

Forum:[Hack Forums](#)

Thread: [\[USB LIVE BOOT\] Gain Local Admin on ANY Windows Workstation \[SHORTCUT EXPLOITS\]](#)

SIM-4581439 - April 5, 2020, 5:43 pm

In this tutorial you will learn how to gain local administrator access to any Windows machine via a shortcut exploit of either Window's StickyKeys or the Utility Manager. This is a well-known and still unpatched exploit to Windows systems that will guarantee easy admin access. Lets begin!

To kick off this process you will need to be able to 'Live Boot' any Linux distribution of your choice off of a USB. Live Booting is essentially where you have an operating system installed to a USB which boots directly from memory. For all intensive purposes, Kali Linux will be used in this tutorial. If you already know how to setup a Live USB then you can skip this step. To begin you will need a USB, typically no smaller in size than 4 gigabytes. This process will automatically format your USB so make sure any important files you want to keep are backed-up elsewhere. When you have your USB ready you will need the image file of the distribution of Linux you are trying to run. As previously stated, Kali Linux will be used. If you are planning to use the same, the image file can be downloaded [here](#). Be sure to choose the Live version opposed to the installer. You will also need to choose the correct architecture that matches your system, either x32 or x64 bit.

When the image file has completed its download, you will need an image writer that will setup your Live USB. Feel free to use whichever writer you want. [Win32 Disk Imager](#) will be used in this tutorial. You will want to select the USB drive letter to write your image to as well as your image itself. If you're using Win32 Disk Imager, it file filter is set to .img Image file types. You will have to choose the *.* all-files option if your image was distributed as a .DD or .ISO disk image. When you're ready, write the image to the drive. It should look something like this:

Nice! The annoying part is out of the way. This is where we boot into the Live USB and begin altering Window's system files. However, there is a minor hiccup to be aware of. This issue lies mainly with the birth of Windows 10 however it has been noted to happen in the past on previous Windows OS's due to other circumstances. Windows often holds onto a hibernation file, forcing the Windows file system to be in a read-only state. Even when you "shutdown," your operating system may choose to hold this file. This will make it next to impossible to setup this exploit. To combat this, fully shutdown your operating system. When done, power on your machine until you arrive at the Windows login screen. Towards either the bottom left or right of your screen you should see your power options. Select the Restart option. As your computer restarts it will completely purge the system's hibernation file in anticipation for a new one to be created.

As your system is restarting you can live boot into your USB. This can be done by plugging in your USB and hitting your computers default boot-menu runkey. It will be different for all machines. It will most likely be F12, F11, or F10. If done correctly, a boot menu should pop up. You will see the name of your USB listed. Select it. The system boot process may be unique if you're using a different Linux distribution.

Once you log into your Live Linux system, open your file explorer. You will need to locate the Windows partition on your HDD or SSD. You will want to select it. If you get an error, you may be required to properly mount the Windows partition from your terminal. If this step is required, open up

your terminal and type in the command statement:

```
Code sudo fdisk -l
```

When done, you will see many listings of the partitions installed to your drive. You will want to locate the one labeled Microsoft basic data. It should look something like this:

Under the drive column, you will want to copy the device's name for Microsoft basic data. Yours may look different from what's shown above. To mount your Windows partition, type in the command statement:

```
Code sudo mount /dev/DEVICE_NAME /mnt/DEVICE_NAME
```

Although the partition in this tutorial was already mounted properly, yours may look something like this:

When the Windows partition is correctly mounted you can begin creating the exploit. You have two programs you can take advantage of, either: Sticky Keys (sethc.exe) or the Utility Manager (utilman.exe). The goal is to backup either one of these executables mentioned and replace them with a copy of Command Prompt (cmd.exe). You can do this either manually or via the terminal. For this tutorial, Utilman.exe was done in the terminal, and Sethc.exe was done manually. If you chose to utilize the terminal, use the "CD" command to change into the System32 directory of the Windows partition and enter in the command statements:

```
Code mv <EXECUTABLE_NAME>.exe <EXECUTABLE_NAME>.bak
```

```
cp cmd.exe <EXECUTABLE_NAME>.exe
```

It will look like this:

If you plan to modify the executables manually, your process may look like this...

Rename executable to .bak (backup) file:

Copy cmd.exe and rename it to the original executable name:

When one of both of the executables have been modified, power off the Live USB operating system and boot Windows. Once returning to the login screen it is time to execute the original executables via their shortcut key., which at this point have been replaced. To run Sticky Keys, hit the SHIFT key x5 times. If you want to execute the Utility Manager, use the combination CTRL + U, or utilize the Utility Manager button at the bottom of your screen:

As long as the previous steps were carried out correctly, a Command Prompt terminal should appear. Since the Command Prompt isn't being executed from a specific group policy, it will be automatically elevated to a local administrator. Proof:

With administrator privileges you can do a multitude of things at this point. You can create admin and regular user accounts, delete user accounts, etc. By default Windows has a default local administrator account built into the operating system. To enable this account, enter in the command:

```
Code net user administrator /active:yes
```

It should then become enabled, like so:

To create a user account, use the command statement:

Code net user /add [username] [password]

...and to make it an administrator, use:

Code net localgroup administrators [username] /add

So, congratz! You now know how to exploit both the Utility Manager and Sticky Key executable and elevate your privileges to create an administrator account. Happy hacking ???