

Lab 4-6 Using the File Signature Verification Utility

Purpose of Lab: To understand how to verify the device driver signatures.

Learning Targets

- Understand file signature verification
- Learn how to look up system files

Checkoff Success Criteria—have you met your mark?

Tory Check	You check	
		Add PowerShell
		Run Sigverif
		Look up nvmpu401.sys
		Answer questions

Directions

1. Log into your server as an administrator. Use either your host server or one of your ADDCs, but choose one which you have NOT turned off driver signing on, or turn it back on. Just go through the same steps to turn it back on.
2. Open the run command.
3. Type **sigverif** and hit return.
4. The File Signature Verification tool will start. It is going to test all the drivers in your system to make sure they signed. This is often used after upgrading a system, where drivers have not been tested for signing.
5. Click start.
6. When it is done you get a list of unsigned drivers. Mine had ONE unsigned driver. To see the log, click the advanced button.
7. What did it save the log as? _____
8. Open that file. Print it out. **Attach to your logs.**
9. My unsigned file is **nvmpu401.sys**. Go online and look up that file. Where does it come from?

10. Should I be concerned?

11. If I do not want any drivers unsigned on my system, what should I do?

Turn in the following:

- ☞ Attach the SIGVERIF.TXT