Увод, въведение, уточнения и теория:

Съществуват няколко вида безжични мрежи, както и няколко вида крептиране на самите връзки.

Безжичните мрежи се подвизават под стандарта 802.11 наречен още Wi-Fi. Съществуват и модификации на този стандарт въведен от световната организация за стандартизиране IEEE които са описани в таблица 1. Изразът 802.11x се използва да обозначи набор от стандарти и не бива да се бърка със нито един от неговите елементи.

Протокол

Дата на излизане

Оперативна честота

Data Rate (Typ)

Data Rate (Max)

Обхват (в сграда)

Обхват (на открито)

Legacy

1997

2.4 GHz

0,9 Mbit/s

2 Mbit/s

~20 метра

~100 метра

802.11a

1999

5 GHz

23 Mbit/s

54 Mbit/s

~35 метра

~120 метра

802.11b

1999

2.4 GHz

4.3 Mbit/s

11 Mbit/s

~38 метра

~140 метра

802.11g

2003

2.4 GHz

19 Mbit/s

54 Mbit/s

~38 метра

~140 метра

802.11n

2007 (чернова)

2.4 GHz / 5 GHz

74 Mbit/s

248 Mbit/s

~70 метра

~250 метра

Таблица: 1

Има три вида за криптиране на предаване на Wi-Fi връзка WEB, WPA и WPA2.

WEP (Wired Equivalent Privacy)

WEP- Wired Equivalent Privacy - е протокол, който добавя сигурност в безжичните локални мрежи (WLAN), базирани на 802.11 Wi-Fi стандарта. WEP е част от втория слой на OSI модела, като има възможност за пускане и изключване. WEP е проектирана да предоставя на потребителите на безжичен интернет същото ниво на сигурност като на LAN. WEP подържа схема за сигурност, известна като RC4 с 40-битов ключ.WEP е по-стар метод за мрежова защита, който все още е достъпен за поддръжка на по-стари устройства, но не е препоръчителен. Когато разрешавате WEP, задавате ключ за защита на мрежата. Този ключ шифрова информацията, която даден компютър изпраща на друг компютър в мрежата. WEP защитата обаче, е изключително лесна да се пробие (заради това не е за предпочитане).

WPA (Wi-Fi Protected Access) - по-устойчивият алгоритъм за кодиране от WEP. Високото ниво на безопасност се постига с използването на протоколите TKIP и MIC.

TKIP - протоколът за интеграция на временния ключ (Temporal Key Integrity Protocol) - всяко устройство придобива променлив код.

MIC - технология за проверка на целостността на съобщенията (Message Integrity Check) - защищава от прихващането на пакети и пренаправлението им. Стандартът TKIP използва автоматически подбрани 128-битови кодове, които се създават с непредсказуеми способи, и общият брой на вариациите им достига 500 милиарда.

Сложната йерархическа система на алгоритъма по подбор на шифри и динамичната им замяна на всеки 10 KB (10 хиляди предаваеми пакета) правят системата максимално защитена. MIC използва съвсем не прост математически алгоритъм, който позволява сверяването на изпратените в една и получените в друга точка данни. Ако забелязаните изменения и резултатът от сравнението не съвпадат, такива данни се считат за фалшиви и се изхвърлят. Съществуват два вида WPA.

WPA-PSK (Pre-shared key) - за генерирането на кодираните мрежи и за вход в мрежата се използва ключова фраза. Това е оптималният вариант за домашни или неголеми офисни мрежи.

WPA-802.1x - входът в мрежата става чрез сървърна аутентификация. Оптималната защита за мрежите на големи компании.

WPA2 е построен предимно на основата на предхождащата го версия - WPA, като използва елементи на IEEE 802.11i. Стандартът предвижда прилагането на шифроването AES, автентификацията 802.1x, а също и защитна спецификация RSN и CCMP. Както се предполага, WPA2 трябва съществено да повиши защитеността на Wi-Fi-мрежа в сравнение с предходните технологии. По аналогия с WPA, WPA2 също се дели на два типа: WPA2-PSK и WPA2-802.1x.

802.1x

IEEE 802.1x - това е сравнително нов стандарт, за основа на който са взети поправените недостатъци в технологията за безопасност, прилагани в 802.11, в частност възможностите за взлом WEP, в зависимост от технологията на производителя и т. н. 802.1x предвижда включване към мрежата дори на PDA-устройства, което позволява по-изгодно да се приложи самата идея за безжична връзка. От друга страна, 802.1x и 802.11 са съвместими стандарти. 802.1x е базирана на следните протоколи.

EAP (Extensible Authentication Protocol). Протокол за разширена автентификация. Използва се съвместно с RADIUS-сървър в големи мрежи.

TLS (Transport Layer Security). Протокол, който осигурява цялостност и кодиране на предаваните данни между сървърите и клиентите, взаимната им автентификация, като предотвратява прихващането и подмяната на съобщения.

RADIUS (Remote Authentica-tion Dial-In User Server). Сървърна автентификация на потребителите с име и парола. Така се появява новата организация на работа с клиентски мрежи. След като потребителят премине фазата на автентификация, му се изпраща секретен ключ в кодиран вид на определен кратък период от време - това е срокът на действие на сеанса. При неговото изтичане се генерира нов шифър, който отново се изпраща на потребителя. Протоколът за защита на транспортно ниво TLS осигурява взаимна автентификация и цялостност на пренос на данните. Всички "ключове" са 128-разрядни.

Същност и цели на курсовата работа:

Теорията през коят минахме е съществена и сбита това е тория която всеки хакер кракер трябва да знае и в по-задълбочен вид. За да се кракне дадена безжична връзка се изискват доста умения и търпение. Методите и стъпките през които минава процедурата по хакване на дадена безжична връзка са описани в курсовата работа, както и инструментите и тяхното предназначение които се използват.

Сканиране и разбиване на wereless с WEB криптиране (encryption).

WEB encryption е найстина гаден и стар метод за кодиране на една безжична връзка. При този метод на защита на връзката, криптирането се осъществява, чрез 3-битов вектор наречен инициализиращ вектор (*Initalization Vector*) или (IVs) които е вмъкнат в пакета на основата на pre-shared key, като всички оторизирани клиенти знаят този ключ. Всъщност този ключ трябва да се прехване, стига да се съберат достатъчно пакети които биват изпратени от клиента (client) или от AP(access point) устройството. Би трябвало да се съберат хиляди милиони пакети за да може да се намали kyespace (интервалът на предаване на ключа за оторизиране в частната мрежа), след това може да се реализира методът на грубата сила (brute force). При сканирането на дадената

мрежа някои неща моеже да се укажат проблем, като на пример:

- ако ключът не е статичен и се миксира във всички IV-s – това ще отнеме цяла вечност за дешифроване на ключа.

- Ако няма трафик (предаване на пакети между устроиствата) – това моеже да се корегира

- MAC ограничение (MAC Address fitering) - това също може да се корегира.

Необхотими инструменти (tools)

преди да започне самото декриптиране трябва да се снабдим с някои необходими инструменти:

трябва да имаме 3 или 4 shell (Шел) конзоли (console) стартирани

инструменти които ще са необходими:

- airodump – прехващане на векторите (IVs)
- aircrack – кракване (cracking) на векторите IVs
- airdecap – декодиран на събраните пакети
- airreplay - Пакетен ижектор (Packet injector) за атака на APs.
- kismet – мрежов снифер (Network Sniffer), за прехващане на Ivs.

За стандартна WEP атака (hack) ще са необходими само airodump, aircrack, and kismet (server and client). Ако се срещнат някои затруднения моеже да използваме и airreplay за да се фиксира проблема.

Прихващане, кракване и хакване на wireless мрежа с WEP encription.

Първата стъпка преди да се премине към самата атака е да се намери подходяща мрежа и да се проучи добре, трябва да се събере достатъчно информация за да може да се усъществи атаката.
За целта се стартира първо kismet за да сканира и прихване всички рутиращи устройста (APs) и мрежи наоколо. Инфорамцията която може да ни предостави този инструмент и която ни е доста необходима за успешното усъществяване на атаката към нароченатa мрежа е:

- какъв вид криптиране използва нароченият рутер WEP 64-bit? 128-bit? WPA и др.
- На кои канал предава устроиството (ще помогне до голяма степен при скороста на събиране на пакетите.
- IP Address. IP адресът на AP's устроиството
- BSSID - Basic Service Set Identifier
- ESSID - Extended Service Set Identifier

Прехващане на пакети със съдържанието на IVs

След като е установено какво ще се хаква може да се премине към сабирането на пакети.

За предпочитане е да се използва airodump за тази цел понеже airodum може да да бъде пуснат да събира пакети докато се докодират и прихване ли IVS автомати обновява базата като помага на aircrack.

Airodump може да се пусне от някои от конзолите като се напише следната примерна команда:

airodump [channel] [IVs flag]

- interface е мрежовият адаптер wireless interface на нашата система Пример: ath0, wlan0 и др.
- output prefix е името на файла под които ще се записват.
- channel е специфичния канал които ще се сканира (може да се пропусне или да се използва префикс 0 за chanel hop.
- IVs flag е с префикс 0 или 1, в зависимост от това дали се нуждаем от всички пакети или само от тези които съдържат IVs vectors.

Пример от реалния свят:

airodump ath0 lucid 6 1

тази команда ще изведе следното:

BSSID PWR Beacons # Data CH MB ENC ESSID

00:23:1F:55:04:BC 76 21995 213416 6 54. WEP hackme

BSSID STATION PWR Packets Probes

00:23:1F:55:04:BC 00:12:5B:4C:23:27 112 8202 hackme

00:23:1F:55:04:BC 00:12:5B:DA:2F:6A 21 1721 hackme

Втория ред от стартиранта команда показва инфорамция свързана с APs, броя на радиовълните и броя пакети. Двата последни реда показват, че в момента на сканирането има два оторизирани потребителя които са свързани и броят на пакетите които предават. Тази информация в реалността може да се използва за активното хакване на wireless мрежата “hackme”.

Тази стъпка може да отнеме доста време или може да бъде много кратка, в зависимост от това колко е заето AP устроиството което атакуваме или колко IVs пакети сме събрали.

Целта на тази стъпка е да популяризираме файла “lucid.ivs” които сме създали с airodump, с всички важни пакети съдржащи информацията с IVs вектори.

ЗАБЕЛЕЖКА: За да преминем към следващата стъпка трябва да съберем повече от 100 000 пакета под данни с airodump.

Използване на Ivs вектора от пакетите за декриптиране на КЛЮЧА

За да се осъществи тази стъпка трябва да имаме достатъчно събрани пакети с вектора. За целта ще използваме инструмента “aircrack” със следната команда но без да спираме “airodump” (трябва да се запомни, че той автоматично обновява базата с пакетите които събираме при намирането на нов пакет съдържащ IVs вектора.).

aircrack [options]

Пример от реалния свят: aircrack -a 1 -b 00:23:1F:55:04:BC -n 128 lucid.ivs

- -a 1: силова атака за WEP attack mode (или 2 за forces WPA)
- или клич -b за bssid или ключ -e за essid: което е по-лесно според случая но за предпочитане е BSSID понеже е по-уникален
- ключ “-n 64” или “-n 128”: това е дължина на криптиране на WEP key (ключа) (тази опция може да бъде пропусната ако не е известна все още.).

Това е всичко което трябва да се направи. Този метод на атака работи при по-стари wireless routers рутери.

Някои очаквани проблеми

Няколко проблема които могат да възникнат или да ни забавят по време на нашата атака.

- Няма трафик
- Няма абонати които да използват интернет. Няма движение на пакети които да се прихванат. За това и няма прихванати пакети съдържащи Ivs вектори.
- Нещото което трябва да се направи е да се “инжектират” (injection) някои специални пакети за да се подведе AP устроиството в broadcasting предаване.
- Решението на тези проблеми са описани по-долу в курсовата работа в секцията WEB атаки

- MAC Address filtering (ограничение по физически адрес).
- AP атакуваното устроиство отговаря единствено на свързаните клиенти. Възможно е защото филтрирането по MAC address на рутера е включено.
- С използването на airodump може да се намери MAC address на оторизираните потребители. Просто трябва да се смени MAC адреса на нашия интерфейс за да продължим безпроблемно.
- Може да използваме опцията -m за да укажем на aircrack да филтрира пакетите по MAC Address, пример -m 00:12:5B:4C:23:27

- Не може да се декриптира дори и с тонове IVs вектори
- някои от атаките някои от атаките може да дава грешка въпреки че извежда че не е
- може да се използва ключа -k N (където N=1..17) или -y за да се различават методите на атака.

- Може да се увеличи фактора на скърпването. По подразбиране той е 2, със специфичния ключ -f N (където N>=2) това може да увеличи шансовете за разкодиране (crack), но може да отнеме прекалено много време.

- Все още нищо
- В краен случай може да се приложи тактиката на социално инженерство.

Dictionary Brute Force – Методът на грубата сила

Повечето от важната част на метода на грубата сила (brute forcing) е добрият речник с думи. Такъв може да се свали от ht tp://www.openwall.com/wordlists/ срещу заплащане. (Добър речник може да представлява от рода на world list 40 000 000 без повторения в текстов файл.

aircrack -a 2 -b 00:23:1F:55:04:BC -w /path/to/wordlist

Дали ще успее да разбие тази атака wireless устроиството всичко зависи от това колко е силна паролата.

Използване на Airplay

Aireplay е най-забавната част. Може да се манипулират пакетите в мрежата така че да ни дават това от което се нуждаем.

WEP Attacks

Атаката се използва за да се създава повече трафик в среда с WEP encryption за да се

извлекат повече пакети с вектори IVs.

ARP Injection

ARP Replay (*Address Resolution Protocol)* е класически начин за извличане на IV вектори от Арустройството. Бавна но стабилна а и винаги работи. Трябва да се разбере BSSID на AP устройството и BSSID на някои ототризиран клиент. Ако няма свързани клиенти в AP устройството може да се усъществи друга WEP атака:
Fake Authentication Attack

Атаката се осъществява с пуснат airodump:

aireplay -3 -b -h ath0

забележка: -3 указва вида на атаката (3=ARP Replay).

Трява да се оставят пуснати заедно двата инструмента като с airodump в друг терминал могат да се прослушат върнатите пакети IVs.

Interactive Packet Replay Интерактивен пакетен отговор

Interactive Packet Reply е за много напреднали и изисква събраните пакети да се реконстроират. И всички получени пакети да се върнат обратно.

Може да се опитаме да изпратим всичките данни, но преди това трябва да се обърнем към AP-то да препрати всичко. Тази атака работи единствено ако AP рекриптира пакетите преди да ги предаде отново (и тогава устройството ни дава векторите IV). Някои устройства не го правят.

aireplay -2 -b -h -n 100 -p 0841 -c FF:FF:FF:FF:FF:FF ath0

Fake Authentication Attack
Тази атака няма да генерира повече трафик в мрежата но ще направи асоцяция на клентските MAC Address полезна е за горните две атаки. Its definately not as good as having a real, connected client, but you gots to do what you gots to do

Най-лесният начин е да се използва друга машина защото се нуждаем от друг MAC address но ако мойем да сменим ръчно нашия MAC това също ще върши работа. Смяната на новият със стария MAC address ще наричаме "Fake MAC".

Повечето APs устроиства се реасоциират клиентите си жсеки 30 сек. Или си мислят че те са изключени. Този метод работи и ако Fake MAC адресът е disconnected,трябва да се расоциира бързо. За изпълнението на тази ата трябва да се използва essid и както и Fake MAC.

aireplay -1 30 -e '' -a -h ath0

След изпълнението на горанта комада, ако всичко е наред трябва да се появи:

23:47:29 Sending Authentication Request

23:47:29 Authentication successful

23:47:30 Sending Association Request

23:47:30 Association successful

След което може да се използват горните две атаки even though there were no clients

connected in the first place.

Хакване на WPA encrition:

Предимствата на WPA

WPA първично идва с два вида защита на криптиране RADIUS или PSK. PSK е податлива на разкодиране докато, RADIUS не е толкова лесен.

PSK използва потребителска предвартелно зададена парола за да се инициализира в TKIP, (temporal key integrity protocol). Там е и паролата която в повечето случаи е разпарчетена.TKIP наистина не е податлив на атака (crackable), тъй като ключат се предава разпарчете по пакети но се инициализира по ключове в TKIP и по време на удостоверяването може да се прехване паролата. Може би здравата речникова атака (dictionary attack)ще се погрижи за голям брой пароли.

Radius включва физическо прехвърляне на ключа и криптиране на канала. Повече от 90% от комерсиялните устроиства не не го поддържат.

WPA HandShake

WPA handshake методът беше създаден за да покрие несигурните канали, като например паролата не се вижда и е разпарчетена или да не е в цял вид. Има някои модерни алгоритми във фонов режим които го превръщат в (primary master key, PMK), и други подобни, но не е това истинската същинската причина. (PMK по принцип е достатъчен за да се канектнием в мрежата).

Единствената стъпка от която се нуждаем е да събираме (capture) пълните оторизиращи пакети чрез handshake метод от реалните клиенти и рутиращото устройство (AP). Това може да се окаже трудно без някой инжектирани пакети, но ако

сме късметлии и сме събрали всичките пълни пакети с handshake методът , тогава може да продължим към атаката.

Можем да придвижем нещата като осъществим authenication handshake метода или (Deauthentication Attack – атака с деоторизация), но това може да се осъществи единствено ако има свързани (connected) потребители към AP устройството (може да се провери с airodump).

Също като при WEP encription, ние трябва да занем канала на предаване, дали наистина криптирането на връзката е с метода WPA. Командите в airodump са леко различни. Не се нуждаем само от IVs векторите. Преименуваме "lucid.ivs" в "lucid.cap". Да приемем че WPA е на channel 6 и интерфеисът ни на wireless картата ни е ath0.

airodump ath0 lucid 6

Единствения начин да се кракне WPA е да се предизвика реавтентикацията на валидните клиенти. Нуждаем се от свързани кленти към рутера.

Deauthentication Attack

Това е наистина мн ефективана атака. Може да принудим свързаните клиенти да се disconnect след което ще прихванем пакетите когато те се re-connect и оторизират authentication, saves time so we don't have to wait for the client to do it themselves (a tad less "waiting outside in the car" creepiness as well). Командата се изпълнява в отделна конзола заедно с предварително пуснат airodump. Командата ще изглежда по следния начин:

aireplay -0 5 -a -c ath0

След няколко секунди реоторизацията ще е приключила и с Dictionary Brute Force може да се намери PMK.

P.S. : Методите и стъпките които са описани в курсовата работа за декриптиране на Wireless мрежи са противозаконни. Държа да се знае, че те са използвани за научни цели и не нося никаква отговорност при евентуално използване от трети лица с цел злонамереност.