

RE: ssh and ids

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2004-06/0106.html>

Peter_Schawacker_at_NAI.com

Date: 06/22/04

Date: Tue, 22 Jun 2004 13:31:21 -0700

To: <focus-ids@securityfocus.com>, <roesch@sourcefire.com>

Hi Marty,

Since you were kind enough to mention us :-) I thought I would offer two comments about what you wrote regarding SSL "key escrow" (is it really "key escrow" when the key isn't handed to a third party?) and IDS/IPS.

First, remember that storing your web server's private key on an external system is something that's done routinely with SSL accelerators. Hardware SSL accelerators are commonplace these days. Second, we fully understand that folks are often squeamish about sharing keys, so great care was taken to protect the private keys on the IntruShield appliance. We believe we have found the best possible strategy for mitigating private key theft risk while eliminating the SSL/NIDS "blind spot". Through the use of public key cryptography, we persist the key in such a way that one would need information that is resident only in the sensor, along with information that is resident only in the IntruShield Manager in order to recover the key. Having just one or the other will not suffice. I won't bore the list with the details, but our implementation is described here:

http://www.nai.com/us/tier2/products/media/sniffer/wp_encr_th_prot.pdf

Should an attacker root your web server, how safe will your private keys be? If your IDS/IPS can't handle TCP/443 to your production web servers, you have a blind spot where attackers can operate unseen and unhindered. Which is worse, copying your web servers' private keys to your IPS to prevent a web server compromise, or being blind to attacks against those same servers? Frankly, I can't think of a single IDS/IPS product that is less secure than a typical web server. Security is all about trade-offs. This is not a difficult one.

You also alluded to the problem of covert channels. I believe that the best protection against covert channels is to stop the attacker before the back door is installed. Failing that, a host based IPS/firewall is the last, strongest line of defense.

Peter Schawacker, CISSP

RE: ssh and ids

SecurityFocus IDS: RE: ssh and ids

IPS Technical Evangelist
McAfee
Office 760 200 4258
Mobile 760 880 4258
ps@nai.com

-----Original Message-----

From: Martin Roesch [mailto:roesch@sourcefire.com]
Sent: Friday, June 18, 2004 5:54 PM
To: Runion Mark A FGA DOIM WEBMASTER(ctr)
Cc: focus-ids@securityfocus.com
Subject: Re: ssh and ids

Hey Mark,

VENDOR ALERT: I'm a vendor and I'm going to talk about my technology. Please take my comments with an appropriate amount of sodium chloride.

Sourcefire's RNA product is capable of isolating/identifying layer-7 protocols (including encrypted protocols) and tracking the flows. For example, if you wanted to find SSH/SSL traffic that it being initiated from outside your network to inside, setting up a query (or automated reporting) is pretty trivial. Hacker busts into your network and sets up an SSH server, RNA picks it up and can let you know that it detected

a new service and logs the flow data, etc. Anyway, if you're interested in seeing a demo or talking more, let me know.

As far as IDS being able to do much with encrypted traffic, there's generally not much to do once the session goes encrypted. You can setup rules in a system like Snort to differentiate between "allowed" and "everyone else" hosts talking to machines on your network pretty easily (and you can query RNA's flow data for the info too).

I know the NAI guys just released a mod to their sensors that allow them to do real-time SSL decryption if you're willing to escrow the private crypto keys on the box (shudder). There's been talk of implementing the same sort of thing in Snort (ala ssldump) for a while,

but it's never come together...

-Marty

On Jun 18, 2004, at 2:18 PM, Runion Mark A FGA DOIM WEBMASTER(ctr) wrote:

> *Lets suppose the attacker is mildly sophisticated, and after making the*
> *initial assault roots the box and installs a secure backdoor or two.*

RE: ssh and ids

SecurityFocus IDS: RE: ssh and ids

> *Is*
> *there any IDS capable of isolating data it cannot read, except to*
> *monitor*
> *authorized port usage of a system or group of systems? Not to*
> *complicate*
> *the question, but when the attacker is using portal gates and all*
> *communications traffic is encrypted in normal channels how can an IDS*
> *participate? Monitoring normal traffic patterns seems a bit slow for*
> *detection.*

>
> -
> *Mark Runion*

>
>
>

> -
> ----
>
>

> -
> ----
>
>

--
Martin Roesch - Founder/CTO, Sourcefire Inc. - (410)290-1616
Sourcefire: Intelligent Security Monitoring roesch@sourcefire.com -
<http://www.sourcefire.com>
Snort: Open Source Network IDS - <http://www.snort.org>

