

Re: Question bruteforcing

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2006-05/msg05314.html>

- *From:* "Jacques B." <jjrboucher@xxxxxxxxxx>
 - *Date:* Wed, 31 May 2006 05:56:38 -0300
-

On 5/29/06, Mike C <Mikec1@xxxxxxxxxxxxxx> wrote:

What exactly is bruteforcing and is their away to stop it in fedora without using a router or firewall box?

Thanks for any help

--

fedora-list mailing list

fedora-list@xxxxxxxxxx

To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>

In the meantime anytime you can throw a router/gateway in front of a computer you get an extra layer of protection. So someone trying to exploit an OS vulnerability by attacking your IP without you having initiated the connection will get dropped by the gateway/router. And because your router does not have the same OS, hence not the same vulnerabilities, then the exploit will fail. I use the D-Link DI-604, a pretty basic and inexpensive router, and it does the trick quite nicely.

To learn more about how a NAT router can act as a firewall, check out podcast #3 at <http://www.grc.com/SecurityNow.htm>. This site offers some good podcasts for beginners, and even intermediates if it's a topic that you are not well versed on.

Defence in depth. The router will give you one extra layer in your defence. Iptables another, hosts.deny & hosts.allow yet another, regular updates another. Each layer is a layer that a hacker must be able to penetrate to eventually compromise your system. The most effective way to bypass all these layers is social engineering where a hack tricks you into opening an attachment or installing an application to give them root access to your system. So if you can defend against that, your properly configured & updated computer with a router should do a good job at taking care of the rest.

Regular OS updates is probably the most significant preventative step a person can take to protect their system. Worms exploit known

Re: Question bruteforcing

vulnerabilities (typically, some may exploit an unknown vulnerability initially until it's reverse engineered to identify the vulnerability being exploited). Keeping your system up to date will patch those vulnerabilities before a worm exploits it. But gone are the days that hackers would need 14–30 days to exploit a new vulnerability being patched. Now they analyse patches being put out and identify the vulnerability, inject that into their existing code and then send it out the same day the patch was released. So we are now seeing zero day exploits. In other words the vulnerability being patched gets exploited the same day the patch is released. So if you don't patch quickly enough you are at greater risk.

But to come full circle this is where a router would offer protection against such worms for reasons noted earlier.

Oh and if you have no intention of running a web server, a mail server, sshd, ftpd, whatever, then don't install it (or at least don't activate it). Because these create points of entry into your system by the nature of being servers allowing connection from others. Misconfigurations of these services

Drifting a bit OT, however all security related.

Jacques B.

—

fedora-list mailing list

fedora-list@xxxxxxxxxx

To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>