

re: Microsoft IPsec

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-02/msg00188.html>

- *From:* "jesse-rink@xxxxxxxx" <jesse-rink@xxxxxxxx>
 - *Date:* Mon, 11 Feb 2008 11:13:59 -0500
-

I agree that forcing complex password requirements would be the best way to go about this, but, unfortunately this won't work in the K12 district where this issue needs to be addressed. It boils down to our single domain architecture and not being able to provide one level of password complexities for K-5, 5-8, 9-12, and staff. Windows 2008 addresses this but, that's not on the horizon anytime soon. I wish Windows 2003 allowed different password complexity requirements for OUs. Setting up multiple domains solely to accommodate different password complexity requirements isn't going to be something I can get the higher-ups to agree to.

We are in process of securing the physical network against potential attacks for people "getting on the wires", but I just want to try and find a good way to minimize sniffing attacks on computers already on the network. We've taken MANY steps to reduce the chance of someone being able to run these tools on our machines (no admin access, making sure they can't boot from cd/usb drives, etc.) but I'm just trying to further minimize the exposure.

I'd think a simpler, and possibly more effective solution, would be to enforce effective password complexity requirements in your domain; make it very difficult to crack your passwords without dealing with all of the issues already described (while also physically securing your network so that potential attackers have a very limited chance to "get on your wires" to sniff internal traffic in the first place).

SC

On Thu, 7 Feb 2008, Jesse Rink wrote:

Perhaps I need to re-think this a bit.

My original intention for enabling IPsec was to prevent users from

re: Microsoft IPsec

sniffing Kerberos hashes. I was under the assumption based on the communication I had with several security "experts" from a couple consulting companies that IPsec could accomplish this.

What I'm here from Rodrigo and Scott, is that IPsec cannot encrypt the packets containing Kerberos hashes that are sent over the network between the XP client and domain controller. Is this correct?

I am not so concerned with encrypting traffic between the clients and members servers or emails servers as I am with encrypting traffic that contains the Kerberos hashes which users can sniff and then hack offline.

Comments welcome. .. Paul? Rodrigo? Scott?

Thanks.

J

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

From: listbounce@xxxxxxxxxxxxxxxxxxxxx

[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx] On Behalf Of Ramsdell, Scott

Sent: Thursday, February 07, 2008 8:36 AM

To: Jesse Rink; Paul J. Brickett

Cc: security-basics@xxxxxxxxxxxxxxxxxxxxx;

security-basics-return-47647@xxxxxxxxxxxxxxxxxxxxx

Subject: RE: Microsoft IPsec via group policy

JR,

Requiring ipsec between a client and a DC via GPO is problematic.

You'll have much more success allowing the initial auth to the domain via Kerberos, then using ipsec to secure communication from the client machine to the file/email servers.

From Microsoft: Currently, we do not support the use of IPsec to encrypt

network traffic from a domain client or member server to a domain controller when you apply the IPsec policies by using Group Policy or when you use the Kerberos version 5 protocol authentication method.

<http://support.microsoft.com/kb/q254949/>

You're putting the cart before the horse, so to speak, by requiring ipsec communication before your client machines can auth and read the GPO that requires the ipsec.

Kind Regards,

re: Microsoft IPsec

re: Microsoft IPsec

Scott Ramsdell
CISSP CCNA MSCE

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

From: listbounce@xxxxxxxxxxxxxxxxxxxxx
[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]
On Behalf Of Jesse Rink
Sent: Wednesday, February 06, 2008 8:04 AM
To: 'Paul J. Brickett'
Cc: security-basics@xxxxxxxxxxxxxxxxxxxxx;
security-basics-return-47647@xxxxxxxxxxxxxxxxxxxxx
Subject: RE: Microsoft IPsec via group policy

Hello.

Sorry for the delayed response. For some reason when I post on this list, my posts sometimes don't show up for 16-30 hours. Not quite sure why.

What I'm attempting is to encrypt network traffic between my clients and my domain controllers and clients and my member servers.

I have tried setting IPsec up in group policy however I'm running into some strange issues. What I've done to set this up for testing is this...

1. In the Domain Controllers OU and GPO, I set the IP Sec policy for Server (request security) – Assigned.
2. In the test PC OU and GPO, I set the IP Sec policy for Client (respond only) – Assigned.

At this time, I think I should be good to go. I go to the XP client and do a gpupdate /force and reboot the computer. Now, here's what's odd.

According to documentation I've read, I should be able to tell the IP Sec policy applied to the client in the following ways:

1. I should be able to do an RSOP.msc from Start|Run on the XP client and see the IP Sec policy. I try that, but nothing shows up.
2. I should be able to look at the Local Security Policy on the XP client and it should show that IP Sec policy has been applied from a GPO. I try that, but nothing shows up.

I am starting to wonder if the documentation I've read is WRONG about these things. I have noticed this... If I look on the XP Client's registry, under HKLM\SOFTWARE\Policies\Microsoft\Windows\IPsec\GPTIPSECPolicy and

re: Microsoft IPsec

under HKLM\SOFTWARE\Policies\Microsoft\Windows\IPsec\Policy\Cache, I
"DO" find that these keys are created/updated after doing the gpupdate

/force and

rebooting, so it SEEMS like IPsec is getting applied? But again,
RSOP.msc
and the Local Security Policy show NOTHING. Why is this?

Also, I am testing what happens if the IPsec policy on the client is
unapplied. This is very strange as well. If after having applied the
IP Sec policy via GPO to the XP Client, I remove it a short time later
by going into the GPO for the PC OU, and changing Client (respond
only) to Unassign, when I then go to the XP client and do a gpupdate
/force and then reboot, the XP client can no longer contact the domain
controller. I can't even
ping it, nor can the domain controller ping the client. This doesn't
make
sense. I am removing the IP Sec policy from the client "by the book"
as far as I can tell by unassigning it first, and then making sure the
new GPO is applied to the PC. Any idea on this particular issue?

I'm about ready to open up a case with Microsoft to figure this stuff
out.

Thanks for any help.

JR

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

From: listbounce@xxxxxxxxxxxxxxxxxxxxx
[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]

On

Behalf Of Paul J. Brickett

Sent: Tuesday, February 05, 2008 11:02 AM

To: jesse-rink@xxxxxxxxxx

Cc: security-basics@xxxxxxxxxxxxxxxxxxxxx;
security-basics-return-47647@xxxxxxxxxxxxxxxxxxxxx

Subject: Re: Microsoft IPsec via group policy

What exactly are you trying to do? Providing detail to the group may
elicit more responses.

I've deployed several IPsec GPOs- I generally have used IPsec GPOs to
more granularly block/allow access to specific ports/protocols. I find
that it's a more precise tool than Windows Firewall. I often find
myself comparing it to IPTables.

-PJB

re: Microsoft IPsec

re: Microsoft IPsec

On Mon, 4 Feb 2008, jesse-rink@xxxxxxxx wrote:

Just curious if anyone on the list has implemented IPsec for Windows 2003/XP via Group Policy? I am testing this out and finding some

strange

results that I'd like to bounce off someone who's done this before. Anyone?

JR

mail2web.com – Enhanced email for the mobile individual based on

MicrosoftR

Exchange – <http://link.mail2web.com/Personal/EnhancedEmail>

mail2web LIVE ? Free email based on Microsoft® Exchange technology – <http://link.mail2web.com/LIVE>