Windows Hax

Benjamin Brewster

Why You Need to Care

- Because someday you'll have to:
  - Break into Windows: it's as easy as forgetting to set the parking brake
  - Have a fun party trick to show off
  - Convince people to protect physical access to their computers
  - Own up to the fact that you forgot that messing with accounts that are Domain or Bitlocker-protected likely means deleting all the data - Ooops - these only work with local accounts

Two Different Windows Hacks

- These two hacks work on any version of Windows or Windows Server, as far as I've been able to find out
- The first abuses the *actual Windows installation CD*'s ability to grant administrator rights to command prompts it runs
- The second uses a Linux distro to edit the password *directly*; special cryptographic code is used which is illegal to re-export from various countries as a result of the same laws which make exporting Playstation 2's illegal:
  - http://www.nytimes.com/library/review/061399china-chips-review.html
- Let's demonstrate both! Pay no attention to the sirens!

Windows 10 Install CD Hack: The Situation

Say

- We've got a Windows box we don't know the local password to. How do we get in?
- With the basic, non-edited, non-strange, stock Windows Installation CD

Demonstrate

- Using the Win10_Reference VM, unplug the network cable from Settings -> Network -> Adapter 1 -> Advanced -> uncheck "Cable Connected"
- Boot the VM
- Click the Accessibility icon
- Hard kill the VM, restore to Base snapshot, if needed
- Insert the Windows 10 CD
- Make sure the network cable is unplugged again

Setting Up the Hack

Say

- Lets get the Windows VM running, but booted from the Windows install disk, not from the hard drive

- Navigate the repair tools until we get an administrator prompt!

Demonstrate

- Boot the Win10 VM
- Watch for the "Press any key to boot from CD" message, hit a key when it appears
- Click Next, then Repair Your Computer

- At the Choose an option screen, click Troubleshoot
- Click Command Prompt
- Note the Administrator note in the upper left!

The Hack

Say	Demonstrate
• Now we need to look for the boot drive - try C	• `C:`
• No files here	• `dir`
• Try D	• `D:`
• Here's our files!	• `dir`
• Go into the directory we need to manipulate	• `cd Windows\System32`
• Move away the existing accessibility tool	• `RENAME Utilman.exe Utilman.exe.lulz`
• Copy a command prompt into the place of the accessibility tool	• `COPY cmd.exe Utilman.exe`
• Reboot back to normal Windows	• Eject the CD: Devices -> Optical Drives -> Remove disk... • Hard Reset the PC: Machine: Reset

The Hack

Say

- Poof, a prompt!

- Reset the password for User

Demonstrate

- Click the screen to show the login prompt
- Click the Accessibility icon in the bottom right

- `net user User *`
- Enter a new password twice
- Close the prompt

- Click the screen to make the password prompt appear
- Log in with your new password

Undo the Hack

Say

- Find the scene of the crime
- Delete our copied command prompt
- You can try to rename the Accessibility program, but you won't be able to: we can't change this file until we gain permissions to do so

Demonstrate

- Open Windows Explorer
- Go to C:\Windows\System32
- Delete Utilman.exe
- Try to rename Utilman.exe.lulz to Utilman.exe

Undo the Hack

Say

- Get into the advanced properties for this file so that we can make the permissions change
- Here, you can see that not even Administrators have rights to modify this file (no modify or)
- First, let's change the owner: the current owner is "NT SERVICE\TrustedInstaller"
- Enter in our user account as the new owner
- Verify that Windows knows who we're talking about

Demonstrate

- Right-click -> Properties -> Security Tab -> Advanced button
- Up above, next to Owner, click the Change link
- Enter in the field at the bottom our username: "User"
- Click the Check Names button to verify the name
- Click OK, click OK to close the advanced permissions.
- Click OK on the Properties dialog box

Undo the Hack

Say	Demonstrate
• Get back into the advanced properties for this file so that we can make the permissions change	• Right-click -> Properties -> Security Tab -> Advanced button
• Time to add ourselves	• Click Add at bottom
• Add our user account	• Click Select a Principal in the new window that appears: enter "User"
	• Click Check Names, then OK
• We want all the power	• Click Full Control, then click OK
	• Click Apply on the security settings box, then Yes on the warning
	• Click OK to exit, then OK on the Properties box
• Now we can finally rename the file!	• Rename the file to Utilman.exe
	• Click Yes and then OK on the warnings

Undo the Hack

Say

- Now we need to reset the permissions.

Demonstrate

- Remove the User permissions we added
- Change the owner back to "NT SERVICE\TrustedInstaller"

- Finally, delete the logs so your hack can't be detected. Note: This clearing is itself logged with your current user name.
- Note: the security activity logs of a system are routinely monitored live on a different machine (i.e. all actions on your target system are immediately sent to a different server for safekeeping as soon as they occur).
- ...so you might have to break into that one as well, and... adjust it.

- WIN+X -> Event Viewer
- Expand "Windows Logs"
- Right click on "Security" and click "Clear Log"

Windows 10 Hack Using Linux Distro

Say

- What we want is:
  - Offline NT Password & Registry Editor
- Runs a 17MB Linux distro designed to edit the password files and registry locations for Windows!
- Read about it here:

https://pogostick.net/~pnh/ntpasswd

- Direct download, or get from Box:

https://pogostick.net/~pnh/ntpasswd/cd140201.zip

Demonstrate

- Restore the Windows 10 Base snapshot
- Insert the CD, then reboot the machine
- When it boots, hit enter to boot at the prompt
- Hit enter to accept the hard drive it assumes has your Windows install
- Hit enter to accept option 1, a password reset
- Hit enter to accept option 1, editing the user data & pass

Windows 10 Hack Using Linux Distro

Say

- This is probably the "User" user account, which is the one we want to blank; type in the user account number (as shown), otherwise
- Feels weird to hit "q" here, but relax: it'll ask if we want to save next
- That's it, folks!

Demonstrate

- Hit enter to accept the default user number
- Type "1" and hit enter
- Hit enter to accept the default "quit" option
- Type "q" and hit enter
- Type "y" and hit enter
- Hit enter to accept "n" for no more runs
- Eject CD and reboot!
- Log in with no password - click the "Sign In" button

Conclusion

- Protecting physical access is the bare-minimum of necessary security
- Getting into Windows is trivially easy, and this hasn't been fixed in forever: the Linux distro shown has worked since at least Windows XP, and works on Windows 10 and Windows Server 2016
- Apple has really led in securing macOS and iOS devices from attack even with unfettered physical device