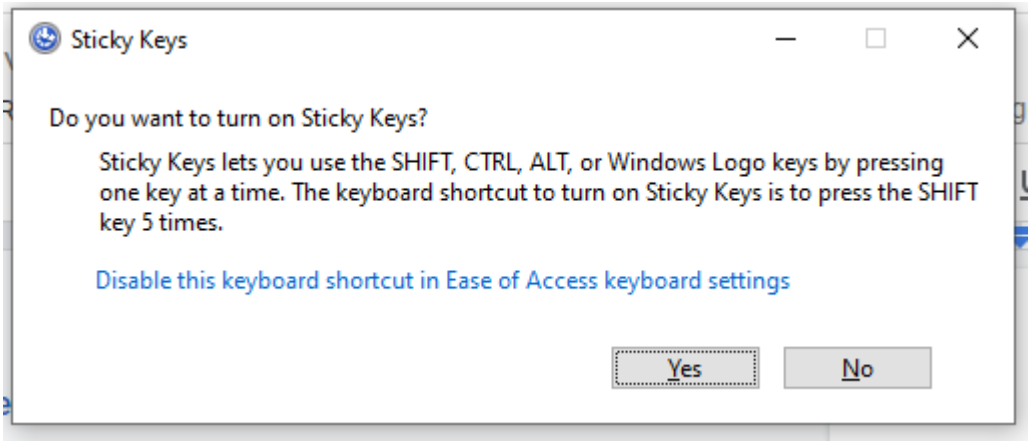
Lock screen/Bitlocker bypass/elevation of privilege in Bitlocker

Provided a windows 10 pc without knowing any passwords and its hard drive being bitlocker protected I can add an administrator account.
A rough overview:
At the sign in screen I select “I have forgotten my password”
I bypass the lock and enable autoplay of removable drives.
I insert an usb stick with my .exe and a junction folder.
I run my .exe.
I take the thumbdrive out and in again, go to main screen.
There I launch narrator, that will execute a dll payload planted earlier.
Now an user account is added called hax with password hax- with membershib in Administrators.
To update the list with accounts to log into you have to click, I forgot my password and then return to main screen.
I have splitted this writeup into 3 parts, 1 parts for each each exploit and one for combining them.

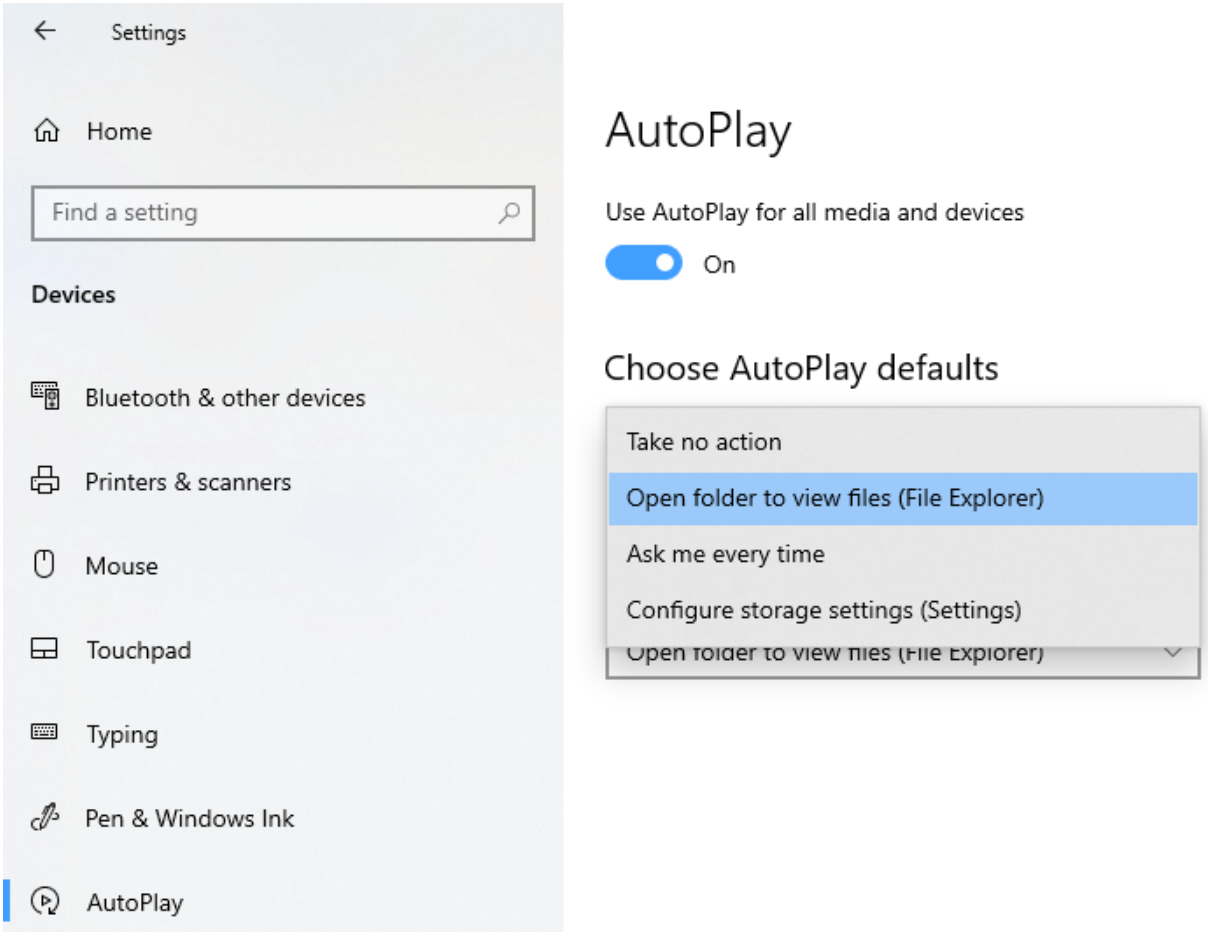
Lock screen bypass:

First we select that I have forgotten my password/PIN.
Now an additional session is launched, with an account that gets created/deleted as needed, user profile service calls it an defaultaccount.
It will have the first avaible name of defaultuser1, defaultuser100000, defaultuser100001 etc.
To escape the lock we have to use Narrator, because- if we manage to launch something we cannot see it, but using narrator we will be able to navigate it.
But how do we launch something?



This screen pops up when pressing shift 5 times quickly, there is a link to open the settings app- and the link actually works, we just cannot see the launched settings app.

Giving the launched app focus is a little bit tricky, you have to click the link and then click a place where the launched app would be if visible, with the correct timing.
The easiest way to learn to do it is, keep clicking the link, like 2 times a second.
The sticky keys windows will disappear, keep clicking- you will now see a focus box drawn that is in the middle of the screen.
That was the settings app, you have to stop clicking when it gets focus.
Now we can navigate the settings app using caps lock + left arrow, press that until we reach “Home”, when home have focus hold down Caps Lock and press enter.
Now using Caps Lock + right arrow navigate to Devices and caps lock + enter when it have focus.



Now navigate to autoplay, caps lock + enter and choose to “Open Folder to view files(File explorer)
Allright, now insert the prepared USB drive, wait some seconds, Narrator will announce the drive have opened and the window have focus.
Now select the file Exploit.exe and execute it with caps lock + enter
That is arbetary code execution without using any passwords, but we are llimited by running as the default profile.
I have made a video with my phone, as I cannot take screenshots etc.
https://www.youtube.com/watch?v=ZdsSgklRoag

Elevation of privilege

The root cause is: when a usb stick is mounted bitlocker will create a directory named ClientRecoveryPasswordRotation in System Volume Information and set permissions to:

NT AUTHORITY\Authenticated Users:(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

To redirect the create operation a symbolic link in NT namepace is needed as that allows us to control the filename and its existence do not abort the operation as it is still creating the directory.
Therefore, take an usb drive and make \System Volume Information a mount point targeting \RPC Control
Then make a symbolic link in \RPC Control\ClientRecoveryPasswordRotation targetting \??\C:\windows\system32\Narrator.exe.local
If the usb stick is reinserted the folder C:\windows\system32\Narrator.exe.local will be created with permissions that allows us to create a subdirectory: amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.18362.657_none_e6c5b579130e3898
and inside that we drop a payload dll named comctl32.dll.
Now next time narrator is triggered it will load the dll, I chose narrator as that is triggerable from the login screen as system and is not autoloaded, so if anything goes wrong we can still boot etc.

Combining them

For the ClientRecoveryPasswordRotation exploit to work it requires a symbolic link in \RPC Control.
The executable on the usb drive creates the llnk using two calls to definedosdevice, as that will make the link permanent- so they can survive a logout/in if needed.
Then a loop is started, the exe will:

- Try to create the subdirectory
- Plant the payload comctl32.dll inside it.

It is easy to see when the loop is running as narrator will every 1 second move its focus box and say Access denied..
Now we can use the link created in “RPC Control”, just unplug the usb stick and reinsert it.
Now the writeable directory will be created in system32, on next loop iteration the payload will get planted and exploit.exe will exit.
To test if the exploit have been successful close Narrator and try to start it again.
If narrator do not work it is because the dll is planted, narrator executes it- but it fails to add an account because it is launched as defaultuser1.
When payload is planted just click back to login screen and start Narrator, 3 beeps should play and an messagebox saying the dll have been loaded as SYSTEM should show.
The account have been created but it is not in the list, press “I forgot my password” and click back to update the list.
A new account named hax should appear- with password hax.

To create the USB drive:

```
C:\Users\jonas>format D: /fs:ntfs /q
Insert new disk for drive D:
and press ENTER when ready...
The type of the file system is NTFS.
QuickFormatting 30.0 GB
Volume label (32 characters, ENTER for none)?
Creating file system structures.
Format complete.
    30.0 GB total disk space.
    30.0 GB are available.
```

Now we need to elevate to admin to delete “System Volume Informartion”

```
C:\Users\jonas>d:

D:\>takeown /F "System Volume Information"

SUCCESS: The file (or folder): "D:\System Volume Information" now owned by user
"DESKTOP-LTJEFST\jonas".

D:\>icacls "System Volume Information" /grant Everyone:(F)
processed file: System Volume Information
Successfully processed 1 files; Failed processing 0 files

D:\>rmdir /s /q "System Volume Information"
```

Now we use james forshaws tool(also attached)

```
D:\>createmountpoint "System Volume Information" "\RPC Control"
```

then we copy the attached exploit.exe to it.

```
D:\>copy c:\Users\jonas\source\repos\exploitKit\x64\Release\exploit.exe .
      1 file(s) copied.
```