

## Re: Some new SSH exploit script?

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-06/msg00198.html>

---

- *From:* Christine Kronberg <[seeker@xxxxxxxxxx](mailto:seeker@xxxxxxxxxx)>
  - *Date:* Sat, 10 Jun 2006 12:11:59 +0200 (CEST)
- 

On Fri, 9 Jun 2006, Adam.Chesnutt wrote:

You see, rather than do all this, I think it's much much smarter to turn over the logs more, and write a script that outputs the log – without the script kiddies if it really bothers you. You could make the script also write a report and call it 'lame ssh hacktards' or something and contain only ip, username and number of attempts..

This is a piss poor solution to a real problem. If you have cruft, correlate. Ignoring what are genuine (albeit lame) attempts to penetrate your security is dumb.

The real problem. That is not the scanning, but the hacked nodes being abused for it. The problem is people not knowing their systems are compromised and ISPs not interested in telling them or enforcing security measurements. The problem is people not caring in the state of their computers, acting irresponsible (I remember someone on usenet arguing that it's not his fault that his computer is being abused by other people) and getting away with it.

The solution to the real problem can neither be moving the door nor blocking it. Moving the door or blocking it are just two strategies about how to deal with the consequences of the problem.

If 3 people connect to this port, by all means, but just moving the port to decrease your viability of hacktards isn't smart. Your not decreasing your access, your moving the door. Firewall them for god's sake. Instead of ignoring the problem, **\*DO SOMETHING\***

I do. I report attacks to the services open. Not attacks to services not open. If port 22/tcp is moved to another portnumber, then there are not attacks on port 22/tcp (to me a single syn is not an attack). At least not on the host with the moved door. There may be attacks on the other port; these attacks should indeed be reported.

This is why I said something about my killapnic script. My killapnic script is a much better solution than moving the port. Why? Because it actually does something to disallow network access from the attacker, rather than continuing to allow them access, and ignoring the signs

Re: Some new SSH exploit script?

of them trying to break in.

No, your script does not do that. It just blocks of apnic. What's about the rest of the world? Although many scans are originating from that region there are more than enough coming from other locations. And btw., I never saw the login after a "successful" scan coming from the scanning node. It was always from an entirely different location. So what is your consequence? Adding the rest of the world to you script? That's a no go for me.

Consider zombies.. your in a house, and zombies are outside. Do you, move the windows and doors to a new location, or board them up where they are? There's

Doing both? What is it you want to archive? Less noise to concentrate on more important topics?  
Making sure the zombies are stopped and withdrawn? How do you enforce that (stopping ok, but how to withdraw them)?

enough traffic, there's enough zombies, and the scripts are mostly smart enough \*already\* to find nonstandard ports. Can we please join the future here in good ole 2002?

Well, the fact, that the ssh kiddies are not only coming from the apnic ranges traces back in around late 2004...

Have a nice weekend,

Chris Kronberg.

---

This List Sponsored by: Cenzic

Concerned about Web Application Security? Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: [http://www.cenzic.com/news\\_events/wpappsec.php](http://www.cenzic.com/news_events/wpappsec.php) And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at [request@xxxxxxxxxx](mailto:request@xxxxxxxxxx) for details.

---

Re: Some new SSH exploit script?