Auditing Windows machines from Linux using SMB2

Background

For those that aren't aware, SMB1 (Server Message Block v1) has effectively been deprecated by Microsoft. SMB1 is seen as having too many security issues, is disabled by default on all new installs and has been patched by Microsoft to turn it off. Windows machines from Vista / 2008 onwards support SMB2. Windows XP / 2003 and older do not support SMB2.

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

NOTE - This page only concerns Open-AudIT running from a Linux server and auditing Windows machines. If you use Open-AudIT *installed* on a Windows machine, you are free to ignore this.

Redhat / Centos 6 issue

Because of this SMB2 requirement, going forward ***support for running Open-AudIT as a server on Centos 6 / Redhat 6 will be deprecated***. The Samba version shipped on those Operating Systems is too old to include SMB2 support. There is a package called samba4-client, but this conflicts with the regular samba package. Hence the deprecation of supporting Centos / Redhat 6 in the short term future.

UPDATE - There is a work-around available for getting SMB2 support on RedHat / Centos 6. This is specifically not enabled by default or in the installer. This could possibly cause Samba to stop working on your Open-AudIT server, so if you are using that server for services other than Open-AudIT, I can't say I'd recommend this. But if Open-AudIT is the only service on your Redhat / Centos 6 machine, read on.

First you'll need to remove the old Samba packages.

```
yum erase samba-common samba-libs samba-client
```

Next installe the newer packages.

```
 yum install samba4-common samba4-client
```

I'd still very much recommend upgrading to Centos / RedHat 8 instead.

How does this affect Open-AudIT?

When Open-AudIT runs on a ***Linux*** server, we use a small utility called winexe to enable us to start processes on the target Windows machines (ie, start the audit_windows.vbs script). Unfortunately winexe uses old Samba sources that are not compatible with SMB v2 or above. "So just recompile it", I hear you say. Hold on there Tex, that won't work either. The new sources have changed a LOT and recompiling against them as-is simply does not work. Having said that, Opmantek have spent the time to be able to get winexe running against SMB2 using newer Samba. It wasn't easy and it has a large caveat. The "new" winexe will not talk to SMB1.

One step forward, two steps back. Sigh.

Going Forward

We do have a solution that will be in an upcoming version of Open-AudIT. Our work-around is to ship both versions of winexe. When we discover a Windows machine we will attempt to connect using the "new" winexe using SMB2 as a first preference. If that fails (and only if that fails) will we attempt to connect using the old winexe and SMB1.

Short Term Fix

"Yeah, yeah, but I can't audit my Windows machines NOW.... help!".

Well, in fact we can do something right now. That should be that YOU can do something right now. Linked from this wiki page (see bottom of page) is the new version of winexe. You can replace your old version and test it against Windows machines that have SMB1 disabled.

NOTE - This will have the effect of NOT working against Windows XP / 2003 machines and older. The actual fix when we ship (as detailed above) will resolve that.

First, move the existing winexe out of the way

```
mv /usr/local/open-audit/other/winexe-static /usr/local/open-audit/other/winexe-static-old
```

Now save the winexe linked from this page into:

```
/usr/local/open-audit/other/winexe-static
```

And try auditing a previously failing Windows machine. If it works, great. If not - check the discovery logs.

To revert the change:

```
mv /usr/local/open-audit/other/winexe-static /usr/local/open-audit/other/winexe-static-new
mv /usr/local/open-audit/other/winexe-static-old /usr/local/open-audit/other/winexe-static
```

You can download a copy of the new winexe from: http://dl-openaudit.opmantek.com/winexe-static