

Re: Detecting Brute-Force and Dictionary attacks

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2006-10/msg00018.html>

- *From:* "Rob Creely" <programmingart@xxxxxxxxxx>
 - *Date:* Sun, 22 Oct 2006 14:36:16 -0400
-

I am looking for a good tool to detect brute-force and dictionary attacks on user >accounts on a Linux system . The tool should also have the intelligence to differntiate >between user mistakes and actual brute-force/dictionary attacks and reduce the >>false positives. SuSE/RedHat included security tools are not helping in this case .

Please , anyone knows any third party security tool or any opensource security tool >which solves my problems.

Have a look at <http://www.ossec.net>. I believe it differentiates between user mistakes and brute-force/dictionary attack by looking at the amount of failed logins for a particaluar user, or from a particular IP, within a particular time frame. After detection of an attack, you can choose to block the IP of the attacker(s).

--Rob