

## 15.3.3 Login Blocking Facts

---

Administrators can prevent users from logging in to a Linux system. This may be necessary while troubleshooting problems or while responding to a security event.

This lesson covers the following topics:

- Pluggable Authentication Modules (PAM)
- Login blocking process

### Pluggable Authentication Modules (PAM)

Login blocking is enabled using the Pluggable Authentication Modules (PAM) module configured in the **/etc/pam.d/login** file. PAM:

- Is a set of modules that enables various authentication systems on a Linux computer.
- Can employ modules concurrently. For example, one PAM module can be used to enable biometric logins while another enables standard user and password authentication.

The **auth requisite pam\_nologin.so** line in the **/etc/pam.d/login** file configures PAM to check and see if a file named **/etc/nologin** exists.

On some distributions (such as Fedora) the **/etc/pam.d/login** file uses the syntax of **auth required pam\_nologin.so** to enable login blocking.

If **/etc/nologin** does exist and the user is not root, authentication is blocked and an optional message is displayed to the end user.

### Login Blocking Process

The following list describes the tasks necessary to configure login blocking:

- Force all users to log out of the system:
  1. Log in directly as the root user.
  2. Use the **w** command to view all active user accounts.
  3. Use **pkill -KILL -u user** to force the user to log out for each active user.
- Disable the ability to login to the system:
  1. Create the **/etc/nologin** file.
  2. Add a message to the file that will be displayed to users when they attempt to log in.

Rename or delete this file to re-enable logins.

---

---

TestOut Corporation All rights reserved.