

[fw-wiz] More Syslog Questions

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-07/0092.html>

From: Nathaniel Hall (halln_at_otc.edu)

Date: 07/19/04

To: <firewall-wizards@honor.icsalabs.com>

Date: Mon, 19 Jul 2004 08:10:46 -0500

The only problem I have with `chattr +a` is that if an intruder gains access to the root account, they can change the attributes, change the log files, and the replace the append only attribute, making it appear that nothing was done to the log file.

Since I started this post, I believe we came up with another solution, but I would still like your opinion. Here it goes...

Server 1 is connected to the main network. Server 2 is connected to Server 1 using a cross over cable. Server 2 listens in promiscuous mode. Physically the servers are secure and the only way to access Server 2 is through KVM over IP.

Server 1 receives all syslog messages and (using IPTables with DNAT) sends the messages to any IP address since Server 2 is listening in promiscuous mode it should pick up all of the messages. This does not allow anybody to compromise Server 1 and gain access to Server 2.

How does that sound?

~~~~~

Nathaniel Hall

Intrusion Detection and Firewall Technician

Ozarks Technical Community College — Office of Computer Networking  
417-799-0552

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

From: Tichomir Kotek [<mailto:tichomir.kotek@lynx.sk>]

Sent: Monday, July 19, 2004 4:54 AM

To: Nathaniel Hall

Subject: Re: [fw-wiz] More Syslog Questions

Nathaniel Hall wrote:

> *Since someone asked a question about syslog, I thought I would add a*  
> *couple of my own.*

## Firewall-Wizards: [fw-wiz] More Syslog Questions

>  
>  
>

> *I am in the process of setting up a centralized syslog server running  
> RedHat AS3. Currently, I am using syslog as our daemon, but have heard  
> there are other, better solutions. What do you suggest?*

syslog-ng can sort messages to various files by regexp, and/or hostname/IP of originating device, etc.

> *In an effort to make the log server as secure as possible, I would like  
> to find a way to use an append only file system. Unfortunately, if this  
> is done, logs cannot be rotated using logrotate so the server must be  
> taken down to single user mode to rotate the logs, causing the loss of  
> many log entries.*

>

> *Does anybody know of a good append only file system or another solution  
> to achieve the same results?*

>

IMHO, chatr -a file works on ext2 in any runlevel, the only thing you have to do is put some prerotate/postrotate lines to logrotate configuration file it's not bulletproof but it makes smaller gap fo intruder to alter logfiles

hope it helps

tk

--

Tichomír Kotek  
IT Security Senior Consultant  
LYNX, spol. s r.o.  
Masarykova 10  
040 01 Kosice  
Tel: 055/633 55 11  
Fax: 055/633 55 20  
E-mail: tichomir.kotek@lynx.sk  
<http://www.lynx.sk>

-----Doverne-----

Tato elektronicka sprava je prisne doverna a urcena vyhradne adresatovi. Sprava moze obsahovat informacie z pravneho, profesionalneho alebo ineho dovodu vyhradene. Pokial nie ste urcenym adresatom, ziadame Vas, aby ste nepreznadili, nezverejnili, nekopirovali a nepodnikali ziadne kroky suvisiace s touto spravou. Pokial Vam tato sprava bola dorucena omylom, informujte nas, prosim, o tom a ihned vymazte prijate udaje.

---

firewall-wizards mailing list  
firewall-wizards@honor.icsalabs.com  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>