1. Link überlasten:

* Script: link\_flooding.py TODO:testen
* Idee hinter dem Angriff:
  + Im Netzwerk besteht ein Static-Flow der erlaubt, UDP Packages über den Port 6 an die IP-Adresse 224.0.2.0 zu senden. Diese Regel wird ausgenutzt sehr viele Packages über den Link zu senden. Diese Packages werden nicht über den Controller weitergeleitet, was dazu führt, dass nur der Link isoliert angegriffen wird. Wenn viele UDP Packages gesendet werden, führt dies zu Auslastung von dem Link.
  + Wir erwarten, dass die Packages über den Link nicht mehr gesendet werden können.
* Wie wir es gemacht haben:
  + TODO
* Angriff zeigen:
  + TODO: Video dafür erstellen
* Ergebnisse des Angriffs:
  + TODO

1. Switch überlasten:

* Script: flood\_table\_one\_dest\_host.py
* Idee hinter dem Angriff:
  + Der SDN Controller erzeugt ein neues Reactive-Flow wenn eine neue Verbindung zwischen zwei IP-Adressen erzeugt worden ist z.B durch ein Ping-Package, da die White-List diese nur erlaubt.
  + Wir wissen dass der Switch gleichzeitig 2000 Flüsse in der Tabelle haben kann, dies bedeutet dass ein Angriff durchgeführt werden kann die diese Tabelle „überfühlt“.
  + Wir erwarten, dass existierende Reactive-Flows aus der Tabelle entfallen, dies führt dazu dass die Kommunikation von den entfernten Reactive-Flows nicht mehr funktioniert und die eine Reactive-Flows können nicht installiert bzw. erzeugt werden.
* Wie wir es gemacht haben:
  + Wir senden viele (über 2000) Ping-Packages von zufälligen IP-Adressen an ein bestimmtes Gerät im Netzwerk, in unserem Fall core-pi4-03 (10.0.0.3). Wir haben core-pi4-03 genommen da dadurch zwei neue Flüsse erzeugt werden, da sich das Gerät auf der „rechten“ Seite des Netzwerks befindet. Dies führt dazu dass neue Reactive-Flows erzeugt worden sind.
* Angriff zeigen:
  + TODO: Video dafür erstellen
* Ergebnisse des Angriffs:
  + TODO: Geht ein ping von einem Gerät zu den anderen? Gehen noch die Static-Flows -> Timos Erwartung: Die Static-Flows funktionieren noch immer?

1. Controller überlasten:

* Script: controller\_flooding.py
* Idee hinter dem Angriff:
  1. Es wird versucht den Controller zu überlasten, dafür werden viele TCP Packages über den Controller gesendet. Da die TCP-Packages von SDN-Controller nicht weiter geleitet werden, werden sie filtriert. Dies bedeutet, dass der Controller mit diesem Prozess beschäftigt ist und wir können sehr viele TCP Packages senden, was zum Überlasten des Controllers führt.
  2. Wir erwarten, dass die Reactive Flüsse nicht mehr funktionieren.
* Wie wir es gemacht haben:
  1. Wir senden viele TCP-Packages von core-NUC2 (10.0.0.42) im Netzwerk zu folgenden Gerät 10.0.0.3. In diesem Angriff ist es egal welche IP-Adresse die Source-Adresse sein wird, da der Controller die Packages gar nicht weiter leiten wird. Dies führt dazu, dass der Controller überlastet wird.
* Angriff zeigen:
  1. TODO: Video dafür erstellen
* Ergebnisse des Angriffs:
  1. TODO

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

TODOs:

* + - Skripte so schreiben, dass wir angeben können wie viele Packages wir senden möchten. Nicht --fast und –faster im Skript mit hping3 senden.