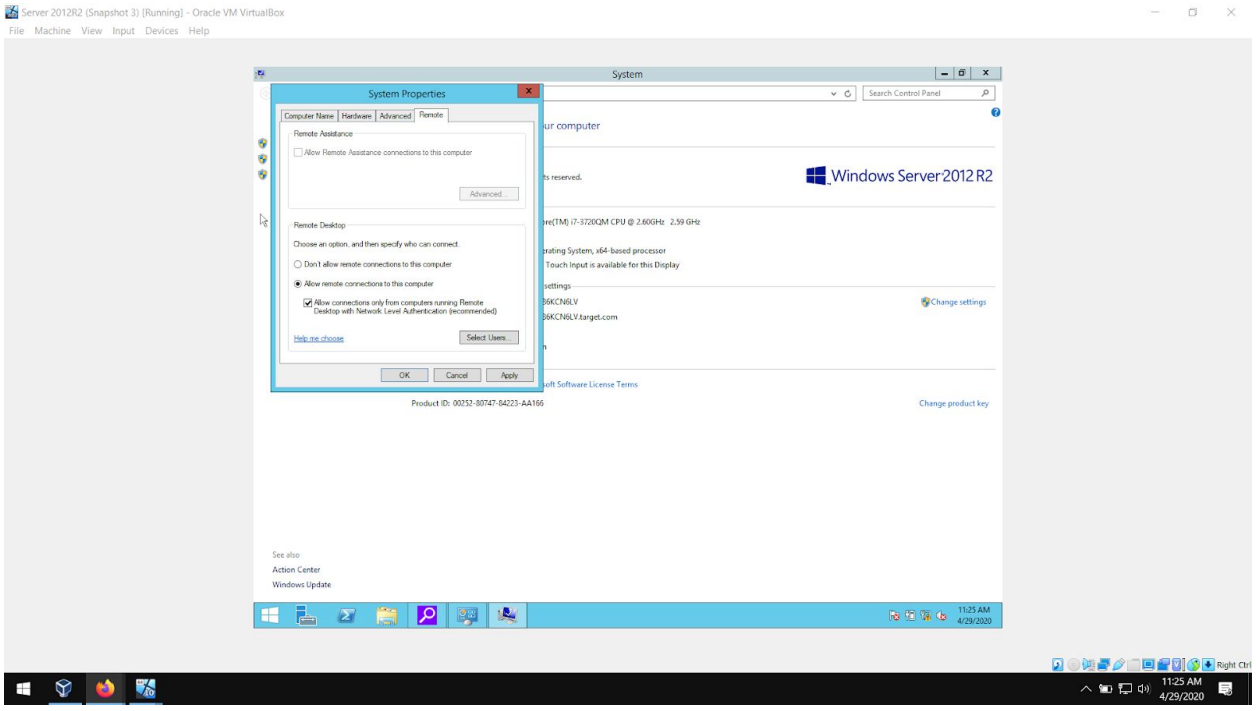
Cyber Report: Remote Desktop

1. Each assignment has a goal. What is the assignment and how will you find the solution?

> The purpose of this lab is to create a Remote Desktop Connection between two virtual machines installed locally via VirtualBox. The connection will be made using Microsoft's Remote Desktop Connection (mstsc), which utilizes Remote Desktop Protocol (RDP). Windows Server 2012 R2 is a Domain controller and will host the second virtual machine, a virtual instance of Windows 10 Professional.

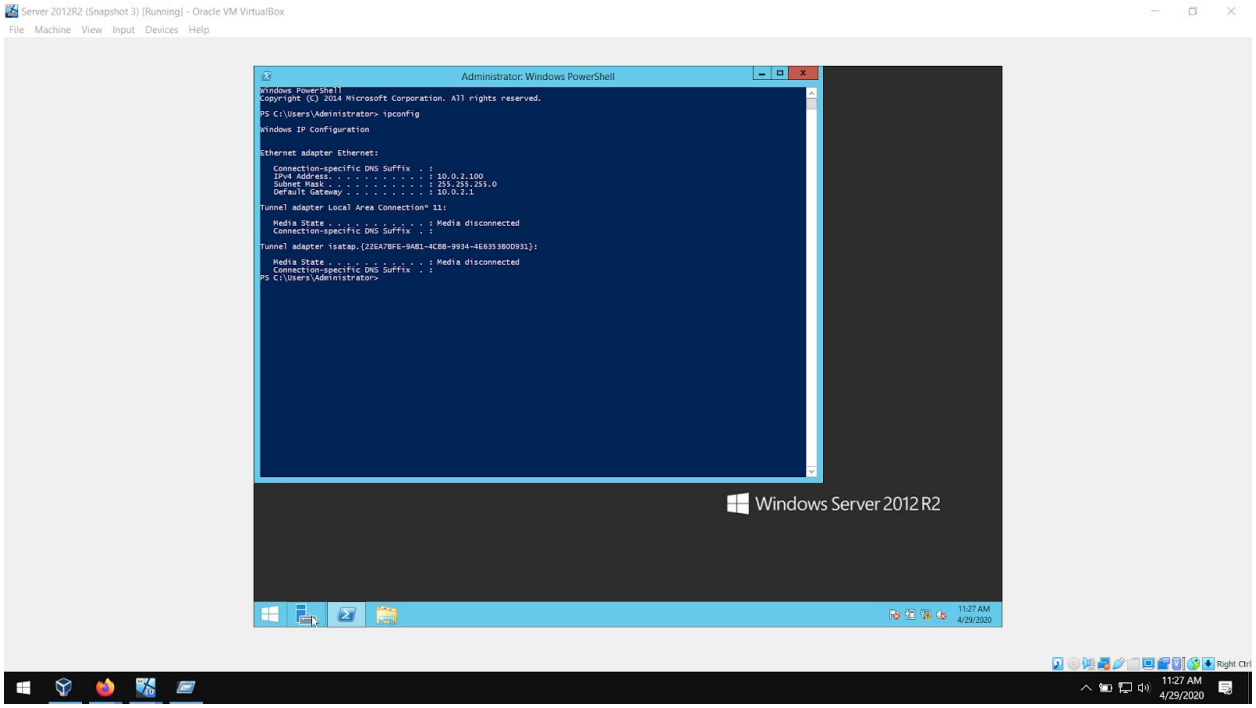
2. Demonstration of the steps taken with screenshots (snipping tool) from your computer. You need to show the steps you took as you took them.

Windows Server 2012 R2



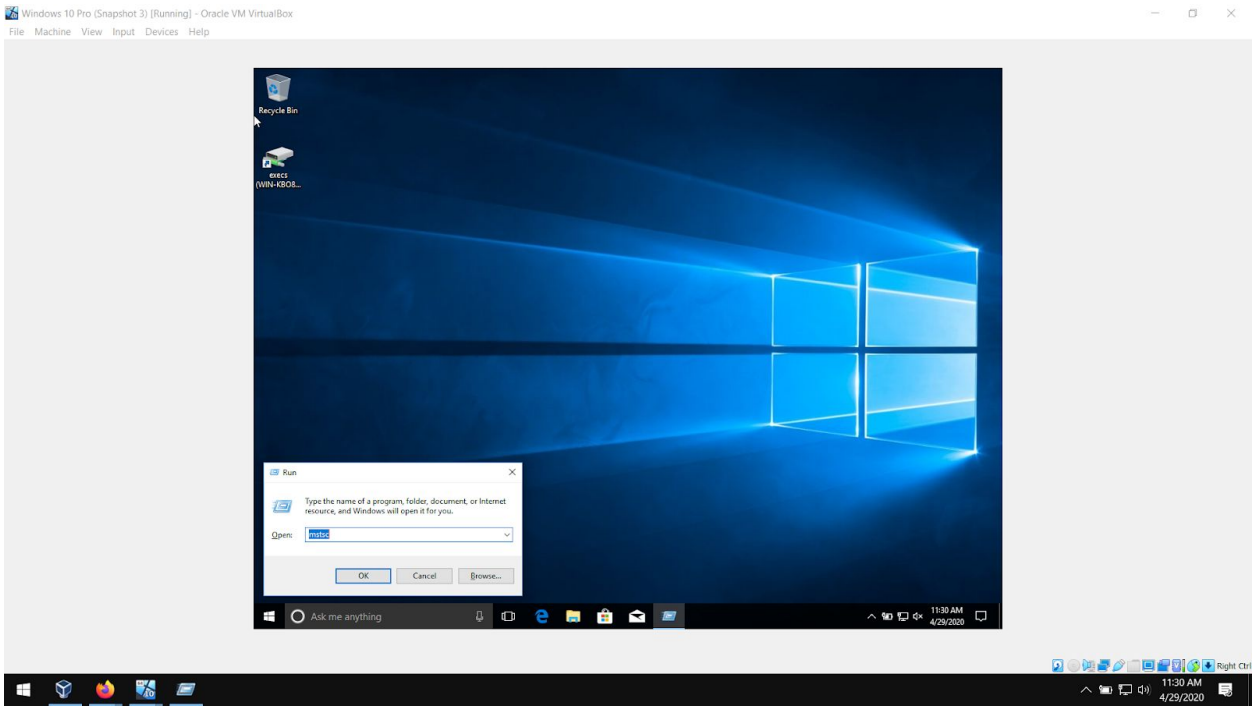

Windows Server 2012 R2 must be set to allow remote connections.

Windows Server 2012 R2



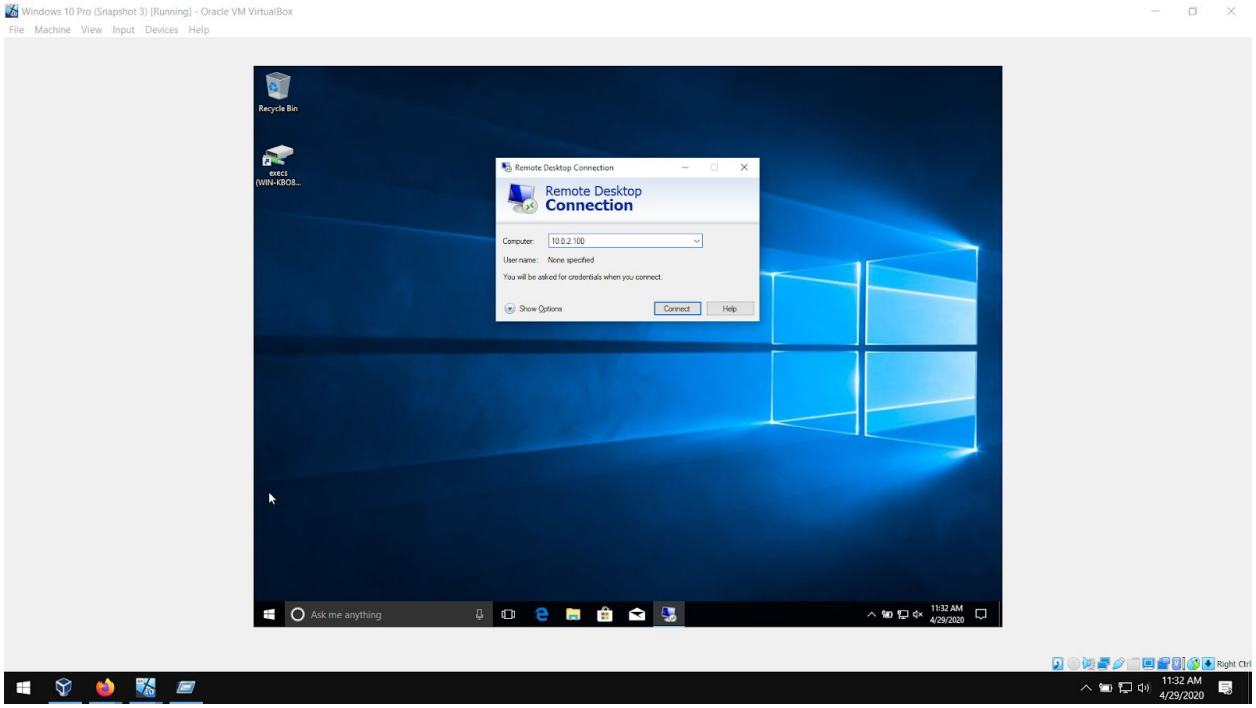

The workstation computer will require the Server's IP address, Results of the ipconfig command to find that IP.

Windows 10 Pro



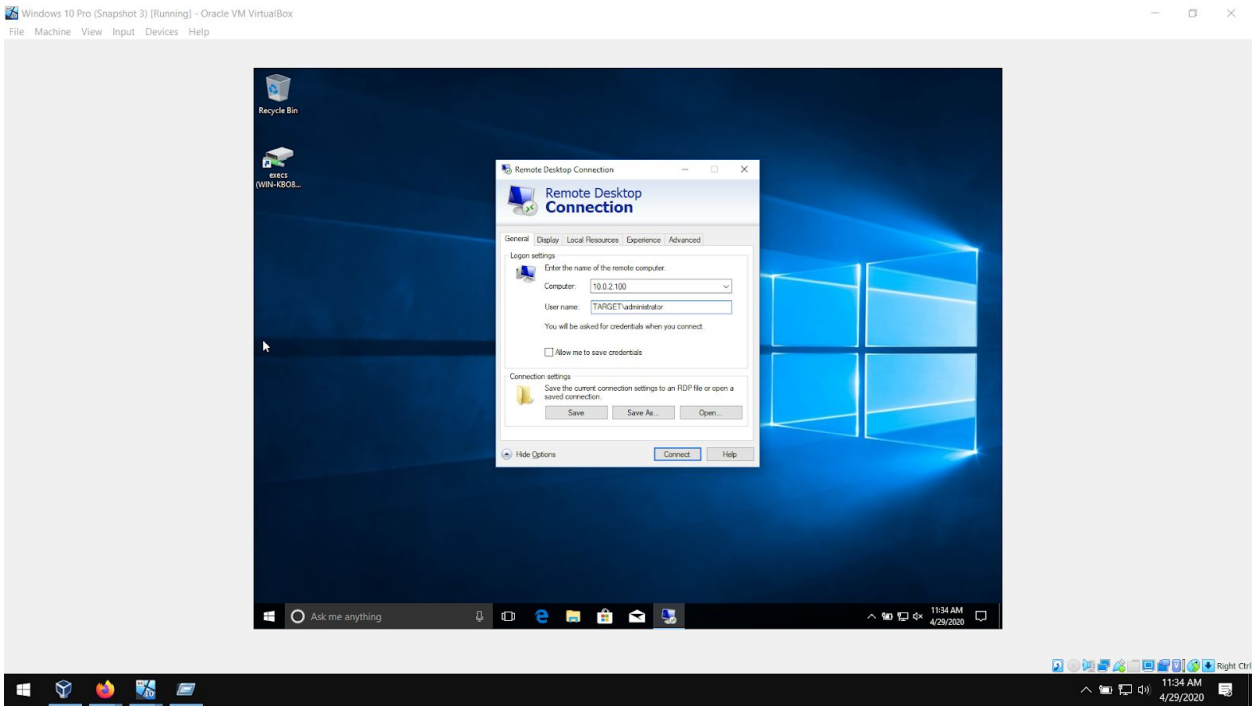

On the workstation computer, “mstsc” is issued at the Run prompt to start Remote Desktop Connection.

Windows 10 Pro



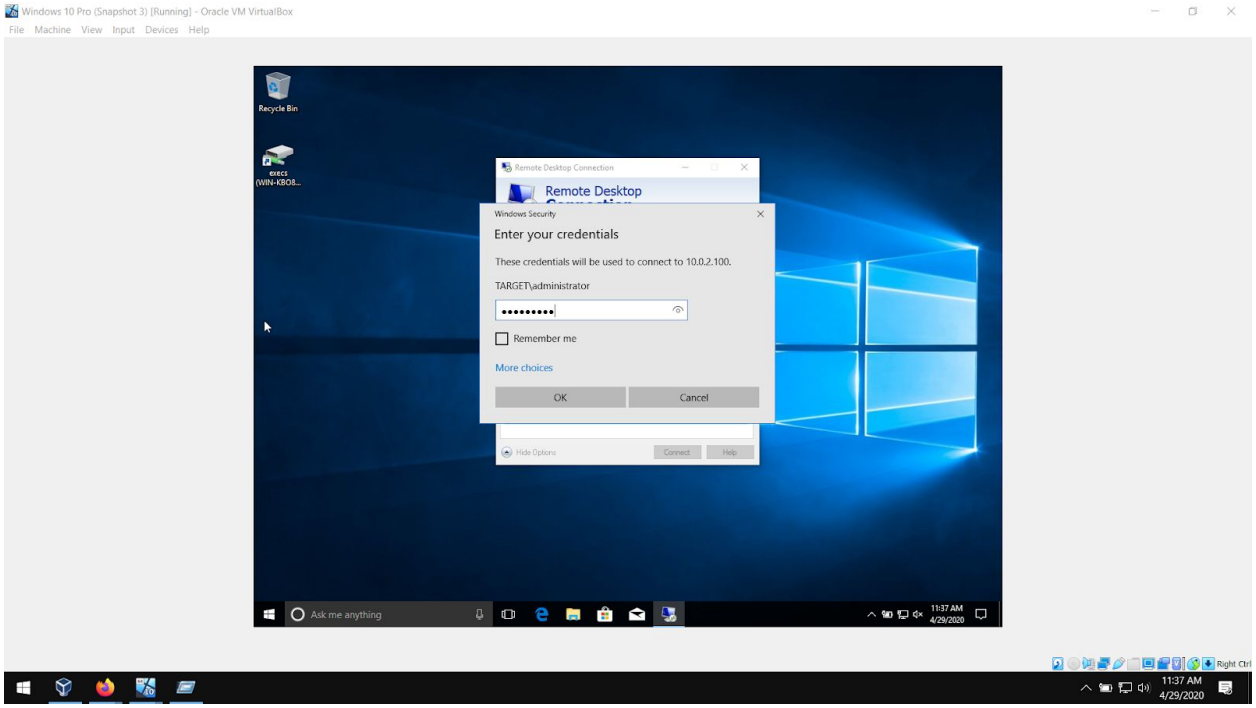

Inputting the Microsoft Server 2012 R2 IP address allows a RDP connection to initiate.

Windows 10 Pro



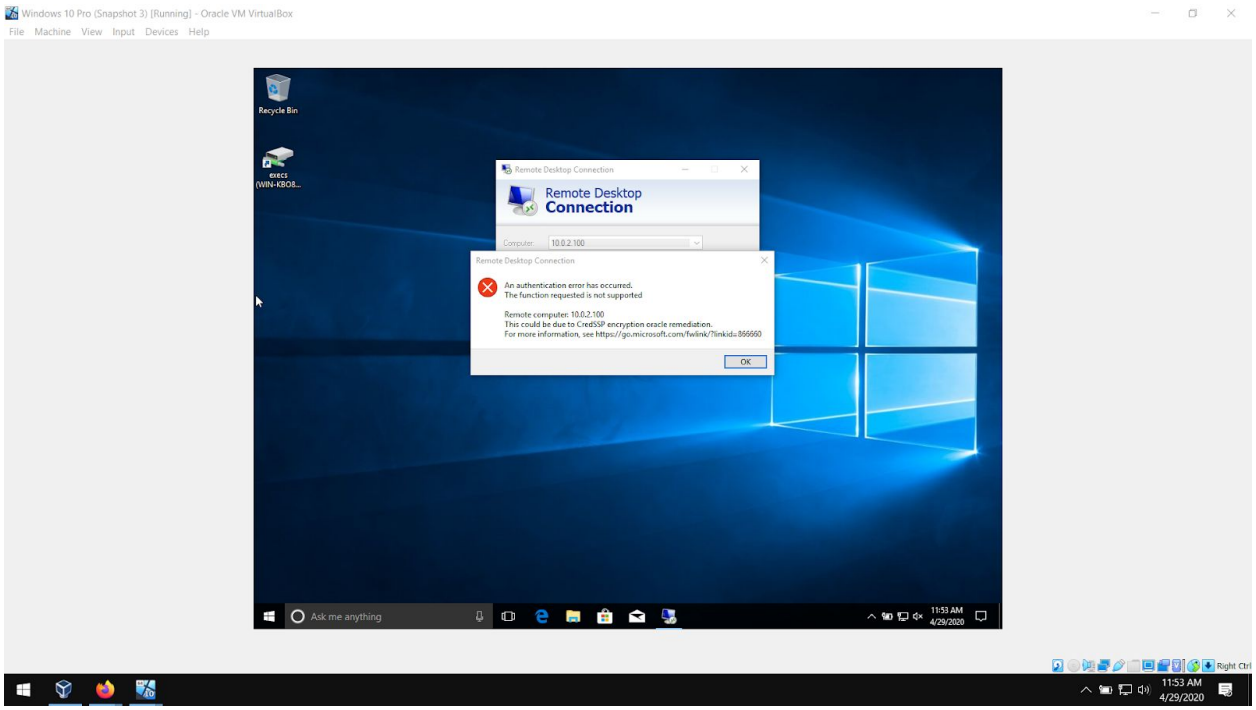

A user name can be entered before the connection begins.

Windows 10 Pro



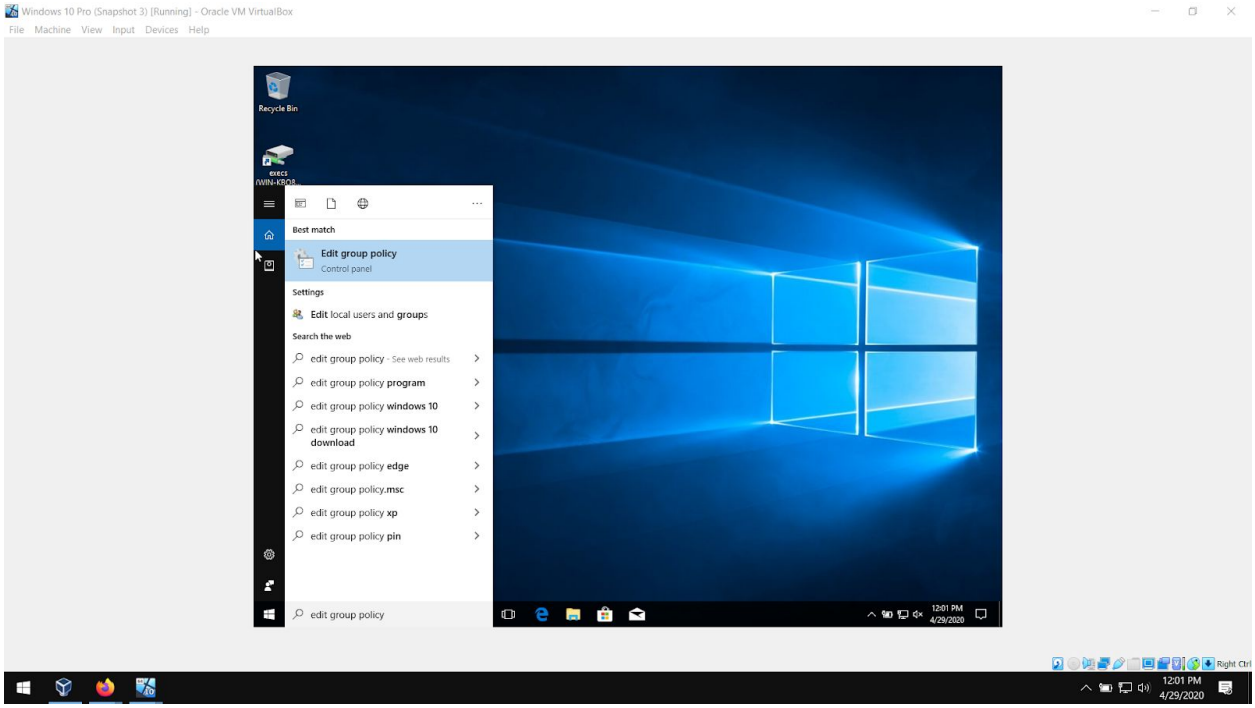

The connection asks for the TARGET\administrator password. Passwords have been elected to not be saved.

Remote Desktop Connection



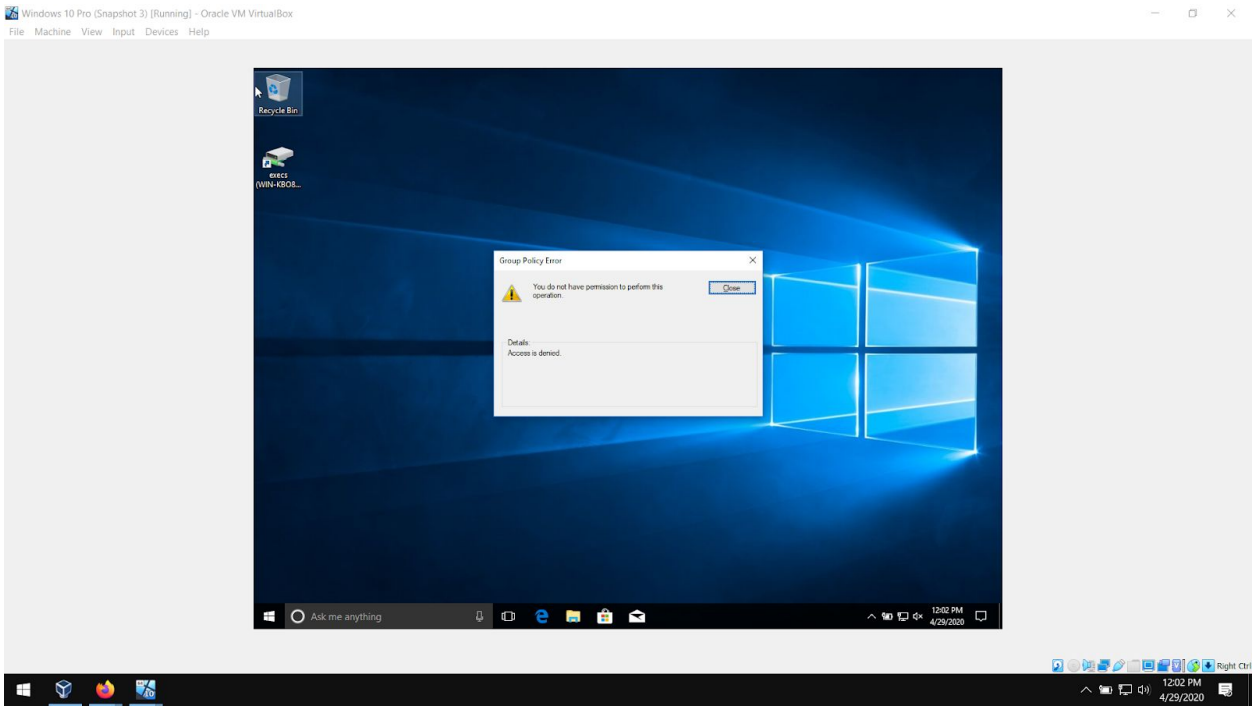

Mitigation for a known vulnerability is in effect. This is normal operation given that the vulnerability has been addressed. To allow the connection, the mitigation effort can be turned off manually.

Windows 10 Pro Search



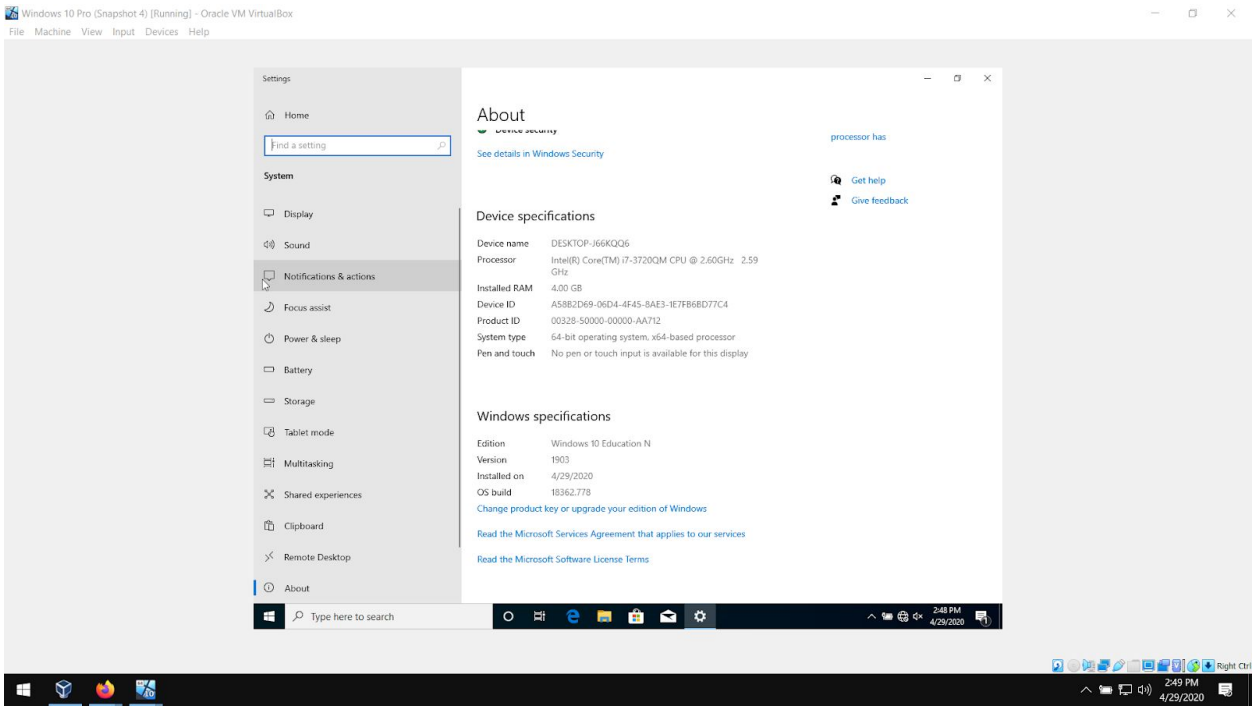

To manually turn off the mitigation effort, editing the Group Policy is necessary.

Group Policy Error



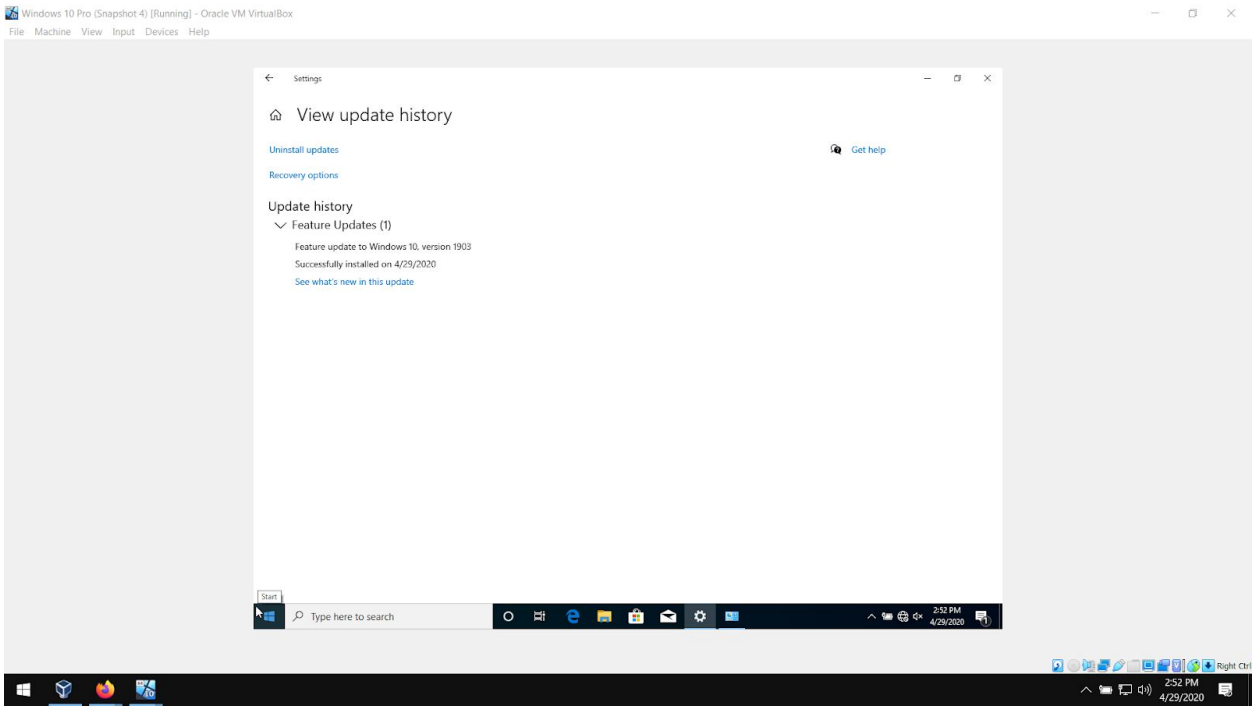

However, access to change the Group Policy is denied.

Windows 10 Pro - About



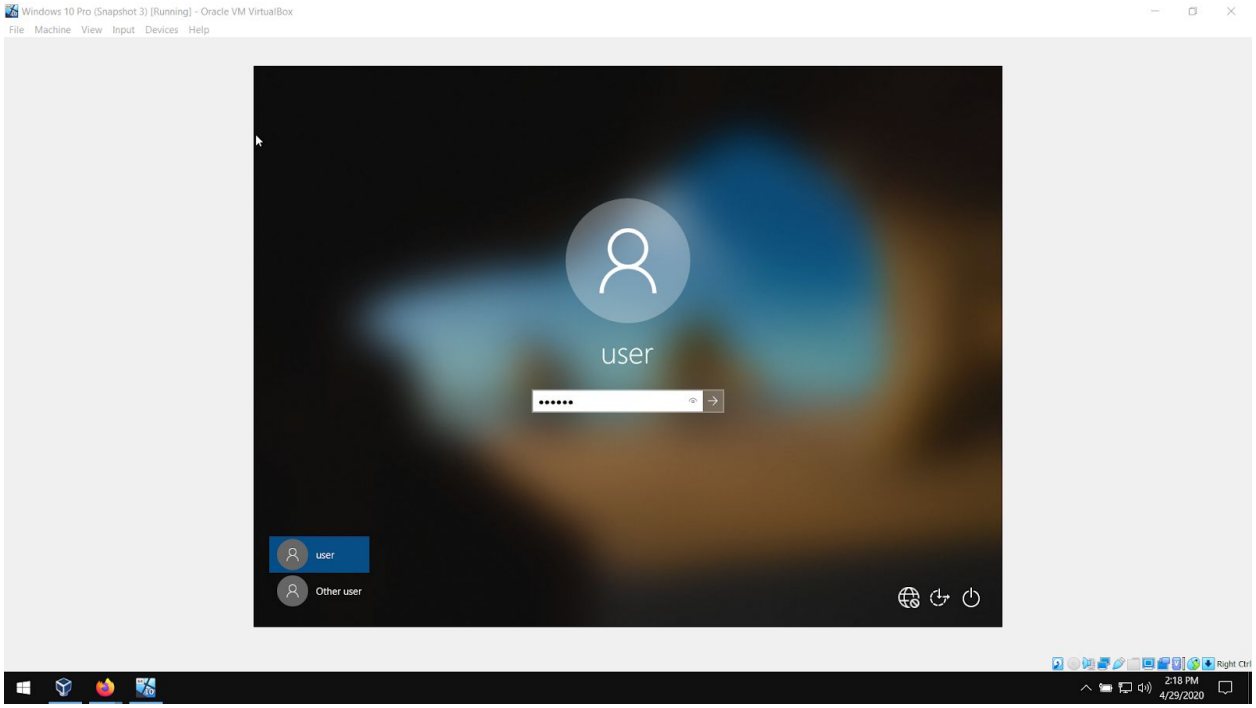

Before going further with any solution, I updated the local Windows 10 Pro virtual machine.

Windows 10 Pro - Settings



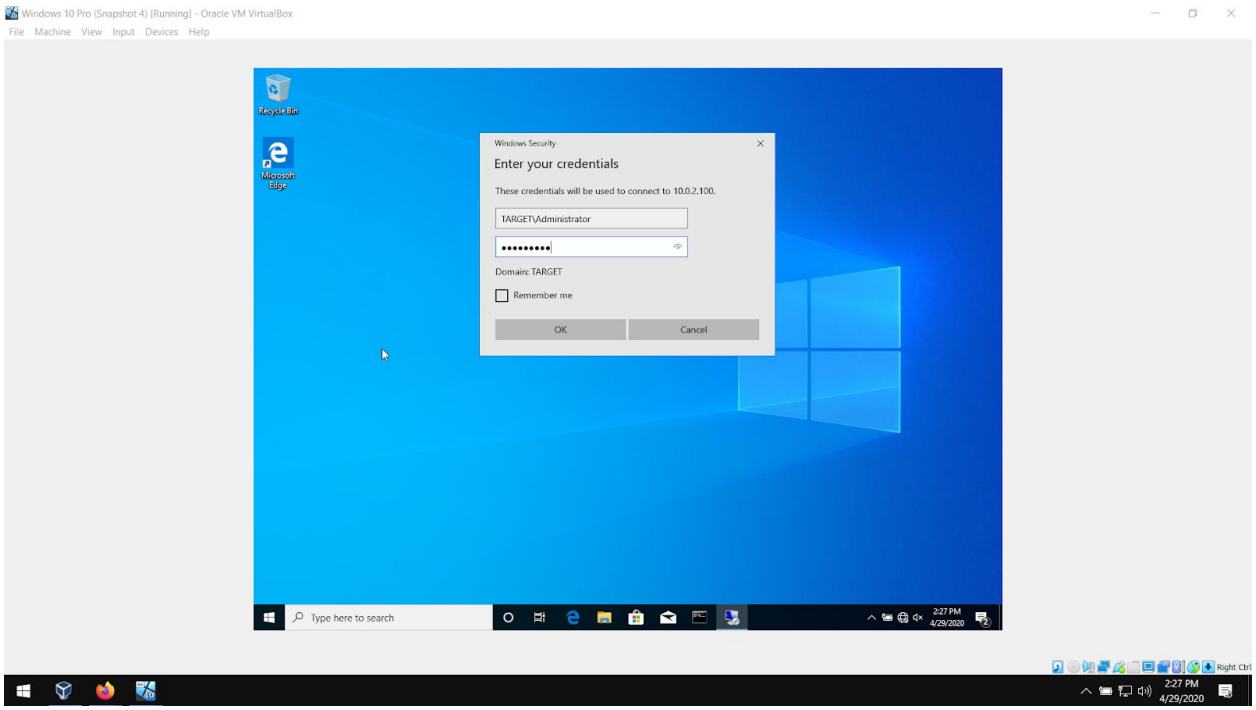

The update took about an hour and a half. Unfortunately, the previous OS version hasn't been recorded. But a VirtualBox snapshot can be utilized to check for the previous version if required.

Windows 10 Pro - Login



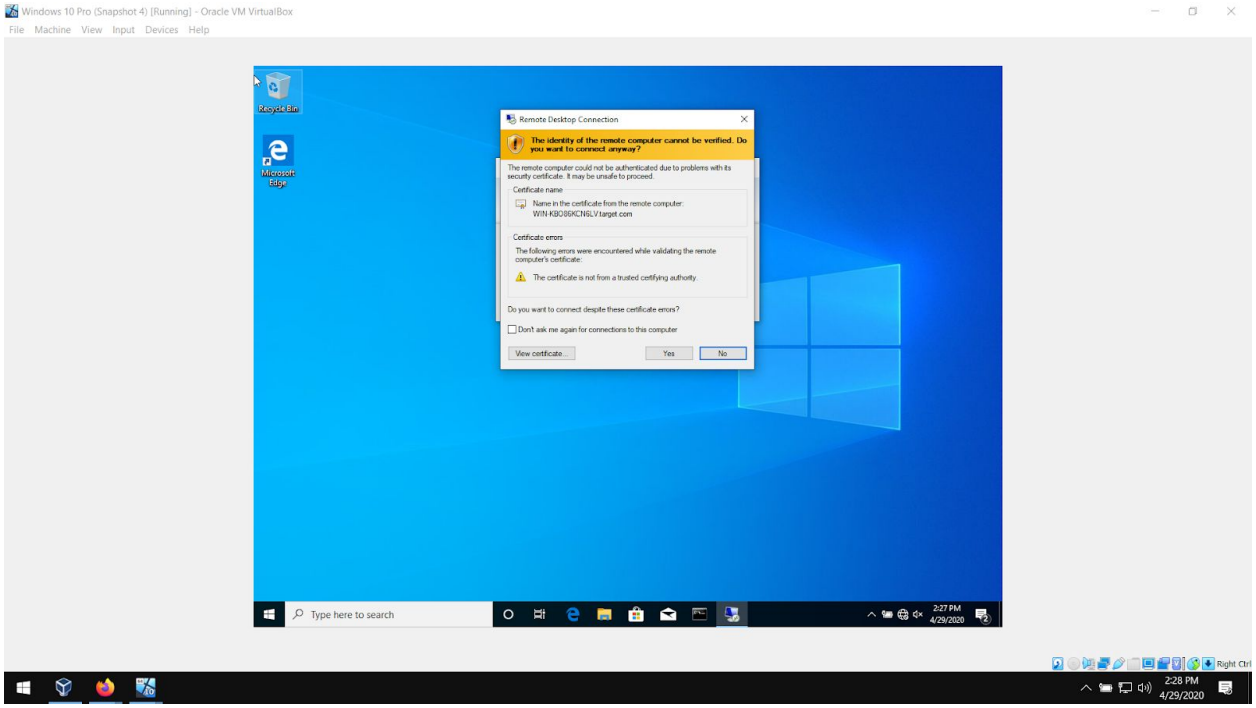

Signing back in as a local administrator after the update.

Remote Desktop Connection



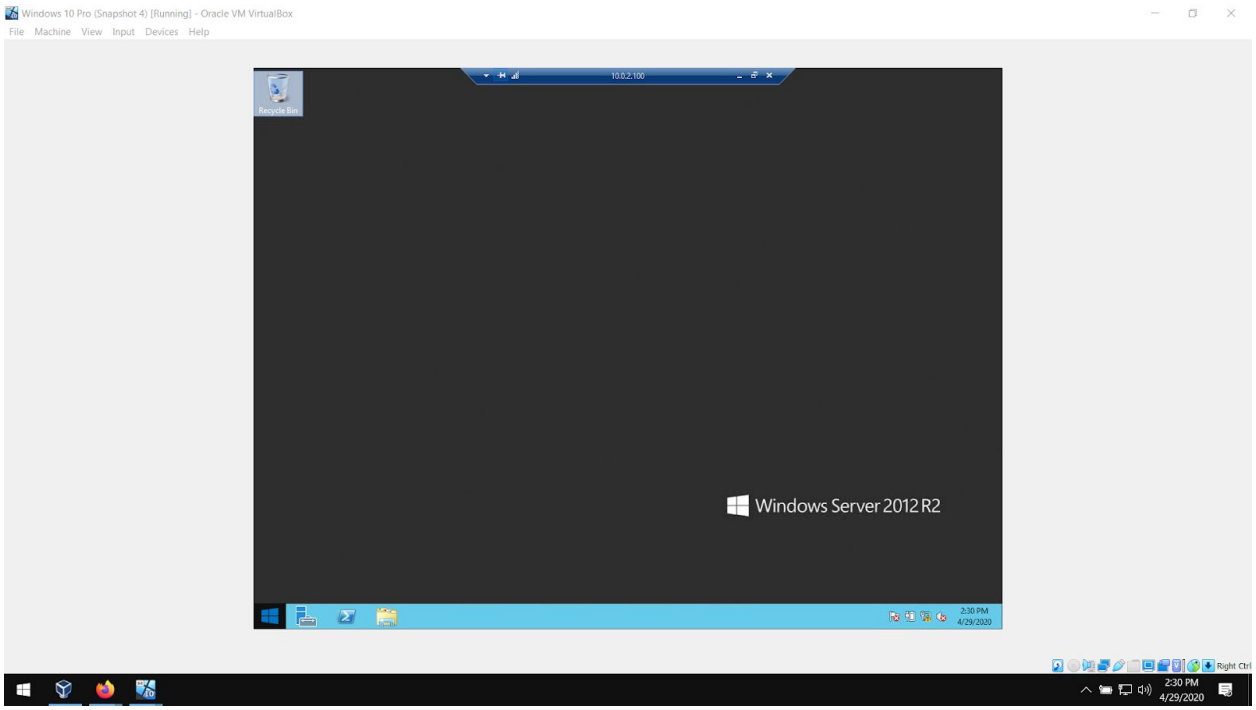

Before any changes made, a connection via the Administrator account is attempted again. The same error should occur because this is a policy mitigation setting imposed by Microsoft, and is independent of the user settings so far. However, the update may have fixed the issue.

Windows 10 Pro



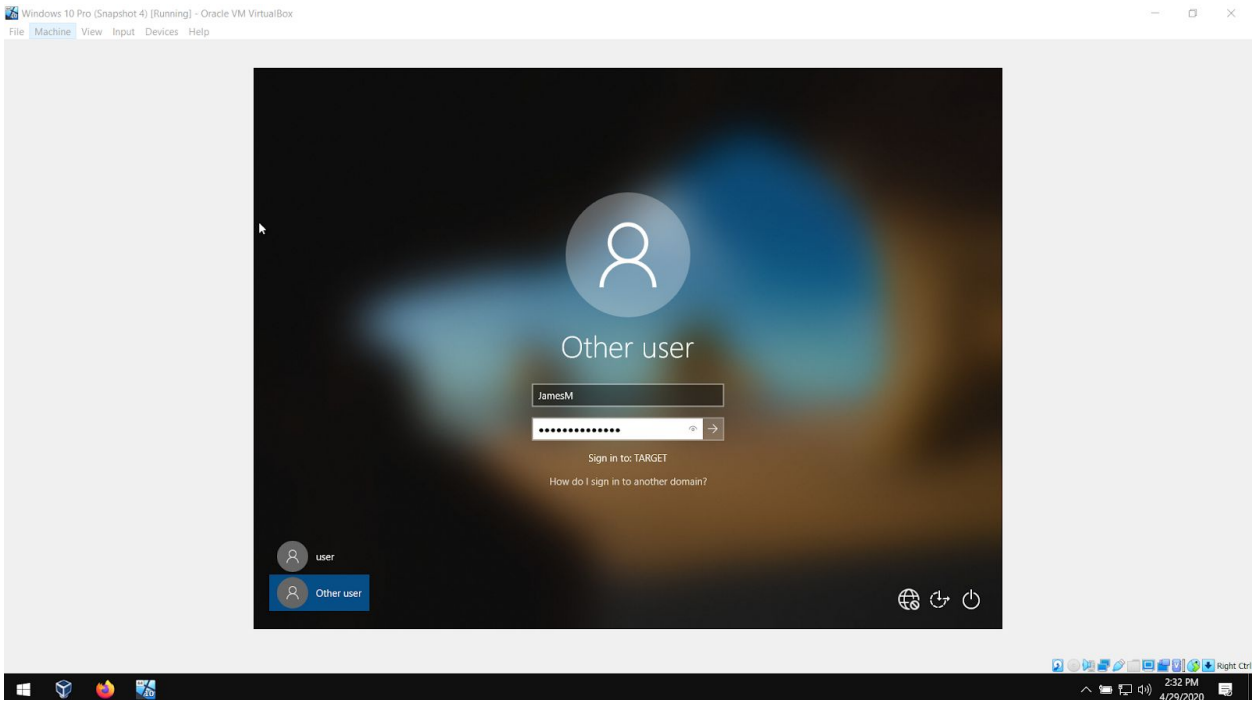

The connection works.

Remote Desktop - Windows Server 2012 R2 Desktop connection



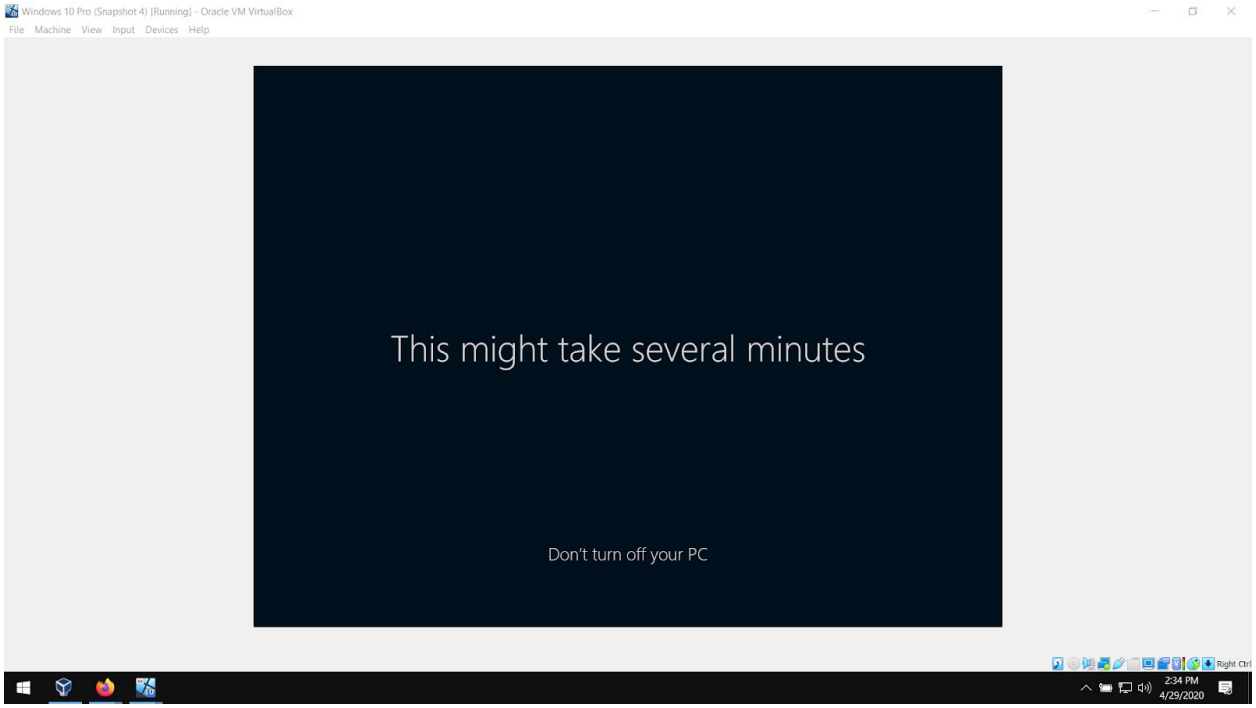

Active Remote Desktop Connection. The update may have fixed the issue. To check I logged back in as the local domain user (JamesM).

Windows 10 Pro - Domain user login



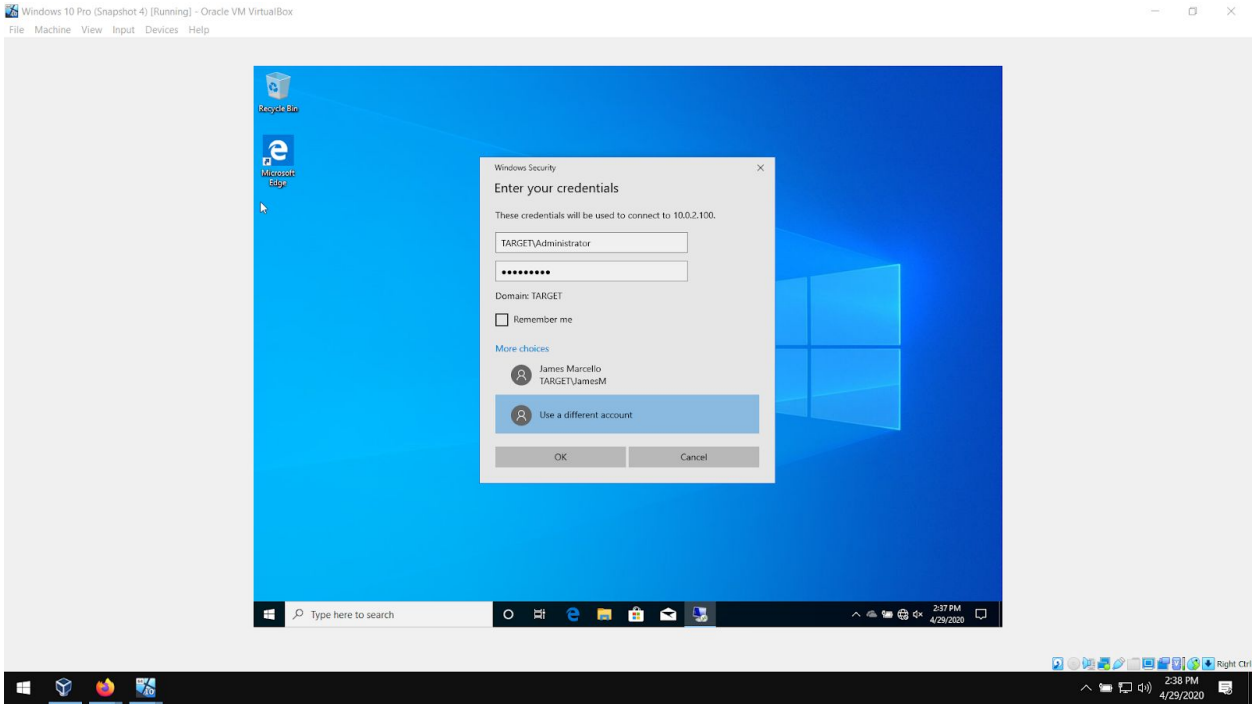

Logging back in as a standard domain user.

Login screen after update



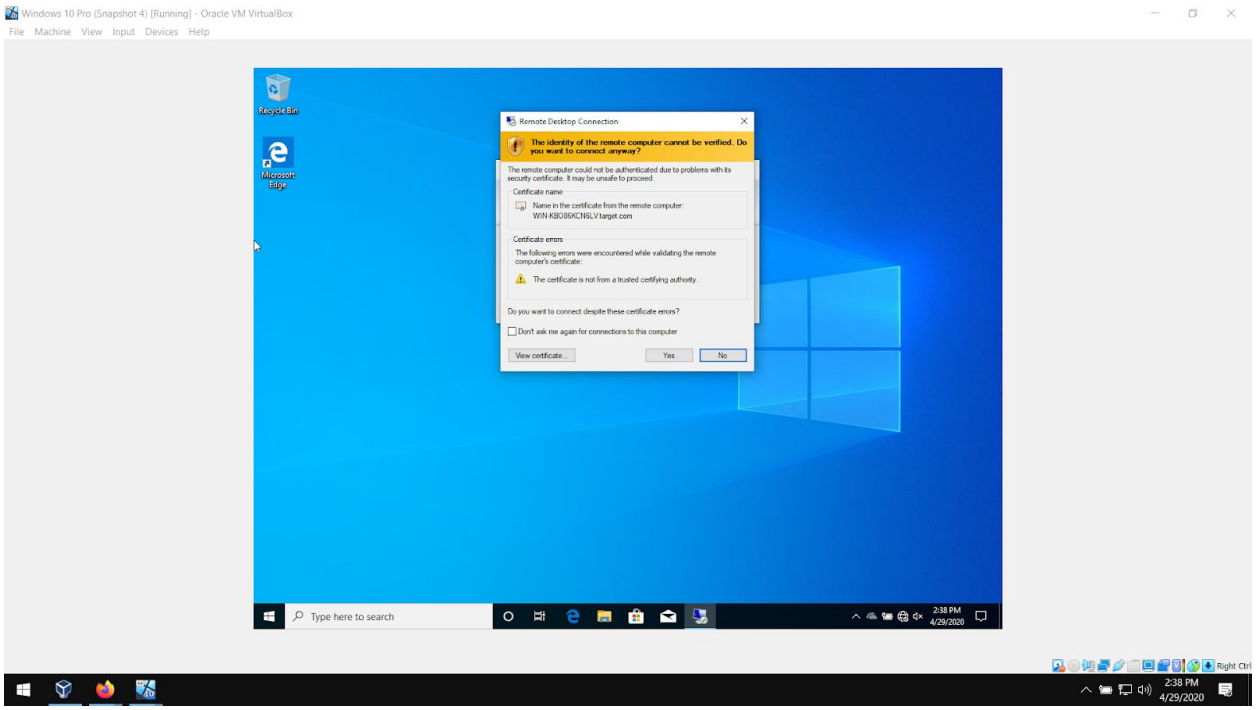

The getting ready screen after a major update for the first time.

Remote Desktop Connection



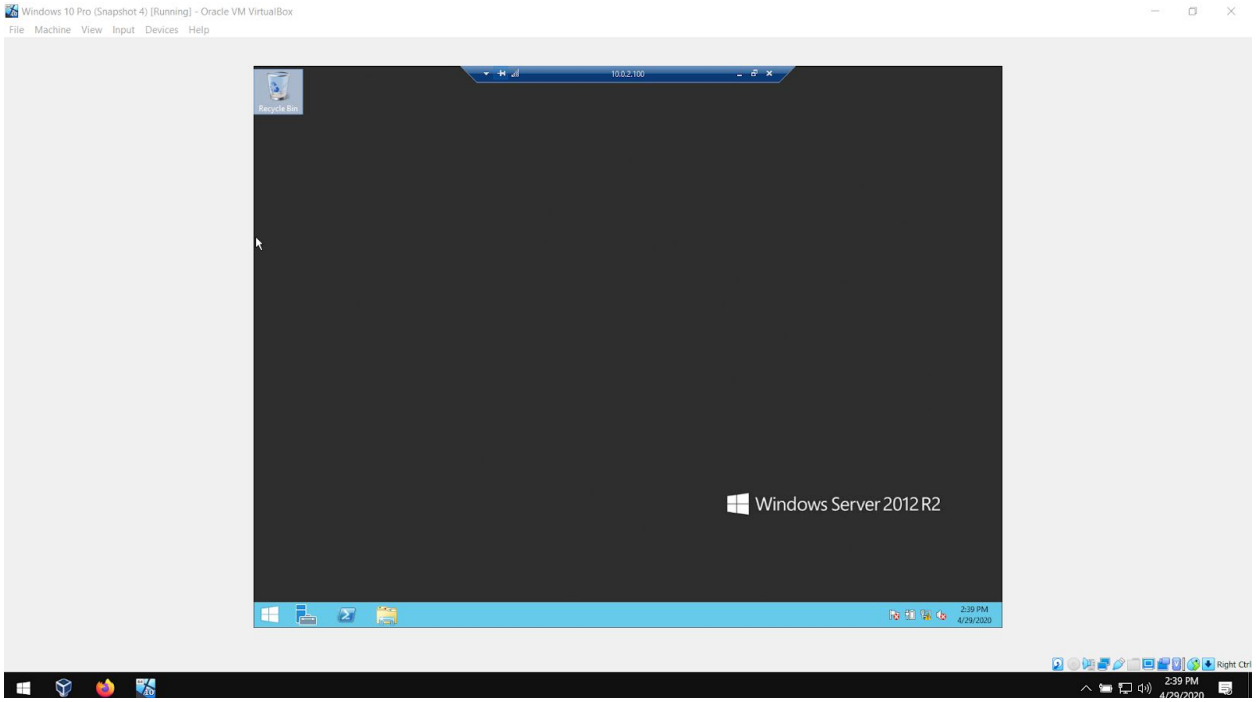

A new Remote Desktop Connection of a non-administrator account.

Remote Desktop Connection



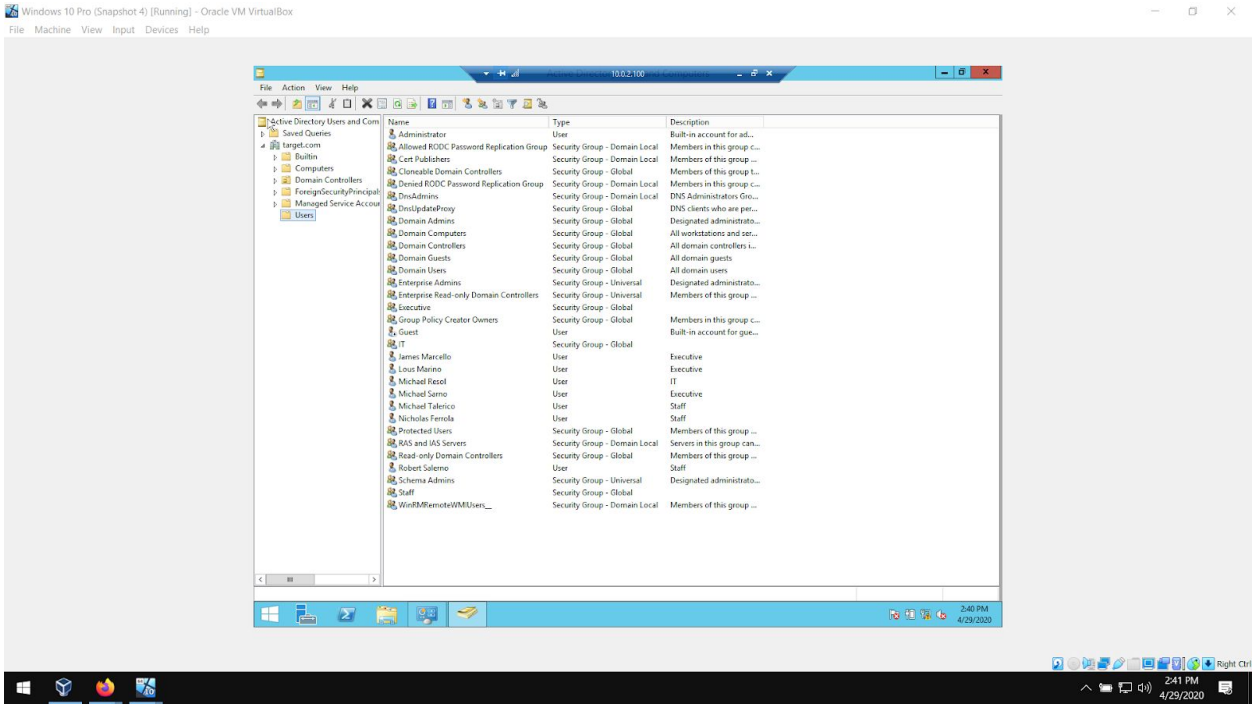

The connection works.

Windows 10 Pro - Server 2012 R2 Remote Desktop Connection



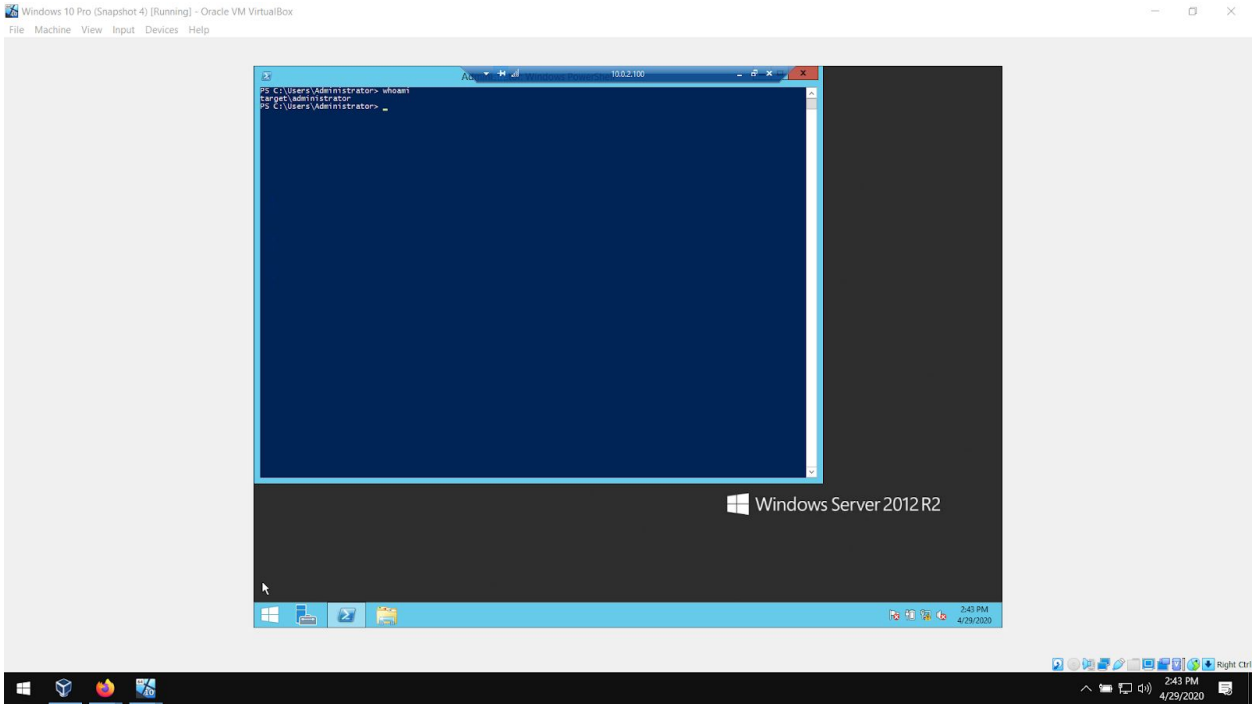

The large update to the Windows 10 Pro computer must have fixed the issue.

Windows 10 Pro - Server 2012 R2 Remote Desktop Connection



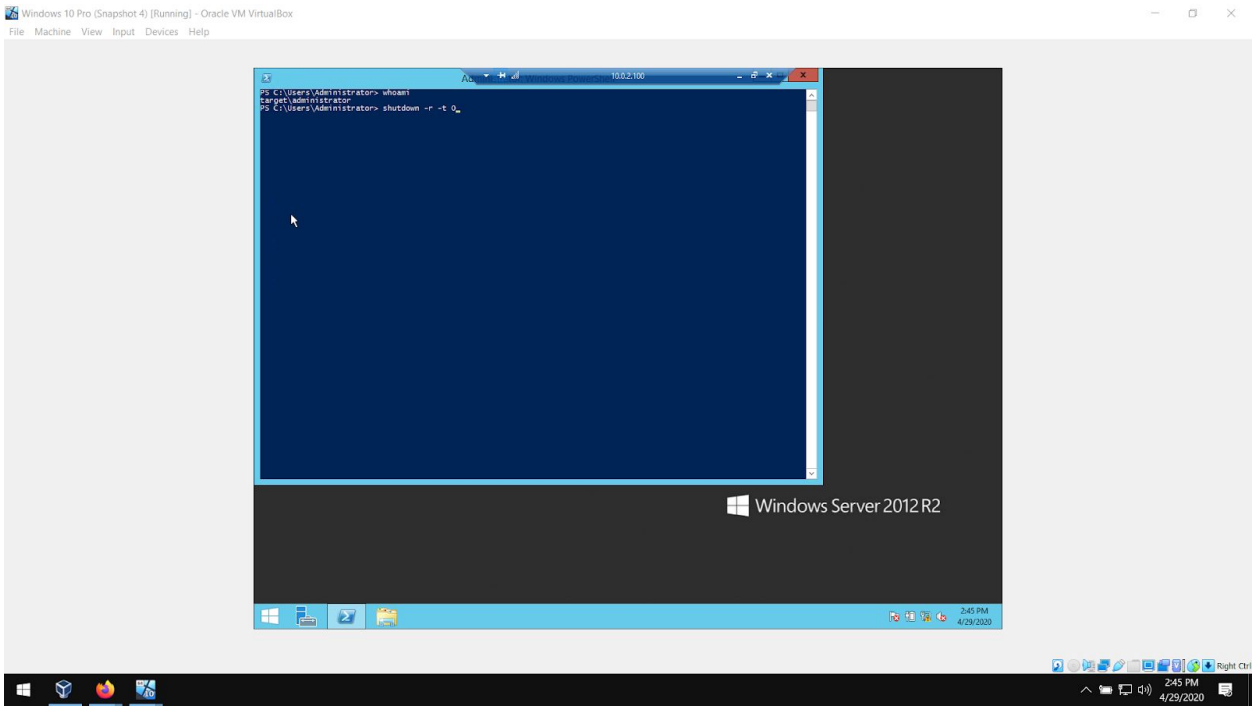

Active Directory Users and Computers is available.

Windows 10 Pro - Server 2012 R2 Remote Desktop Connection PowerShell



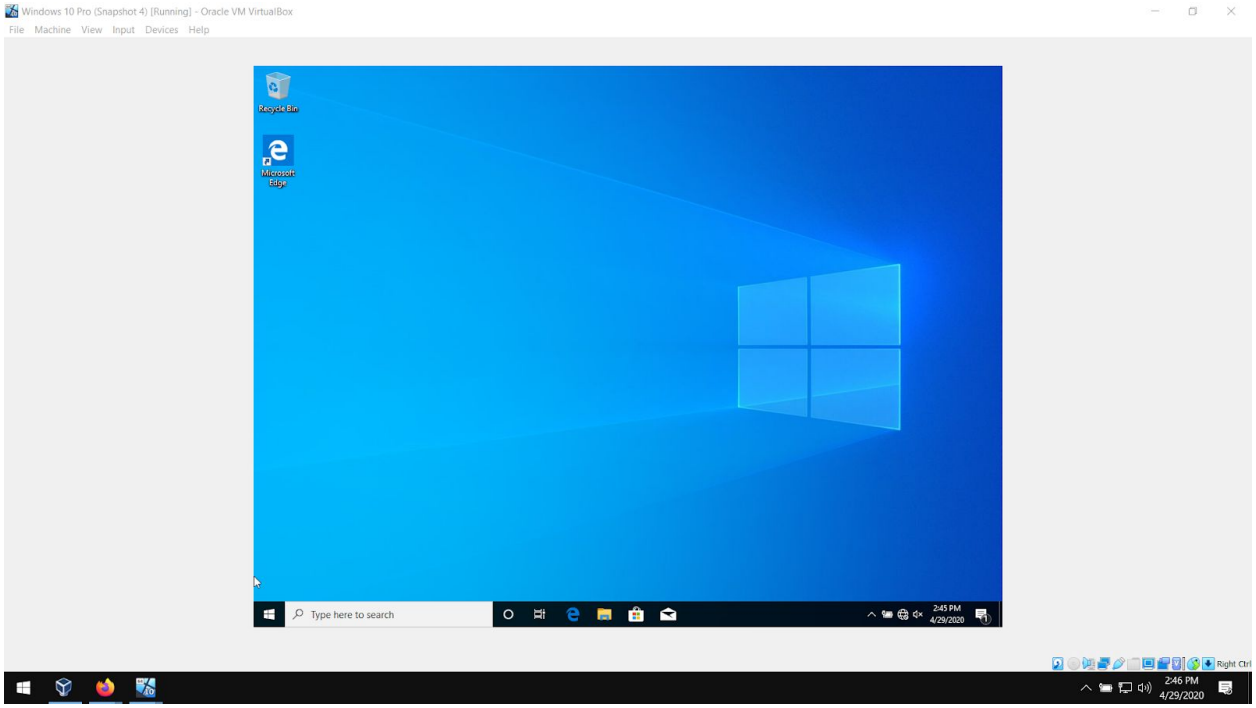

The command whoami shows which user Remote Desktop Connection has established a connection with.

Windows 10 Pro - Server 2012 R2 Remote Desktop Connection PowerShell




To test for a remote shutdown command, shutdown -r -r 0 is issued.

Windows 10 Pro




Upon execution of the code, the connection ends and the Windows 10 Pro Desktop comes back into focus.

3. Surprises. Things rarely go as planned. Include this in your report. If things aren't working, documenting the problem can help you to find the solution.

The initial Remote Desktop Connection attempt failed, which was a surprise. The error turned out to be a known vulnerability identified as CVE-2018-0886,

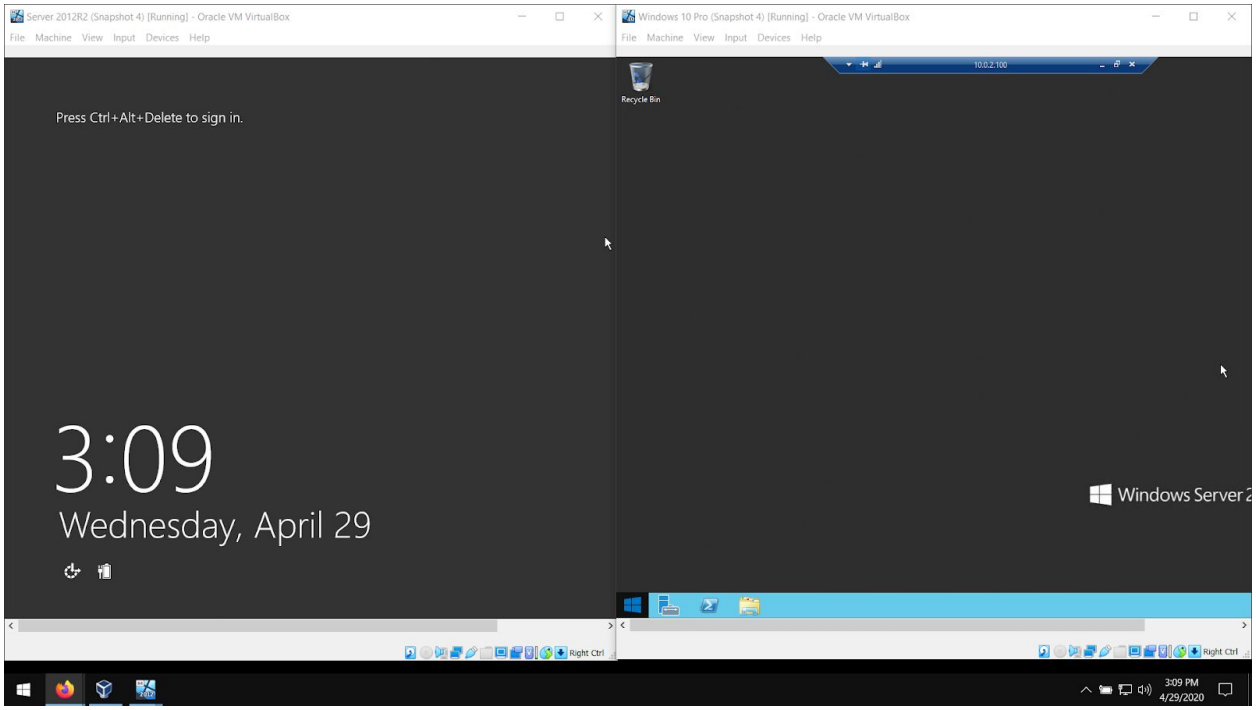
> The Credential Security Support Provider protocol (CredSSP) in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709 Windows Server 2016 and Windows Server, version 1709 allows a remote code execution vulnerability due to how CredSSP validates request during the authentication process, aka "CredSSP Remote Code Execution Vulnerability".[1]

A remote code execution vulnerability allows an attacker to "...execute arbitrary commands or code on a target machine or in a target process."[2] A RCE attack is also known as arbitrary code execution (ACE). Microsoft first published an update to CVE-2018-0886 in the April 2018 Security Update release.[3]

The next surprise was the fact that a Windows Update couldn't be ignored. Given the core nature of the problem faced, and the fact that the issue was a known vulnerability, updating before any other course of action was a safe bet.

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0886
[2] https://en.wikipedia.org/wiki/Arbitrary_code_execution
[3] https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2018-Apr

4. A screenshot of the final result of the assignment.




The remote desktop connection made from Windows 10 Pro (right) and Windows Server 2012 R2 (Left).

5. Summary. Did it work as expected? Did you need more research?

After some quick research I found out the error is really a known vulnerability defined as CVE-2018-0886 by Common Vulnerabilities and Exposures. Not taking the few minutes to research the error and discover a Windows update may fix the issue, would have made the problem a much more strenuous affair. However, I was hesitant to update at first. I knew that Windows Updates can wreck havoc or bring salvation when unexpected behavior occurs. Was this issue large enough to gamble the update process? On one hand I had put off the update for a few weeks. As it turned out the update was necessary and could not be avoided. Thus, making the decision to update before continuing the lab that much more easier.

Most likely the update fixed the vulnerability and thus allowed Remote Desktop to continue it's connection. Perhaps the update was noted in the system's changelog when I had initially failed the RDP connection. To verify this, I could reload a previous VirtualBox snapshot, update before a RDP connection and see what results play out.

Moreover, previous snapshots of each virtual machine may provide insights into how the attack plays out with freshly installed workstation and domain controller systems. Many proof of concept code builds exist for this vulnerability[4] and in the metasploit framework.[5]

[4] https://github.com/preempt/credssp
[5] https://www.rapid7.com/db/?q=CVE-2018-0886&type=nexpose