**NSSECU2 - Hacking Tool Project**

**Deadline:** Dec. 5, 2022

**Members:** Escalona, Fadrigo, Manzano, Sy

1. **Topic:** Wi-Fi Hacking Tool
2. **Description:** The objective of this project is to create a packaged tool that will be able to do Wi-Fi scanning, cracking, and admin control access.
3. **Tools Selected for Each Capability:**
   1. Wi-Fi Scanning
      1. Airmon-ng
   2. Wi-Fi Cracking
      1. WiFite
      2. Airmon-ng
      3. Aircrack-ng
   3. WAP/Router Admin Control Access
      1. Hydra
   4. Password Cracking/Wordlist Generators
      1. crunch - <https://www.kali.org/tools/crunch/>
      2. fluxion - <https://github.com/FluxionNetwork/fluxion>
      3. hashcat - <https://hashcat.net/wiki/doku.php?id=cracking_wpawpa2>
4. **Pre-packaging implementations:**
   1. Wi-Fi Scanning
   2. Wi-Fi Cracking
      1. Notes:
         1. WiFite runs on Python2 and not on Python3, though a rewrite was made for Python3 compatibility (<https://github.com/derv82/wifite2/>)
         2. Railink WLAN cards are deemed to be best for use in WiFite
      2. WiFite Issues
         1. Module ‘pyrit’ not found
            1. git clone <https://github.com/JPaulMora/Pyrit.git> /pyrit
            2. cd pyrit
            3. sudo pip install psycopg2
            4. sudo pip install scapy
            5. sudo apt-get install python-scapy #IF 0.4 DIDN'T WORK, TRY THIS
            6. python setup.py clean
            7. python setup.py build
         2. Python.h not found (during 0.6) -> sudo apt-get install python2-dev
         3. openssl/hmac.h not found (during 0.6) -> sudo apt-get install libcap-dev && sudo apt-get install libssl-dev
         4. pcap.h not found (during 0.6) -> sudo apt-get install libpcap-dev
      3. WiFite Commands
         1. WPA Only, No PMKID, Skip-crack: wifite --wpa --no-pmkid --skip-crack
         2. WPS Only: wifite --wps-only
         3. WPA Only, No PMKID, Custom Dictionary: wifite --wpa --no-pmkid --dict <path to dict>