**Manta Mădălin-Ștefan  
Incident report – Authentication Issue**

Every incident escalated will be assigned an incident severity level.

These severity levels range from one to four, with one being the most severe incident. The procedure for determining the Severity Ratings for incidents can be broken down as follows:

**Priority 1**: This has the highest priority. **Immediate action to be carried out**, **the SLA for P1 was agreed to 30 minutes**. High impact on business. An email will be followed up with a phone call from Smarttech247 to raise the alert. E.g. Ransomware attack in progress.

**Priority 2**: This is the second highest level of priority. **Action will need to be carried out within one hour** of alert being triggered by Smarttech247. This alert will arrive via an email. E.g. Brute force login – conficker virus.

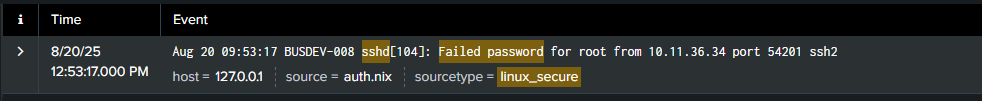
**Priority 3**: This is the third highest severity level. **Action will need to be carried out within 4 hours** of the alert coming in from Smarttech247. This alert will arrive via an email. E.g. If a user accesses a website that has a high threat score.

**Priority 4**: This is the fourth highest severity level. **Action should be carried out in one working day** of the alert coming in from Smarttech247. Low to no impact on the business. This alert will arrive via an email. E.g. Use of a proxy server.

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | **Authentication Issues** | **Priority 4** | |

**Details**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Notable ID:** | ddcba8d96433b212ee28d42a94dffc9a | | | **Location:** | Lab Environment – 12:53:17 20/08/2025 | | | | |
| **Description:** | Failed password | | | | | | | | |
| **Source IP(s):** | 10.11.36.34 | **Source Port:** | 54201 | **Destination IP(s):** | | 127.0.0.1 | | **Dest. Port:** | 22 |
| **Asset Name:** | 127.0.0.1 | | | **Username:** | | root | | | |
|  |  | | |  | |  |  | | | |
| **Log Sources:** | | | | **Categories:** | | | | | |
| Linux\_secure / sshd | | | | Failed password, PAM authentication failure, Invalid user | | | | | |

****

****

****

**Event Information**

We have identified multiple authentication failures for the following users: [squid; mysql; root; uucp; webalizer; nobody; newuser; gopher; usr5; dovecot; games; usrabc; apache; xfs] originating from [giant-device.local.com; 10.11.36.17; 10.11.36.34; abc.dobotsv3.net; demo-instance.dobotsv3.com; 10.11.36.21; hosted-by.newhost.com; 10.11.36.43; 10.11.36.19; 10.11.36.21; 10.11.36.48; 10.11.36.33; 10.11.36.34; system-enterprise.com; 10.11.36.10; 10.11.36.14; 10.11.36.31] to the destination IP(s) [127.0.0.1].

The following table illustrates the detected events, on 20th of August 2025, from 12:50 P.M. – 12:53 P.M.:

O imagine care conține captură de ecran, text

Conținutul generat de inteligența artificială poate fi incorect.

All attempts failed with the following failure reasons:

* PAM authentication failure
* Failed password
* Invalid user

**Recommendations**

We recommend investigating the authentication attempts from [giant-device.local.com; 10.11.36.17; 10.11.36.34; abc.dobotsv3.net; demo-instance.dobotsv3.com; 10.11.36.21; hosted-by.newhost.com; 10.11.36.43; 10.11.36.19; 10.11.36.21; 10.11.36.48; 10.11.36.33; 10.11.36.34; system-enterprise.com; 10.11.36.10; 10.11.36.14; 10.11.36.31] to [127.0.0.1] for the usernames [squid; mysql; root; uucp; webalizer; nobody; newuser; gopher; usr5; dovecot; games; usrabc; apache; xfs].

Based on the findings, the following recommendations are proposed to enhance the system's authentication security:

Implement Account Lockout Policies: To deter brute-force attacks, a policy should be established to temporarily lock an account after a specified number of consecutive failed password attempts. This prevents attackers from making limitless attempts to guess credentials.

Enhance Password Complexity Requirements: Enforce strong password policies that require a combination of uppercase and lowercase letters, numbers, and special characters. Additionally, prevent the use of easily guessable passwords, such as common words or sequential numbers.

Deploy Multi-Factor Authentication (MFA): The single most effective recommendation is to implement MFA. By requiring a second form of verification (e.g., a one-time code from a mobile app or a physical token) in addition to the password, even if a password is compromised, the account remains secure.

Monitor and Alert on Failed Login Attempts: Implement real-time monitoring of authentication logs. Configure the system to generate alerts for suspicious patterns, such as an unusually high number of failed logins from a single IP address or multiple invalid user attempts in a short period.

Regularly Review PAM Configurations: Conduct a regular audit of all PAM service configurations to ensure they are properly secured and configured according to the principle of least privilege. This will prevent potential authentication bypasses due to misconfiguration.

Use a Dedicated Authentication Service: For large-scale environments, consider using a dedicated, centralized authentication service (e.g., LDAP or Active Directory) rather than relying on local user accounts. This streamlines management and provides a more secure framework.

Additionally, we suggest enforcing a Maximum Password Age policy to ensure that passwords are changed regularly and enhance security.