

microsoft.public.win2000.security: Re: All accounts get locked out!

Re: All accounts get locked out!

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-08/0580.html>

From: Erik Presnell (presnell_at_milltec.com)

Date: 08/06/03

Date: Wed, 6 Aug 2003 08:46:16 -0500

I am going through the same trouble now...I get alot of NTLM authentication problems and some kerberos issues where they are trying to use that as a service. I have no idea what causes it. I've been working on it about a week. You can try downloading the lockout tool analyzer. Alockout.exe
<http://microsoft.com/downloads/details.aspx?FamilyId=7AF2E69C-91F3-4E63-8629-B999ADDE0B9E&displaylan>

However it didn't give me much useful information. I would also enable Kerberos logging. That is where I'm at in my troubleshooting process. Let me know if you come up with anything. Thanks. BTW, this is my latest Kerberos event id message if anyone has any clues.

Event Type: Error

Event Source: Kerberos

Event Category: None

Event ID: 4

Date: 8/6/2003

Time: 7:14:58 AM

User: N/A

Computer: "An actual computer in my domain"

Description:

The function InitializeSecurityContext received a Kerberos Error Message:
on logon session

Client Time:

Server Time: 12:14:58.0000 8/6/2003 (null)

Error Code: 0x20 KRB_AP_ERR_TKT_EXPIRED

Client Realm:

Client Name:

Server Realm: mydomain.COM

Server Name: krbtgt/mydomain.COM

Target Name: krbtgt/mydomain.com@mydomain.COM

Error Text:

File:

Line:

Error Data is in record data.

Erik

Re: All accounts get locked out!

microsoft.public.win2000.security: Re: All accounts get locked out!

"Rohan" <gt_rohan@hotmail.com> wrote in message
news:eqiI2u\$WDHA.2360@TK2MSFTNGP12.phx.gbl...

> Hello,
>
> I have a Windows 2000 network with 3 domain controllers (Advanced Server)
> and about 50 Windows 2000 Professional clients.
> All the accounts get locked out, strangely, about three times a day. The
> frequency of this has increased. The account lockout policies are set to
> default only. I have checked the Domain Security Policy as well as the
> Default Domain Policy. I don't notice anything out of way.
> However, in Event log, I get messages like:
> Logon Failure:
>
> Reason: Unknown user name or bad password
>
> User Name: administrador
>
> Domain: BRBROWN
>
> Logon Type: 3
>
> Logon Process: NtLmSsp
>
> Authentication Package: NTLM
>
> Workstation Name: BRBROWN
>
> My domain name is GLOBALTECH, and there's no workstation named BRBROWN!!!
>
> I also get some messages like:
> Logon Failure:
>
> Reason: Account locked out
>
> User Name: harshal
>
> Domain: ISERVE
>
> Logon Type: 3
>
> Logon Process: NtLmSsp
>
> Authentication Package: NTLM
>
> Workstation Name: COMP21
>
> Here, the username is true, even though the domain name and workstation do
> not exist!!
>
> The above are Failure Audits.
> There are also success audits:

Re: All accounts get locked out!

microsoft.public.win2000.security: Re: All accounts get locked out!

> *Domain Policy Changed: Password Policy modified*
>
> *Domain: GLOBALTECH*
>
> *Domain ID: GLOBALTECH*
>
> *Caller User Name: NETFIN\$*
>
> *Caller Domain: GLOBALTECH*
>
> *Caller Logon ID: (0x0,0x3E7)*
>
> *Privileges: –*
>
> *and*
> *Kerberos Policy Changed:*
>
> *Changed By:*
>
> *User Name: NETFIN\$*
>
> *Domain Name: GLOBALTECH*
>
> *Logon ID: (0x0,0x3E7)*
>
> *Changes made:*
>
> *('--' means no changes, otherwise each change is shown as:*
>
> *<ParameterName>: <new value> (<old value>))*
>
> *--*
>
> *NETFIN is my main domain controller.*
> *I have Microsoft ISA on a domain controller called SERVER3.*
> *IIS isn't running anywhere on a live IP.*
>
> *Am I getting attacked?? Please help!!*
>
> *--*
>
> *Thank you,*
> *Rohan*
>
>
>

Re: All accounts get locked out!