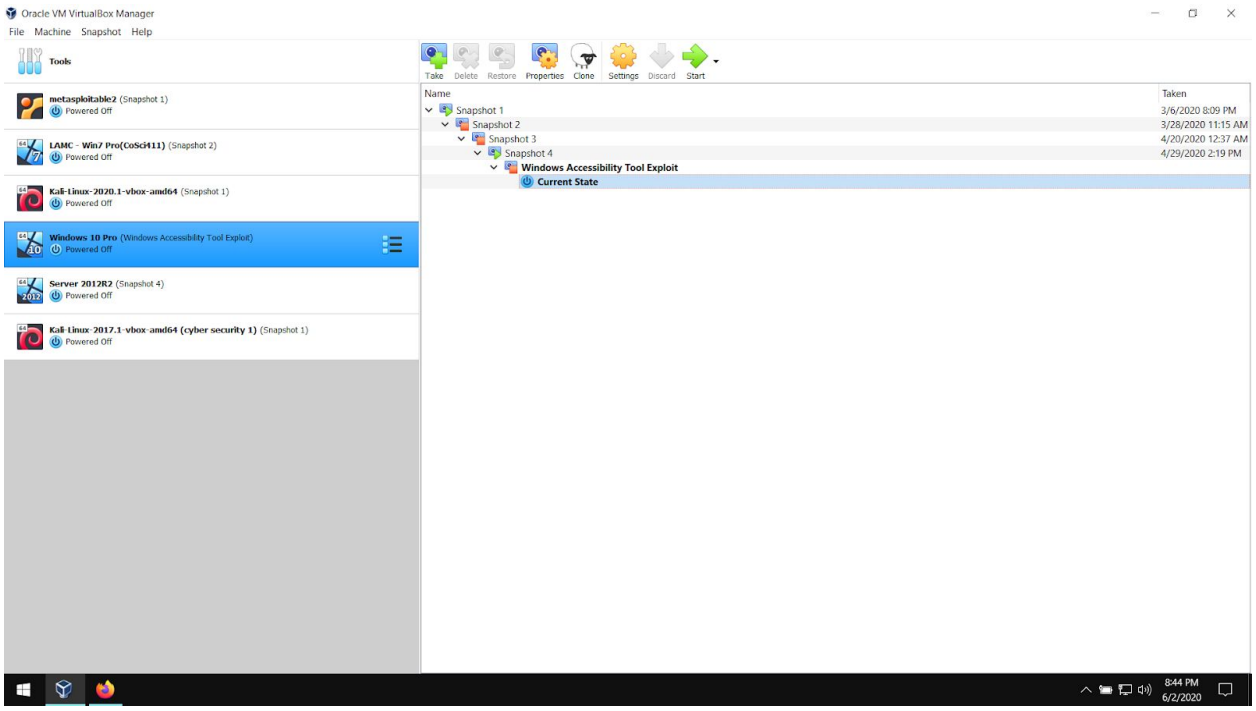
Cyber Report - Exploiting Windows Accessibility Tool

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

The goal of this lab is to exploit a vulnerability found in the Windows Accessibility Tool on a Windows 10 Pro virtual machine. This virtual machine is installed inside of Virtualbox, connected to a local network named Cyber Range. The exploit will require an installation ISO file first used to install Windows 10 Pro. The exploit will rename two files, tricking the Operating System in running a command line when the Windows Accessibility Tool is selected at login.

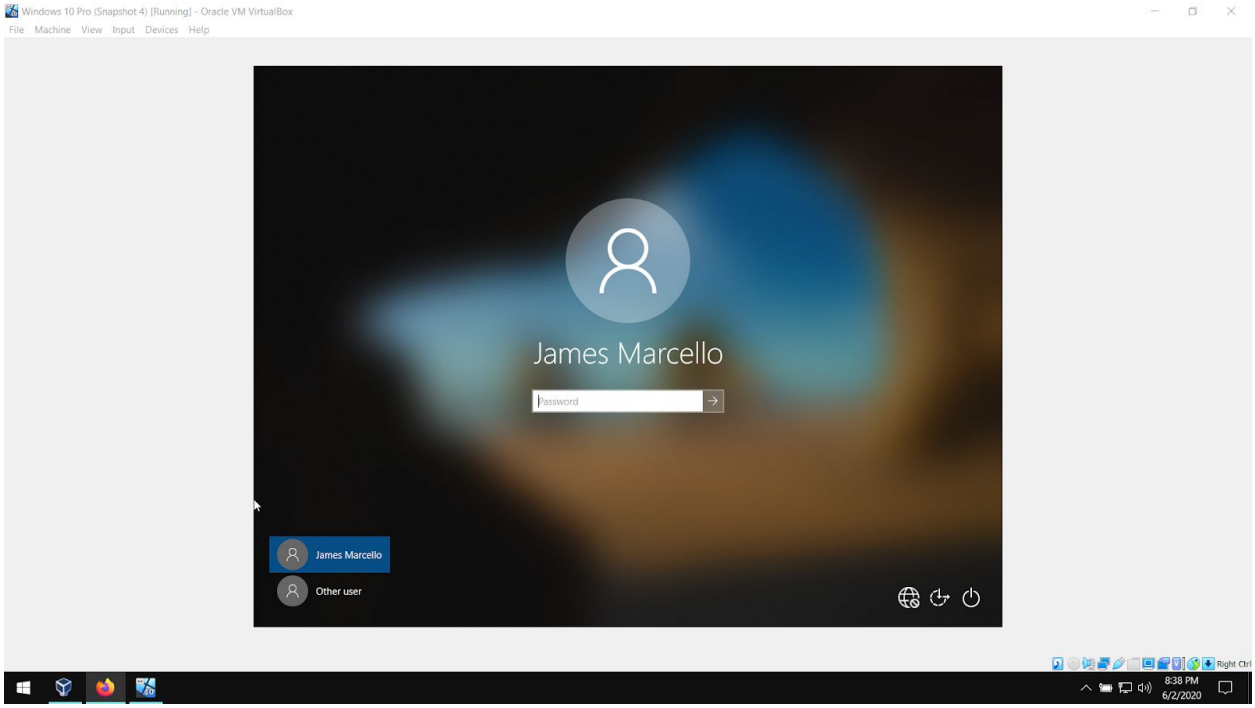
2. Demonstration of the steps taken with screenshots (snipping tool) from your computer. You need to show the steps you took as you took them.

Virtualbox - Create Snapshot



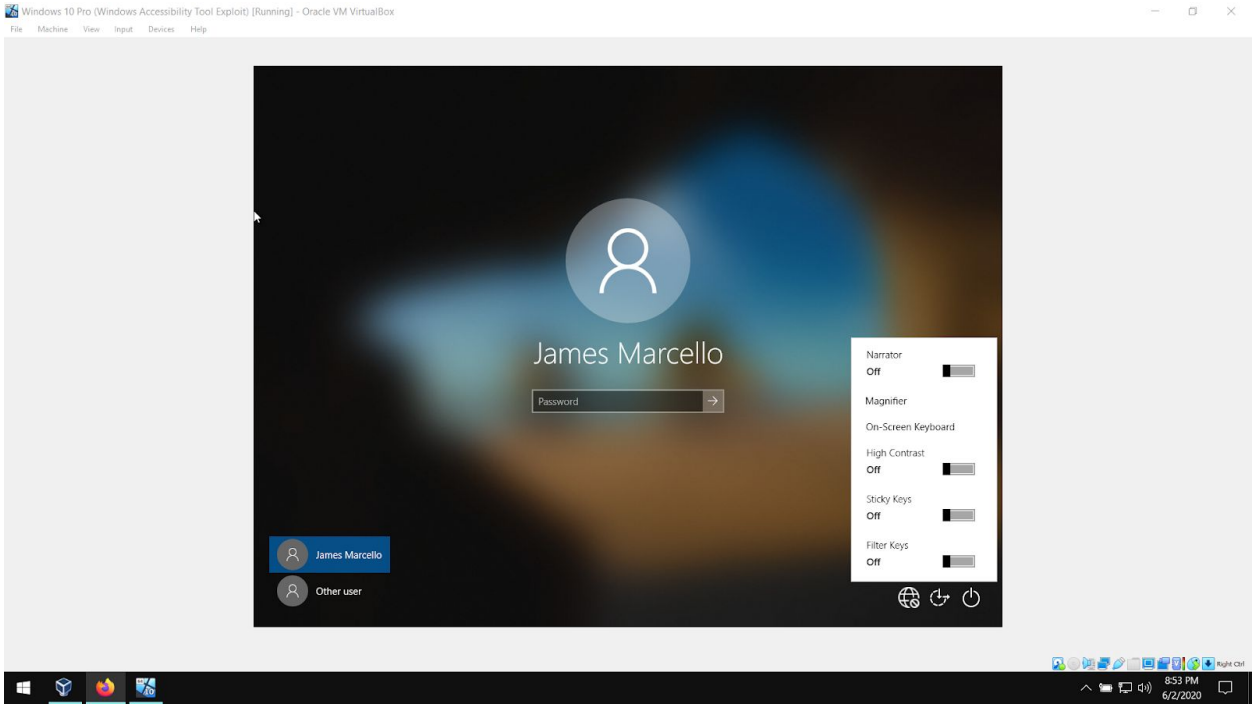
As a best practice, a snapshot was created before any experiments were conducted in the cyber range. A rollback to before this lab was started will fix any problems that may occur along the way.

VirtualBox - Windows 10 Pro



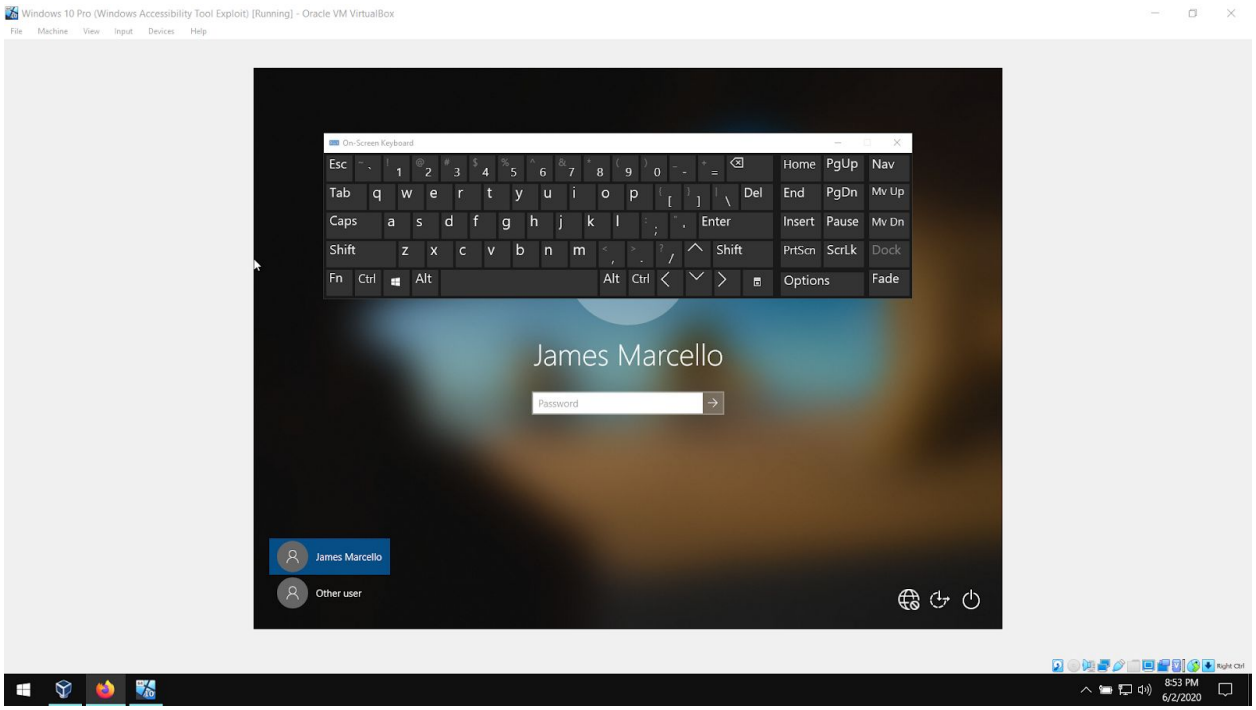
The Windows 10 Pro login screen

VirtualBox - Windows 10 Pro



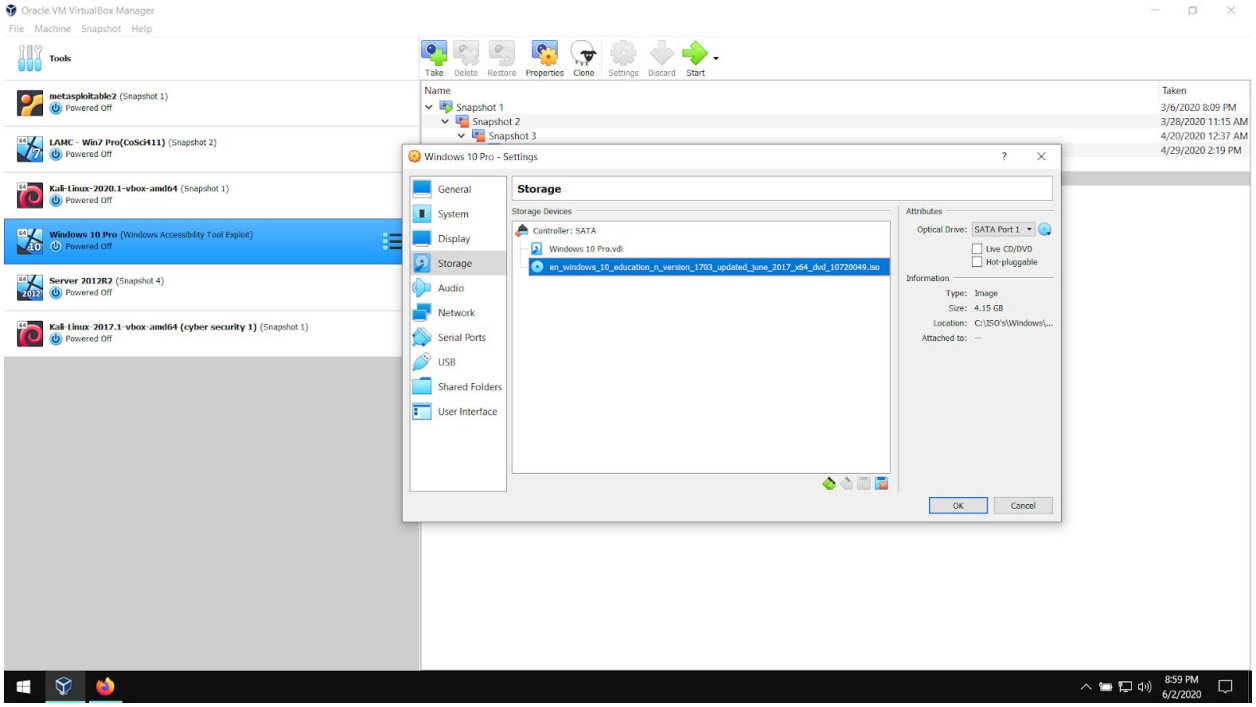
After selecting the Windows Accessibility Tool, an option for On-Screen Keyboard is displayed.

VirtualBox - Windows 10 Pro



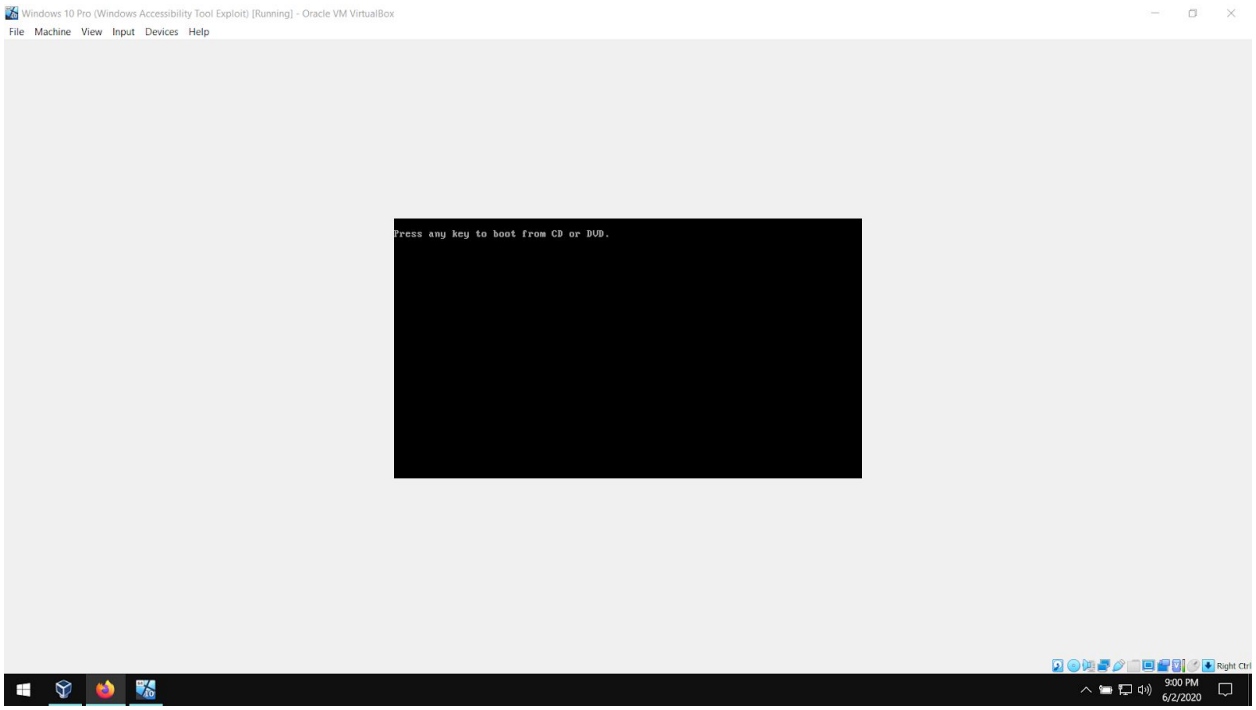
The On-Screen Keyboard allows users without access to a keyboard to use Windows 10. This is normal Windows 10 behavior.

Virtualbox - DVD drive



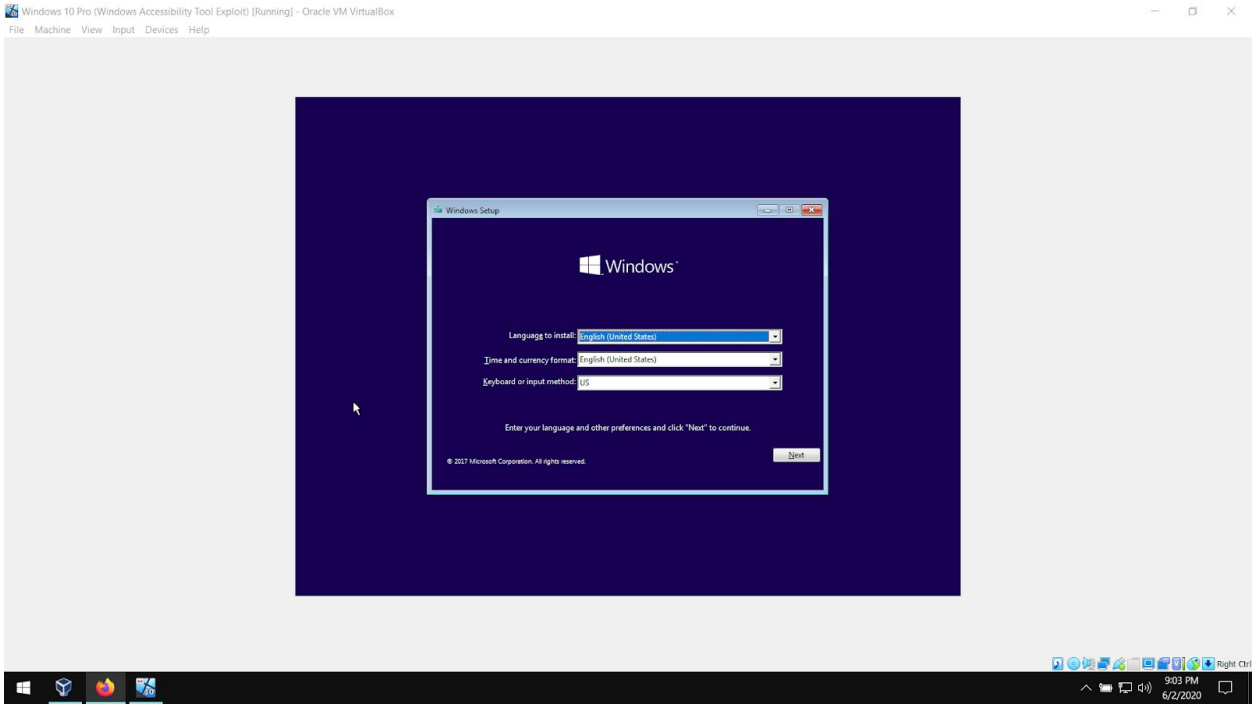
To start the exploit, an installation ISO file must be loaded into the virtual DVD drive. For this lab, a Windows 10 Educational Version is used.

VirtualBox - Windows 10 Pro Boot



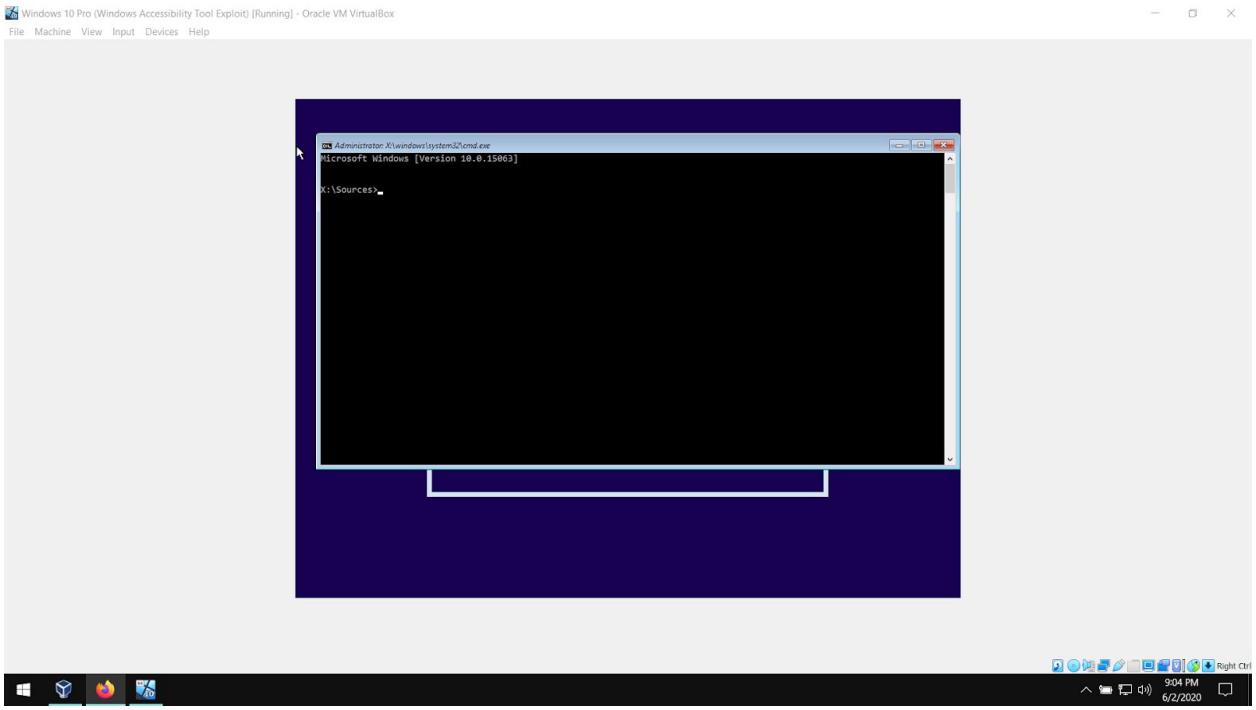
In order to start the exploit, the boot must occur from the ISO. Pressing any key will start the DVD media boot sequence.

Virtualbox - Windows Setup



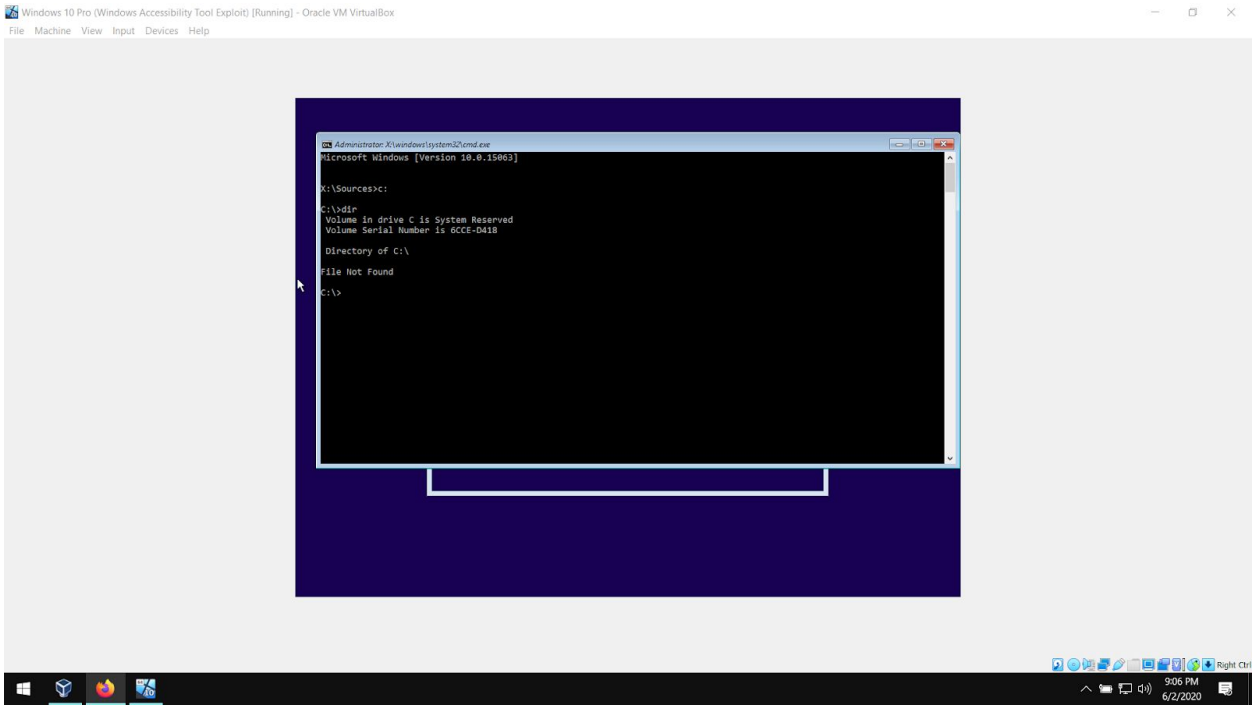
The set up DVD has been booted.

Virtualbox - Administrator command prompt



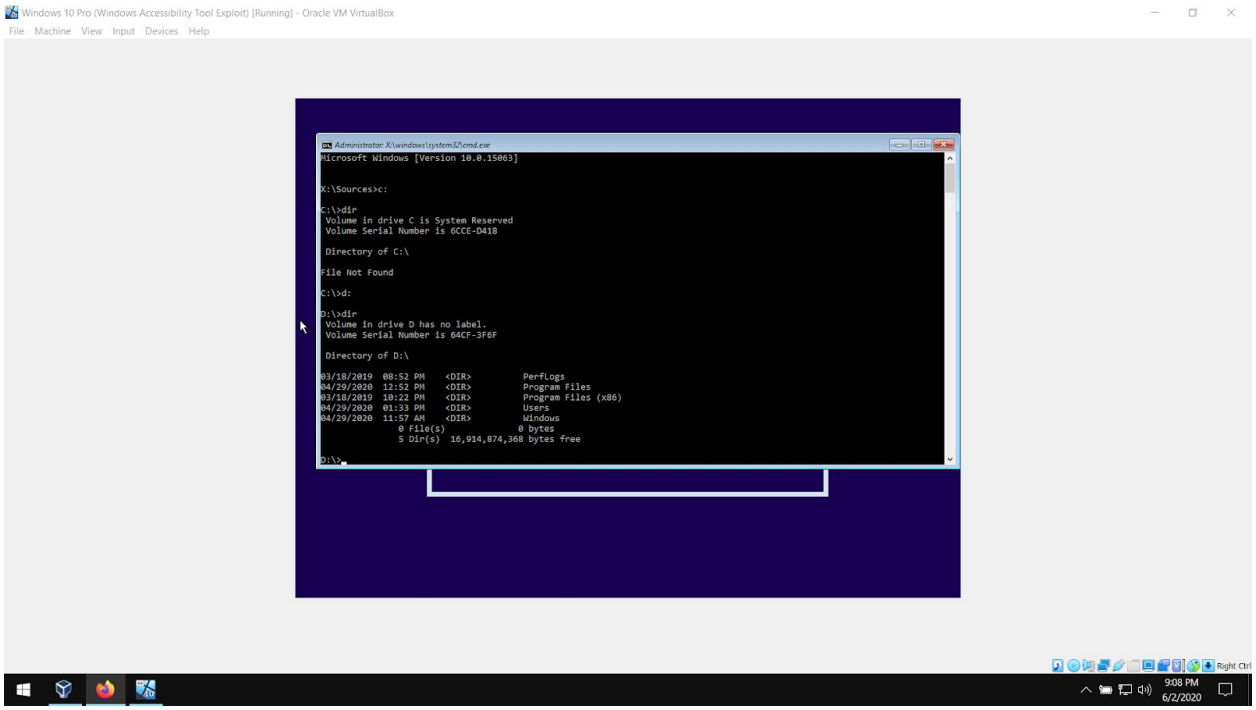
Shift F10 will activate the command prompt.

Virtualbox - Administrator command prompt



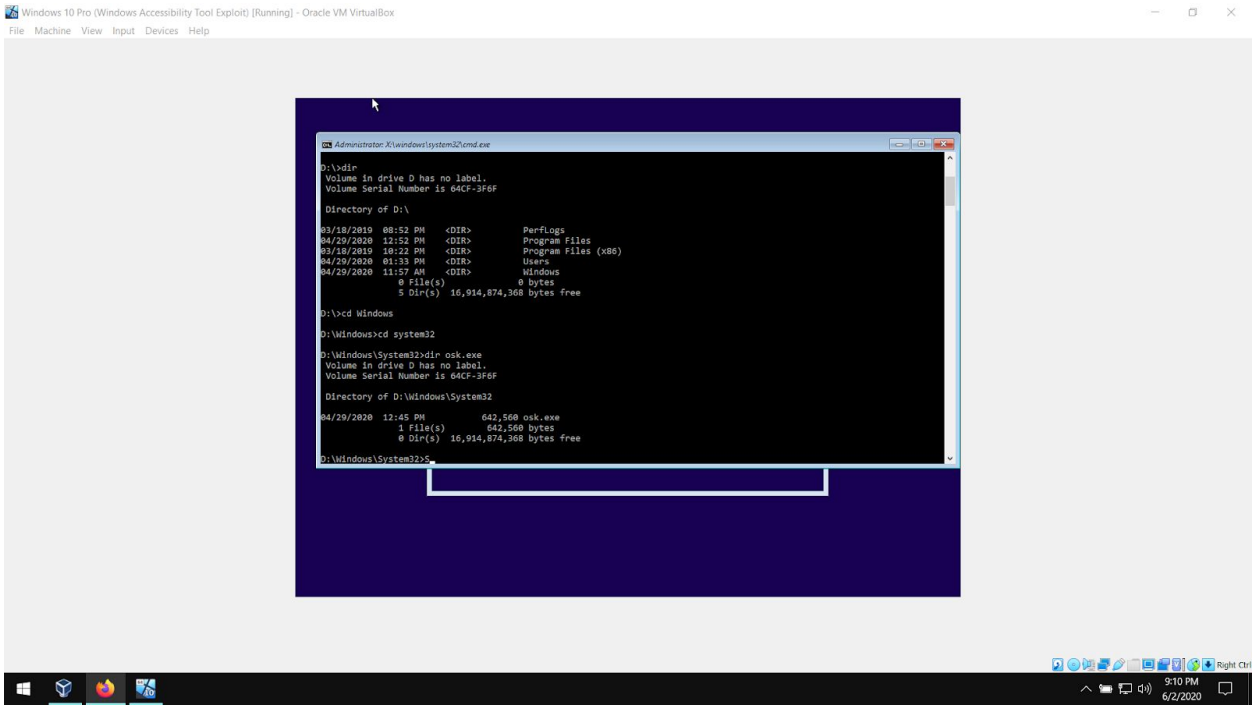
The next phase of the exploit requires us to find a directory that holds a file we want to rename. Using the dir command displays the files in drive c:\ however, no files are located in c:\

Virtualbox - Administrator command prompt



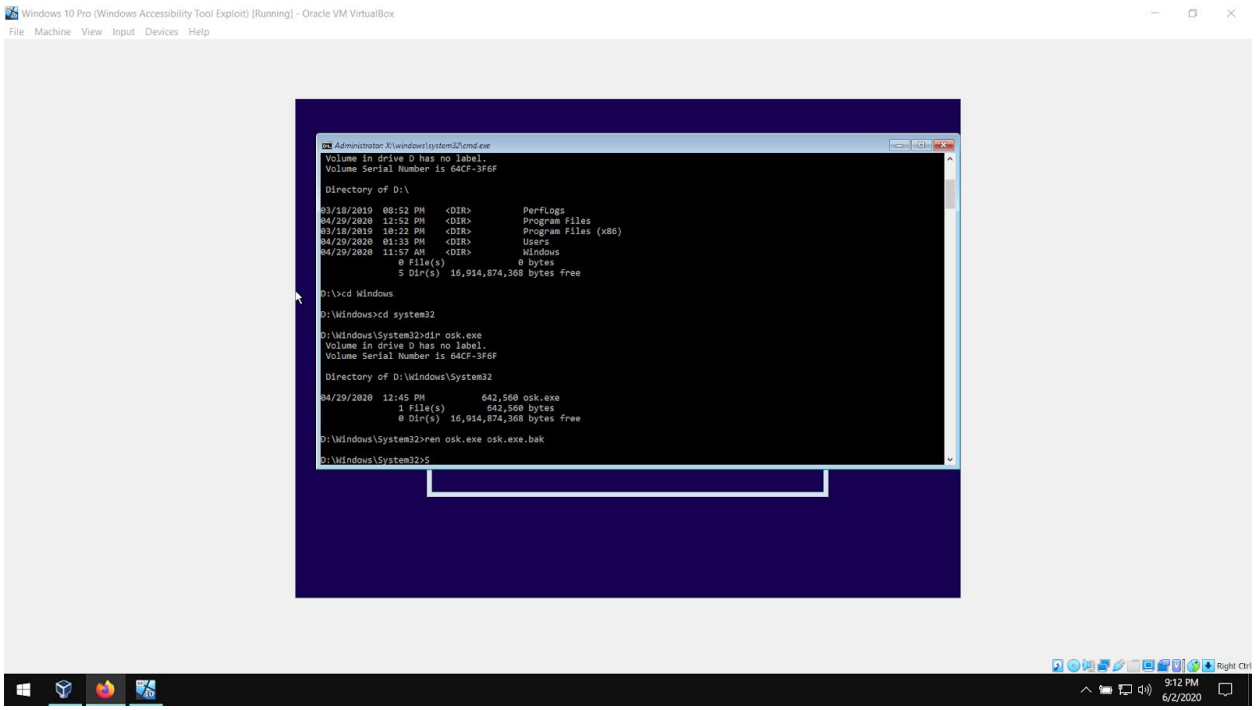
Changing the director to d:\ brings success, here we can see there are 5 directories.

Virtualbox - Administrator command prompt



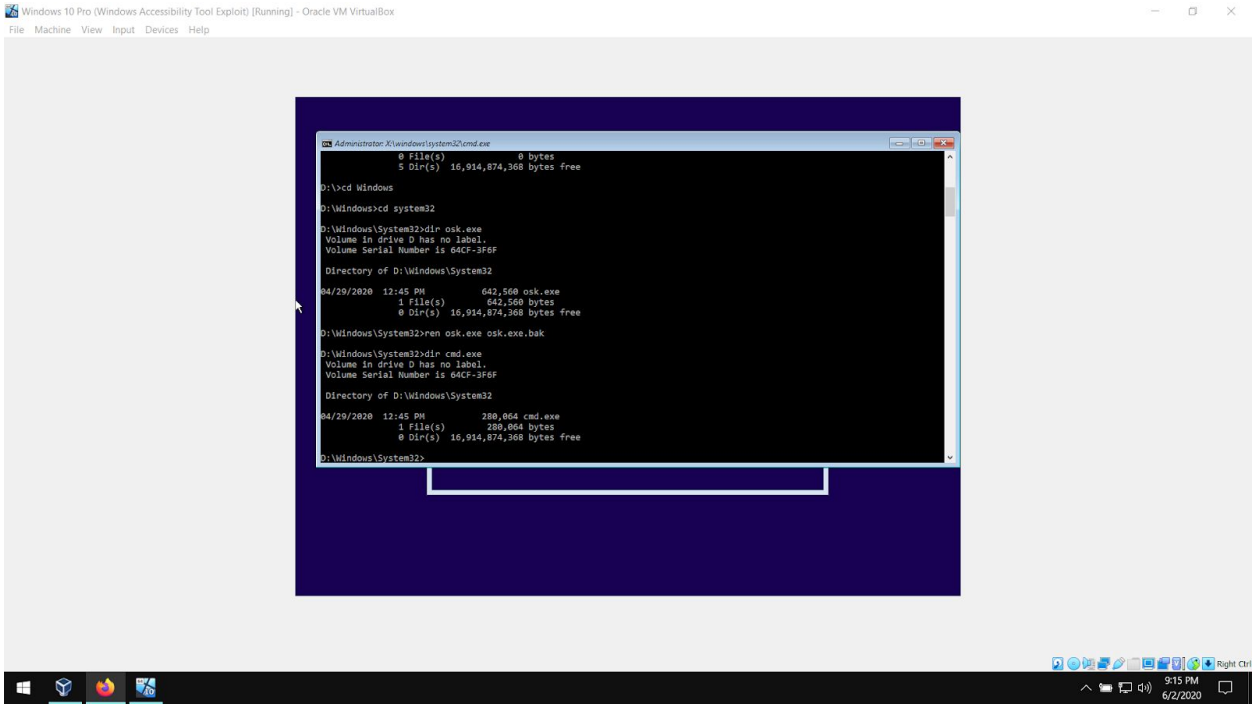
The file is located in \Windows\system32 and is called osk.exe, On-Screen Keyboard.

Virtualbox - Administrator command prompt



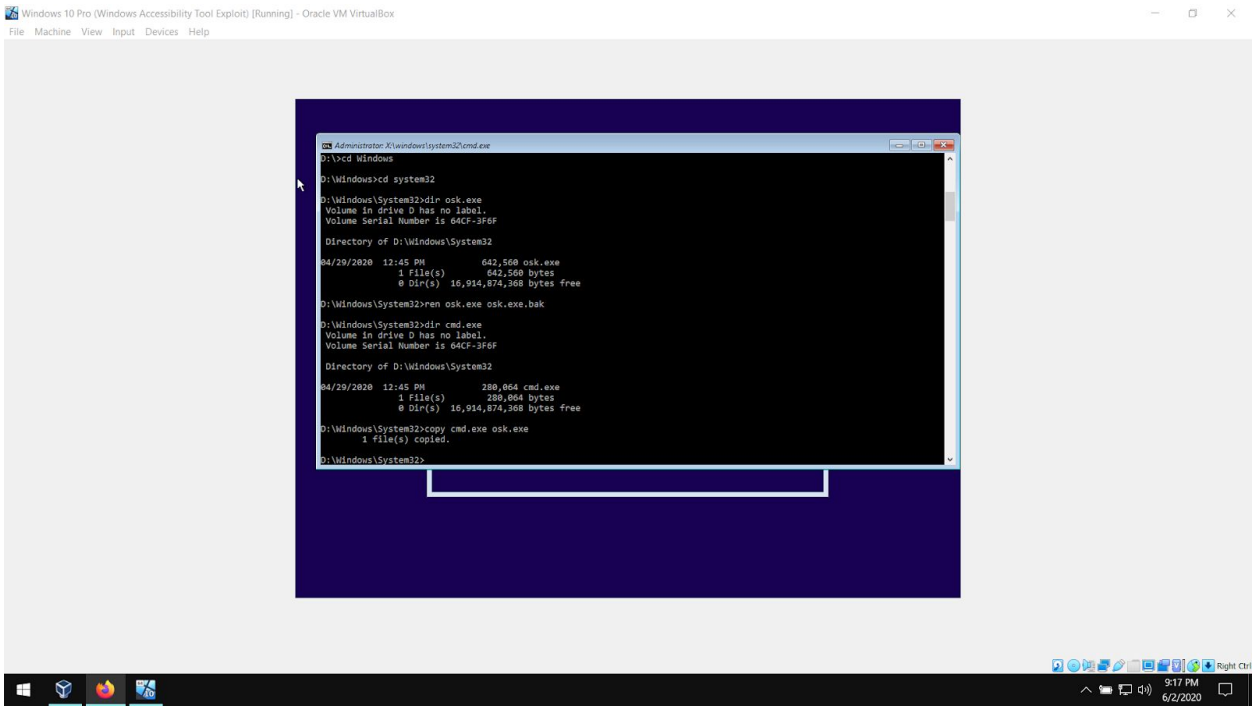
osk.exe is renamed to osk.exe.bak, not deleting the file but merely renaming it. The file can be restored once the lab is over or the virtual machine can simply be rolled back to a previous version.

Virtualbox - Administrator command prompt



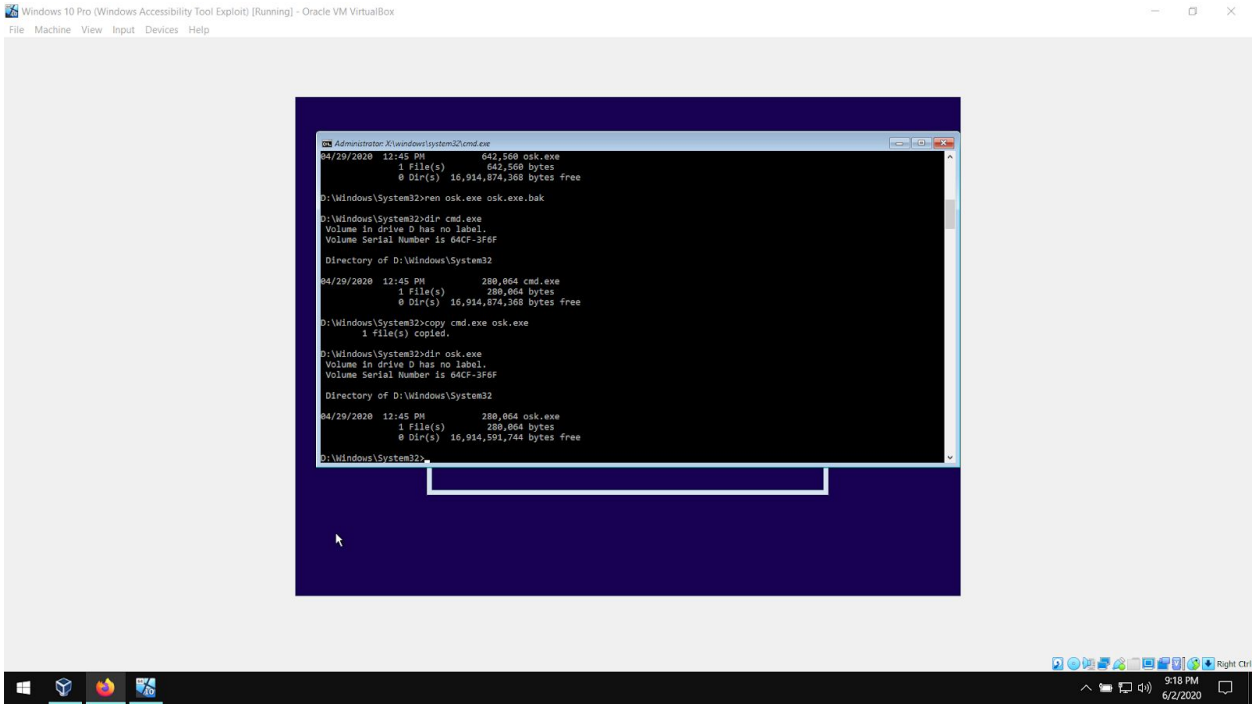
The second file is the command prompt itself known as cmd.exe. It is located in the same system32 fold as the osk.exe is located.

Virtualbox - Administrator command prompt



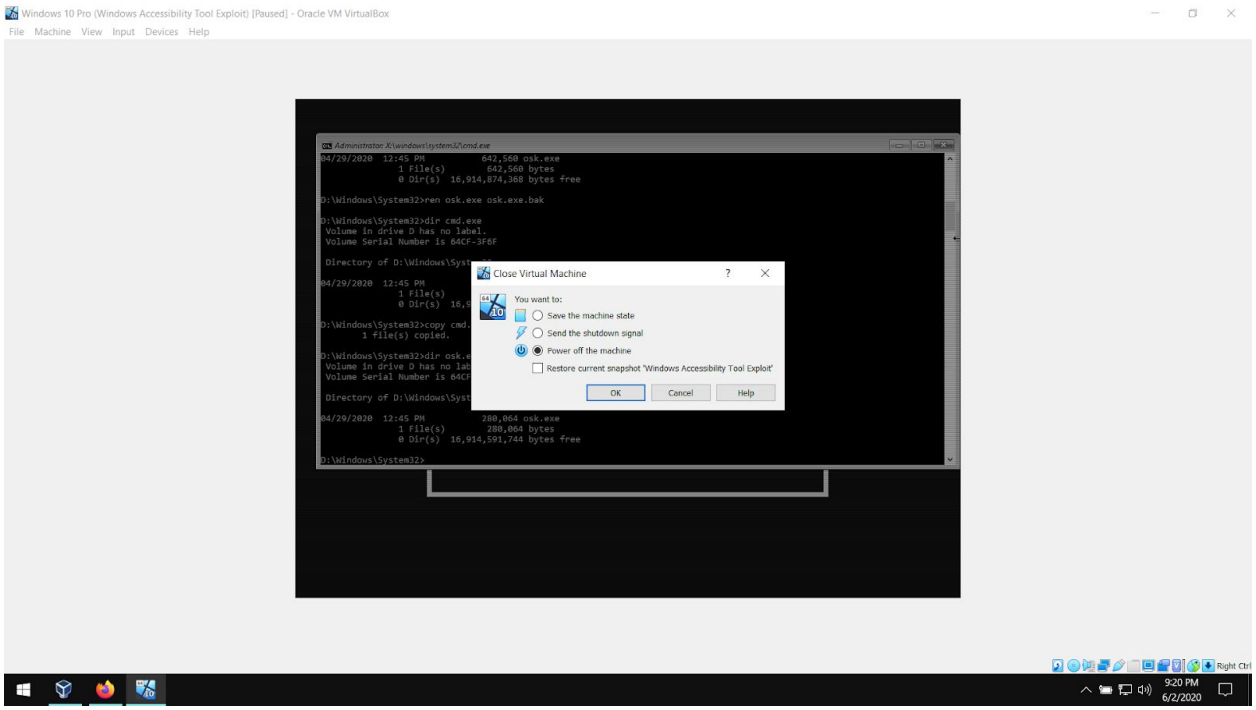
The command prompt executable is not erased from the system32 folder, rather is copied to the now available osk.exe file name and path.

Virtualbox - Administrator command prompt



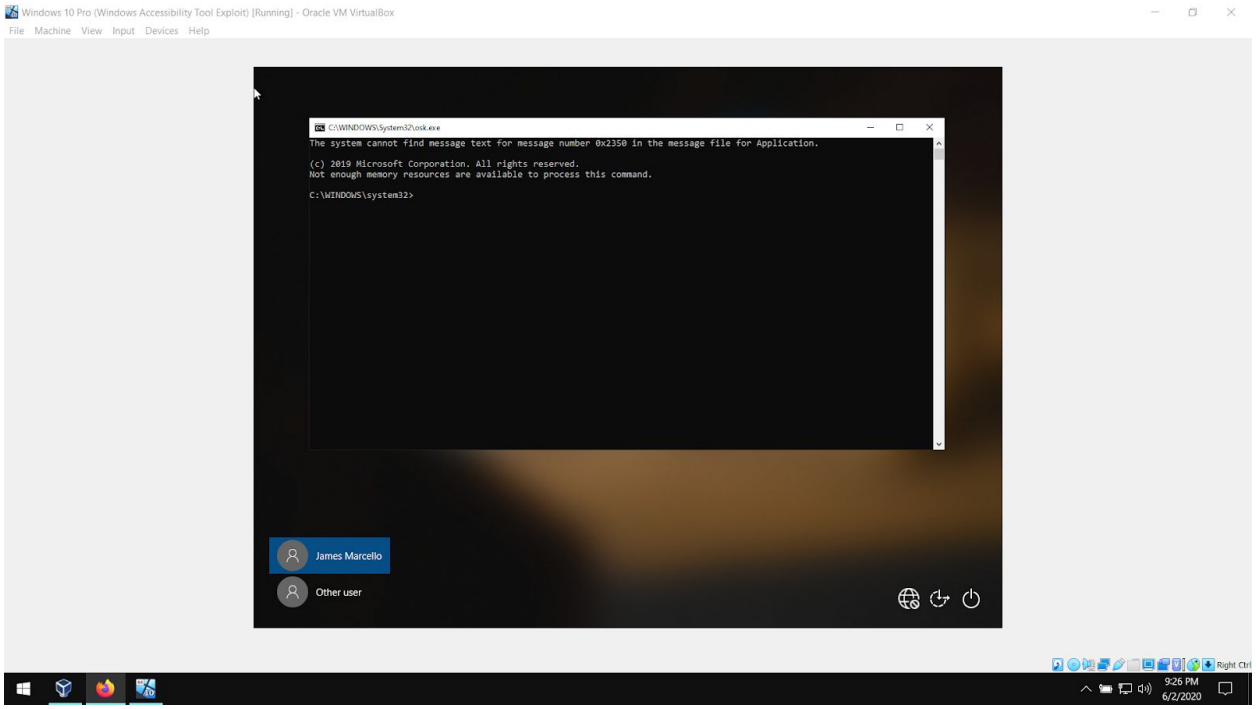
Searching for the fake osk.exe files returns a file.

Virtualbox - Close virtual machine prompt



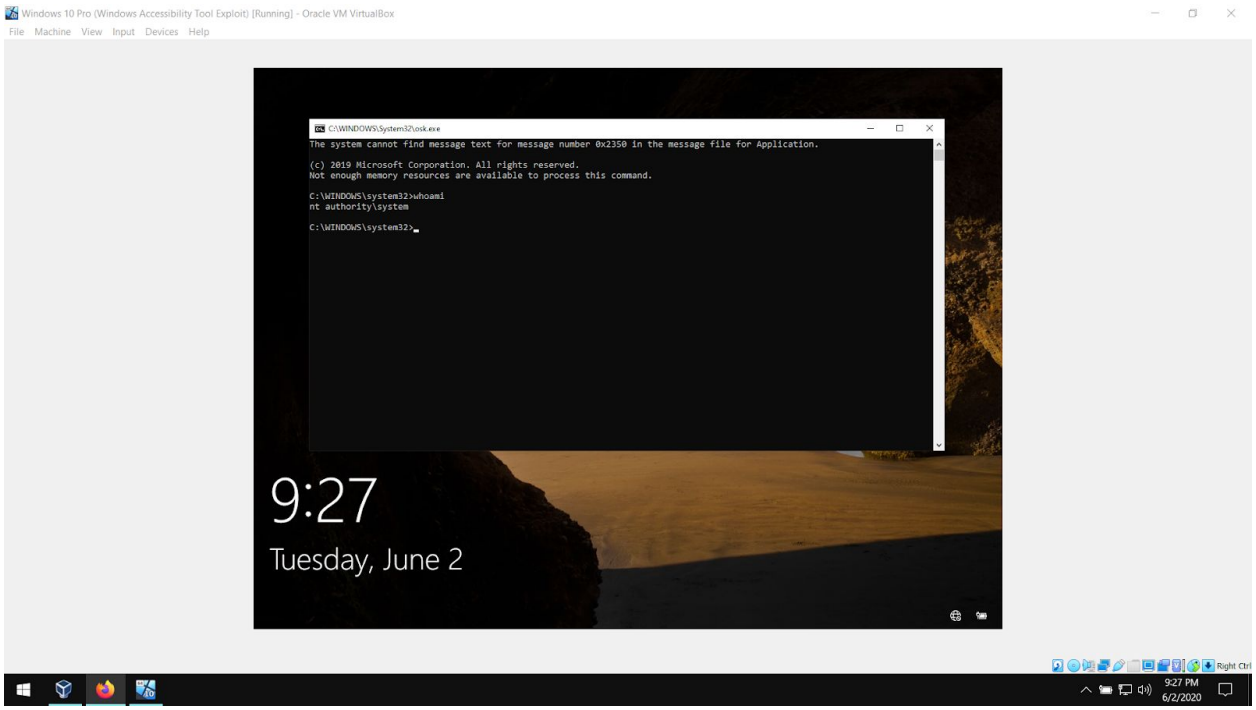
The system will now reboot.

Virtualbox - Close virtual machine prompt



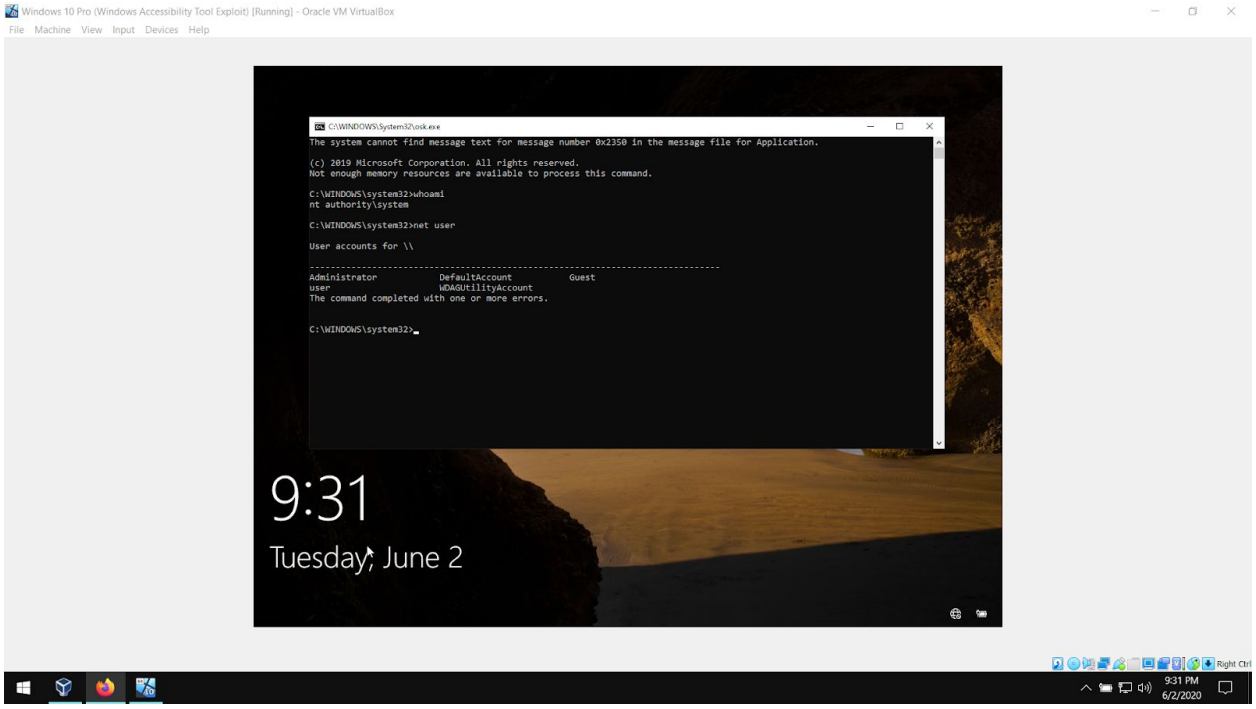
The system is NOT booted from DVD but rather the local install. After OnScreen Keyboard is selected, the command prompt executes.

Virtualbox - Windows 10 Pro



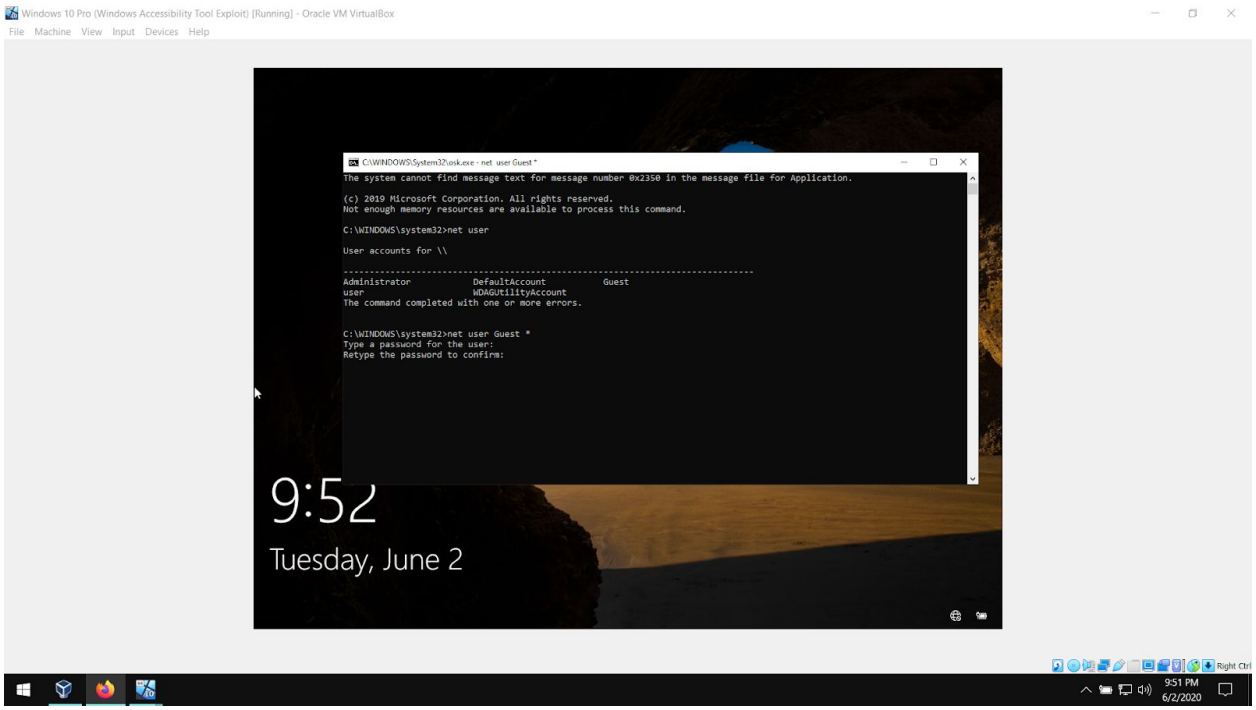
Using the whoami command will establish what privileges are available. For this exploit, system user is accessible.

Virtualbox - Windows 10 Pro CMD



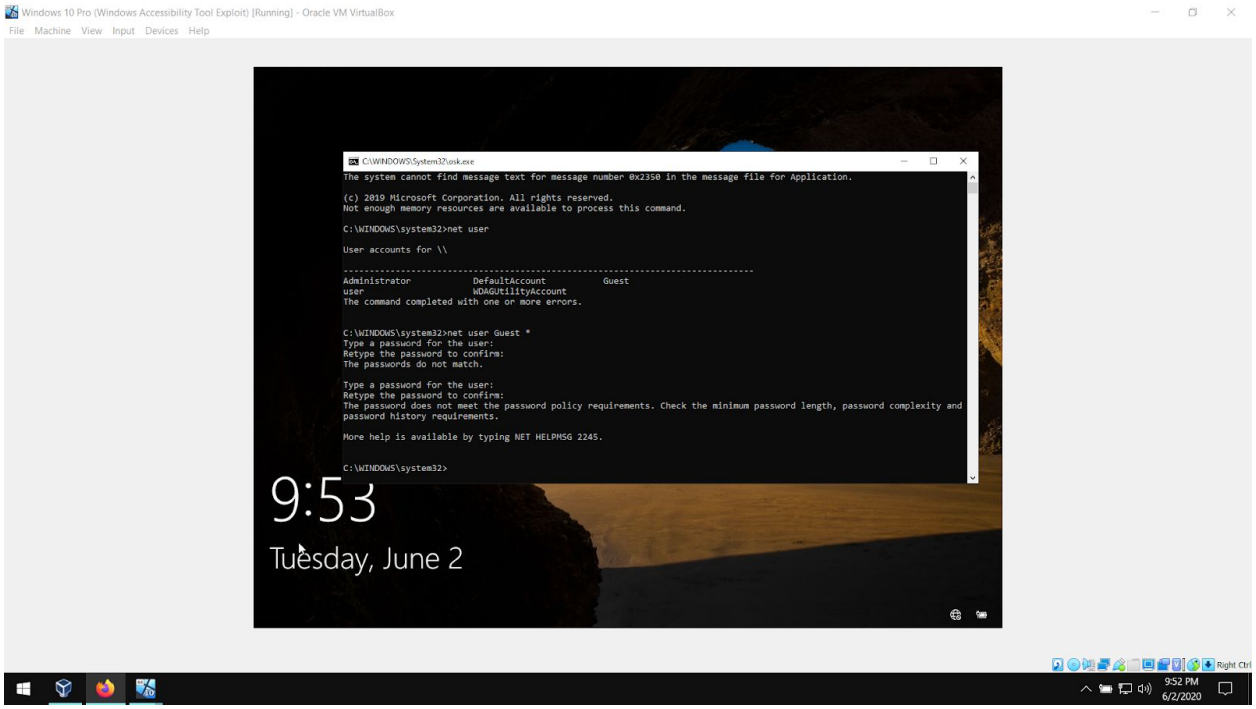
Using the command net user displays the Administrator and user accounts on the machine. For this particular Windows 10 Pro install, the Administrator is Guest.

Virtualbox - Windows 10 Pro CMD



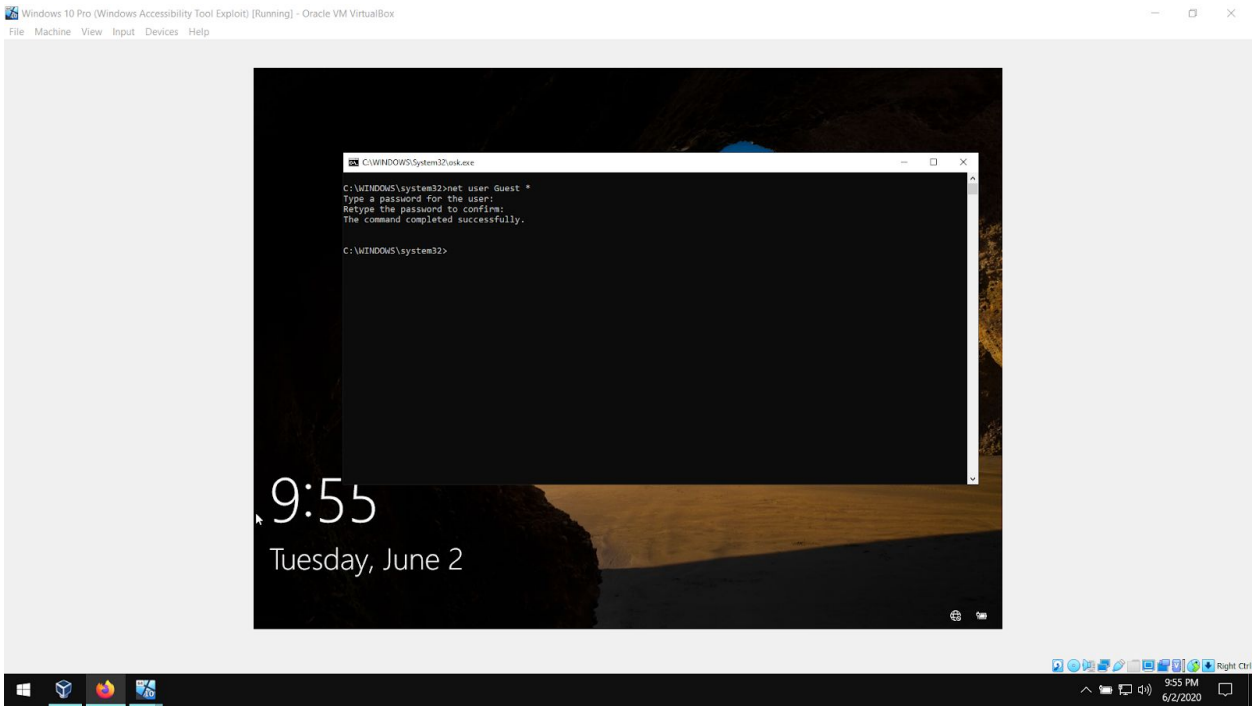
Using the command net user Guest * will reset the password for the Guest account.

Virtualbox - Windows 10 Pro CMD



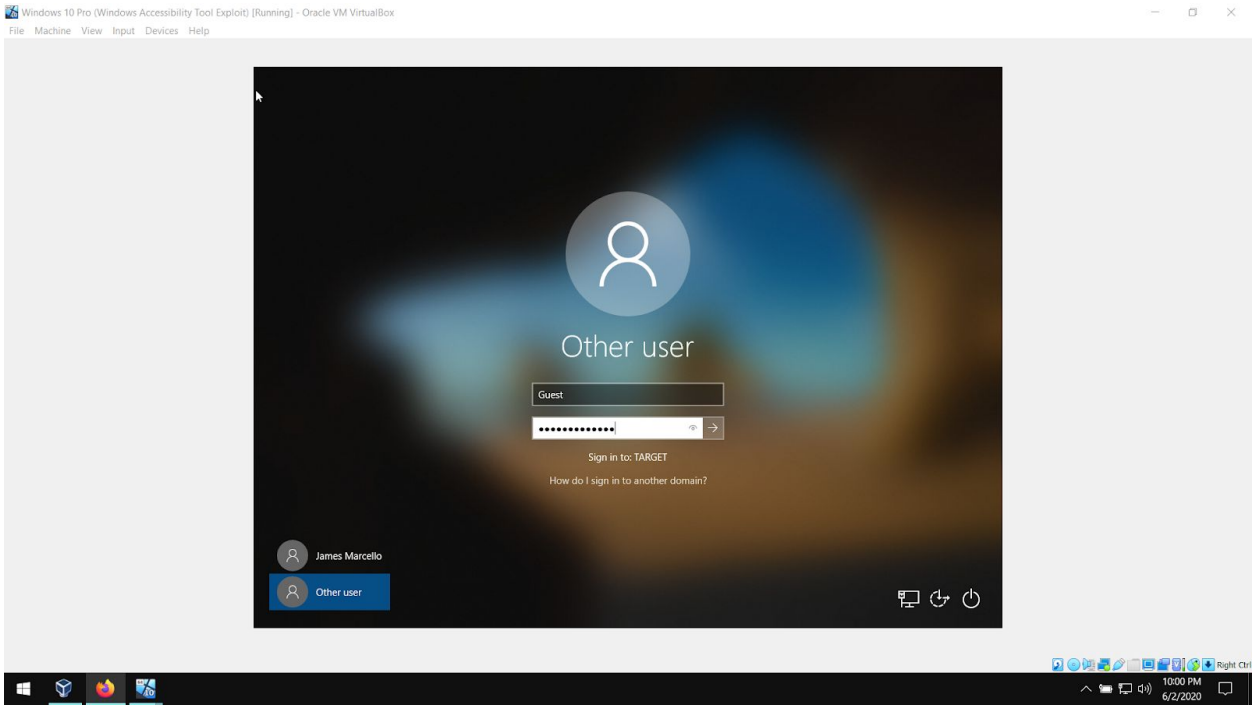
However, there is a password policy in place from the domain controller.

Virtualbox - Windows 10 Pro CMD



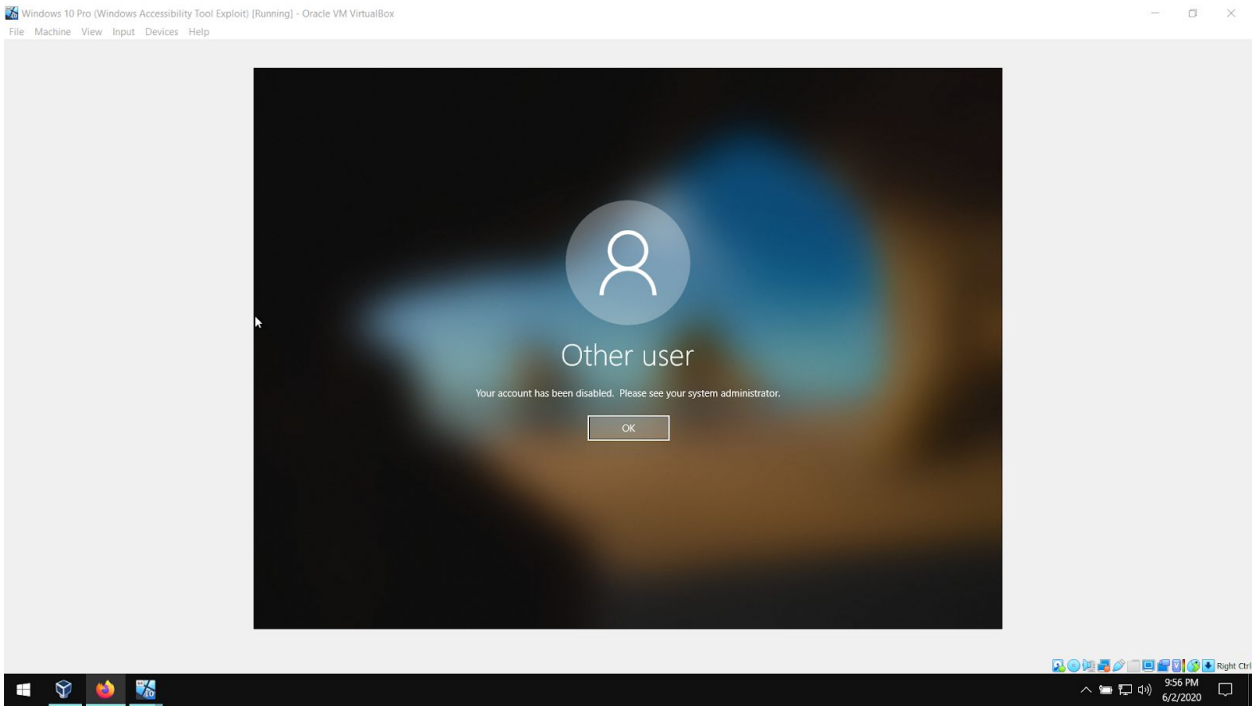
The password was successfully reset with Password123!

Virtualbox - Windows 10 Pro



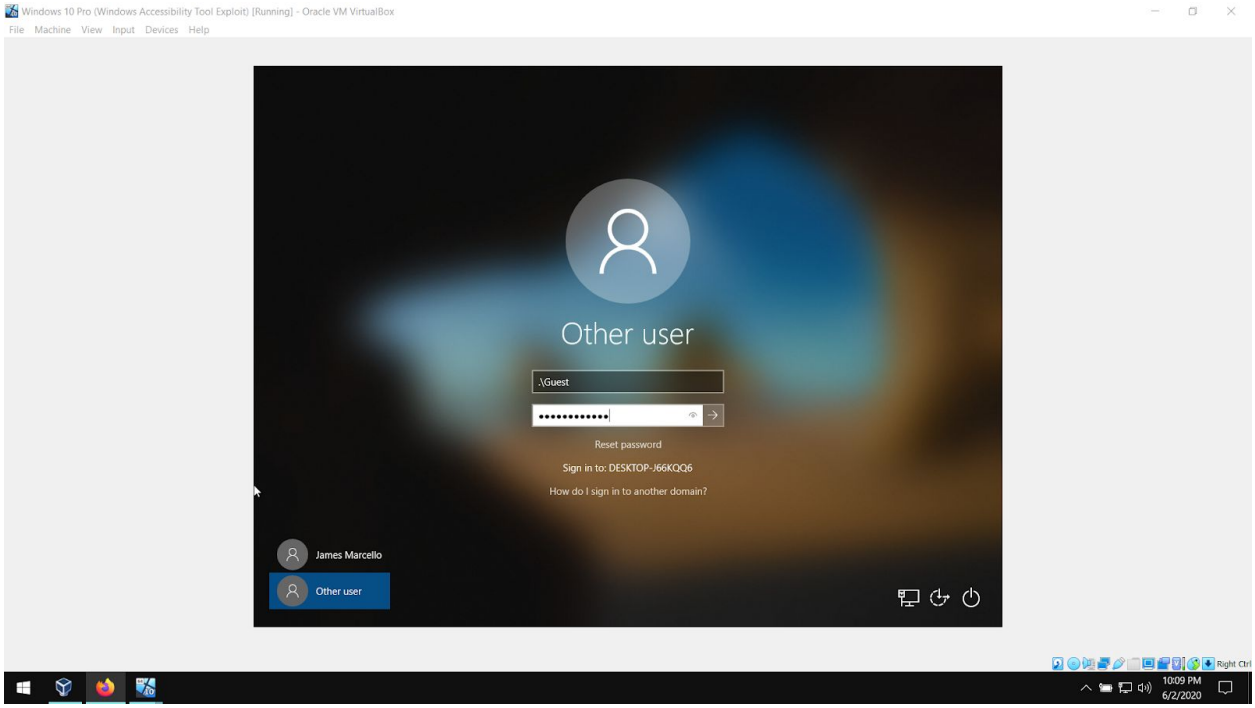
Back at the login screen, “Other user” is selected with Guest as the user name and Password123!

Virtualbox - Windows 10 Pro



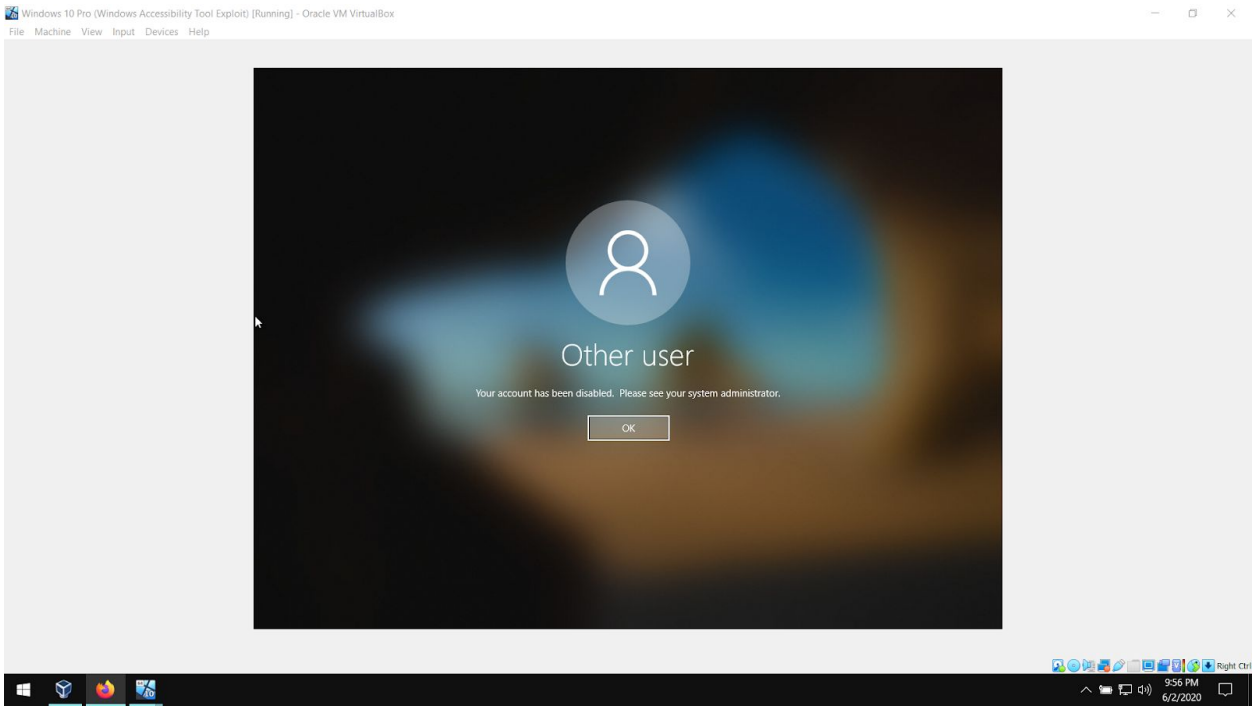
Instead of logging in, the account has been disabled. This may be due to a windows update that checks file integrity.

Virtualbox - Windows 10 Pro



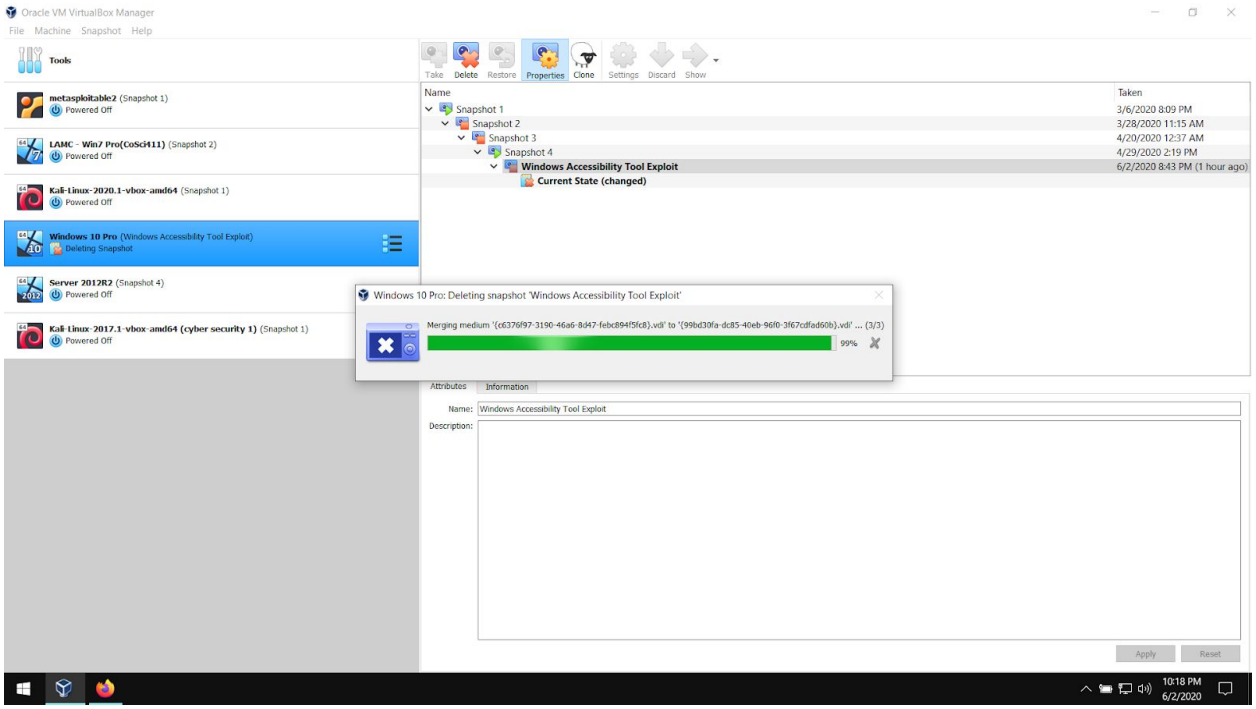
Using the .\Guest as login also did not work.

Virtualbox - Windows 10 Pro



.\Guest login results

Virtualbox - Snapshot Deletion

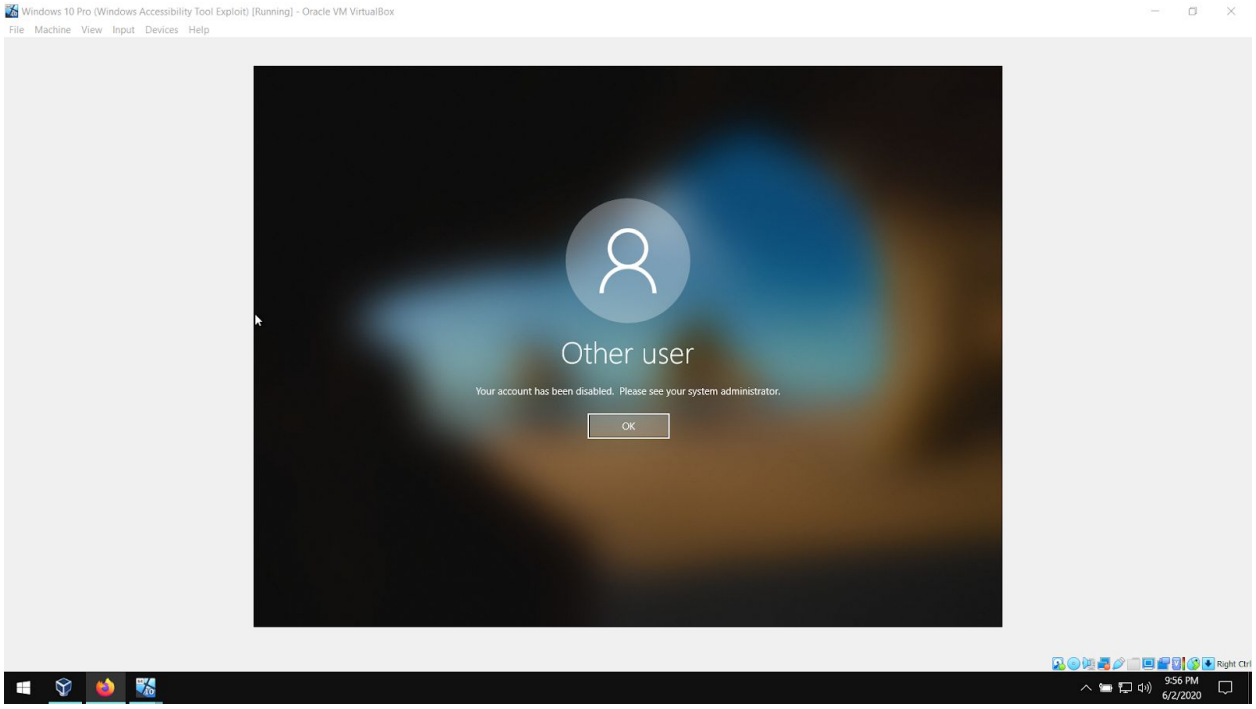


Deleting the snapshot brings the machine back to a working state.

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.

> Having the system throw an account disabled error was a surprise. This was most likely due to a windows update that fixed the file rename and copy exploit.

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



Final screenshot

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

> The exploit worked up to a point. Changing the password was successful but logging into the system was prevented. However, having the command prompt enabled as system user all but ensures any malicious attempts could proceed if a hacker had physical access to a machine. For the purposes of this lab the virtual machine will be rolled back to a previous snapshot. However, if that was not possible, safe mode could be used to re-enable the administrator account.[1] This may be the easier solution given that system user privileges are enabled.

[1] https://support.microsoft.com/en-us/help/814777/how-to-access-the-computer-after-you-disable-the-administrator-account