Wi-Fi texnologiyasini crack qilish.

Wi-Fi - bu qisqa masofalarga yuqori tezlikda ma'lumotlarni uzatish imkonini beruvchi radio to'lqinlaridan foydalanadigan tarmoq texnologiyasi.

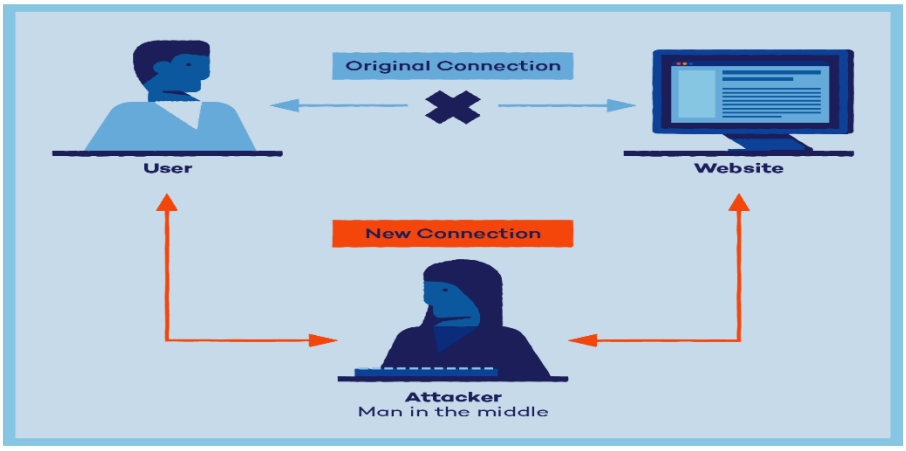
Wi-Fi texnologiyasi yillar davomida rivojlanib bordi bunga sabab bu texnologiyaning foydalanuvchilarga foydalanish uchun qulayligi hisoblanadi. Har bir texnologiya qulay bo'lishi bilan birga ma'lumotlarning xavfsiz uzatilishi ham muhim hisoblanadi. Misol tariqasida ayrim odamlar menga tegishli malumotlar kimga keragi ham bor yoki boshqa bir mazmundagi gaplarni o'ylashadi. Ko'pchilik Wi-Fi parolini boshqa odamlardan nega yashirayotganini mazmunini ham tushunishmaydi, ayrimlari esa Wi-Fi dan malumot yetib kelish tezligiga ta'sir qiladi deb hisoblashadi yoki ayrimlari shunchaki parolni boshqa shaxslarga berishni hohlashmaydi.

Hozirda internet va axborot texnologiyalar asrida yashar ekanmiz.Har bir ma'lumot muhim hisoblanadi, chunki bu muhim ma'lumot orqali bizga yoki bizning tanishimizga zararga ishlashi mumkin.

O'zi aslida Wi-Fi parolini nega boshqa shaxslardan yashirishimiz kerak? Faqatgina Wi-Fi ning ma'lumot uzatish tezligi pasayb ketmasligi uchunmi? Yo'q albatta.

Odatda ko'p hujumlar tashqi tarmoqdan amalga oshiriladi ya'ni hujumchi biz bilan bitta LAN tarmoqda bo'lmasligi yoki bitta Wi-Fi tarmoqdan foydalanmasdan hujumni amalga oshiradi. Lekin hujumchi biz bilan bitta tarmoqda bo'lgan holda hujumni amalga oshirsa ma'lumotlarni qo'lga kiritish imkoniyati ko'proq bo'ladi.

Misol tariqasida "Man in the Middle Attack" ni olsak bu hujum turi o'rtadagi odam hujumi hisoblanadi.



1-rasm. MITM

Bu hujum turida bizning qurilmamiz orqali yuborilayotgan barcha so’rovlar va ma’lumotlar uchinchi shaxs orqali o’tadi.Agar biz foydalanayotgan web site http bo’lsa bemalol barcha yozgan login parol yoki credit karta raqamlarimizni ko’rib turishi mumkin.

Wi-Fi tarmog’imizga begona shaxslar nega ulanmasligi kerakligi bilib oldik, endi buni qanday amalga oshirishimiz mumkinligi haqida to’xtalamiz.Birinchi navbatta hujumni o’zimiz amalga oshiramiz.

WiFi buzish texnikalari

1. **Fishing usuli orqali amalga oshirish**: bu usulda foydalanuvchiga Wi-Fi router sozlamasini amalga oshirishda paydo bo’ladigan web-sahida uchun link jo’natiladi va foydalanuvchi parolni yozadi va bu hujumchiga yetib keladi bu usulda qo’shimcha qurilma ham kerak emas.
2. **Lug'at hujumi** : Hujumchi eng ko’p userlar tomonidan terilgan so'zlar ro'yxatidan foydalangan holda hujumni amalga oshiradi bu usulda ham qo’shimcha qurilma kerak emas.
3. **Handshake Attack** : Hujumchi ulanish vaqtida qurilma va router o‘rtasida almashilgan hesh qiymatni ushlaydi, so‘ngra bu hesh qiymatning aslini topish

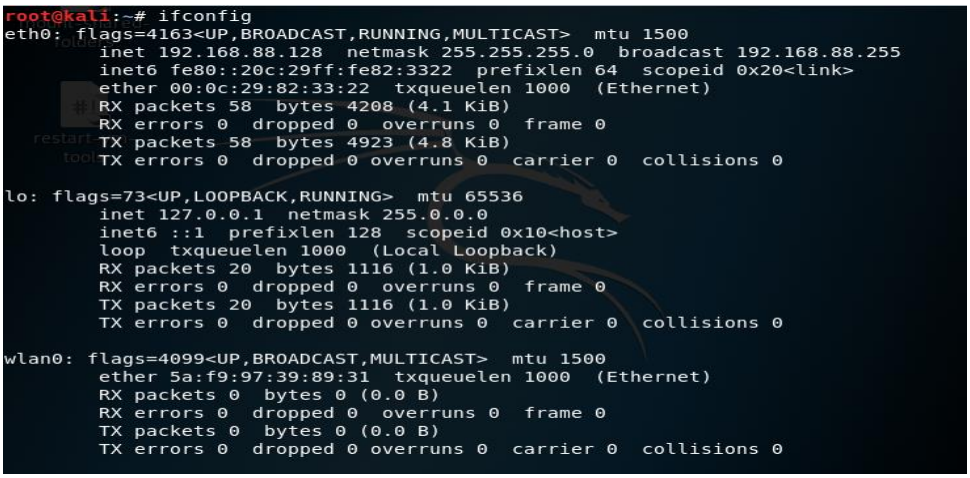
uchun solishtirish usuli orqali haqiqiy parolni topadi.Bunda qo’shimcha monitor mode funksiyasi mavjud bo’lgan Wi-Fi adapter kerak bo’ladi.

4. **Evil twin attack** : Bunda hujumchi qonuniy nomga o'xshash soxta WiFi tarmog'ini yaratadi va foydalanuvchini soxta tarmoqqa ulanishga majbur qiladi va foydalanuvchi soxta oldingi nomdagi Wi-Fi tarmoqqa ulanganda parolni teradi va bu parol hujumchiga yetib boradi.Bu hujum turi boshqalariga qaraganda amalga oshish ehtimoli yuqorisi hisoblanadi.Bu hujumni amalga oshirish uchun ikkita Wi-Fi adapter kerak bo’ladi.

Handshake Attack hujumini amalga oshirilishini ko’rib chiqamiz.

Biz buni Kali Linux OS orqali amalga oshiramiz. Kali ni ishga tushirib olamiz va ishlar ketma-ketligini amalga oshiramiz.

1. **ifconfig**(interfays konfiguratsiyasi) commandasi orqali tizimdagi tarmoq interfacelar konfiguratsiyasini ko’ramiz.



2-rasm. ifconfig commandasi.

Bu yerda:

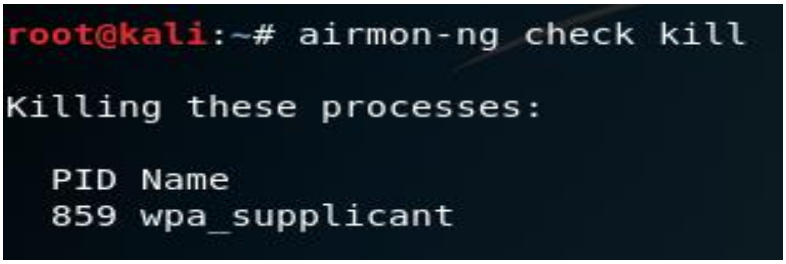
eth0: Ethernet interfaysi.

lo: local tarmoq interfaysi.

wlan0: tizimdagi simsiz tarmoq interfaysi.

2. WiFi interfeysidan foydalanadigan joriy jarayonlarni to’xtatish.

   airmon-ng check kill commandasi yoziladi.

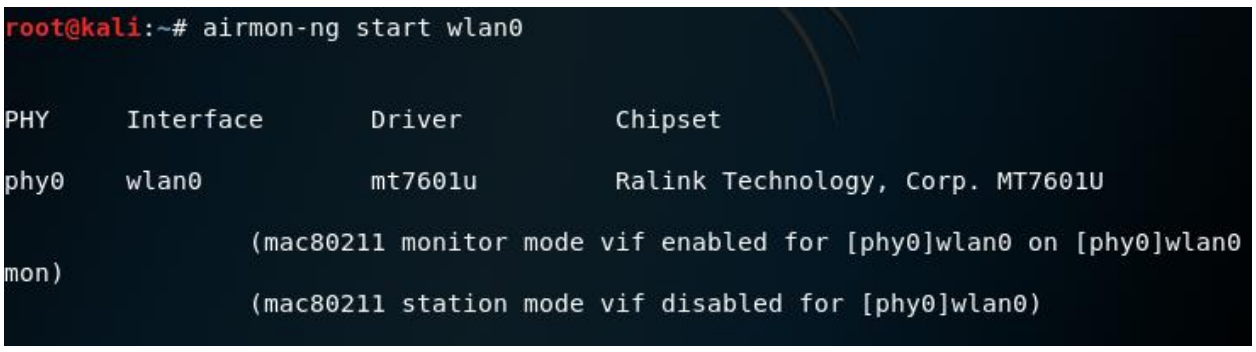


3-rasm. Joriy jarayonlarni to’xtatish.

3. Wi-Fi adapterni monitor rejimiga o’tkazamiz chunki bu bizga atrofimizdagi wifi to’lqinlarini ushlashga yordam beradi.

   Monitor rejimi ma’lum simsiz tarmoq interfeyslarida mavjud bo‘lib, WiFi trafigini yozib olish va tahlil qilish imkonini beradi.

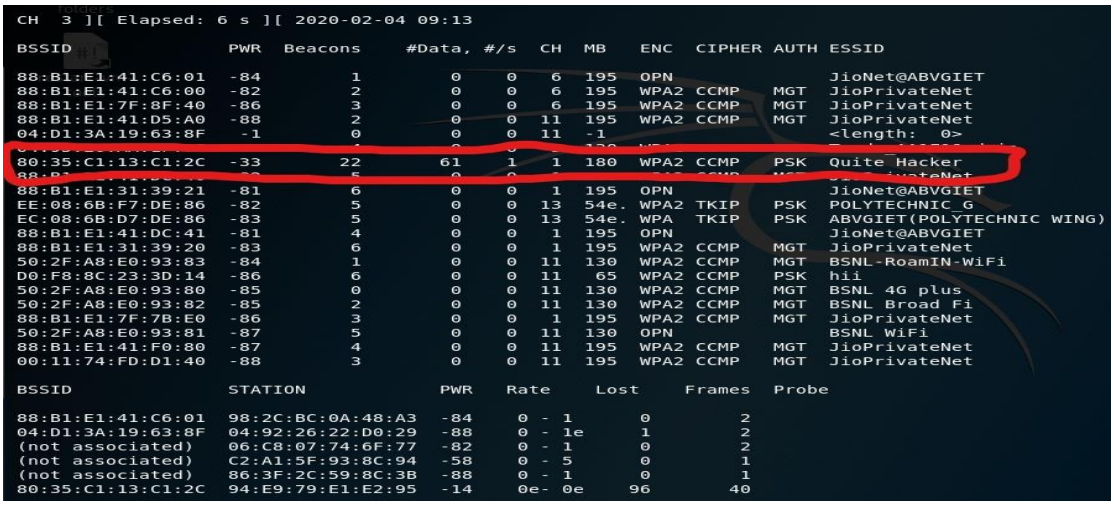
airmon-ng start wlan0 commandasi yoziladi.



4-rasm. Wifi adapterni monitor rejimiga o’tkazish.

4. Endigi navbatta atrofimizdagi barcha wifi tarmoqlarni ko’rishimiz mumkin.

   Buning uchun **airodump-ng wlan0mon** commandasi yoziladi.



5-rasm. Wifi adapter orqali wifi tarmoqlarni kuzatish.

Bu yerda,

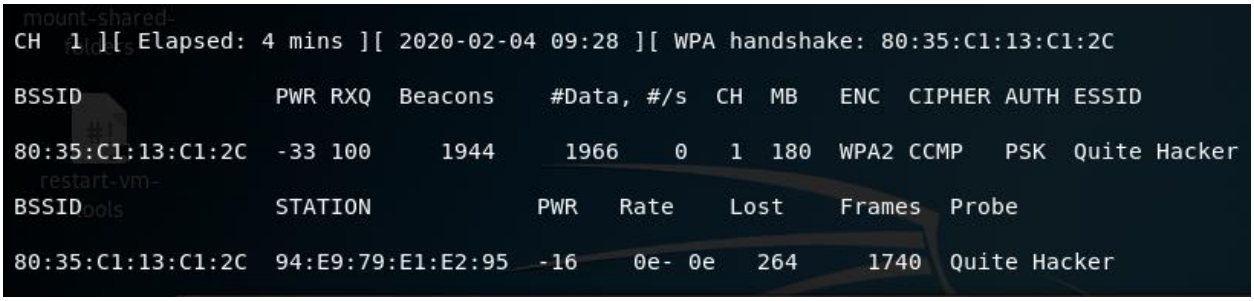
- **airodump-ng** : paketlarni yozib olish uchun.
- **wlan0mon** : interfeys nomi (turli qurilmalarda bu nom boshqacha bo'lishi mumkin)

Aniq ko’zlagan wifi tarmoq topilgach ctrl+c tugmalarni bosiladi va jarayon to’xtatiladi.

5. Aniq bir tarmoqqa ulangan foydalanuvchilarni ko’rish

Buning uchun quyidagi commanda yoziladi:

airodump-ng -c 1 --bssid 80:35:C1:13:C1:2C -w /root wlan0mon



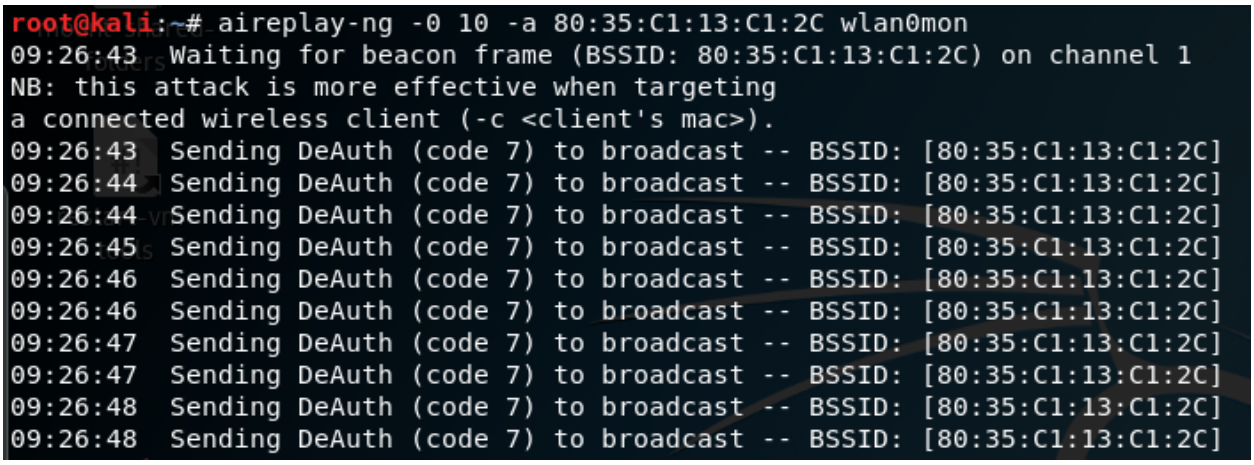
6-rasm. Tarmoqdagi foydalanuvchilarni kuzatish.

Bu yerda,

- **airodump-ng** : paketlarni yozib olish uchun
- **-c** : Kanal raqami uchun
- **–bssid** : Simsiz ulanish nuqtasining MAC manzili.
- **-w** : Faylni saqlamoqchi bo'lgan katalog (hesh qiymat fayli).
- **wlan0mon** : interfeys nomi.

6. Maqsadli tarmoqqa ulangan mijozlarni uzish uchun yangi terminal oynasini ochiladi.Bunda quyidagi commanda yoziladi:

aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0mon

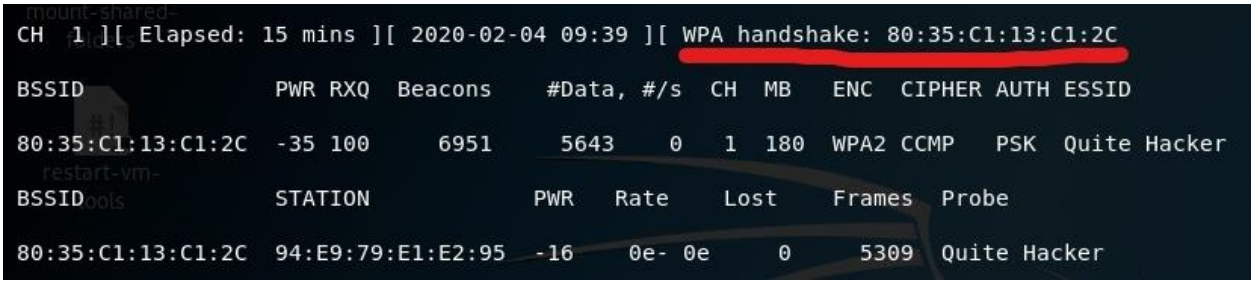


7-rasm. Maqsadli tarmoqdan mijozlarni uzish.

- **aireplay-ng** : Paketlarni uzish uchun

- **-0** : autentifikatsiya qilish uchun
- **10** : Yuboriladigan autentifikatsiya paketlari soni
- **-a** : maqsadli tarmoqning **bssid** uchun
- **wlan0mon** : interfeys nomi.

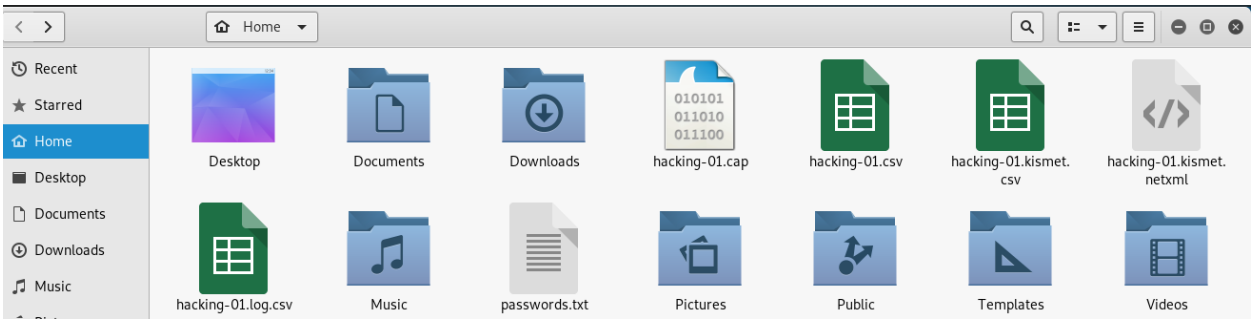
Mijoz maqsadli tarmoqdan uzilganida. U tarmoqqa qayta ulanishga harakat qiladi va ulanayotgan paytda terminalning oldingi oynasida **hesh qiymat** belgilangan file ichiga saqlab olinadi**.**



8-rasm.Handshake ni qo’lga kiritish jarayoni.

Biz maqsadli WiFi tarmoqning parolini qo’lga kiritdik faqat u hesh qiymat ko’rinishida biz uni solishtirish usuli orqali parolning aslini topamiz.

7. Biz saqlagan file ni ko’ramiz.



9-rasm.hesh qiymatlar saqlangan filelar

Bu yerda **hacking-01.cap** bizga kerak bo'lgan fayl.

8. Bu bosqichda saqlangan hesh qiymatni eng ko’p WiFi egalari tomonidan qo’yilishi mumkin bo’lgan parollar ro’yxati orqali solishtirish orqali mos hesh qiymat topiladi.Bu ro’yxat ochiq holatda internetda mavjud.
   Buning uchun quyidagi commanda yoziladi:

aircrack-ng -a2 -b 80:35:C1:13:C1:2C -w /root/passwords.txt /root/hacking-01.cap

10-rasm. Mos hesh qiymatni aniqlash.

- **aircrack-ng** : 802.11 **WEP** va **WPA-PSK** kalitlarini buzish dasturi
- **-b** : maqsadli tarmoqning BSSID
- **-w** : Parollar ro'yxati faylining joylashuvi
- **/root/hacking-01.cap** : hesh faylining joylashuvi

Biz uchun muhim bo’lgan WiFi tarmoqning paroli topildi bu: **liker1**

Bu usul yordamida WiFi parolini topishda amalga oshmay qolish ehtimoli yuqori chunki biz hujum qilayotgan WiFi egasi bizni ro’yxatimizda yo’q bo’lgan parolni qo’ygan bo’lsa biz uni topa olmaymiz.Eng oxirgi bosqichda ya’ni hesh qiymat orqali solishtirish bosqichida boshqa dasturlar ham mavjud bularga misol qilib **John the Ripper , hashcat** dasturlarini aytish mumkin.

Hashcat- dasturining imkoniyati boshqalariga qaraganda ko’proq bunda siz qurilmangizning video kartasi orqali ko’proq va tezroq ro’yxatlarni solishtirishingiz mumkin.

Wi-Fi tarmog'ingiz uchun himoya choralari

1. **Kuchli shifrlash** : eski protokollarning zaifliklaridan qochib, tarmog'ingizni himoya qilish uchun WPA3 yoki WPA2 shifrlashdan foydalaning.
2. **Kuchli parol** : Qo'pol kuch hujumlarining oldini olish uchun harflar, raqamlar va maxsus belgilardan iborat murakkab paroldan foydalaning.
3. **Doimiy yangilanishlar** : So'nggi xavfsizlik tuzatishlaridan foydalanish uchun routeringiz yangilanganligiga ishonch hosil qiling.
4. **MAC manzilini filtrlash** : Faqat tasdiqlangan MAC manzillari bo'lgan qurilmalarga tarmoqqa ulanishga ruxsat bering.

Xulosa

Wi-Fi tarmog'ingizni himoya qilish ma'lumotlaringiz va maxfiyligingizni onlayn tahdidlardan himoya qilish uchun juda muhimdir. Umumiy xakerlik usullarini tushunish va kuchli shifrlash va murakkab parollar kabi himoya choralarini qo'llash orqali siz xakerlik xavfini sezilarli darajada kamaytirishingiz mumkin.