Lab 4-5 Driver Signing Options

Purpose of Lab: To understand driver signing options and be able to disable driver signing to install an older driver.

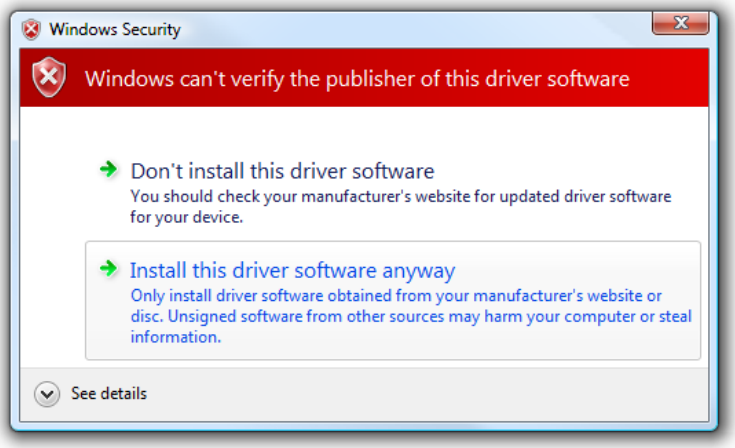
Learning Targets

- Understand driver signing
- Understand how to turn driver signing on and off

Checkoff Success Criteria—have you met your mark?

Tory Check	You check	
		Configure your server to warn if someone tries to install a driver that is not signed
		Fill out table
		Use BCDedit to change the driver signing
		Show me the command
		Attach screenshot
		Answer questions

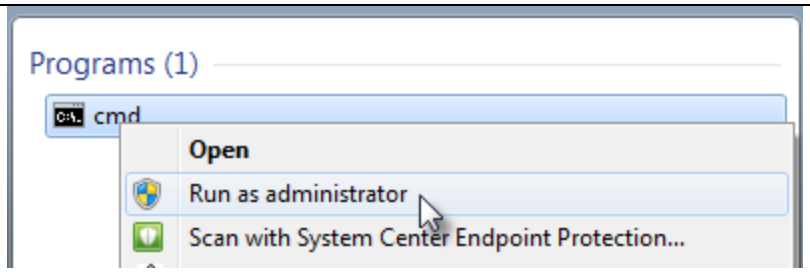
Windows security requirements want you to install only signed drivers. A signed driver contains a confirmed piece of code and verifies that the driver has been tested and is safe. If the driver has been modified since the testing, or has not been tested you will see a warning box that looks like this:

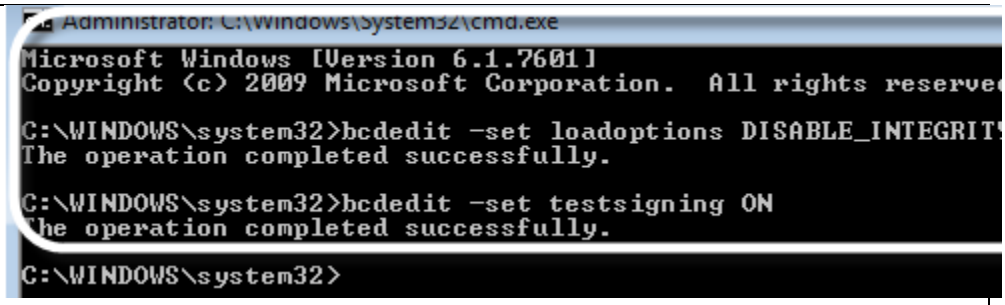


Supposedly in Windows 8 and Server 2012 you can't install unsigned drivers at all. Best practices are that you set your network to block ALL unsigned drivers so your users do not install unsigned drivers. However, in case you want to go ahead and live on the edge…here's how you can disable driver signing in Server 2008 R2.

Directions

1. Boot into your Server 2008 as an administrator.
2. Configure it to warn if someone tries to install a driver that is not magically signed by Microsoft.
3. Right click on Command Prompt and Run As Administrator

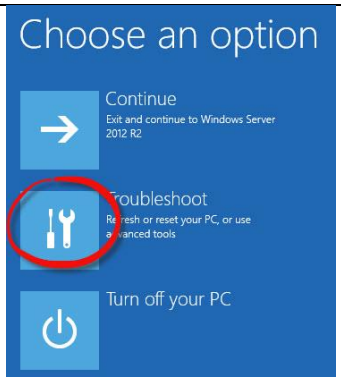


4. Type the following command: 5. **bcdedit -set loadoptions DISABLE_INTEGRITY_CHECKS** 6. Hit enter. Now type 7. **bcdedit -set TESTSIGNING ON** 8. Hit enter 9. **Take a screenshot.**	 You have just used a program called BCDEDIT. Boot Configuration Data (BCD) files provide a store that is used to describe boot applications and boot application settings. The objects and elements in the store effectively replace Boot.ini. BCDEdit is a command-line tool for managing BCD stores. It can be used for a variety of purposes, including creating new stores, modifying existing stores, adding boot menu options, and so on. BCDEdit serves essentially the same purpose as Bootcfg.exe on earlier versions of Windows.
10. Now if you attempt to install a driver that is not digitally signed, it will allow you. NOTE: this is a risky venture on a server and a good network administrator probably would not do this. However, there you go.	

Now let's try the same thing in Windows 8 and see if it works.

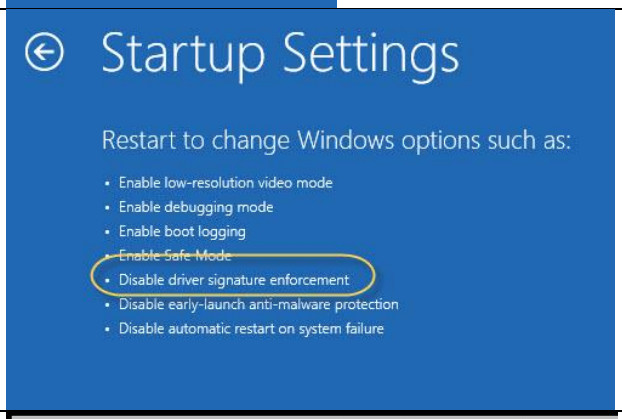
According to Microsoft if you want to disable driver signing in Server 2012 or Windows 8 you can just suck it, but this guy here http://thephuck.com/end-user-computing/how-to-disable-driver-signing-requirement-in-windows-8/ has figured out a way how to do it, so let's give it a whirl! Unfortunately his directions are dated, so I had to go figure out the new way to do it so what WAS going to take me three minutes (fixing this lab) took me a few hours when it didn't work. It's all good now! I tested it on Windows 8.1 and on Server 2012.	
1. When might you need to do this? Well let's say you have an old piece of hardware and it works but the company hasn't created a driver that works with Windows 8.1 so you're out of luck due to no updates. You can try to install the old one using this trick.	
2. Shut down all programs and everything. 3. In Server 2012 R 2 or Windows 8.1 type the following at the command prompt. 4. Open the Run command and type **shutdown /r /o /t 0** 5. Hit return 6. This will force a reboot with options (that's what the –o does).	

7. It's going to ask you what you want to do. On the first screen click **Troubleshoot**.

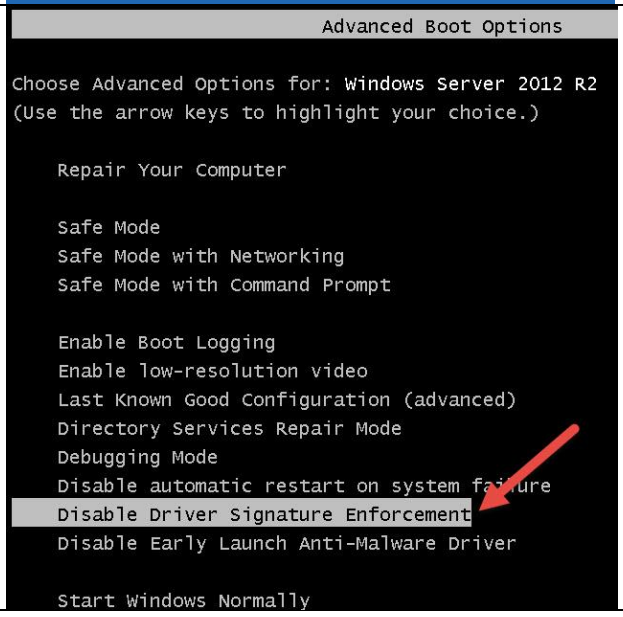


8. Now click **Startup Settings.**

9. On the next screen it lists the things you'll be able to do when you restart. Notice one is to be able to disable driver signing.
10. Go ahead and click restart.



11. When you restart you're going to get a black screen with white lettering.
12. Read the screen until you find Disable Driver Signature Enforcement.
13. Hit your down arrow until you get to it, hit return to start Windows,
14. Now Driver Signing will be disabled.
15. Now go answer questions.



Questions

1. When might you want to disable driver signing?	
2. What is Microsoft's "Best Practice" for driver signing?	
3. What is the benefit to the network security of having the driver signed?	
4. Why can this be a hassle for you, the administrator?	
5. When you are an administrator someday, how do you think you'll handle driver signing in a real world situation? Will you require all drivers to be signed or will you allow non-signed drivers?	
Clarify your answer from the question above in two paragraphs.	