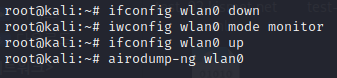
hashcat 실습

1. 아이폰(iPhone) 핫스팟 연결

비밀번호 : test987654, test9876543, test987654321

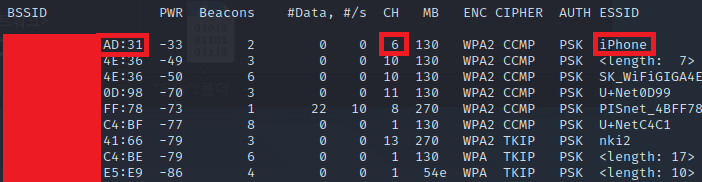
2. 랜카드 모니터 모드로 변경



3. iPhone 패킷 캡처

airdoump-ng wlan0

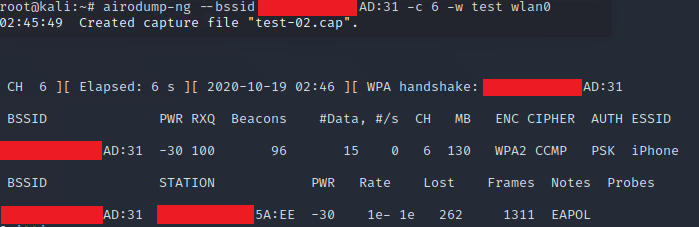
BSSID : AD:31, CH : 6

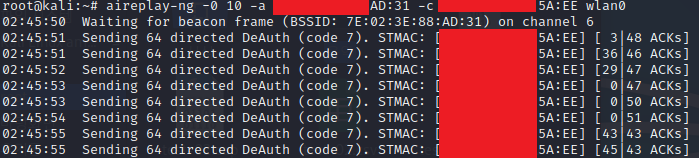


4. 해당 iPhone 핫스팟 모니터링 캡처 후 파일로 저장 & 연결 Device 확인 & WPA handshake 확인을 위해 Deauthentication Attack으로 연결 끊기 & WPA handshake 확인

airodump-ng —bssid XX:XX:XX:XX:AD:31 -c 6 -w test wlan0

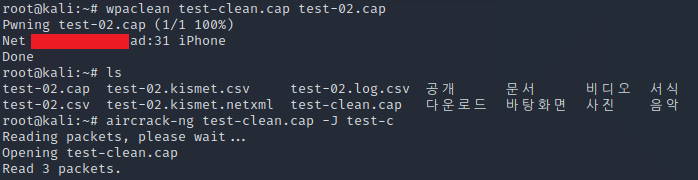
aireplay-ng -0 10 –a XX:XX:XX:XX:AD:31 -c XX:XX:XX:XX:5A:EE wlan0



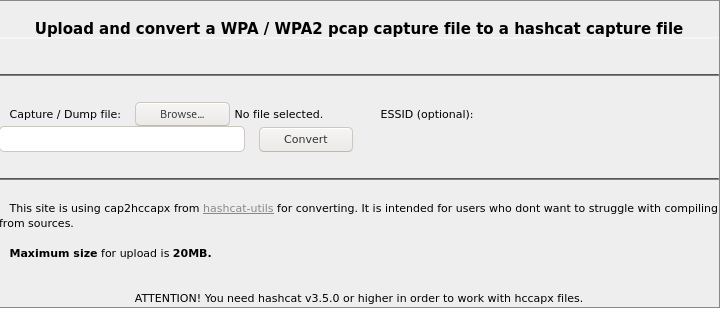


5. 캡처파일 정리(4-way handshake와 beacon만 추출)

wpaclean test-clean.cap test-02.cap

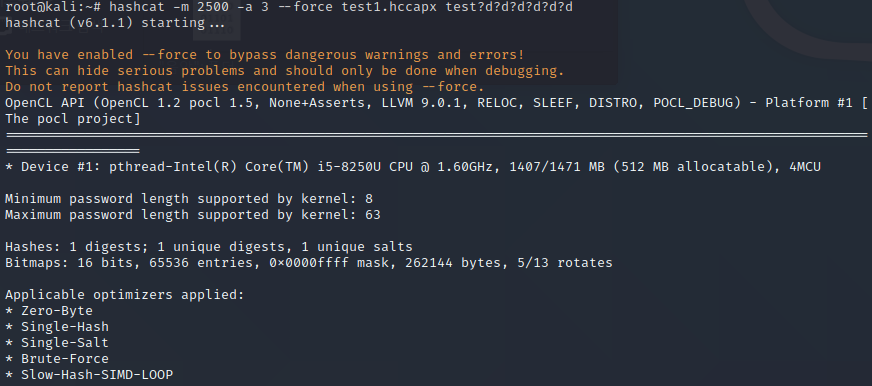


6. cap을 hccapx로 변환



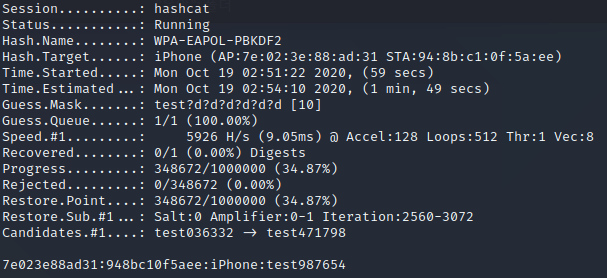
7. hashcat 실행

ⅰ. 비밀번호 : test987654 (6자리 숫자)

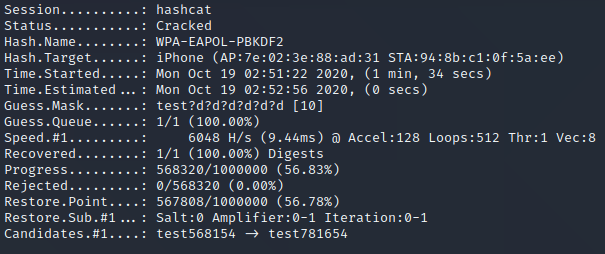


8. 예상시간 및 크랙 성공시간

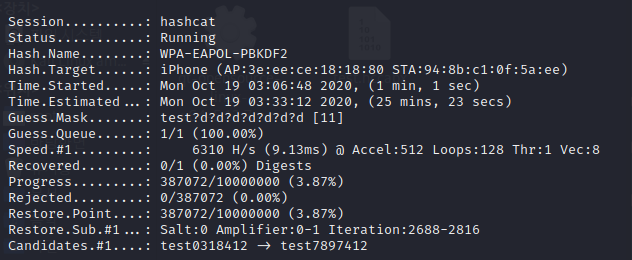
ⅰ. 비밀번호 : test987654 예상시간(1min, 49secs)



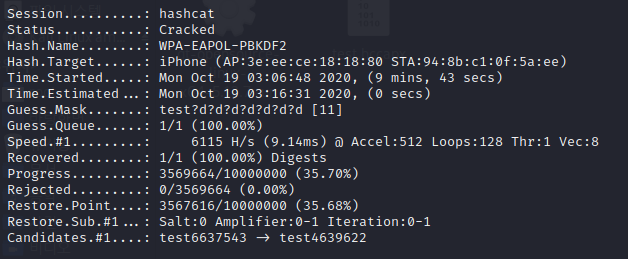
ⅱ. 크랙 성공시간(1min, 34secs)



ⅲ. 비밀번호 test9876543 예상시간(25mins, 23secs)



ⅳ. 크랙 성공시간(9min, 43secs)



ⅳ. 비밀번호 test987654321 예상시간(1day, 18hours) 너무 길다ㅠㅠ

