CyberT Incident Report

Date: January 10, 2025

Investigator: deletec00kiesb4leaving / d44h

Incident Overview

An employee, who was arrested for running a phishing operation, was suspected of malicious activities against CyberT's assets. Investigation revealed unauthorized actions including installation of software, permission changes, creation of a new user with elevated privileges, and the setup of a destructive script.

Immediate Actions Taken

System Isolation: The compromised machine was isolated from the network to prevent any further unauthorized access or data exfiltration.

Data Backup: Before any changes were made, a full backup of the system was performed to ensure no critical data was lost.

Detailed Findings

Installation of DokuWiki: The employee installed DokuWiki, potentially exploiting a known vulnerability.

Ownership Changes: Changed ownership of critical directories to www-data, which could facilitate unauthorized access by the web server.

Creation of New User: A new user 'it-admin' was created with sudo privileges, allowing further unauthorized actions.

Malicious Script: A script named 'bomb.sh' was transferred, modified, and scheduled to run every 8 hours, which would delete the DokuWiki installation and leave a taunting message.

Resolutions

Security Enhancements

- **Password Change:** All passwords for root, cybert, and it-admin were changed immediately.
- **User Account Management:**
  - Remove Unauthorized User: The user 'it-admin' was removed from the system.
  - Audit User Permissions: Review and adjust permissions for all users, ensuring least privilege principle is followed.
- **Sudoers File:** The sudoers file was restored to its original state, removing any unauthorized entries.
- **SSH Key Management:** All SSH keys associated with the compromised accounts were reviewed and unauthorized keys were removed.

System Repair

- **Remove Malicious Scripts:**
  - Delete 'bomb.sh': Ensure 'bomb.sh' and '/bin/os-update.sh' are removed from the system.
  - Crontab Cleanup: Remove the scheduled task from /etc/crontab that was set to run the malicious script.
- **File Permissions:**
  - Correct file ownership to revert changes made by the employee, particularly ensuring critical directories like /usr/share/dokuwiki are owned by root or the appropriate user.

Monitoring and Logging

- **Enhanced Logging:** Increase logging detail for sudo commands, user logins, and file system changes to better track future incidents.

- **Implement IDS/IPS:** Consider implementing an Intrusion Detection/Prevention System to monitor for similar patterns of malicious behavior.

Documentation and Training

- Incident Documentation: This report has been compiled to document the incident for future reference and training.

- Security Awareness Training: Conduct a session on security awareness, focusing on the risks of insider threats and the importance of monitoring and reporting suspicious activities.

Follow-up Actions

Regular Audits: Schedule regular audits of user permissions, system logs, and installed software.

Vulnerability Assessments: Perform regular vulnerability assessments to identify and patch any known vulnerabilities, especially in software like DokuWiki.

Review Policies: Review and update corporate policies regarding employee access, side businesses, and conflict of interest to prevent similar incidents.

Conclusion

The incident was resolved by isolating the system, removing unauthorized access, restoring compromised data, and enhancing security measures. Continuous monitoring, training, and policy enforcement will be key in preventing future incidents.