

## Re: ssh and ids

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2004-06/0112.html>

---

**From:** Bamm Visscher (*bamm.visscher\_at\_gmail.com*)

**Date:** 06/22/04

Date: Tue, 22 Jun 2004 16:35:42 -0500

To: Frank Knobbe <frank@knobbe.us>

Real quick point. Don't assume the backdoor is going to be listening on the server. It's a simple task to instead install a backdoor that makes an outbound connection to a central server that lets the attacker issue commands on the compromised host. This comm channel could be encrypted (reverse ssh) or even use a http proxy.

With that said, I agree that prevention (Firewalls, IPS, regular audits, patch management, etc), is an important factor in network defense. But I think the thread here is meant to be focused on detection. We aren't talking so much about attack detection, but the true capability to be able to detect compromise (either as it happens or after it has taken place) and more importantly, having the information and capability to respond quickly to it. Although it would be nice to be able to detect a compromise as it occurs (or prevent it), we can't assume that will be the case 100% of the time. To augment that fact, we need to define practices that will help us identify 'after access events'. Whether it's an FTP session and the downloading of a hax0r toolkit, or a covert comms channel.

When I first started out, the organization I worked for spent a lot of time analyzing telnet connections. We did this because at the time, it seemed the attackers first step after compromising a host, was to create a backdoor account, and then stroll through the front door (yes, telnet is now considered a 'bad thing' but at the time, it was the common place). Some of the more interesting things we would do was at the '100 ft level', looking at a connection as a whole versus the data inside. For instance, most people can't type fast enough to get more than one character in a telnet packet, but if you cut 'n paste some source code thru that connection, all of a sudden the byte/packet ratio goes thru the roof. So, we could query our connections DB, identify suspicious sessions, and then, since we logged the pcap, we could look more closely and determine if the connection was indeed malicious. When DNS exploits initially became all the rage, we were concerned our IDS that didn't decode DNS was missing zero-day attacks. So, from the 100 ft level, we would query our cnxs DB for sessions to port 53 and where the source sent more the 1000 bytes during the duration of the connection. Again, once we identified those

## SecurityFocus IDS: Re: ssh and ids

suspicious connections, we would use the actual packet captures to determine if there was a true attack (and if it was successful).

Telnet has long been replaced by secure shell (damn you encryption), but that doesn't mean you still can't take a look from the 100 ft view. For instance, it seems like it would be trivial to determine which connections were used as a command terminal, and which ones were actually tunneling other data thru them (X or scp). In a cmd connection, I could also fairly accurately identify which packets contained the carriage return and probably figure out the number of chars each command contained (of course tab completion could b0rk some of this). If the internal IP addr initiated the connection, but the external (server) IP addr appeared to fit the template of a controlling terminal, I could theoretically tag the connection as a possible reverse ssh backdoor.

There is a catch. Doing this 100ft analysis doesn't come cheaply. First you have to collect the data and then you have to find the time to mine it. Personally, I view it as money well spent, but other organizations may not find it so. A few of us on this list have blabbered about the concept of Network Security Monitority (NSM) before. Richard Bejtlich has a book [0] on the subject coming out soon. And with sguil [1], we are trying to make analysis at this level more effecient (the above DNS example is actually a standard query in sguil).

Bammkkkk

[0] <http://www.taosecurity.com/books.html>

[1] <http://sguil.sf.net>

On Tue, 22 Jun 2004 10:11:03 -0500, Frank Knobbe <frank@knobbe.us> wrote:

>

> *On Mon, 2004-06-21 at 07:43, Gary Flynn wrote:*

> > *The Juniper/Netscreen IDP comes with a feature called Profiler*

> > *that you can set to discover and alert on new port or host*

> > *appearances. You set it to discover whats normal, then turn on*

> > *alerting.*

>

> *Before we're diving too far into the list of IDS/IPS that can profile*

> *traffic, I just want to remind everyone that a good firewall*

> *configuration does exactly that; it creates a profile and prevents*

> *unauthorized connections.*

>

> *It seems these days we're quick to jump to IDS/IPS systems to have them*

> *detect and prevent unauthorized and/or abnormal traffic. It seems we're*

> *forgetting that a correctly configured firewall does the same thing. It*

> *prevents backdoors into web servers, it prevents web servers to*

> *establish sessions to the outside.*

>

> *The IDS needs to catch those conditions where for example an attacker*

Re: ssh and ids

SecurityFocus IDS: Re: ssh and ids

> launches a cryptcat shell from the web server to the outside, and I  
> agree that the IDS needs to know the normal traffic profile for that  
> purpose. But guess what... your firewall (which is blocking said  
> shell-shovel-attempt) can detect it as well. Not just that, it can  
> prevent it!  
>  
> It seems nowadays we tend to augment lax and leaky firewalls with IPS  
> systems when we should really go back and tighten our firewall rule  
> sets.  
>  
> Now that I'm done ranting, let me ask you: How do you detect a listening  
> port on a rooted server when no one is able to send packets to that  
> port?  
>  
> (Seems like nmap would do the trick, and is cheaper than profiling IDS  
> appliance.)  
>  
> Cheers,  
> Frank  
>  
>  
>  
>  
> signature.asc - 1K  
>

--

<http://squil.sf.net>

---

---