

Re: Audit Account Logon Events, Client IP address incorrect?

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2004-12/0928.html

From: Herb Martin (*news_at_LearnQuick.com*)

Date: 12/15/04

Date: Wed, 15 Dec 2004 13:35:49 -0600

"ptwilliams" <ptw2001@hotmail.com> wrote in message
news:#QWFAjt4EHA.2592@TK2MSFTNGP09.phx.gbl...

> > *By now, I really should have written a Perl program to do that (probably
> > something simple based on time
> stamps would get me close.)*
>
> *Well, don't just talk about it!!! Get too it!*
>
> *And post it free for all of us when you're done ;-)*
>

Ok, let's try a simple design and IF I have some
time I will hook it up....

What sort of messages do we need to capture in
Snort? (You don't have to answer but pointing me
to the current docs for Kerberos and NTLM authentication
and secure channel packet types would help...)

- 1) Find Account Logon or Logon events in event log
(I can do that.)
- 2) Find messages of the relevant types in Snort log
- 3) Filter Snort messages to plus or minus N seconds
or milliseconds of each Audit event.

Can that (little bit) be useful?

Do you run Snort and Perl? Would you run them if
this worked?

Comments from PT or ANYONE welcome.

microsoft.public.win2000.active_directory: Re: Audit Account Logon Events, Client IP address incorrect?

Alternative:

4) Find something in Audit that can be directly matched to the Snort log....

```
--
Herb Martin
>
> --
>
> Paul Williams
>
> http://www.msresource.net
> http://forums.msresource.net
>
>
> "Herb Martin" <news@LearnQuick.com> wrote in message
> news:O0tq2ws4EHA.3368@TK2MSFTNGP10.phx.gbl...
> "Lori" <Lori@discussions.microsoft.com> wrote in message
> news:DBB04A1E-77B7-4E36-9D01-6F7277131B4C@microsoft.com...
> > Thanks Herb! Now I at least have an explanation for the "powers that
be"
> > when they look at the logs.
>
> The next step is to run an IDS (Intrusion Detection
> System) but that is a LOT of work UNLESS you will
> actively read and use the logs.
>
> I hope someone will pipe in here and suggest a way
> to match Snort (a free IDS) logs with Windows logs.
>
> By now, I really should have written a Perl program
> to do that (probably something simple based on time
> stamps would get me close.)
>
>
> --
> Herb Martin
>
>
> >
> > Lori
> >
> > "Herb Martin" wrote:
> >
> > > "Lori" <Lori@discussions.microsoft.com> wrote in message
> > > news:40C60175-847A-47F1-A829-F486907C862C@microsoft.com...
> > > > Hi,
> > > >
> > > > We recently set up an audit policy to audit failed account logon
> > > > events
> > > > for
> > > > our domain controllers. If I look at the logs, I can see Event ID
675
> > > > for
> > > > the failed logons. However, when I look at the detail, the Client
IP
> > > > address
> > > > does not have the address of the client, but instead the IP of one
of
> > > > the
> > > > domain controllers (and often not even the closest DC). For
```

Re: Audit Account Logon Events, Client IP address incorrect?

microsoft.public.win2000.active_directory: Re: Audit Account Logon Events, Client IP address incorrect?

```
example,  
> I  
> > > deliberately entered a bad password to log onto a client at IP  
> address  
> > > 192.168.22.126. The Security log on the local DC showed Event ID  
675  
> for  
> > > the  
> > > userID I used, but the Client IP address shows as 192.168.7.17 which  
> is a  
> > > DC  
> > > at a remote location.  
> > >  
> > > Can anyone help me understand why this is happening?  
> > >  
> > > Probably because historically logon might happen over  
> > > any supported network protocol so these events never  
> > > included the IP address (it might not even have been IP.)  
> > >  
> > > It is sort of silly these days, but it's one of those things  
> > > (I believe) the developers know needs improving.  
> > >  
> > > When I have a bad logon attempt, I would much prefer  
> > > to know the IP address of the offender -- if he's on my  
> > > network I can find him with that but if he is NOT on  
> > > my network I have no chance of finding him by NetBIOS  
> > > name or some other irrelevant information.  
> > >  
> > >  
> > > --  
> > > Herb Martin  
> > >  
> > >  
> > > >  
> > > > Thanks so much!  
> > >  
> > >  
> > >  
>  
>  
>
```