Neptune Enterprises External Audit Report on NIST SP 800-53 AC-9: Previous Logon Notification

December 6th, 2024

Auditors: Connor Bressler, Cordell Rager, Jimmy St Cin

Contents

[Audit Scope 3](#_Toc183525758)

[Executive Summary 4](#_Toc183525759)

[Discovered Issues and Solutions 5](#_Toc183525760)

[Appendices 7](#_Toc183525761)

[Audit Procedure 7](#_Toc183525762)

[Fieldwork and Documentation 9](#_Toc183525763)

|  |
| --- |
| Audit Scope |
|  |

This audit is designed to ensure a focus on evaluating Neptune Enterprises’ systems and accounts and their adherence to the requirements outlined in NIST SP 800-53 for the AC-9 (Previous Logon Notification) control. The auditing procedure will assess the policies, procedures and practices related to previous logon notifications on user accounts within Neptune Enterprises to ensure that they meet the security and operational requirements of the organization. Specifically, this audit will cover:

1. **Logon Notification Implementation:** Determining and evaluating if there is any tool or mechanism in place within Neptune Enterprises to notify users of previous logon activity.
2. **Details of Information Provided:** If there is a previous logon notification, there will be an assessment of what information that notification provides such as date and time of the last logon and other possible attributes.

|  |
| --- |
| Executive Summary |
|  |

The audit of the Neptune Enterprises server revealed one security issue that did not align with the requirements of NIST SP 800-53 Access Control 9 – (last logon notification). This vulnerability increases the risk of not being able to detect unauthorized access in Neptune Enterprise accounts.

1. **No Last Logon Notification For Graphical Logins**
   1. The audit identified one issue under AC-9. The issue is that graphical logons lack last logon notifications due to no /etc/pam.d/gdm directory being in place. Not having a last logon notification via the graphical interface creates accountability issues and increases the chance of not detecting suspicious activity.

|  |
| --- |
| Discovered Issues and Solutions |
|  |

**Issue 1:** The main focus of AC-9 is that the system in focus needs to provide a previous logon notification when a successful logon occurs. This notification needs to provide the date and time of the last logon notification. The accounts for Neptune Enterprises have a last logon notification for secure shell logins, but there is no equivalent notification for graphical logons due to there being no /etc/pam.d/gdm directory.

**Issue 1 Risk:** Without a last logon notification for graphical logins, which is most likely the more used way of logging into Neptune Enterprises’ systems, there is accountability issues for user access and logging. Not providing a last logon notification for graphical logins may make it harder to detect unauthorized use of an account when logging in via the graphical interface.

**Issue 1 Solution:** Create last logon notifications for graphical logins by setting up an /etc/pam.d/gdm directory with the pluggable authentication module (PAM). Once this is created, ensure that the information that is provided for last logon notifications in secure shell is the same for graphical logins. Mark will be responsible for implementing this although it is highly recommended he seeks outside help to create and configure this control. The last logon notification for graphical logins should be created and implemented within one month from the submission date of December 6th.

|  |
| --- |
| Appendices |
|  |

|  |
| --- |
| Audit Procedure |
|  |

Goal

Verify that previous logon notification practices for Neptune Enterprises’ accounts align with NIST SP 800-53 AC-9 requirements, ensuring secure, compliant, and effective handling of all user accounts.

Required Software, Tools and/or Documentation

1. NIST SP 800-53 AC-9 (Previous Logon Notification) documentation
2. Standard Access to Neptune Enterprises’ server
3. Mark Smith’s contact information
4. Documentation regarding auditing questions to evaluate if Neptune Enterprises has a previous logon notification control in place and Mark Smith’s answer to those questions

Directions

1. Below are the questions that will be asked to evaluate Neptune Enterprises’ systems pertaining to NIST SP 800-53 AC-9. These questions will be asked by the auditor and answered by Mark Smith. Mark’s responses to these questions will be reported in the fieldwork documentation below along with whether or not Mark’s answers can be verified and any issues that arise.

**Auditing Questions to be asked by the auditor and answered by Mark Smith:**

1. Does Neptune Enterprises have a tool or mechanism in place to notify users of previous logon activity? If there is, could you describe how this notification is delivered to users upon a successful logon? Whether it is an email, on-screen message, or something else?
2. What specific information is included in the previous logon notification? Does the information include date and time of the last logon, and other information such as the location of the logon?

|  |
| --- |
| Fieldwork and Documentation |

Auditor Information

| Auditor Number | Auditor Name | Date Audited |
| --- | --- | --- |
| 1 | Connor Bressler | 11/19/2024 |

**Auditing Questions, Mark’s Responses, and Arising Issues/Notes**

1. Does Neptune Enterprises have a tool or mechanism in place to notify users of previous logon activity?

Response From Mark:

The Neptune system was originally set-up by my IT consulting firm.  I remember the company asked a similar question.  After some discussion and debate, I decided to use their recommendations.  My recollection is that they set it up to follow industry standards of the time.  So, I assume it is set-up that way.  Is this still sufficient today?

Issues/Notes: This is good, although, this has to be verified that there is some sort of system logging actually in place on the system. Mark needs to show an actual picture of him getting a last logon notification when he logs in to verify this. The /etc/pam.d directory has to be viewed for this to be confirmed as well on the graphical login as this directory handles all logon notifications for graphical logins.

11/22/24: Mark was asked to show pictures of the /etc/pam.d directory. He also showed a terminal screenshot where the last logon notification is clearly visible. Here are the two pictures below:

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer error

Description automatically generated

Issues/Notes: So, from what can be observed from these screenshots, there is clearly a last logon notification for secure shell logins. Although, there is no /etc/pam.d/gdm directory. What this means is that there is a last logon notification for secure shell logons, but there is no notification for graphical logons, so this is an issue. On the bright side, the information that is provided for the last logon notification in the terminal provides all the information that is needed to align with AC-9.

1. What specific information is included in the previous logon notification? Does the information include date and time of the last logon, and other information such as the location of the logon?

Response From Mark:

From my experience, when I log into the system, I do get a message that tells me the last time I logged into the system.

Issues/Notes: All information that is provided for the last logon notification within the terminal aligns with AC-9. No issues here.