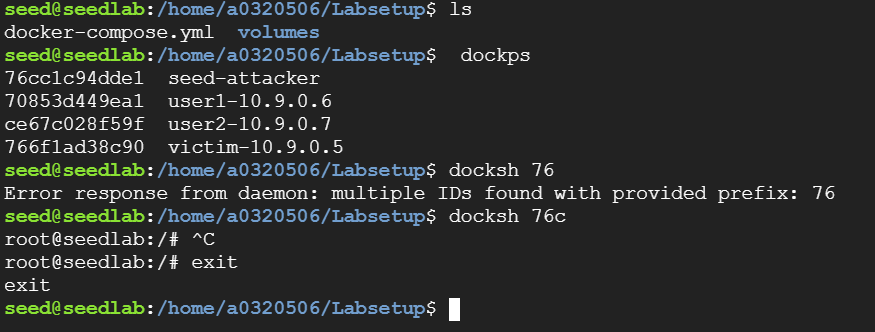
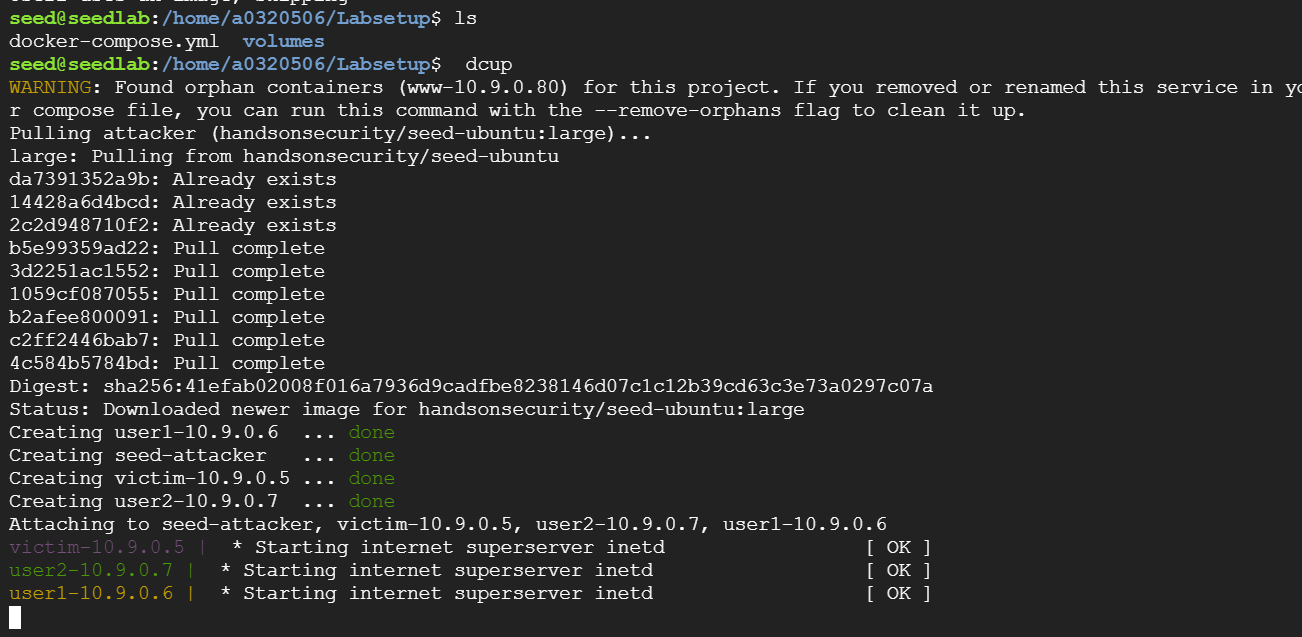
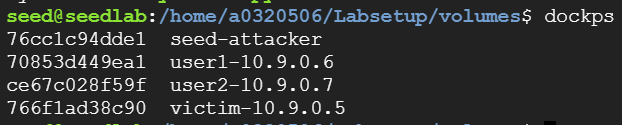
<https://hackmd.io/@ephemeral-instance/rkDSvBv-_>



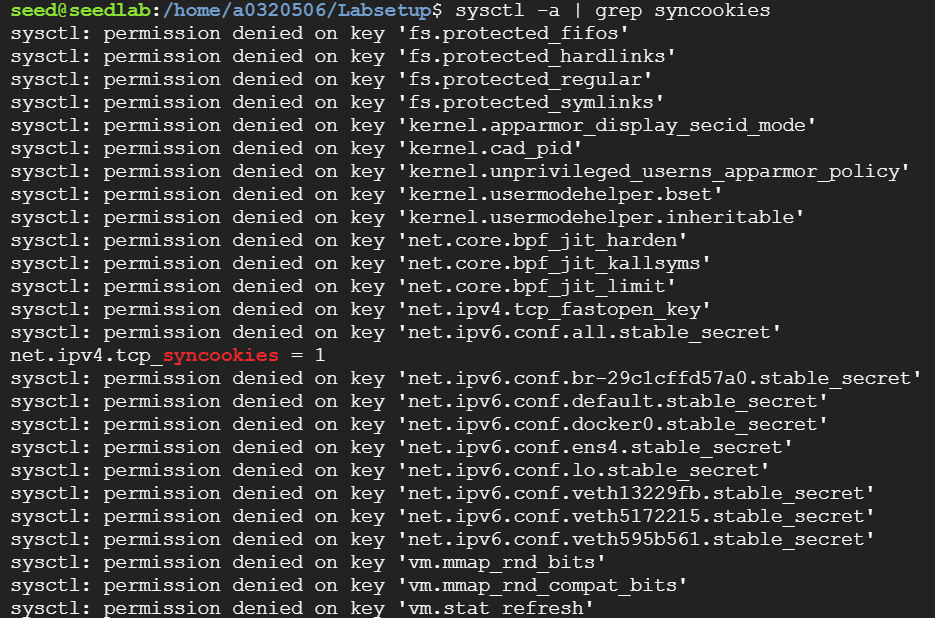


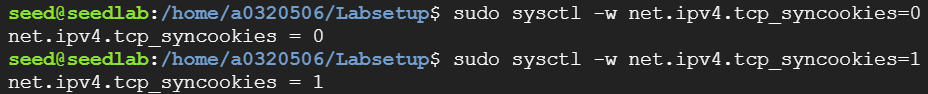


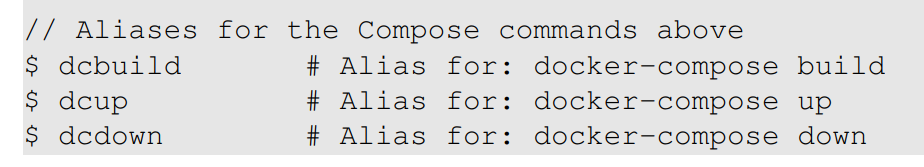


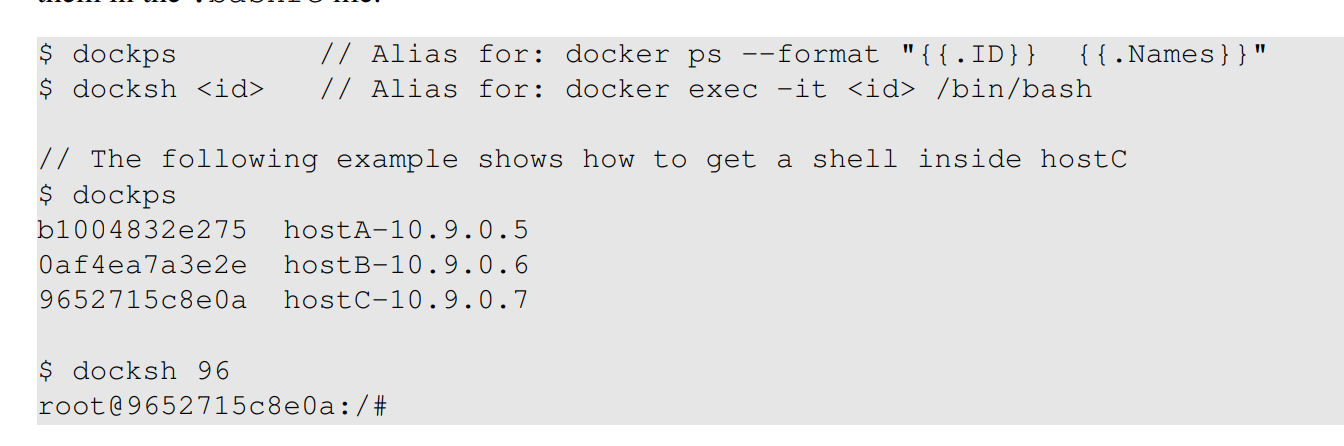


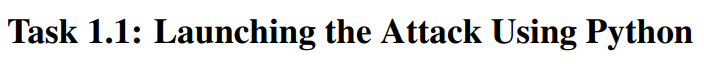


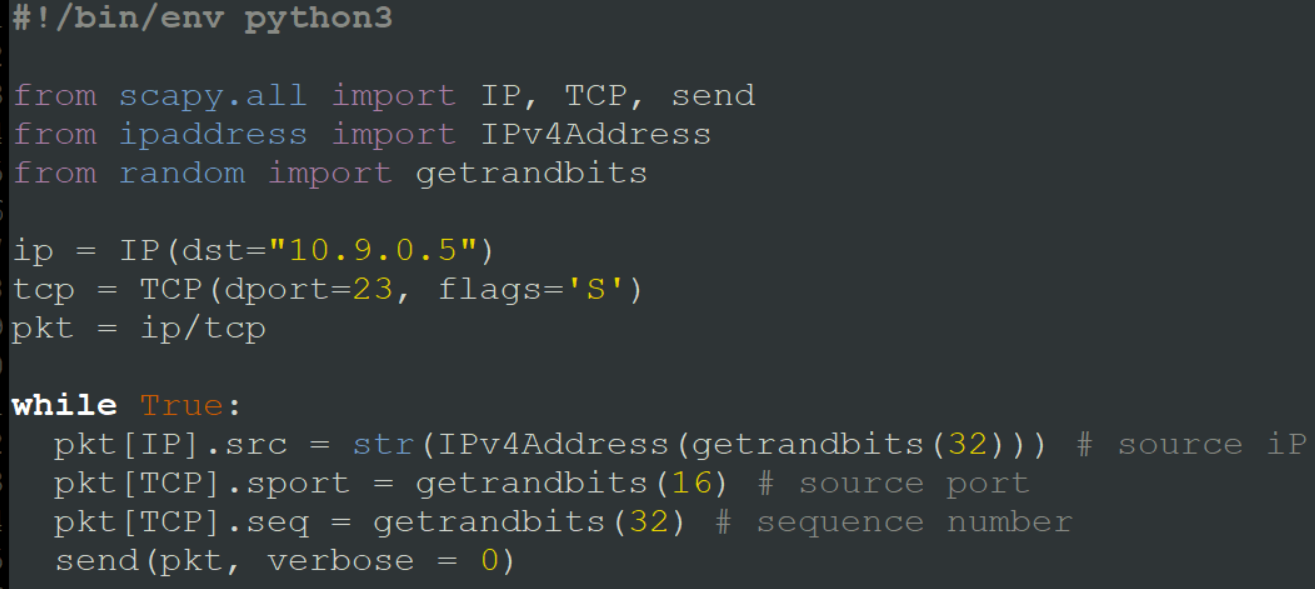


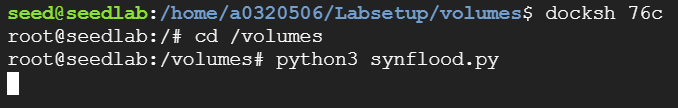


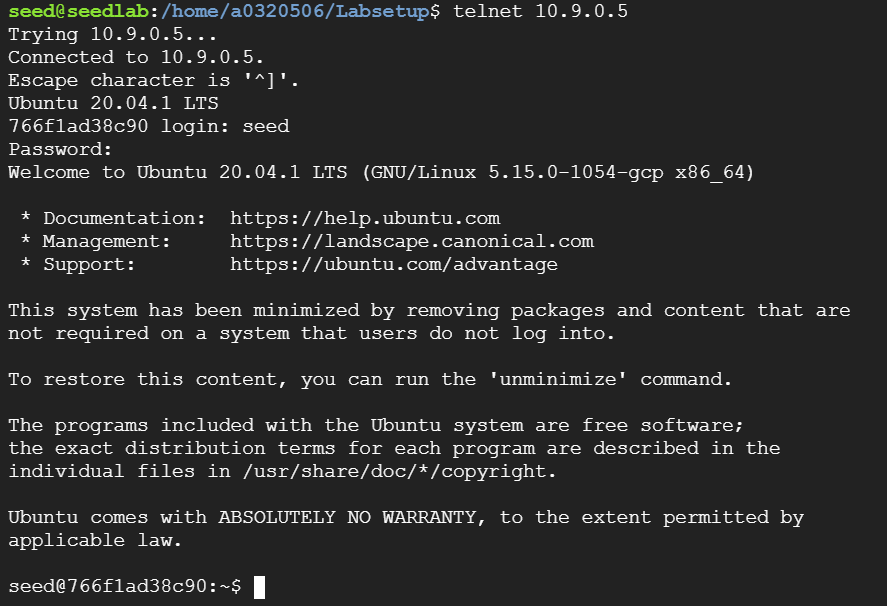






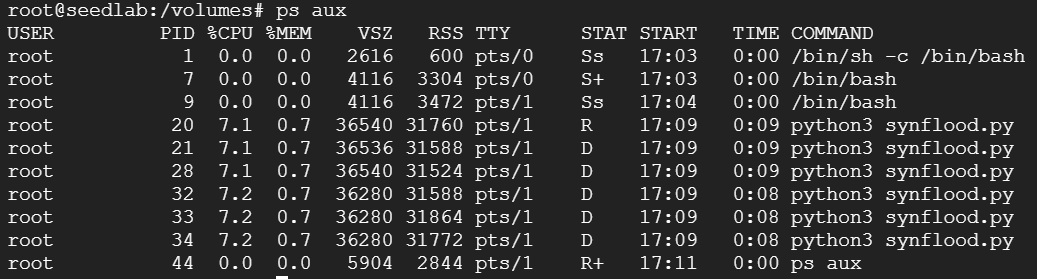
synflood.py

 在seed-attacker執行攻擊

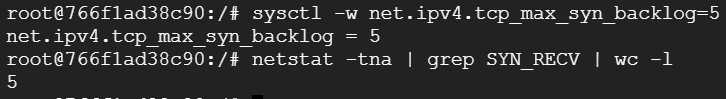
可以登入victim：攻擊失敗

**【為了讓攻擊成功】**

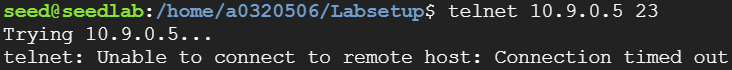
1. 強化攻擊：在seed-attacker同時執行6個攻擊程式



2. 削弱防禦：將victim-10.9.0.5的半開區間減到5



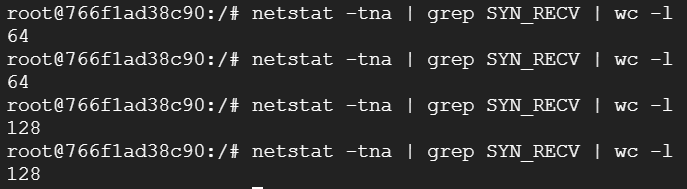
攻擊成功：無法連線至victim-10.9.0.5

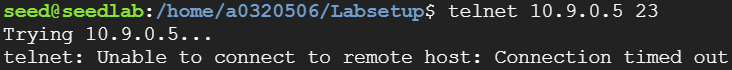








攻擊前64 攻擊後128

攻擊成功

**比較：**和python相比，用C語言攻擊一次就成功，不需要增加攻擊程式執行次數或調整半開區間

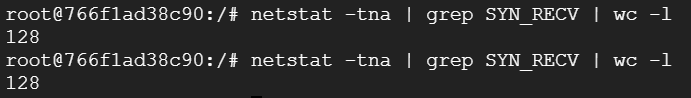
**可能的原因：**

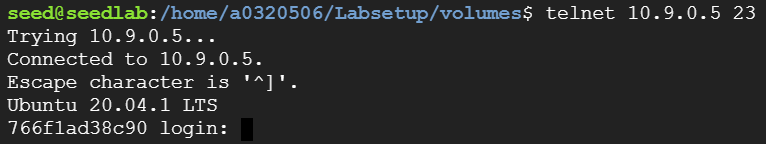
1. 攻擊速度：C語言的程式比Python程式更快速，能夠以更快的速度發送大量的攻擊封包，導致目標機器的半開連接隊列迅速被填滿

2. 封包生成和發送效率：C語言通常比Python更靠近硬體層，能夠更有效地生成和發送封包，從而降低攻擊的延遲和效率損失









SYN cookie機制允許狀態資訊作為SYN-ACK和ACK封包的一部分儲存在cookie中，而不是儲存在victim的flow table中，由於流程表沒有被填滿，因此當發生SYN洪氾攻擊時，flow table不會出現緩衝區溢位問題，因此victim將能夠服務更多請求

