

Re: HIDS solution for NT4 machines

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2005-10/0013.html>

From: Jason Thompson (securitux_at_gmail.com)

Date: 10/06/05

Date: Thu, 6 Oct 2005 10:30:24 -0400
To: OnlyIknow 4sure <bcihak@gmail.com>

What about Snort? They have binaries for Win32, and as long as Winpcap will run under NT4, snort should be a breeze. I haven't run Snort myself in NT4, but it's definitely worth a test.

And as far as price goes, it doesn't get much cheaper :)

-J

On 10/6/05, OnlyIknow 4sure <bcihak@gmail.com> wrote:

> We did think about putting an IDS/IPS device in front of the NT4 machines or
> even a Cisco Pix FW, but the expense knocked that idea down. Some of the
> boxes are already on segregated networks in some of our manufacturing
> plants, but someone could plug an infected system up unknowingly to that
> network segment and then game over. I know we're not the only company out
> there that unfortunately has NT4 machines running, I'm just surprised that
> there's not a company out there servicing this area.

>
> I looked at Osiris and am trying to figure out if that will work for our
> needs or not. I'd appreciate any other software/hardware ideas you guys
> might have.

>
> Thank!

>
> Bcihak

>
>
>

> On 10/5/05, Jason <securitux@gmail.com> wrote:

>> If you can't find a HIDS, then you can always put in a network IPS and use
>> it to separate your NT4 servers from the rest of the environment. If 6a
>> breaks your software, a HIDS may as well, even if you find one that works
> on

>> less than 6a. So a network IPS would be a good alternative.

>>

>> -J

>>

>> -----Original Message-----

SecurityFocus IDS: Re: HIDS solution for NT4 machines

> > *From: bcihak@gmail.com [mailto:bcihak@gmail.com]*
> > *Sent: Monday, October 03, 2005 12:52 PM*
> > *To: focus-ids@securityfocus.com*
> > *Subject: HIDS solution for NT4 machines*
> >
> > *I work in a large distributed network. We have several workstations and*
> > *servers that are running on NT4. I've been tasked with finding some sort*
> > *of*
> > *a HIDS (Host based Intrusion Detection System) software solution to*
> > *protect*
> > *these machines from zero day exploits, worms, and BO's. I've looked at*
> > *Cisco, Blink by Eeye, Destop Protector by ISS, and Primary Response by*
> > *Sana*
> > *Security. None of these will support anything lower than NT4 SP6a. My*
> > *biggest problem is I have several machines that are running below SP6a and*
> > *because of the flaky software running on these machines, I can't install*
> > *SP6a without breaking the app. Does anyone have any good experience with*
> > *other products for NT4 server/workstation below SP6a.*
> >
> > *Just a side note, most of these machines will be replaced within 2 years,*
> > *but that is a long time to leave exposed machines on the network.*
> >
> > *Thanks!*
> >
> > *Bcihak*
> >
> >
> >

> > *Test Your IDS*
> >
> > *Is your IDS deployed correctly?*
> > *Find out quickly and easily by testing it with real-world attacks from*
> > *CORE*
> > *IMPACT.*
> > *Go to*
> > *http://www.securityfocus.com/sponsor/CoreSecurity_focus-ids_040708*
> > *to learn more.*
> >
> >

> >
> >
>
>

Test Your IDS

Is your IDS deployed correctly?
Find out quickly and easily by testing it

SecurityFocus IDS: Re: HIDS solution for NT4 machines

with real-world attacks from CORE IMPACT.

Go to http://www.securityfocus.com/sponsor/CoreSecurity_focus-ids_040708
to learn more.
