

# Re: ID-ing Hackers

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-02/msg02245.html>

---

- *From:* Joe <joe@xxxxxxxxxxxxxxxx>
  - *Date:* Sat, 16 Feb 2008 23:03:57 +0000
- 

MikeG wrote:

My Server Security Log recorded (160) 529 logon failure events during a 10 minute interval, one failure about every 6-7 seconds.

Is there a way to trace this to the source to find out who is doing this? I have SBS 2003 STD R2 Edition.

A sample of the event follows. Thanking you in advance for your help.

Security 529 Logon Failure: Reason: Unknown user name or bad password User Name: crack  
Domain: Logon Type: 3 Logon Process: Advapi Authentication Package:  
MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0 Workstation Name: SERVER  
Caller User Name: SERVER\$ Caller Domain: domain Caller Logon ID: (0x0,0x3E7) Caller  
Process ID: 1828 Transited Services: - Source Network Address: - Source Port: -

There is a log level for RRAS that can be enabled, called 'tracing' in the RRAS manager, but it generates a large volume of fairly incomprehensible logs. A more cost-effective way is to buy a router which can log usefully, if your present one cannot.

It's not really very useful, as nearly all malevolent activity on the Internet is carried out from some home computer which has been cracked, possibly for months or years. For every home user who has up-to-date AV and spyware detection, there are ten or twenty who don't. The level of awareness of security issues of most computer users is on a par with their knowledge of quantum mechanics.

Almost certainly, you're being hit by a script rather than by a human, and you'll never track the real culprit. You won't even get a single IP address to block, as there is probably a collection of 'owned' machines, a so-called botnet, involved.

I'm sure you know the score: don't open any ports you don't need, restrict remote access to the users who really need it, beat them with a stick (sorry Susan) until they use decent passwords, use a second method of authentication if possible (certificates etc.), restrict connection to a few IP addresses or ranges, and so on. If the remote users are managers, and therefore immune to sticks, reason and suchlike, at least tell them in writing that the security of the network depends on the quality of their passwords.

.