

Forum:[Hack Forums](#)

Thread: [Bypass Huawei \(Android\) screenlock password](#)

Dzam - May 9, 2022, 3:01 am

Hi there!

I have a Huawei Y5 device. USB debugging wasn't enabled. No google account was used (so I can't just recover my password from there). Is it a way to bypass it without a factory reset?

CryptixHacking - May 22, 2022, 12:09 am

if its a pin password you can use a USB ducky to brute force it. When you plug in the USB ducky using port adapter your device will see it as a external Keyboard nothing more nothing less. From there you can have the code in the USB ducky brute force the pin.

Black koala - June 15, 2022, 12:31 am

(May 22, 2022 12:09 AM)CryptixHacking Wrote: [\[CITE\]](#) if its a pin password you can use a USB ducky to brute force it. When you plug in the USB ducky using port adapter your device will see it as a external Keyboard nothing more nothing less. From there you can have the code in the USB ducky brute force the pin.

but using brute force the phone will block before you have the code

CryptixHacking - June 19, 2022, 3:59 pm

(Jun 15, 2022 12:31 AM)Black koala Wrote: [\[CITE\]](#) but using brute force the phone will block before you have the code

Depends on how they setup the pincode and the OS of the phone. On android it would ask you when setting up a pin code if you even want blockouts or a course action taken upon so many failed entered pin codes. But not all pincode lockscreens will have such blockouts or actions. Wont know till you try but yeah if its setup to lock you out for so many minutes after failed pins then a rubberducky brute force wouldnt work.

There is probably a way you can ssh or shell into the device's HDD from a external PC or device, Much like how you would manually root a device but rather than root it you extract/decrypt the pin its gotta be stored somewhere on the device locally for it to check against to know if the pin code is correct. Now as to where this encrypted pin code file hash is located I have no clue or as to its encryption/hash algorithms. But both android and iOS are just custom linux distros at their core so give you have a decent understanding of unix file structure cant be to hard to find it.

And of course you could always do a safeboot and re-install a fresh OS onto the device to bypass the lockscreen but of course this will also delete everything that was previously on the device, Unless you were able to make copy of the OS before hand and then copy over its media and temp files. In essence you could just extract/rip all the media files and temp data from the apps on the device without going past its lockscreen, Give you can shell into the device from a external PC.