Red Hat Enterprise Linux 9 (RHEL 9) is the latest version of Red Hat’s flagship operating system, released at the Red Hat Summit in May 2022. New capabilities added to RHEL 9 help simplify how organizations manage security and compliance when deploying new systems or managing existing infrastructure. This article takes a brief look at three of the new security features available in this release.

The default superuser account in Unix- and Linux-based systems is "root". Because the username is always "root" and access rights are unlimited, this account is the most valuable target for hackers. Attackers use bots to scan for systems with exposed SSH ports, and when found, they attempt to use common usernames and brute-force passwords to gain entry. Of course, the impact of a successful exploit would be a lot lower if the compromised user has unprivileged access. The breach would then be contained and limited to one user only.

[3]