute to a more resilient security posture.