Force SMB3 encryption

server smb encrypt = required ## This is a Auxillary parameter to be set individually on every share

client smb encrypt = required ## this is a global configuration to be set in Services -> SMB

Run these two commands to verify SMB signing is required

"nmap --script smb2-security-mode.nse -p445 <ip address>"
"nmap -p 139 --script smb2-security-mode <ip address>"

Capture packets in WireShark to confirm the data is actually encrypted

There are two places the you should configure SMB encryption. In the Global SMB or Samba configuration, and on each SMB share. Both are done within the TrueNAS settings. First, you want to configure your SMB or Samba service with the folowing two auxiliary parameters:

```
server signing = required
client smb encrypt = required
```

This will do two things. First, it enables server signing of each SMB packet sent. The server will sign each data packet with a hash of that packet, thus alerting the client computer if the data packet is changed in transit. Second, it will enable smb encryption globally, but will not turn it on, each share still needs to be told to use encryption. You can also set

```
client smb encrypt = desired
```

if you do not want to prevent clients that do not support encryption from accessing the share.

Clients that do not support SMB encryption will not be able to connect to the share. By default, clients should be attempting to negotiate encryption when connecting, but I prefer to force it for all clients. Almost all modern devices capable of connecting to an SMB share will support SMB encryption. These are the global parameters. Next the local parameters.

On the configuration page of each share you can set:

```
smb server encrypt = required
```

This allows you to force encryption of each share individually. Again, clients that do not support SMB encryption will not be able to connect. You can also set:

```
smb server encrypt = desired
```

This will set clients to use encryption if possible, but will not lock out clients that do not support encryption. In all cases, you must set encryption globally and on each share. smb server encrypt can be used as a global parameter in some samba iterations, but TrueNAS requires it be set on a share by share basis.

You can use

```
server smb encryption algorithims = *
```

This allows you to specify which algorithims are used, or not used. for example

```
server smb3 encryption algorithms = -AES-128-GCM -AES-128-CCM
```

Should remove the algorithims from use. I have chosed to remove the 128 bit algorithims that are in use by default. You can see the - symbol prefix.

Go into the shell as root and run `smbstatus`

This should tell you all open SMB sessions, and if those are encrypted.

You can confirm this by using a Wireshark, or other packet sniffer, on and SMB share before and after enabling these.

This webpage https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html shows detailed explinations of all possible SMB configuration options. I highley recommend forcing the use of SMB encryption on your TrueNAS ASAP. Encryption of data in flight is a good thing. This guide will apply to both Scale and Core.

Revision #4
Created 22 December 2023 01:58:46 by ColtM
Updated 6 September 2024 22:50:35 by ColtM