System Hardening

Paul G. Gurke

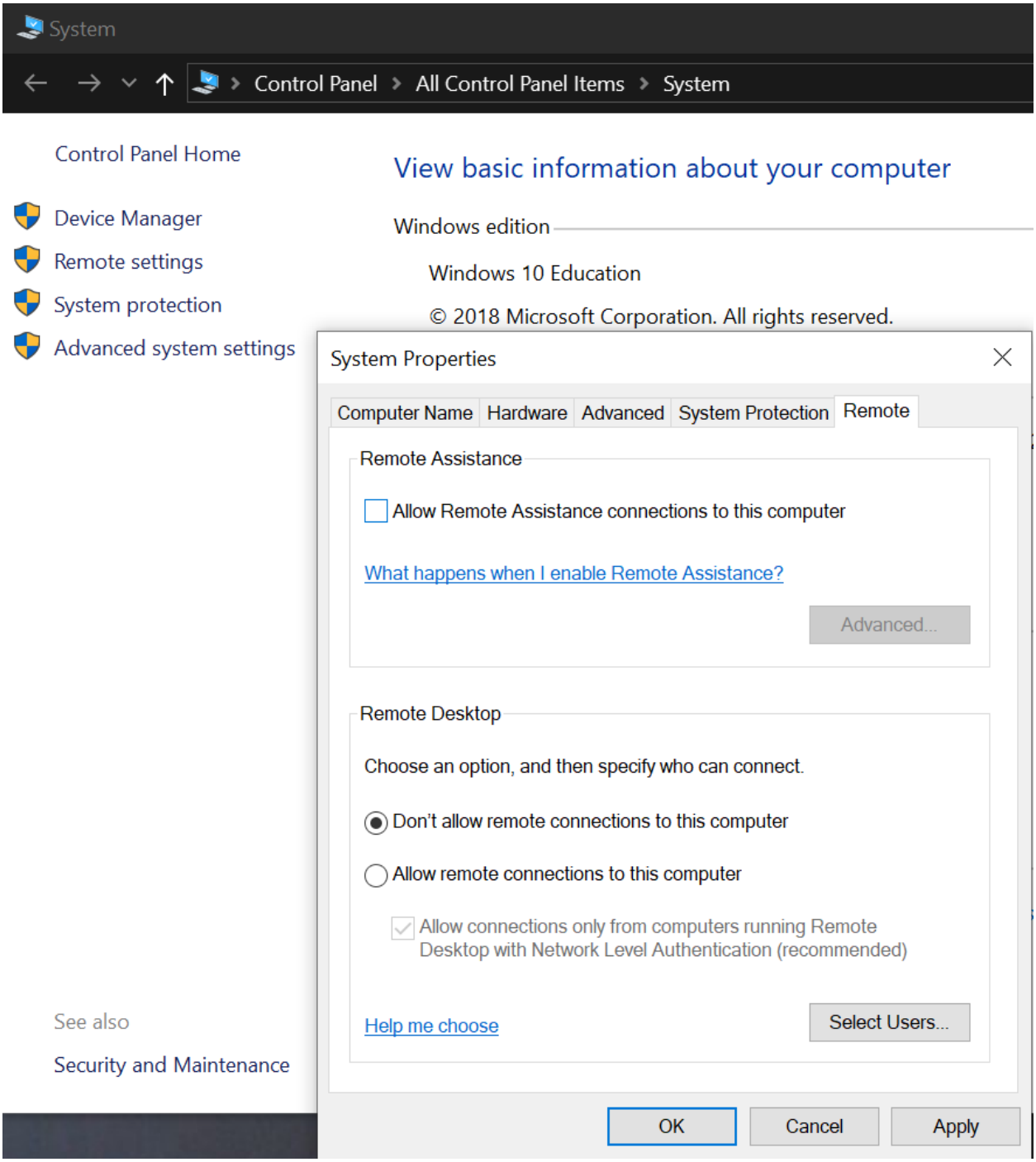
University of Advancing Technology

System Hardening

This document shows steps taken to harden a Windows 10 Operating System.

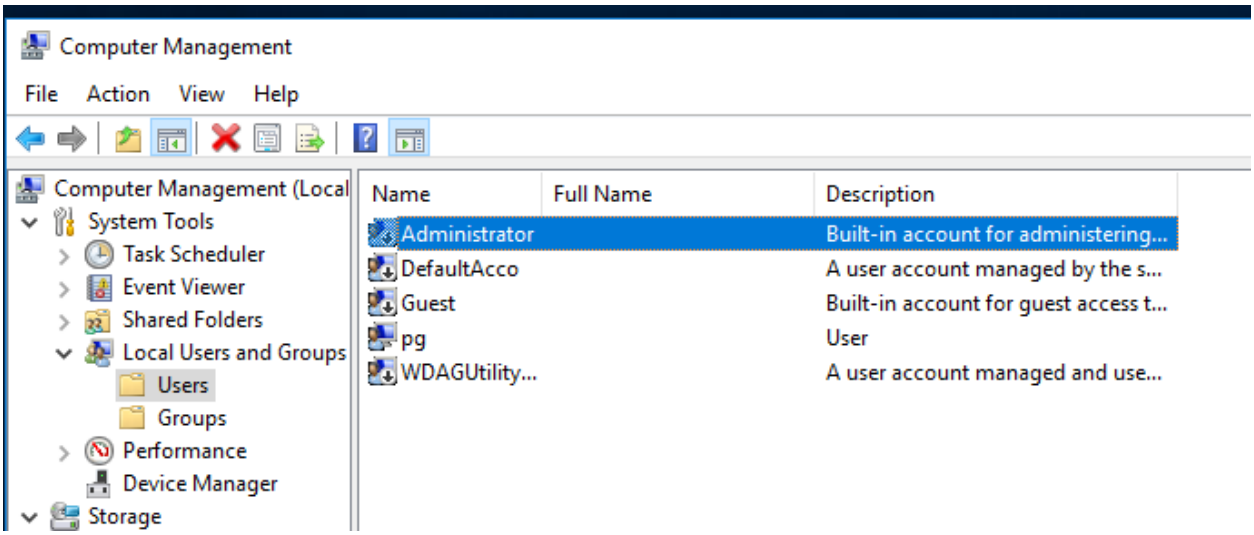
Disabling Remote Access

Surprisingly, Remote Assistance is enabled by default. Chose to uncheck “Allow Remote Assistance […]” and select “Don’t allow […]” in the remote tab of system properties.


System
Control Panel > All Control Panel Items > System
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
View basic information about your computer
Windows edition
Windows 10 Education
© 2018 Microsoft Corporation. All rights reserved.
See also
Security and Maintenance
System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Remote Assistance
Allow Remote Assistance connections to this computer
What happens when I enable Remote Assistance?
Advanced...
Remote Desktop
Choose an option, and then specify who can connect.
Don't allow remote connections to this computer
Allow remote connections to this computer
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)
Help me choose
Select Users...
OK
Cancel
Apply

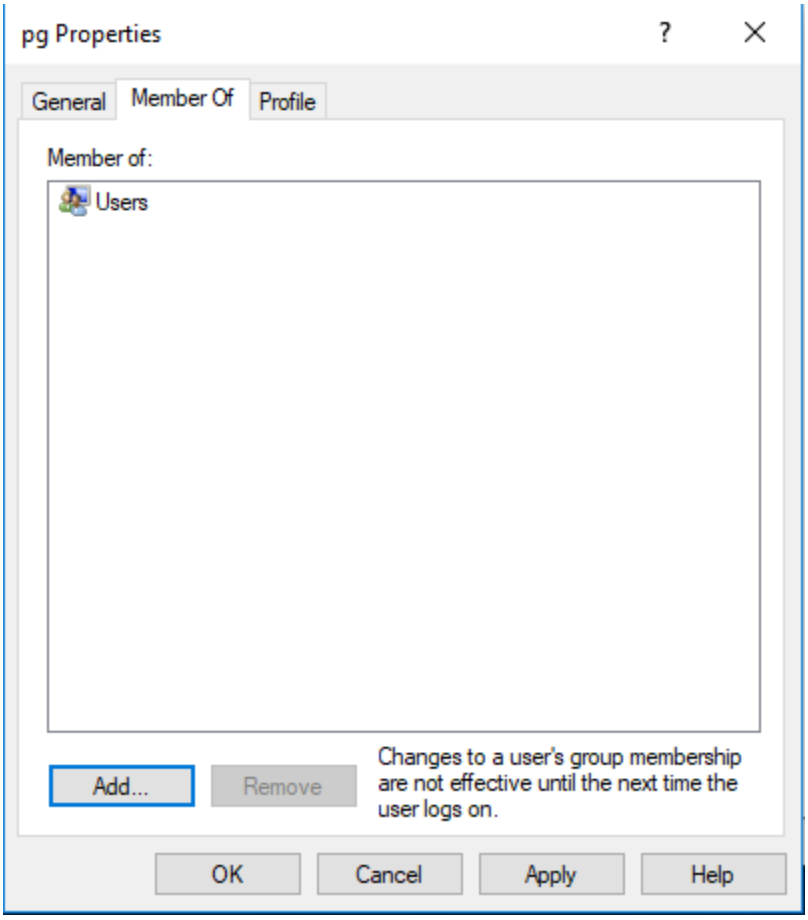
Deleting Unnecessary Accounts

Make sure there are no active unused local accounts. (This host is a member of a domain.)



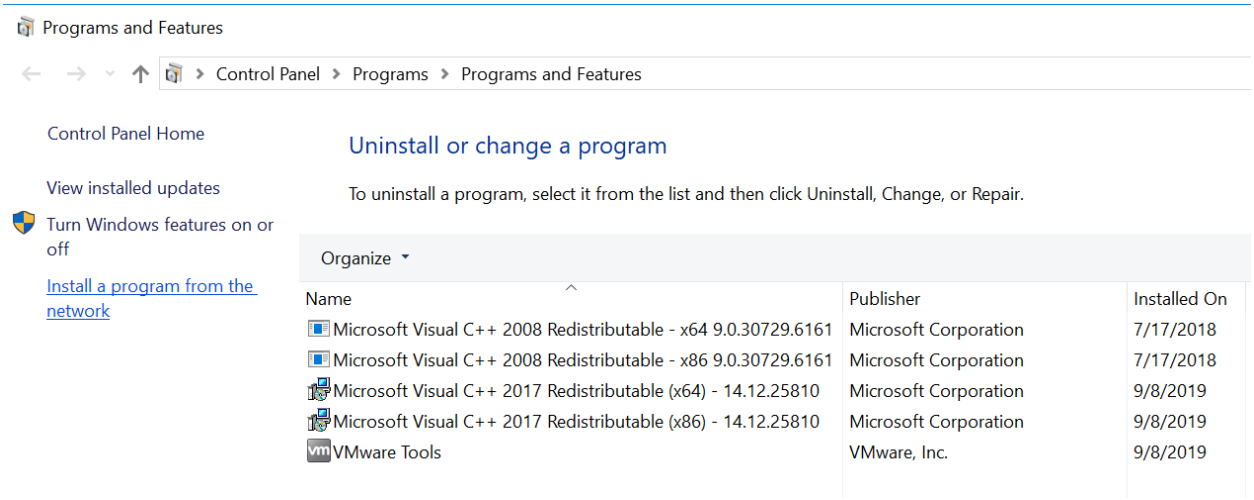
Create a Lower Than Admin Account

Ensure that the remaining user account is not an administrator.



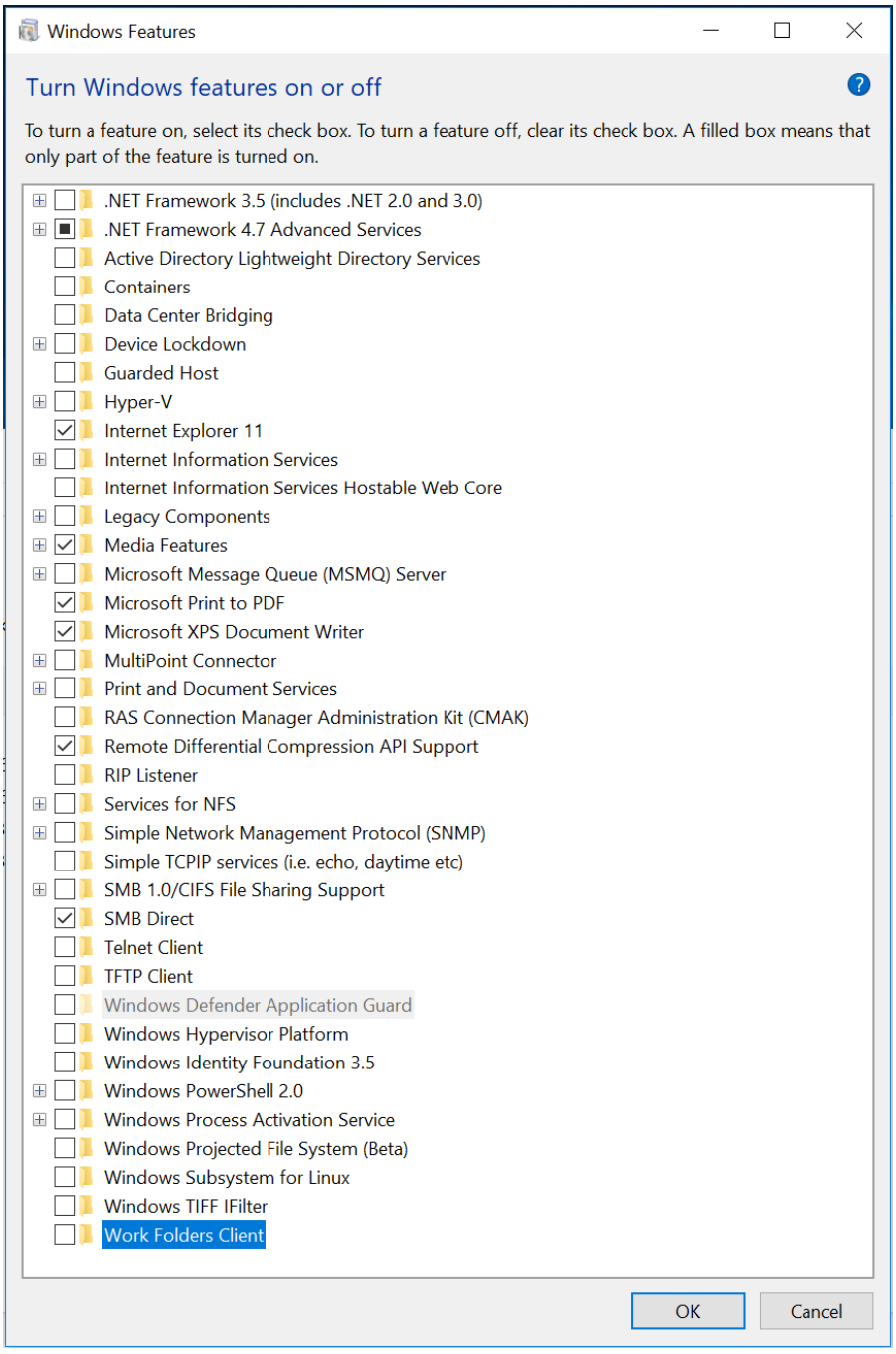
Removal of Unnecessary Applications

This is what remained after I removed all but what I thought were necessary for core functionality.



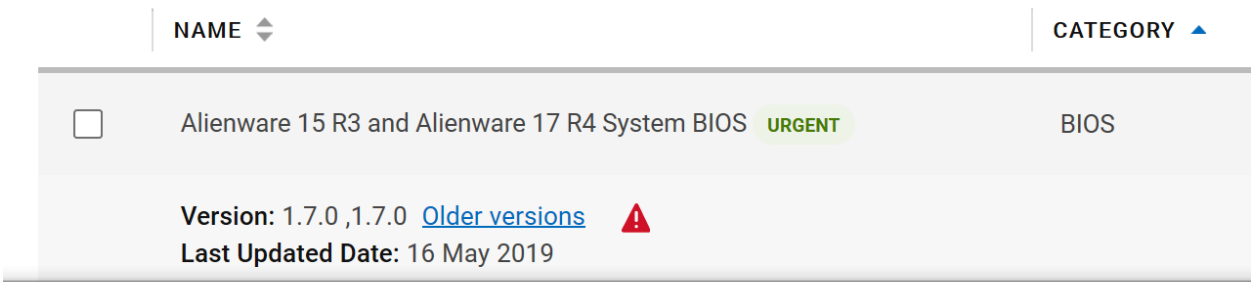
Turn Off Unused Features

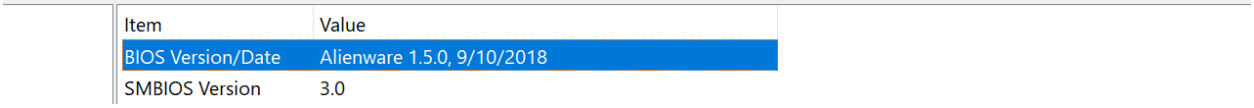
Navigate to “Turn Windows features on or off” and make sure that .net 3.5, SMB v1 and PowerShell 2 are unchecked.



BIOS Update

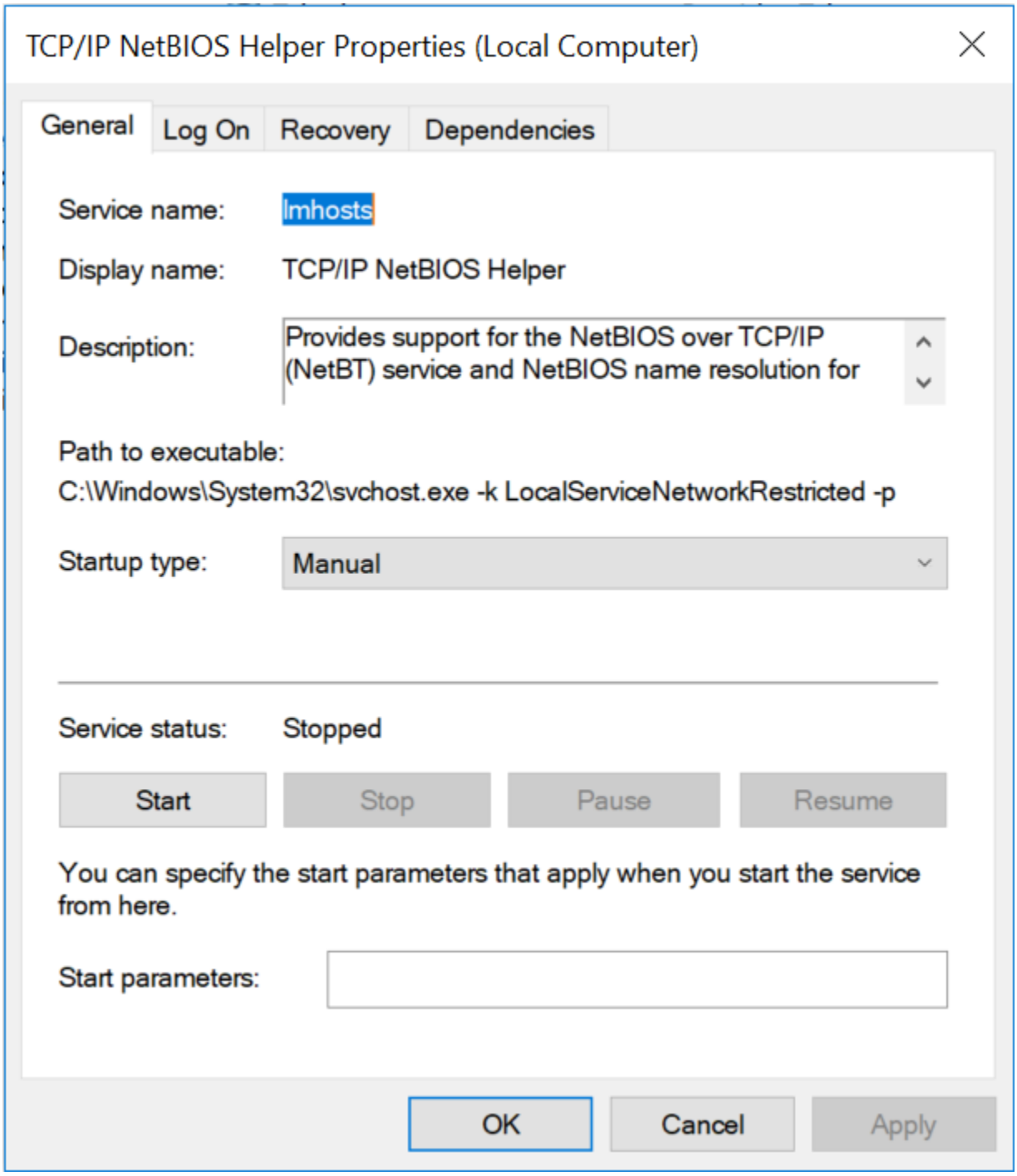
Update BIOS through computer or motherboard manufacturer. In this case, I went to Dell to get the latest BIOS update.





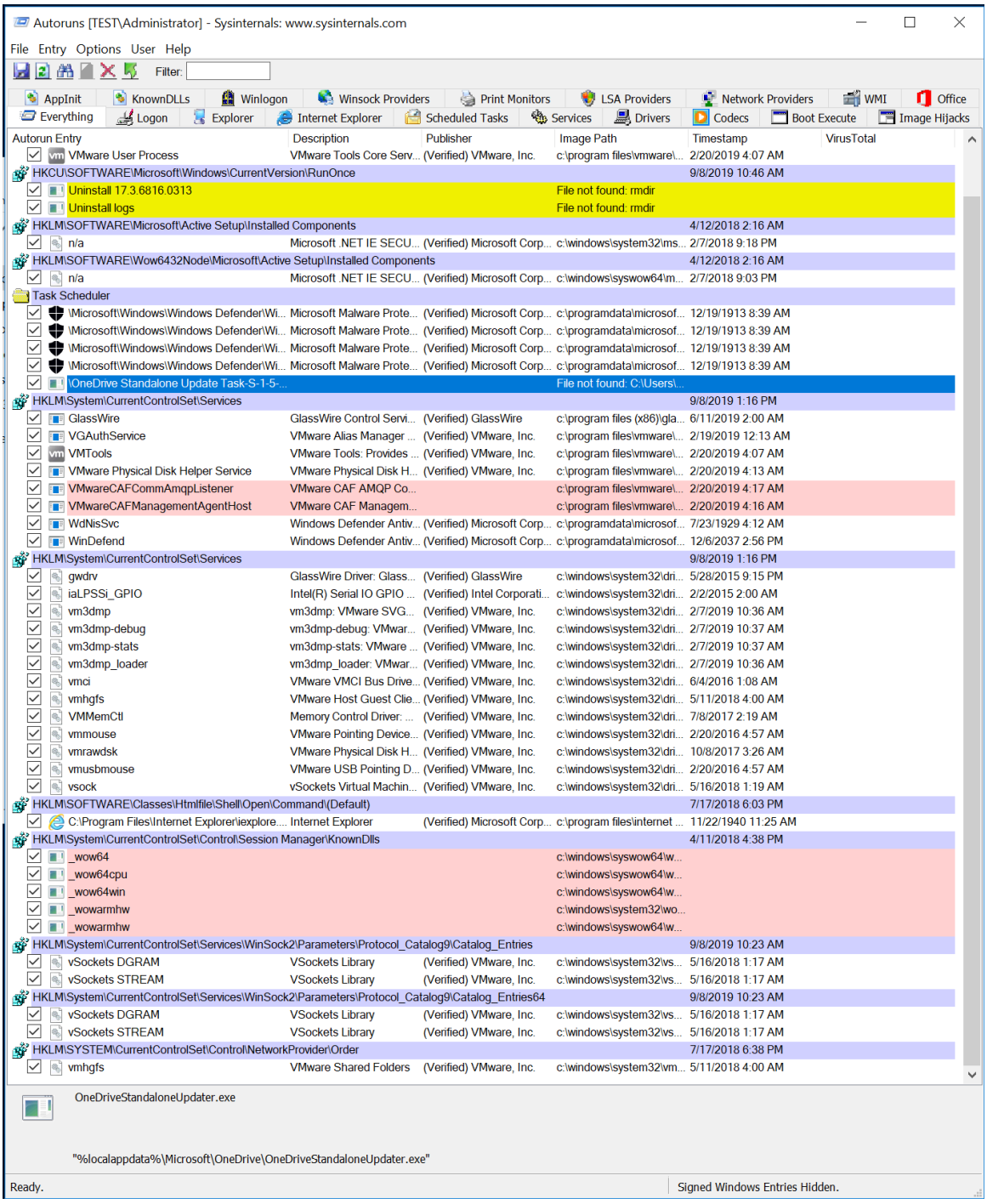
Stop TCP/IP NetBIOS Helper

Navigate to services via Run: services.msc and stop the TCP/IP NetBIOS Helper.



Autoruns (Sysinternals)

If the Sysinternals suite is available, run “Autoruns” to identify what is being ran automatically. On the machine I checked, I could see that even though OneDrive was uninstalled in a previous step (and restarted since), there was still a triggered task to run an update.



Remove Unused Shares

Check the shares with the Net Share command to ensure that there are no unutilized shares.

```
C:\Users\administrator>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.
```

Drive Encryption

To enable security control to your physical drives, BitLocker Drive Encryption can be turned on to encrypt your data. This even includes your running operating system.