27.2.2023

Enrique Munoz

Hirslanden AG

BadUSB

Enrique Munoz

Inhalt

[Erste Schritte 2](#_Toc128379358)

[Los geht’s 2](#_Toc128379359)

[Was nun? 2](#_Toc128379360)

[Das zweite Script 2](#_Toc128379361)

[Jetzt wird es interessant 3](#_Toc128379362)

[Webserver 3](#_Toc128379363)

[Das Ergebnis 3](#_Toc128379364)

[Ein grosses Problem 3](#_Toc128379365)

[Das erste grosse Script 3](#_Toc128379366)

[Auf der Suche nach einer Lösung 4](#_Toc128379367)

[Die Lösung erklärt 4](#_Toc128379368)

[Das Problem 7](#_Toc128379369)

[Methode 2 7](#_Toc128379370)

[Zufrieden? 8](#_Toc128379371)

[Das letzte Ziel 8](#_Toc128379372)

[Lösung 8](#_Toc128379373)

[Bin ich nun fertig? 8](#_Toc128379374)

[Fazit 8](#_Toc128379375)

Einleitung

Sportferien sind angekommen und innerhalb von 8 Tagen starte ich ein Projekt. In diesem Projekt geht es darum, einen BadUSB selbst von Grund auf zu erstellen. Zur Verfügung habe ich ein Gerät namens Flipper Zero. Dieses Gerät soll mir helfen beim Konfigurieren des USBs und bei der Ausführung.

# Erste Schritte

Als erstes muss ich den Flipper reseten, damit dieser wie neu ist und keine Konfigurationen von früher hat. Unter Settings-> Storage-> Factory-Reset habe ich das Gerät zurückgesetzt. Jetzt muss ich nurnoch die neue Firmware updaten. Mit der Applikation qFlipper kann ich per GUI das Firmware Update durchführen.

## Los geht’s

Als erstes wollte ich ein Script schreiben, welches schnell geht und einfach zu testen ist. Ich habe mich für ein Script entschieden, welches direkt ein Youtube Video abspielt. Zuerst musste ich sehr viel Google benutzen, da ich keinen Plan hatte wie das funktioniert. Sehr schnell bin ich auf die Übersicht der Sprache gekommen. Ich habe direkt angefangen zu testen und mithilfe eines Scripts online habe ich meinen ersten Test durchgeführt. Der Test ist gescheitert und ich musste herausfinden warum. Das Problem war, dass Gerät, welches ich benutze «Flipper Zero» unterstützt nur das US Tastaturlayout was heisst, alle Y werden zu Z etc. Ich habe danach ein Python Script benutzt, welches die Zeichen umwandelt und somit hat der Youtube Link etwa so ausgesehen.

«https>&&www.zoutube.com&watch\_v)dQw4w9WgXcQ ab?channel)RickAstlez»

Nochmals getestet und es funktionierte. Beim zweiten Mal überraschenderweise nicht. Manchmal ging es und manchmal nicht. Ich war sehr verwirrt und ich wusste es war etwas mit dem Link. Nach vielen Tests habe ich gesehen, dass das Script nicht genau weiss, wo der Link startet. Rapide habe ich das US Zeichen für Doublequotes gesucht und es war ein «@». Somit hat der Link nun wie folgt ausgesehen.

«@https>&&www.zoutube.com&watch\_v)dQw4w9WgXcQ ab?channel)RickAstlez@»

Hiermit funktionierte es perfekt. Schliesslich war ich so stolz auf mich, weil ich das Script selber umgeschrieben habe und ich mich langsam sehr gut mit der Sprache ausgekannt habe. Ich war sehr motiviert und wollte direkt weiter machen.

### Was nun?

Nachdem mein erstes Script funktioniert hat, wusste ich nicht mehr weiter. Ich hatte Ideen aber keinen Plan mit welcher ich starten wollte. Mir war bewusst ich kenne mich langsam gut aus, also habe ich mich für ein Script entschieden, welches alle WLAN-Passwörter des Gerätes holt.

# Das zweite Script

Mit ein wenig Recherche habe ich die richtigen Schritte gefunden und das Script hat alle Passwörter in Files aufgeschrieben. Ich war aber nicht zufrieden. Die Files wurden auf demselben Gerät gespeichert und dies hat mich sehr gestört, weil die Passwörter auf dem anderen Gerät mir nichts bringen. Selbst bin ich auf die Idee gekommen und habe meine externe Disk mit dem Laufwerkbuchstaben W benennt. Das ist wichtig, weil der Pfad fest sein muss und da der Laufwerkbuchstabe W nie benutzt wird, habe ich diesen gewählt. Daraufhin habe ich den Befehl abgeändert und gesagt, die Files sollen auf meine externe Disk gespeichert werden. Getestet und es hat perfekt funktioniert. Je mehr ich gemacht habe desto mehr Motivation habe ich bekommen. Ich konnte schon Passwörter stehlen.

# Jetzt wird es interessant

Nach vielen weiteren Scripts habe ich herausgefunden, wie ich mir Dateien mithilfe eines Discord Bots zusenden kann. Daraufhin habe ich lange an einem Keylogger gearbeitet und nach einigen Tagen habe ich diesen auch zum Funktionieren gebracht. Das grösste Problem bestand darin, mir die Daten zuzusenden. Bei diesem Script konnte in den Discord Bot nicht anwenden, weil es nicht funktioniert hat. Ich habe lange überlegt und bin auf die Idee gekommen einen Webserver zu machen und somit die Daten dort hochzuladen.

## Webserver

Nach wenigen Minuten hatte ich schon meine Lösung für den Webserver. Mithilfe von Python habe ich einen Upload Server gestartet. Jetzt musste ich nur noch ein weiteres Script hinzufügen, welches die Datei auf meinen Server hochlädt, somit kann ich sie auf meinem Gerät herunterladen.

### Das Ergebnis

Einige Stunden später hat das Ganze dann auch schon funktioniert. Ich hatte ein Script welches alle Tasten aufnimmt und in ein File schreibt. Dieses Script läuft unsichtbar im Hintergrund. Danach hatte ich ein Script mit welchem ich dieses File hochladen kann auf meinem Server.

# Ein grosses Problem

Für alle Scripts muss das Gerät entsperrt sein. Dies hat mir nicht gefallen. Was will ich mit diesen Scripts, wenn ich sie nicht einsetzen kann, weil mir das Windowspasswort fehlt. Der Keylogger funktioniert ebenfalls nur im entsperrten zustand, sobald das Gerät gesperrt ist, dann nimmt er die eingegebenen Tasten nicht auf.

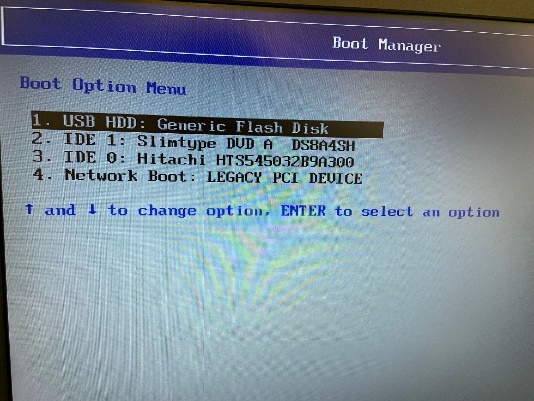
# Das erste grosse Script

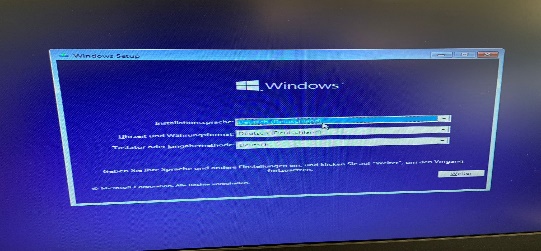
Auf der Suche nach einer Lösung bin ich auf ein Script gestossen, welches das CMD im gesperrten Zustand starten soll. Rapide habe ich das getestet und es funktioniert wirklich. Ich habe es geschafft. Einmal ist das Gerät entsperrt und ich lasse mein Script darauf laufen und schon kann ich auch im gesperrten Zustand darauf zugreifen. Ich war jedoch nicht zufrieden. Immer noch musste das Gerät zuerst entsperrt sein.

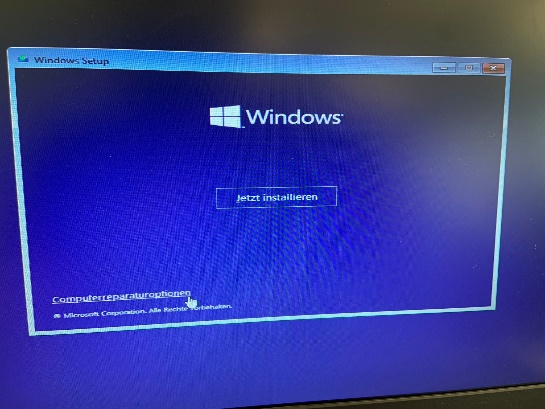
## Auf der Suche nach einer Lösung

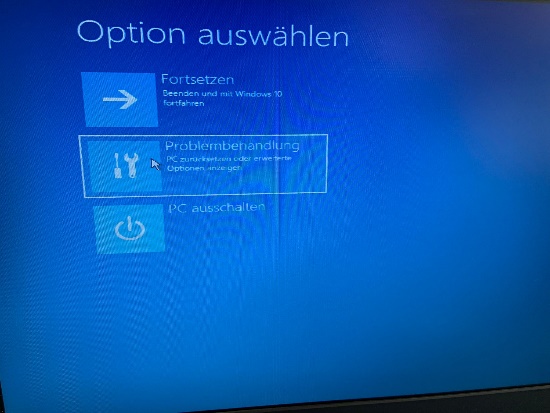
Nach vielem recherchieren bin ich auf die Lösung gestossen. Mithilfe eines Bootsticks kann man das Gerät neu Booten und statt Windows neu zu installieren klickt man auf “Dieses Gerät reparieren”. Diese Funktion ist da, um Fehler beim Starten zu beheben oder allgemeine Systemkonfigurationsfehler zu beheben. In den Einstellungen habe ich dann einen Knop im Sperrbildschirm auf das CMD gebunden, wenn man im Sperrbildschirm auf diesen Knopf drückt, dann startet das CMD statt Einstellungen für den Benutzer wie z.b Kontrast.

### Die Lösung erklärt

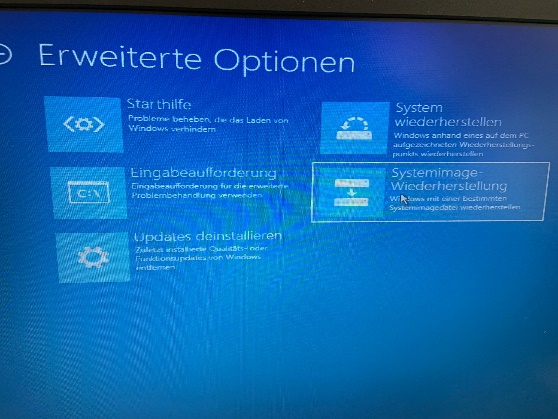
1.) Als erstes braucht man einen USB-Stick, von dem man Booten kann. Diesen steck man in den PC und startet ihn neu. Beim Neustart drückt man ganz oft F12, bis man in das Boot Menü kommt. Daraufhin wählt man seinen Stick aus, somit Booted man jetzt Windows neu.

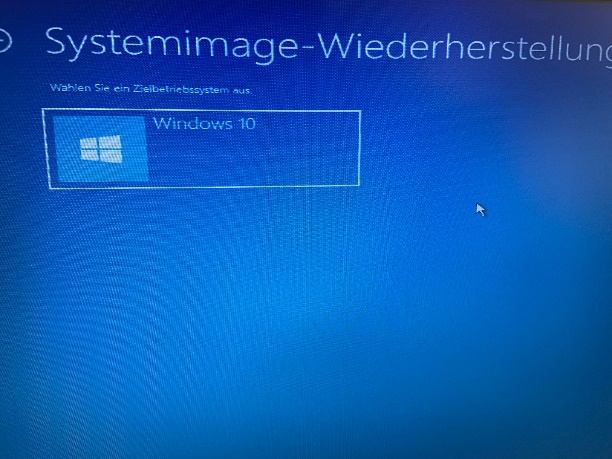
2.) Nun wählt man seine Sprache, Region und sein Tastaturlayout aus.  


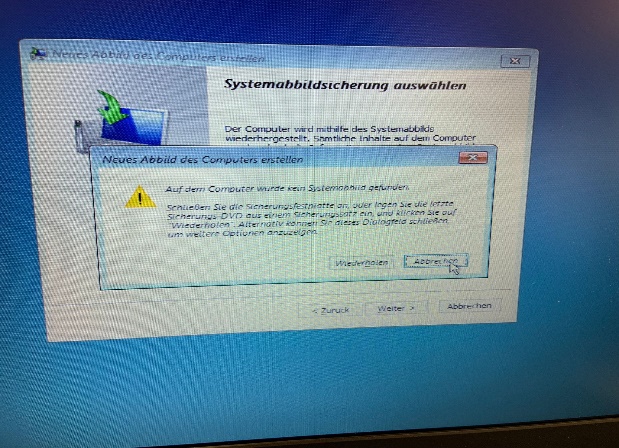
3.) Jetzt klickt man unten links auf ”Computerreperaturoptionen”, denn wir wollen ja nicht wirklich Windows neu Booten, sonst sind unsere Daten weg.

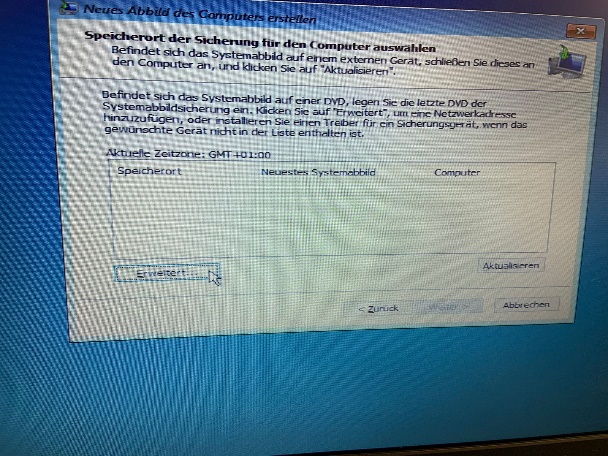


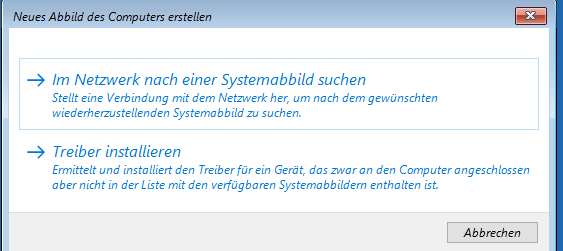
4.) Nachdem man den dritten Schritt gemacht hat, mussman nun «Problembehandlung» auswählen.

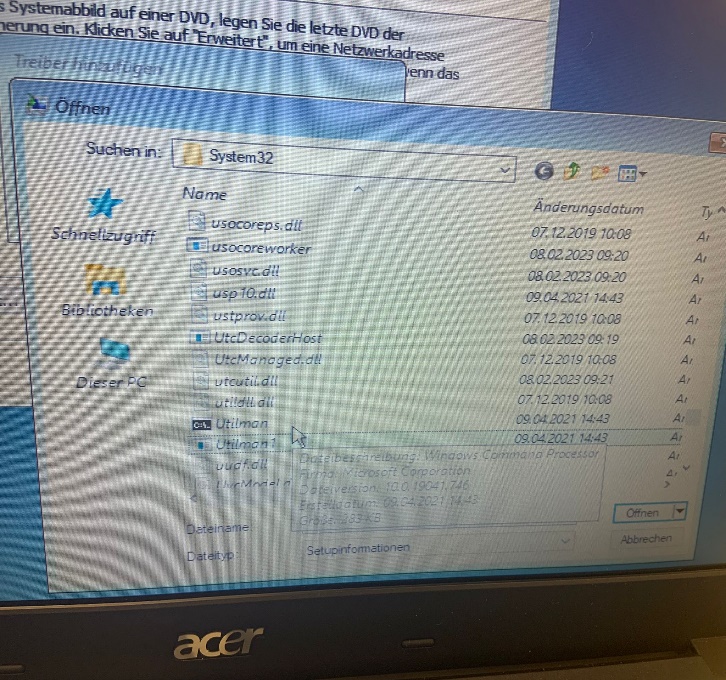
5.) Wir sehen verschiedene Optionen für eine Problembehandlung, unsere ist ”Systemimagewiederherstellung”. Klicken Sie diese an.

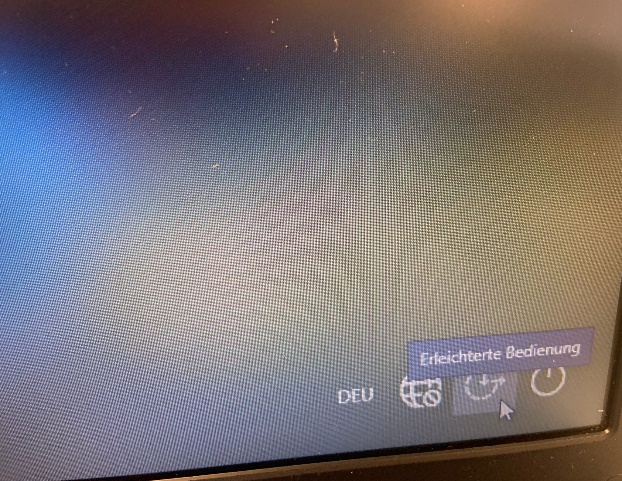
6.) Bitte Wählen sie ihre Windows Version.

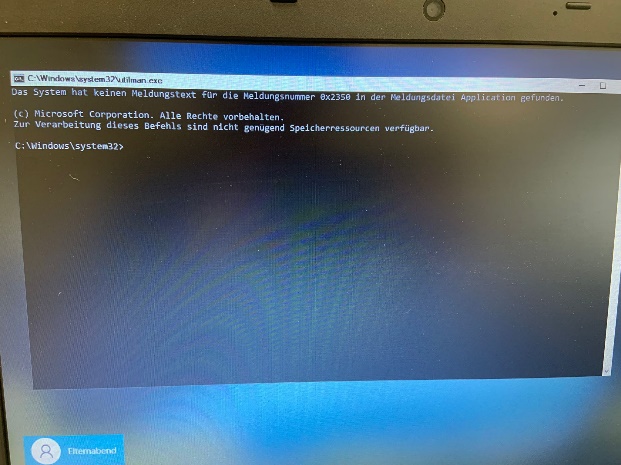
7.) Nachdem sie diese gewählt haben, drücken sie beim ersten Fenster auf ”Abbrechen”.

8.) Beim zweiten Fenster auf ”Erweitert”.

9.) Daraufhin auf ”Treiber installieren” und ”ok”

10.) Jetzt öffnet sich der Ordner mit allen Dateien. Suchen Sie im System32 eine Datei Namens ”Utilman”. Diese Datei nennen Sie ”Utilman1”. Daraufhin suchen Sie eine Datei namens ”cmd”. Diese kopieren sie und mit rechtsklick aktualisieren sie das Ganze. Nach jedem Schritt müssen sie aktualisieren, um die Veränderungen sehen zu können. Nachdem sie das ”cmd” kopiert haben, haben sie nun ein ”cmd” und ”cmd-kopiert” o.ä. Die Datei, welche ”cmd-kopiert” heisst nennen sie nun ”Utilman”. Wir haben gerade den key ”Utilman” auf das ”cmd” gebunden, somit wenn man den ”Utilman” Knopf drückt, kommt statt der normale ”Utilman” unser ”cmd”.

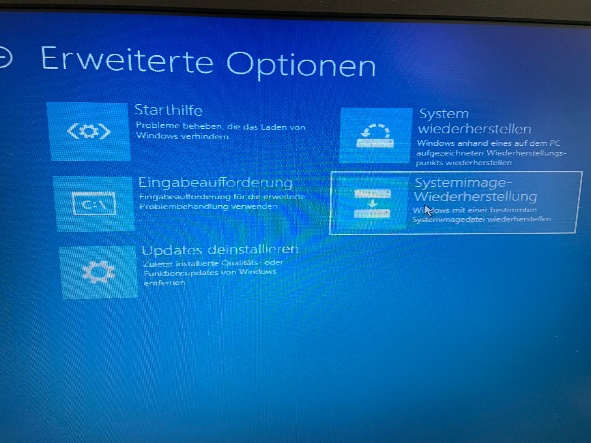
11.) Nachdem sie dies gemacht haben, schliessen sie alle Fenster und drücken fortfahren. Sobald das Gerät gestartet ist, drücken sie unten links auf ”Erleichtere Bedienung” oder anders gesagt ”Utilman”.

12.) Schliesslich öffnet sich das ”cmd”. Sollte es sich nicht direkt öffnen, dann drücken Sie weiter oder warten Sie einen Moment, es kommt vor, dass es ein paar Sekunden benötigt. Schliesslich mit dem Befehl ”Net user <username> <neues Passwort>” können sie das Passwort ändern. Sie können auch ”Net user <username> <Passwort> /add” benutzen, somit erstellen sie einen neuen Benutzer.

# Das Problem

Diese Lösung ist leider bekannt und auf den neuen Windows Versionen funktioniert sie nicht mehr. Ich wäre aber nicht ich, wenn ich nicht eine zweite Lösung für die neuen Versionen hätte. Ab Windows 10 1809 funktioniert die erste Methode nicht mehr und man muss die zweite anwenden.

### Methode 2

Als erstes muss man alle Schritte der ersten Methode anwenden, bis man zu den reperraturoptionen kommt. Hier wählen Sie statt ”Systemimagewiederherstellung” ”Eingabeaufforderung”.Hier wählen Sie statt ”Systemimagewiederherstellung” ”Eingabeaufforderung”.

In das cmd schreibt man “Diskpart”. Nach einem kurzen Moment sollte links “Diskpart” stehen. Daraufhin schreiben Sie “list volume” und drücken Enter. Jetzt sehen sie wo Windows installiert ist, in meinem Fall ist es im c:. Geben Sie nun “exit” ein.

In meinem Fall mache ich es hier mit c:, sollte ihr Windows auf einem anderen Laufwerk gespeichert sein, dann ersetzen sie das c mit ihrem Laufwerkbuchstaben.

Nun Geben sie den Befehl “ cd /d c:\windows\system32” ein. Damit wechseln sie in den system32 Ordner.

Im Ordner angekommen ist der nächste Befehl “ rename utilman.exe utilman.bak”. Hiermit bennen sie die utilman Datei um.

Daraufhin kommt der letzte Befehl “copy cmd.exe utilman.exe”. Hiermit wird das cmd zur utilman.

Nun starten sie ihr Gerät neu.

Im Anmeldebildschirm angekommen halten sie die Shift Taste gedrückt und drücken unten links auf Neustarten. Ein blaues Fenster sollte sich nun öffnen und unter Problembehandlung -> Erweiterte Optionen -> Starteinstellungen finden sie “Neustart”, drücken Sie dies und warten Sie. Sobald das Gerät aufstarten kommt für wenige Sekunden einen Blauen Bildschirm, hier drücken sie schnell “8” oder “F8”.

Wieder im Anmeldebildschirm machen sie dasselbe nochmal. Startet das Gerät nun nochmal Drücken Sie statt “8” oder “F8” “4” oder “F4”. Sobald Sie im Anmeldebilschirm angekommen sind, drücken sie schnell unten links auf das utilman Symbol. Das cmd sollte nun aufgehen und sie geben entweder “net user <benutzername> <neues Passwort>” ein oder “net user <benutzername> <passwort> /add” ein. Dieser Ablauf muss schnell gehen, da Windows das cmd erkennt und abschalten will. Jetzt können Sie sich einloggen und falls Sie einen neuen Benutzer erstellt haben mit dem Befehl “net localgroup Administratoren <benutzername> /add” den Benutzer zur Admin Gruppe hinzufügen.

# Zufrieden?

Endlich war ich zufrieden. Ich brauche das Windowspasswort nicht mehr. Nach 19 Scripts habe ich es geschafft. Ohne das Windowspasswort war es nun möglich das Gerät zu entsperren und alles zu machen, was ich will. Ich fühlte mich Mächtig, da ich auf jedes Gerät nun zugreifen kann. Zugleich war ich auch sehr stolz, da ich mir das ganze Wissen selber und rapide angeeignet habe.

# Das letzte Ziel

Der ganze Vorgang dauert eine Weile, deshalb wollte ich eine Lösung finden, bei welcher ich weniger Zeit brauche oder mithilfe von Fernzugriff Dinge machen kann. Bis ich alles gemacht habe wäre der Besitzer des Gerätes schon wieder vor Ort.

## Lösung

Ich habe lange gesucht und bin auf ein Script gestossen, welches im Hintergrund eine Tür über PowerShell offenlässt. Rapide habe ich das Script unter die Lupe genommen und umgeschrieben. Endlich war es fertig und ich konnte es testen. Als ich es getestet habe funktionierte es nicht. Ich habe gesucht und gewühlt bis ich den Fehler gefunden habe. PowerShell wollte das Script nicht ausführen, da es nicht signiert war. Ich habe schnell ein neues Script geschrieben, welches die Berechtigungen von PowerShell ändert. Endlich war ich fertig. Es funktionierte.

# Bin ich nun fertig?

Ich habe lange überlegt und mir ist nichts mehr eingefallen. Ich konnte ohne Passwort das Gerät entsperren, konnte somit eine Hintertür öffnen und von meinem Gerät aus im Hintergrund mit Adminrechte machen, was ich will. Ich war sehr stolz auf mich. Ich habe von 0 gestartet und innerhalb von 8 Tagen es geschafft mir das ganze Wissen anzueignen.

# Fazit

Das war das beste Projekt, welches ich jemals gemacht habe. Es war sehr interessant zugleich aber auch sehr kompliziert. In diesem Projekt hatte ich sehr viele Up und Down’s. Dinge funktionierten direkt oder ich musste mehrere Stunden lang Fehler suchen. Ich habe Funktionen von Windows kennengelernt, von denen ich nie etwas wusste. Diese acht Tage waren sehr spannend, aber auch anstrengend. Gegen Ende habe ich gemischte Gefühle. Ich bin froh, dass es fertig ist, jedoch auch traurig, weil es fertig ist. In den letzten Tagen habe ich alles gegeben und alles rausgeholt was möglich war. Das Endresultat hat sich definitiv gelohnt. Ich hoffe meine Geschichte hat Ihnen gefallen und Sie konnten das ein oder andere mitnehmen.

Enrique Munoz