

Re: Account Lockouts

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-02/0176.html

From: Steve Athanas (*stephen_athanas_at_NOSPAMHEREuml.edu*)

Date: 02/01/05

Date: Tue, 1 Feb 2005 16:39:10 -0500

It is not, but it hasn't caused any problems for anyone except me. Should I do that? I was under the impression that doing so is a security risk.

–Steve Athanas

"ptwilliams" <ptw2001@hotmail.com> wrote in message
news:uA2HGGKCFHA.904@TK2MSFTNGP12.phx.gbl...

> *Is this computer trusted for delegation?*

>

> *(to find out, right-click on the computer object and choose properties).*

>

> --

>

> *Paul Williams*

>

> <http://www.msresource.net/>

> <http://forums.msresource.net/>

>

> "Steve Athanas" <stephen_athanas@NOSPAMHEREuml.edu> wrote in message

> news:OhZPszJCFHA.4008@tk2msftngp13.phx.gbl...

> *Thanks for the reply!*

>

> *I checked that before I sent the message (I should have included that.)*

> *That's what's so confusing. None of the services in Service Manager show
> anything other than Local System or Network Service.*

>

> *Is there something that I'm missing?*

>

> –Steve

>

> "Allen Firouz" <AllenFirouz@discussions.microsoft.com> wrote in message

> news:46989BE0-ACB2-4DC0-9071-F64908A98C53@microsoft.com...

>> Steve,

>>

>> *I parsed through the logs you provided. Seems as though your account is*

>> *being locked out by an IIS service. Check to ensure that your account*

>> *isn't*

>> *being used by one of the IIS services on OWA or Exchange.*
>>
>> *-Allen Firouz*
>>
>> *"Steve Athanas" wrote:*
>>
>>> *Hello, everyone:*
>>>
>>> *I'm having some difficulty, and I'm hoping that someone out there has*
>>> *some*
>>> *insight. I have attached a lot of materials to this post, so if I refer*
>>> *to*
>>> *something, and you don't see it right away, just scroll down.*
>>>
>>> *Last week, I implemented an account lockout policy on our Windows Server*
>>> *2003 domain. Almost immediately, my account was locked out. I set the*
>>> *account lockout threshold to 5 attempts, over a 30 minute period, and to*
>>> *lock out indefinitely.*
>>>
>>> *I assumed that I had logged onto someone's machine and they had then*
>>> *typed*
>>> *in their password and locked me out. I unlocked my account and the*
>>> *server,*
>>> *and proceeded to work fine. A short while later (maybe an hour or two),*
>>> *I*
>>> *was locked out again. Thinking it a bit strange, given I hadn't really*
>>> *logged onto any other workstations with my domain admin account, I*
>>> *started*
>>> *investigating. I looked through the security logs, and it showed that my*
>>> *account was getting used by my Exchange Server, whose name in this*
>>> *document*
>>> *is changed to ExchangeSvr. I have included the output from one such*
>>> *invalid*
>>> *login in the security log on both Domain Controllers and ExchangeSvr. It*
>>> *notes that the caller is ExchangeSvr\$.*
>>>
>>> *Thinking it was a service logging on as me, I got the Lockout Tools from*
>>> *Microsoft, and installed the alockout.dll tool on my Exchange Server. I*
>>> *got*
>>> *some readouts, but cannot understand exactly what they are indicating.*
>>> *It*
>>> *seems that at the time of the Bad Password attempts, there is definitely*
>>> *some activity, but I don't know what it is indicating. It seems like the*
>>> *inetinfo.exe process is faulted by alockout.dll (see output from*
>>> *ExchangeSvr*
>>> *app log, first [bottom] event).*
>>>
>>> *I also started logging Netlogon attempts to all three servers (see below*
>>> *for*
>>> *output). Additionally, I have included the output from LockoutStatus.exe*
>>> *from Microsoft.*

>>>
>>> *Any help on this would be GREATLY appreciated, because I cannot seem to*
>>> *find*
>>> *what service is logging on as me, so I can correct the issue. I have*
>>> *checked*
>>> *every service on ExhcangeSvr, and cannot find anything other than "Local*
>>> *System" or "Network Service".*
>>>
>>> *If I can provide any more information, please let me know, and I will*
>>> *respond ASAP.*
>>>
>>> *Thank you for your time and assitance.*
>>>
>>> *-Steve Athanas*
>>> *MCSE (2003)*
>>>
>>>
>>> **REFERENCE MATERIALS**
>>>
>>>

>>> *******From Netlogon.log on DC1:**

>>>
>>> *02/01 09:33:19 [LOGON] DOMAINNAME: SamLogon: Transitive Network logon of*
>>> *(null)\username@domainname.local from EXCHANGESVR (via EXCHANGESVR)*
>>> *Entered*
>>> *02/01 09:33:19 [CRITICAL] NlPrintRpcDebug: Couldn't get EEInfo for*
>>> *I_NetLogonSamLogonWithFlags: 1761 (may be legitimate for 0xc000006a)*
>>> *02/01 09:33:19 [LOGON] DOMAINNAME: SamLogon: Transitive Network logon of*
>>> *(null)\username@domainname.local from EXCHANGESVR (via EXCHANGESVR)*
>>> *Returns*
>>> *0xC000006A*
>>>
>>>

>>> *******From Netlogon.log on DC2:**

>>>
>>> *02/01 09:33:10 [LOGON] DOMAINNAME: SamLogon: Transitive Network logon of*
>>> *(null)\username@domainname.local from EXCHANGESVR (via DC1) Entered*
>>> *02/01 09:33:10 [LOGON] DOMAINNAME: SamLogon: Transitive Network logon of*
>>> *(null)\username@domainname.local from EXCHANGESVR (via DC1) Returns*
>>> *0xC000006A*
>>> *02/01 09:33:10 [MISC] DOMAINNAME: DsGetDcName function called:*
>>> *Dom:(null)*
>>> *Acct:(null) Flags: DS*
>>> *02/01 09:33:10 [MAILSLOT] Received ping from DC2 domainname.local.*
>>> *(null)*
>>> *on*
>>> *<Local>*
>>> *02/01 09:33:10 [MAILSLOT] DOMAINNAME: Ping response 'Sam Logon Response*
>>> *Ex'*

```
>>> (null) to \\DC2 Site: SiteName on <Local>
>>> 02/01 09:33:10 [MISC] DOMAINNAME: DsGetDcName function returns 0:
>>> Dom:(null)
>>> Acct:(null) Flags: DS
>>>
```

```
-----
>>> *****From LockoutStatus.exe:
>>>
>>> Server Name,Site Name,User State,Bad Password Count,Last Bad
>>> Password,Pwd
>>> Last Set,Lockout Time,Original Lock
>>> DC2 [PDC],SiteName,Not Locked,0,2/1/2005 9:33:10 AM,1/26/2005 7:25:58
>>> PM,N/A,N/A
>>> DC1,SiteName,Not Locked,0,2/1/2005 9:33:19 AM,1/26/2005 7:25:58
>>> PM,N/A,N/A
>>>
>>>
```

```
-----
>>> *****From alockout.txt on ExchangeSvr:
>>>
>>> Tue Feb 01 09:33:10 2005, PID: 2240, Thread: 1600, Image
>>> C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE,ALOCKOUT.DLL -
>>> DLL_PROCESS_ATTACH
>>> Tue Feb 01 09:33:18 2005, PID: 2240, Thread: 1600, Image
>>> C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE,ALOCKOUT.DLL -
>>> dll_process_detatch
>>> Tue Feb 01 09:33:18 2005, PID: 4916, Thread: 5480, Image
>>> C:\WINDOWS\system32\inetsrv\inetinfo.exe,ALOCKOUT.DLL -
>>> dll_process_detatch
>>> Tue Feb 01 09:33:18 2005, PID: 5664, Thread: 4320, Image
>>> C:\WINDOWS\system32\iisreset.exe,ALOCKOUT.DLL - DLL_PROCESS_ATTACH
>>> Tue Feb 01 09:33:18 2005, PID: 2416, Thread: 1604, Image
>>> C:\WINDOWS\system32\inetsrv\iisrstas.exe,ALOCKOUT.DLL -
>>> DLL_PROCESS_ATTACH
>>> Tue Feb 01 09:33:18 2005, PID: 5040, Thread: 3168, Image
>>> C:\WINDOWS\system32\inetsrv\inetinfo.exe,ALOCKOUT.DLL -
>>> DLL_PROCESS_ATTACH
>>> Tue Feb 01 09:33:18 2005, PID: 2416, Thread: 3376, Image
>>> C:\WINDOWS\system32\inetsrv\iisrstas.exe, ***StartServiceW Failed!***
>>> (0),
>>> Service: Service: IIS Admin Service
>>> (C:\WINDOWS\system32\inetsrv\inetinfo.exe), RC was: Incorrect function.
>>> (1), GLE was: Overlapped I/O operation is in progress. (997)
>>> Tue Feb 01 09:33:19 2005, PID: 2416, Thread: 3376, Image
>>> C:\WINDOWS\system32\inetsrv\iisrstas.exe, ***StartServiceW Failed!***
>>> (0),
>>> Service: Service: Simple Mail Transfer Protocol (SMTP)
>>> (C:\WINDOWS\system32\inetsrv\inetinfo.exe), RC was: Incorrect function.
>>> (1), GLE was: Overlapped I/O operation is in progress. (997)
>>> Tue Feb 01 09:33:19 2005, PID: 2416, Thread: 3376, Image
>>> C:\WINDOWS\system32\inetsrv\iisrstas.exe, ***StartServiceW Failed!***
```

microsoft.public.windows.server.active_directory: Re: Account Lockouts

```
>>> (0),
>>> Service: Service: Microsoft Exchange Routing Engine
>>> (C:\WINDOWS\system32\inetsrv\inetinfo.exe), RC was: Incorrect function.
>>> (1), GLE was: Overlapped I/O operation is in progress. (997)
>>> Tue Feb 01 09:33:19 2005, PID: 2416, Thread: 3376, Image
>>> C:\WINDOWS\system32\inetsrv\iisrstat.exe, ***StartServiceW Failed!***
>>> (0),
>>> Service: Service: FTP Publishing Service
>>> (C:\WINDOWS\system32\inetsrv\inetinfo.exe), RC was: Incorrect function.
>>> (1), GLE was: Overlapped I/O operation is in progress. (997)
>>>
>>>
>>>
-----
>>> *****From Netlogon.log on ExchangeSvr:
>>> 02/01 09:33:10 [LOGON] SamLogon: Network logon of
>>> (null)\username@domainname.local from EXCHANGESVR Entered
>>> 02/01 09:33:10 [CRITICAL] NlPrintRpcDebug: Couldn't get EEInfo for
>>> I_NetLogonSamLogonEx: 1761 (may be legitimate for 0xc000006a)
>>> 02/01 09:33:10 [LOGON] SamLogon: Network logon of
>>> (null)\username@domainname.local from EXCHANGESVR Returns 0xC000006A
>>> 02/01 09:33:10 [MISC] In control handler (Opcode: 4)
>>> 02/01 09:33:19 [MISC] DsGetDcName function called: Dom:DOMAINNAME
>>> Acct:(null) Flags: DS NETBIOS RET_DNS
>>> 02/01 09:33:19 [MISC] NetpDcGetName: domainname.local. using cached
>>> information
>>> 02/01 09:33:19 [MISC] DsGetDcName function returns 0: Dom:DOMAINNAME
>>> Acct:(null) Flags: DS NETBIOS RET_DNS
>>> 02/01 09:33:19 [SITE] DsrGetSiteName: Site name 'SiteName' is old.
>>> Getting a
>>> new one from DC.
>>> 02/01 09:33:19 [MAILSLOT] NetpDcPingListIp: domainname.local.: Sent UDP
>>> ping
>>> to 192.168.1.11
>>> 02/01 09:33:19 [MISC] NlPingDcNameWithContext: Sent 1/1 ldap pings to
>>> DC1.domainname.local
>>> 02/01 09:33:19 [MISC] DsGetDcName function called: Dom:DOMAINNAME
>>> Acct:(null) Flags: DS NETBIOS RET_DNS
>>> 02/01 09:33:19 [MISC] NetpDcGetName: domainname.local. using cached
>>> information
>>> 02/01 09:33:19 [MISC] DsGetDcName function returns 0: Dom:DOMAINNAME
>>> Acct:(null) Flags: DS NETBIOS RET_DNS
>>> 02/01 09:33:19 [MISC] NlPingDcNameWithContext: DC1.domainname.local
>>> responded over IP.
>>>
>>>
-----
>>> *****From Application Log on ExchangeSvr:
>>>
>>> 2/1/2005 9:33:19 AM MSExchangeTransport Information Exchange Store
>>> Driver
```

microsoft.public.windows.server.active_directory: Re: Account Lockouts

>>> 332 N/A EXCHANGESVR SMTP service has been started, initializing queues.
>>> 2/1/2005 9:33:19 AM MExchangeTransport Information Routing
>>> Engine/Service
>>> 1008 N/A EXCHANGESVR RE service instance 1 has been started.
>>> 2/1/2005 9:33:19 AM MExchangeTransport Information Routing
>>> Engine/Service
>>> 1005 N/A EXCHANGESVR RE service has been started, Version:
>>> 6.5.7226.026.0.
>>> 2/1/2005 9:33:10 AM Microsoft Exchange Server Error None 1000 N/A
>>> EXCHANGESVR Faulting application inetinfo.exe, version 6.0.3790.0, stamp
>>> 3e8000f7, faulting module alockout.dll, version 0.0.0.0, stamp 3cb59a2a,
>>> debug? 0, fault address 0x0000be2c.
>>>
>>>

>>> *****From Security Log on ExchangeSvr:

>>>
>>> Event Type: Failure Audit
>>> Event Source: Security
>>> Event Category: Account Logon
>>> Event ID: 680
>>> Date: 2/1/2005
>>> Time: 9:33:10 AM
>>> User: NT AUTHORITY\SYSTEM
>>> Computer: EXCHANGESVR
>>> Description:
>>> Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
>>> Logon account: username@domainname.local
>>> Source Workstation: EXCHANGESVR
>>> Error Code: 0xC0000064
>>>
>>>
>>> For more information, see Help and Support Center at
>>> <http://go.microsoft.com/fwlink/events.asp>.

>>>
>>> Event Type: Failure Audit
>>> Event Source: Security
>>> Event Category: Logon/Logoff
>>> Event ID: 529
>>> Date: 2/1/2005
>>> Time: 9:33:10 AM
>>> User: NT AUTHORITY\SYSTEM
>>> Computer: EXCHANGESVR
>>> Description:
>>> Logon Failure:
>>> Reason: Unknown user name or bad password
>>> User Name: username@domainname.local
>>> Domain:
>>> Logon Type: 3
>>> Logon Process: Advapi

Re: Account Lockouts

>>> *Authentication Package: Negotiate*
>>> *Workstation Name: EXCHANGESVR*
>>> *Caller User Name: EXCHANGESVR\$*
>>> *Caller Domain: DOMAINNAME*
>>> *Caller Logon ID: (0x0,0x3E7)*
>>> *Caller Process ID: 4916*
>>> *Transited Services: -*
>>> *Source Network Address: -*
>>> *Source Port: -*
>>>
>>>
>>> *For more information, see Help and Support Center at*
>>> *<http://go.microsoft.com/fwlink/events.asp>.*
>>>
>>>

>>> ******From Security Log on DC1:*
>>>
>>> *Event Type: Failure Audit*
>>> *Event Source: Security*
>>> *Event Category: Account Logon*
>>> *Event ID: 680*
>>> *Date: 2/1/2005*
>>> *Time: 9:33:19 AM*
>>> *User: NT AUTHORITY\SYSTEM*
>>> *Computer: DC1*
>>> *Description:*
>>> *Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0*
>>> *Logon account: username@domainname.local*
>>> *Source Workstation: EXCHANGESVR*
>>> *Error Code: 0xC000006A*
>>>
>>>
>>> *For more information, see Help and Support Center at*
>>> *<http://go.microsoft.com/fwlink/events.asp>.*
>>>
>>>

>>> ******From Security Log on DC2:*
>>>
>>> *Event Type: Failure Audit*
>>> *Event Source: Security*
>>> *Event Category: Account Logon*
>>> *Event ID: 680*
>>> *Date: 2/1/2005*
>>> *Time: 9:33:10 AM*
>>> *User: NT AUTHORITY\SYSTEM*
>>> *Computer: DC2*
>>> *Description:*
>>> *Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0*
>>> *Logon account: username@domainname.local*

microsoft.public.windows.server.active_directory: Re: Account Lockouts

>>> *Source Workstation: EXCHANGESVR*
>>> *Error Code: 0xC000006A*
>>>
>>>
>>> *For more information, see Help and Support Center at*
>>> <http://go.microsoft.com/fwlink/events.asp>.
>>>
>>>
>>>
>
>
>