WLAN-Sicherheit und seine Schwächen

Eine Facharbeit von Lars Jonen, im Fachbereich Informatik, mit betreuendem Lehrer Rolf Faßbender aus dem Informatik Leistungskurs 2019.

Inhaltsverzeichnis

1. Einleitung

Wireless Local Area Network, kurz WLAN ist in der heutigen Zeit nicht mehr weg zu denken. WLAN wird in fast jedem Haushalt und auch auf jedem Arbeitsplatzt benötigt und verwendet. Wir tätigen Käufe im Internet, schreiben private Emails an Freunde oder erledigen Überweisungen über Online Banking, unser Geräte sind unterdessen mit dem WLAN verbunden. WLAN ist extrem essentiell für unsere Gesellschaft geworden und in der Zukunft noch wichtiger. Der Grund für diese extrem hohe Benutzeranzahl ist die sehr komfortable Übertragungsmethode, die im Gegensatz zum Local Area Network (LAN),was auf Kabel Übertragung basiert, auf die Übertragungsmethode durch elektromagnetische Funksignale setzt. Das Heißt es ist möglich in einem begrenzten Radius zu einem Access Point, beispielsweise ein Router, eine Funkverbindung herzustellen und somit Daten über den freien Raum zu übermitteln und zu empfangen .Die übertragen Daten sind sowohl in der privaten als auch in der kommerziellen Benutzung meistens geheim oder privat. Aus diesem Grund werden die Daten durch Verfahren vor der Übertragung verschlüsselt und beim Empfangen wieder decodiert. Hinzu kommt das der Zugang zum Netzwerk durch ein Passwort geschützt ist. Niemand möchte das diese Daten an Fremde gehen die sich in das Netzwerk gehackt haben. Doch ist genau dies möglich, sich in ein Netzwerk was geschützt ist ein zu klinken ohne jegliches Passwort oder Hinweise auf das Passwort? In Folge dieser Fragestellung werde ich die Sicherheitsstandards WEP (Wired Equivalent Privacy), WPA(Wi-Fi Protected Access) und WPA2 (Wi-Fi Protected Access 2) vorstellen und auf ihre Schwächen, Stärken und Verbesserungen vergleichen. Als zweiten Punkt werde ich in einer virtuellen Maschine die mit dem Betriebssystem Kali Linux läuft ein Penetration Test auf ein mit WPA2 geschütztes Test WLAN starten das mit einem einfachen Passwort gesichert wurde. Im dritten Schritt zeige Ich auf wie man sich vor möglichen Angreiffern schützen kann durch konfigurationen am Router sowie

eine gute Wahl des Passwortes mit einer zusätzlichen Laufzeitanalyse. Abschließend werde ich eine Fazit aus den enstandenen Materialien und informationen ziehen .

2. WLAN-Sicherheit

Der Vorteil aber auch gleichzeitig die größte Schwachstelle von WLAN ist die Übertragung durch elektromagnetische Funksignale durch den freien Raum. Durch diese Funksignale ist es möglich mithilfe eines Empfangsgerätes, in einer bestimmten Reichweite, die übertragenen Datenpakete mit zu schneiden und auszuwerten, im Gegensatz zu einer LAN Verbindung die nur durch ein physikalisches Anzapfen, mit geschnitten werden kann, was durch die Lage der Kabel sehr erschwert wird. Um diese Schwachstelle auszubessern wurden im Laufe der Jahre drei große Sicherheitsstandards eingeführt. Der Sicherheitsstandard WEP aus dem Jahre 1999 zur Authentifizierung und Verschlüsselung von WLAN , sein Nachfolger WPA aus dem Jahr 2003 und die Nachfolgerversion WPA2.

2.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy oder kur WEP, ist ein Verschlüsselungsprotokoll was 1999 als Sicherheitsstandard für WLAN verwendet wurde[1]. WEP verwendet bei der Verschlüsslung der Daten den RC4 Algorithmus. Dieser Algorithmus arbeitet auf der Basis von Stromschiffren. Der Algorithmus erzeugt durch einen initialisierten Pseudo-Zufallszahlengenerator Zufallszahlen[2] die das XOR verfahren mit den normalen Datensätzen verknüpft , somit entstehen nicht lesbare Datensätze die einem Angreifer der den Datenverkehr mit schneidet nicht mehr von nützen sind ohne den

[1] WEP WLAN https://www.security-insider.de/was-ist-wep-a-742205/ 17.04.2019
[2] RC4 Algorithmus http://www.tacticalcode.de/2013/03/rc4-verschlusselung-grundlagen.html17.04.2019

entsprechenden Schlüssel und Initialisirungsvektor.[3]
Die Entschlüsselung wird durch den Vorher geteilten Schlüssel (Pre-Shared-Key), denselben zufallszahlen und dem Initialisirungsvektor ermöglicht[4]. WEP besitzt aber auch eine großen und erhebliche Anzahl von Sicherheitslücken. Ein der größten ist der Initialisirungsvektor der bei jeder Übermittlung neu erzeugt wird und an den Anfang jeder Nachricht gestellt wird um eine Entschlüsselung überhaupt zu ermöglichen. Die Schwachstelle besteht in seine Kürze von 24 bit. Dies ermöglicht einem Angreifer der lange genug den Traffic mitschneidet die Möglichkeit, aufgrund der begrenzten möglichen Kombinationen in kürzester Zeit eine Wiederholung des Initialisirungsvektor mit zu schneiden und somit ist eine Rückschließung auf den Schlüssel möglich. WEP ist so anfällig das man bei einem gering genutzten WLAN den benötigten Traffic sehr leicht provozieren kann umso möglichst viele Daten in möglichst geringer Zeit verwerten zu können und so einer Erschließung des Schlüssels zu beschleunigen[5]. Die Fehlerhafte Programmierung und die daraus resultierenden Sicherheitslücken sind seit 2001 bekannt und wurden versucht zu lösen mit übergangsvarianten wie WEP+ doch erst 2004 mit WPA weitgehend behoben. Abschließend ist WEP nicht mehr zeitgerecht und in wenigen Minuten knack bar und somit unbrauchbar für die heutige Zeit.[6]

2.2 Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access oder kurz WPA ist der Nachfolger vom veralteten WEP und wurde 2004 als Sicherheitsstandard festgelegt.[7] Es basiert im Grundlegenden auf dem WEP, hat aber zusätzlich fundamentale Zusätze in der Verschlüsslung. WPA verfügt über dynamische Schlüssel die auf dem Temporal Key Integrity Protocol (TKIP)

[3] XOR Verknüpfung WLAN https://de.wikipedia.org/wiki/Wired_Equivalent_Privacy 12.04.2019
[4]PSK WLAN https://www.security-insider.de/was-ist-ein-pre-shared-key-psk-a-792430/ 13.04.2019
[5] WEP Sicherheitslücken https://www.security-insider.de/wep-bietet-keinerlei-schutz-fuers-wlan-a-92868/ 11.04.2019

[6] WEP knacken https://www.golem.de/0704/51549.html 11.04.2019

[7] WPA https://de.wikipedia.org/wiki/Wi-Fi_Protected_Access 11.04.2019

basieren. TKIP benutzt wie WEP den RC4 Algorithmus zur Verschlüsselung zusätzlich stellt TKIP sicher dass jedes Datenpaket mit einem anderen Schlüssel verschlüsselt wurde[8]. Hinzu wird ein Message Integrity Check Verfahren, kurz MIC, benutzt um die Vertrauenswürdigkeit der Daten zu überprüfen. Um dies zu gewährleisten werden die Datenpakete durch nummeriert beim Verschicken und beim empfangen durch gezählt, so werden Datenpakete die nicht vertrauenswürdigem Ursprung sind sofort erkannt und aussortiert[9]. Die Authentifizierung im WLAN findet entweder über einen Externen Server oder über einen sogenannten PSK (Pre-Shared-Key) besser bekannt als WLAN-Passwort statt. Dieser vorher vereinbarte Schlüssel muss jedem Nutzer bekannt sein um sich damit im Netzwerk einzuloggen. 2008 wurde WPA als unsicher gemeldet und der Nachfolger WPA2 angekündigt.[10]

2.3 Wi-Fi Protected Access 2 (WPA2)

Wi-Fi Protected Access 2 oder kurz WPA2 ist der Zurzeit genutzte Sicherheitsstandard. Bei einem starken Passwort gilt es als sehr schwer bis nicht knack bar. WPA2 implementiert die grundlegenden Funktionen des neuen Sicherheitsstandards IEEE 802.11i der auf Advanced Encryption Standard (AES) basiert. Durch den AES in Kombination mit dem Counter Mode with Cipher Block Chaining Message Authentication Code Protocol kurz CCMP als Protokoll schafft WPA2 eine extrem hohe und sichere Verschlüsselung die bei einem ausreichend starkem Passwort als sicher gilt. Die Authentifizierung ist über einen PSK oder einen Server möglich.[11]

---

[8] WPA https://www.security-insider.de/was-ist-wpa-a-742206/ 11.04.2019
[9] message integrity check https://www.itwissen.info/MIC-message-integrity-check.html 11.04.2019

[10] WPA https://de.wikipedia.org/wiki/Wi-Fi_Protected_Access 12.04.2019
[11] WPA2 https://www.elektronik-kompendium.de/sites/net/0907111.htm 15.04.2019

3. Aircrack-ng

Aircrack-ng ist eine kostenloses Tool was legal und frei im Internet herunter zu laden ist. Mit diesem Tool, was unter dem Betriebssystem Linux läuft ist es möglich durch mitschneiden der Daten, ein Passwort Attacke auf ein WLAN-Netzwerk zu starten. Benötigt wird dazu ein WLAN-USB und ein Linux Fähiger Computer oder eine Virtuelle Maschinen die auf Linux oder Kali Linux läuft.

3.1 USB Konfigurieren

Für den Versuch habe ich mich für die virtuelle Maschine, Oracle VM VirtualBox entschieden mit dem Betriebssystem Kali Linux. Nach der Installation wird im ersten Schritt der WLAN-USB in den Monitormode versetzt. Durch den Befehl “iwconfig“ überprüfen wir ob es eine verwendet bare WLAN-Karte gibt. In diesem Fall wird der USB-stick angezeigt der den Namen “wlan0“.Weiter erkennen wir das er sich im Managed Mode befindet, was bedeutet das der USB-stick nur den Traffic mitließt der von dem Router kommt mit dem er verbunden ist(Abb.1). Mit dem Befehl “airmon-ng check“, wird überprüft welche Prozesse den WLAN-USB daran hindern auch den

Traffic von den Anderen Routern mit zuschneiden. Es werden alle Prozesse auf gelistet und mit dem Befehl “ airmon-ng check kill“ werden alle Prozesse die den USB aufhalten sich in den Monitormode zu versetzten und somit davon abhält alle Datenpakete mit zuschneiden beendet(Abb.2).Mit dem Befehl “airmon-ng start wlan0“ wir die WLAN-Karte des USB-Sticks in den Monitormode versetzt(Abb.3). Nach erneuter Eingabe von dem Befehl “iwconfig“ wird deutlich das nun die WLAN-Karte vom USB-Stick sich im Monitormode befindet und das sich der Name von “wlan0“ zu “wlan0mon“geändert hat.(Abb.4).

3.2 Netzwerk finden und Daten mitschneiden

Durch den Befehl “airodump-ng wlan0mon“ sucht die sich nun im Monitormode befinden WLAN-Karte nach allen empfang baren Netzwerk-verbindungen die sie empfängt. Es wird mein Test WLAN mit dem Namen “another“ gefunden, zusätzlich bekommen wir die Informationen das es mit dem Sicherheitsstandard WPA2 in Kombination mit dem CCMP Protokoll gesichert wurde. Hinzu kommt das ein vorher vereinbarter Schlüssel nötig zur Authentifizierung nötig ist und die MAC Adresse des Routers wird gezeigt(Abb.5). Der nächste Schritt ist die Datenpakete mit zuschneiden um somit ein mitübertragenen Schlüssel aufzuzeichnen. Mit dem Befehl “airodump-ng“ gefolgt von “--bssid“ und der Mac Adresse (bssid) des Routers mit dem Zusatz “-c“ und dem Chanel sowie “--write “ und einem Namen wo die mit geschnittenen Daten gespeichert werden sollen plus den Namen der verwendeten WLAN-Karte in diesem Falle “wlan0mon“(Abb.6).Im Normal Fall müsste man darauf warten das sich ein Nutzer neu verbindet mit dem Netzwerk oder man kann mit bestimmten Tools alle verbundenen Benutzer dazu zwingen sich neu zu verbinden .Diesen Fall habe ich durch mein Handy das sich neu verbunden hat simuliert. In diesem Moment sendet das Handy den Schlüssel verschlüsselt an den Router zu Authentifizierung. Der USB-stick der sich im Monitormodus ist in der Lage diese Übermittlung mit zu schneiden und zu speichern und hat somit den verschlüsselten Schlüssel und den Initialisirungsvektor aufgezeichnet

und gespeichert was zur Erschließung des Passwortes führt. Der Handshake wurde aufgezeichnet(Abb.7).

3.3 Mögliche Passwörter

Um die möglichen Passwörter einzugrenzen generieren wir eine Liste von Passwörtern mit bestimmten Bedingungen. Das ist mit dem Tool crunch möglich. Der Befehl “crunch“ sowie der minimalen Anzahl und drauf die maximale Anzahl der Zeichen gefolgt von Buchstaben, Zeichen, zahlen oder Wörtern die in dem Passwort Inhalten sein könnten. Der Befehl endet mit “-o“ und einem Namen der Dateien wo diese Passwörter gespeichert werden sollen. Das Tool generiert nun alle möglichen Kombinationen mit den vorgegeben Bedingungen, denkbar wäre auch ein Wörterbuchangriff(Abb.8).

3.4 Passworte mittels Brute Force knacken

Im letzten Schritt wird über den Befehl “aircrack-ng“ und darauf folgend den Datei Namen mit dem Handshake sowie “-w“ und den Dateinamen wo die durch crunch generierten Passwörter gespeichert wurden(Abb.9). Das Tool versucht nun jede Möglichkeit aus das Passwort mit dem aufgezeichneten Handshake zu knacken(Abb.10). Es startet mit AAAAAAAA und endet mit HHHHHHHH. Bei diesen sehr konkreten Konfigurationen von crunch wird das Passwort in wenigen Minuten (3,5 min)gefunden(Abb.11).

4. Sicheres WLAN

Ein WLAN Netzwerk komplett zu sichern ist im Grunde nicht möglich aber man kann es durch verschiedene Konfigurationen so sichern das es Angreiffern so sehr erschwert wird das es fast unmöglich wird es anzugreifen.

4.1 Sicheres Passwort

Ein gutes Passwort ist der Hauptbestandteil eines gut gesicherten WLAN-Netzwerks. Das optimale Passwort ist mindestens 8 Zeichen Lang, optimal auch länger und besteht aus nicht zusammenhängenden Buchstaben in Groß und Klein Schreibung, Zeichen und Zahlen. In Folge dessen habe ich eine Laufzeit Analyse auf Länge und Kombination gemacht wenn man das Passwort eines mit WPA2 gesicherten WLAN Netzwerk über Aircrack-ng knackt mittels Brute Force(Abb.12). Bei einem Passwort das Groß- und Kleinbuchstaben, zahlen und eine Länge von 5 Zeichen hat brauch ein normaler Computer bei 3000 überprüften Schlüsseln in der Sekunde ohne Zugabe von Informationen wie Buchstaben oder Zahlen die verwendet werden könnten ca.3,5 Tage im längsten Fall. Bei einem Passwort mit den gleichen Bedingungen aber mit der Zeichen Länge von 6 brauch ein Angreifer ca. 219 Tage und somit 62 mal länger als mit 5 Zeichen. Bei einer Länge von 7 Zeichen ist es mit einer Laufzeit von ca. 37 Jahren (13586 Tagen) sehr unwahrscheinlich dass es geknackt wird. Ab 8 Zeichen und einer Laufzeit von 2307 Jahren ist es so gut wie unmöglich das Passwort zu knacken. Durch das einbauen von ca. 20 möglichen Zeichen wird bei einer Passwortlänge von 5 Zeichen die Laufzeit auf 14 Tage erhöht. Bei einer Passwortlänge von 8 Zeichen erhöht sich die Laufzeit auf 21606 Jahre und ist damit so gut wie nicht knack bar. Ein Zufalls Treffer ist immer möglivh und somit kann sich die Laufzeit auch erheblich verkürzen. Das ändern des Passwortes machtest dem Angreifer zunehmend schwer.

4.2 WPS

WiFi Protected Setup kurz WPS sollte möglichst deaktiviert und nicht benutzt werden. Es ist einem Angreifer möglich durch belauschen des Traffics den 8 Zeichen langen Schlüssel zu errechnen und sich somit Zugang zum Netzwerk zu verschaffen. Das ist möglich da es nur eine sehr geringe Anzahl von möglichen Passwörtern gibt hinzu kommt das der Router nach jedem versuch preis gibt ob die ersten oder die letzten 4 falsch waren, was das errechnen durch ausschließen extrem beschleunigt.[12]

4.3 Sicherheitsstandert

Die neuste und beste Verschlüsselung durch WPA2 und bald WPA3 ist ein großer Bestandteil. Die Aktualisierung sollte regelmäßig geschehen um ein veralten auszuschließen. Nicht nur die Software sondern auch die Hardware sollte zeitgerecht aktualisiert sein um eine möglichst sichere Datenübertragung zu ermöglichen.

[12] WPS Sicherheitslücke https://www.computerbild.de/artikel/cb-Aktuell-Sicherheit-WPS-Luecke-bei-WLAN-Routern-7012708.html 25.04.2019

5. Fazit

Ein WLAN Netzwerk deckt ein großer Teil unserer Datenübertragung, besonders im privaten ab. Die Übertragungen über den freien Raum bildet bis zum heutigen Stand der Technik und Verschlüsselung die größte Sicherheitslücke. Durch ein starkes und gutes Passwort und eine Einstellung des Routers ist es möglich das Heim Netzwerk für schwache Angreifern zu Sichern. Bei einem WPA oder WEP geschützten Netzwerk ist der Angriff auf das Netzwerk in wenigen Minuten möglich genau wie bei einem WPA2 geschützten WLAN mit einem schlechten gewähltem Passwort. Ein Netzwerk anzugreifen ist in der heutigen Zeit nicht mehr schwer. Die Softwear und das Betriebssystem kann für umsonst und legal heruntergeladen werden. Die Sicherheitsstandards stehen im ständigen Wettlauf gegen diese die versuchen ein Netzwerk anzugreifen. Abschließend stellt sich die Frage wie kann unsere Daten Übertragung gesichert werden wenn alles was man braucht um eine solche Übertragung anzugreifen legal und frei erhältlich ist oder wird somit der Sicherheitsstandards von WLAN nur sicherer weil alle Sicherheitslücken gefunden werden je mehr Leute daran arbeiten es anzugreifen ?

6.Abbildungen

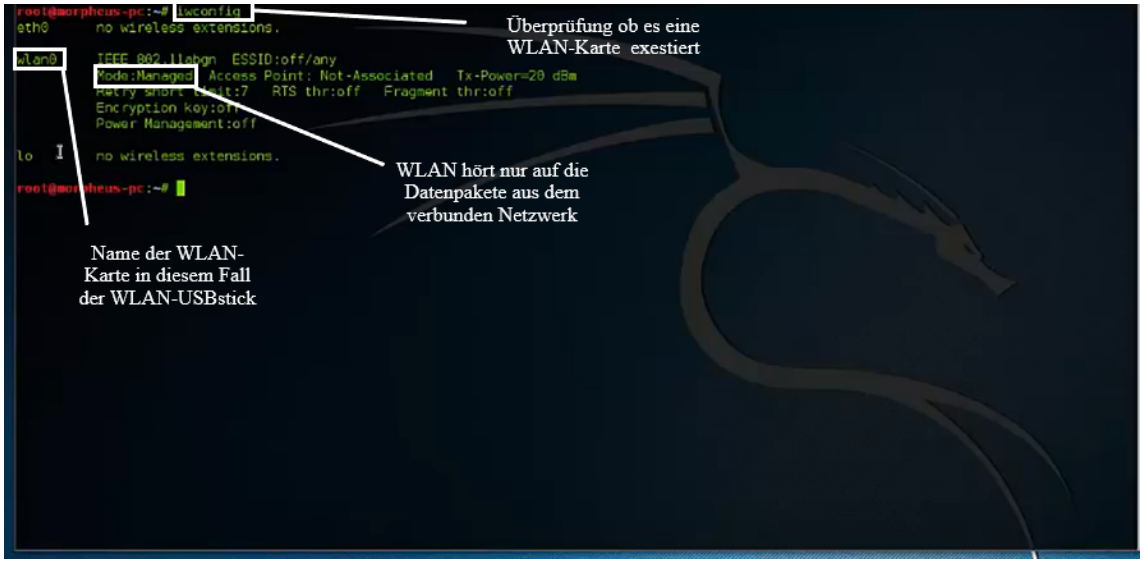

Abb.1

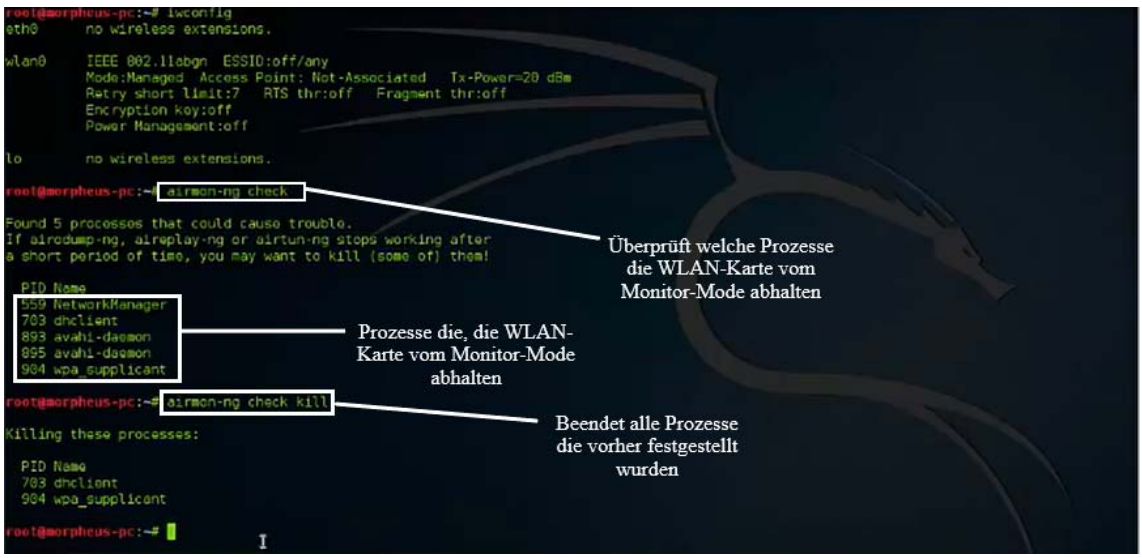

Abb2

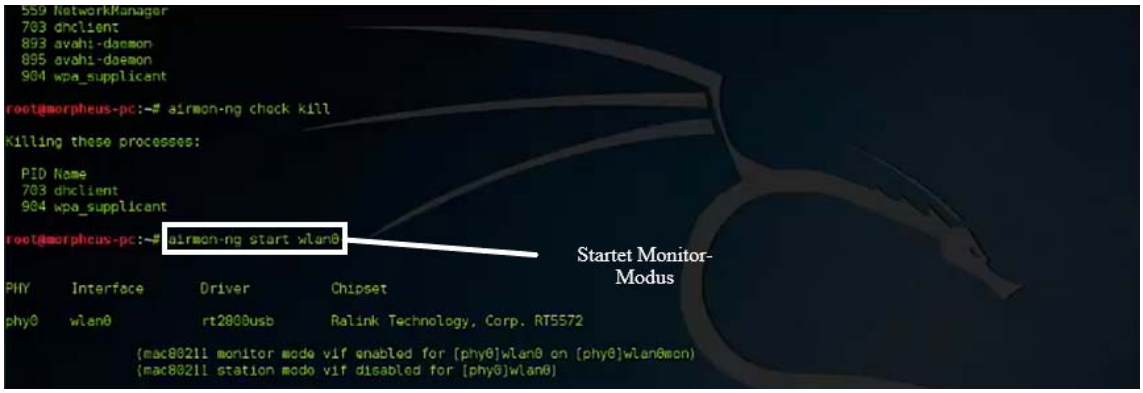

Abb.3

Abb.4

Abb.5

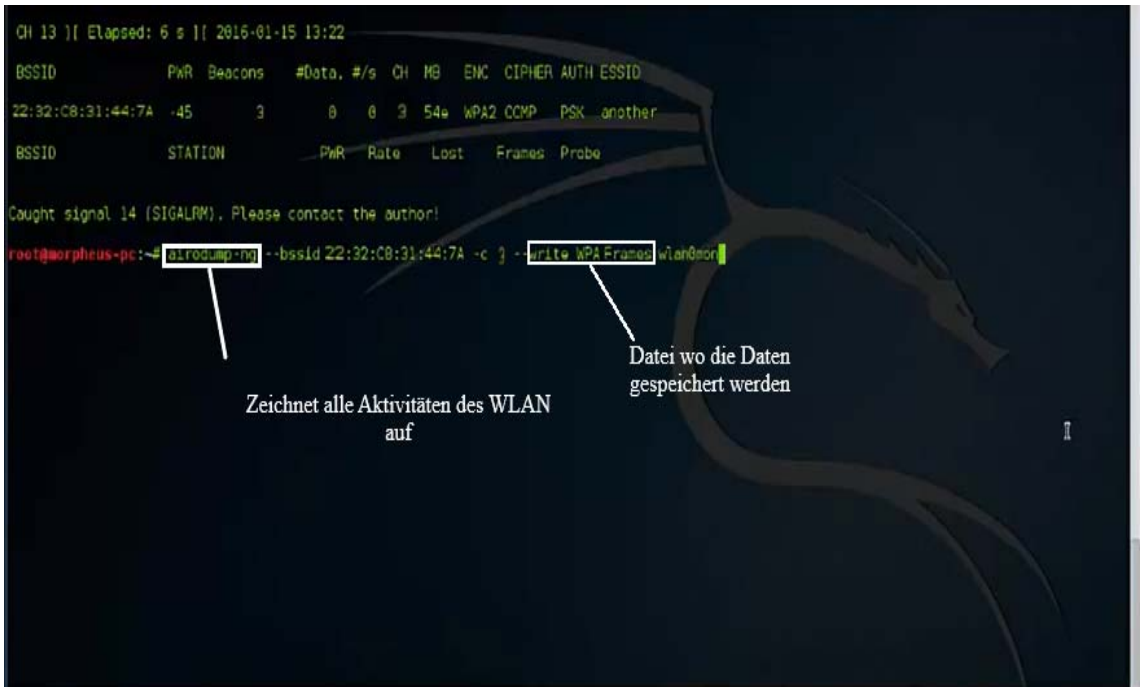

Abb.6

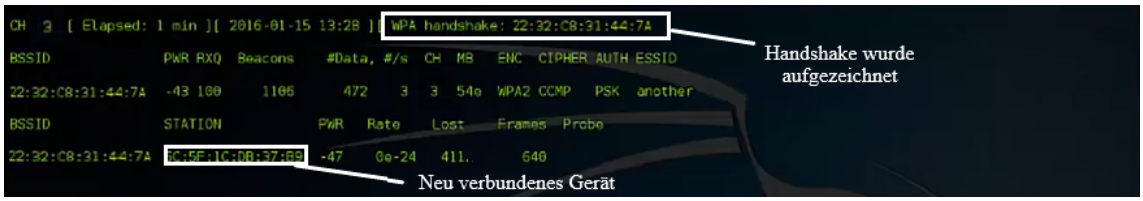

Abb.7

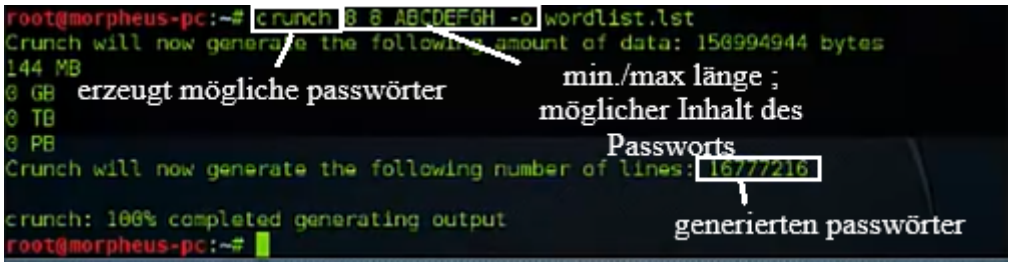

Abb.8

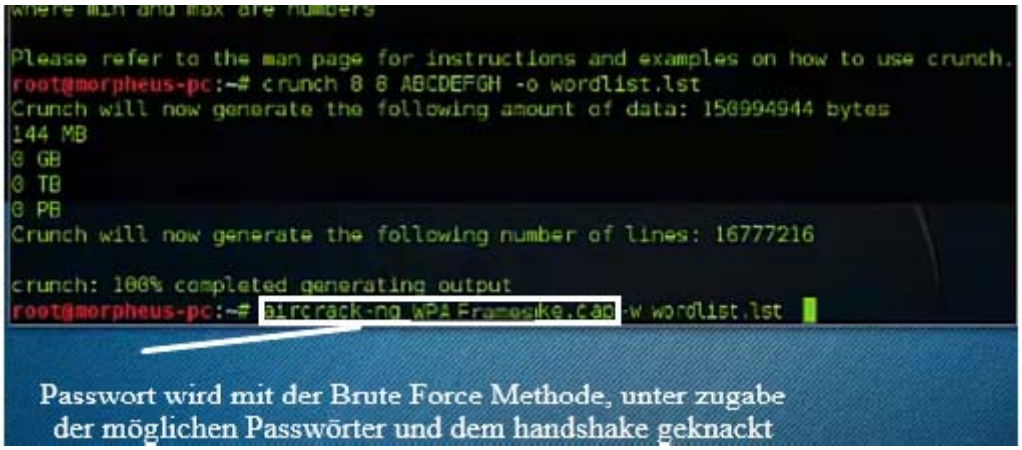
where min and max are numbers
Please refer to the man page for instructions and examples on how to use crunch.
root@morpheus-pc:~# crunch 8 8 ABCDEFGH -o wordlist.lst
Crunch will now generate the following amount of data: 150994944 bytes
144 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 16777216
crunch: 100% completed generating output
root@morpheus-pc:~# aircrack-ng WPAFramesike.cap -w wordlist.lst
Passwort wird mit der Brute Force Methode, unter zugabe der möglichen Passwörter und dem handshake geknackt

Abb.9

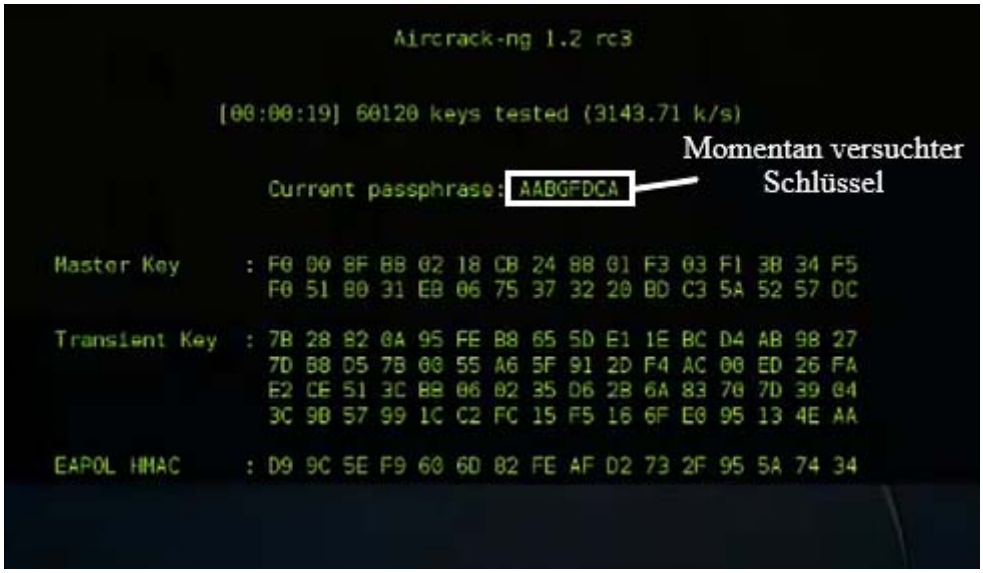
Aircrack-ng 1.2 rc3
[00:00:19] 60120 keys tested (3143.71 k/s)
Momentan versuchter Schlüssel
Current passphrase: AABGFDCA
Master Key : F0 00 8F B8 02 18 CB 24 88 01 F3 03 F1 3B 34 F5
F0 51 80 31 E8 06 75 37 32 20 BD C3 5A 52 57 DC
Transient Key : 7B 28 82 0A 95 FE B8 65 5D E1 1E BC D4 AB 98 27
7D B8 D5 7B 00 55 A6 5F 91 2D F4 AC 00 ED 26 FA
E2 CE 51 3C B8 06 02 35 D6 2B 6A 83 70 7D 39 04
3C 9B 57 99 1C C2 FC 15 F5 16 6F E0 95 13 4E AA
EAPOL HMAC : D9 9C 5E F9 60 6D 82 FE AF D2 73 2F 95 5A 74 34

Abb.10

Abb.11

A	B	C	D	E	F	G
Länge	A,B,C	a,b,c	Zahlen	Laufzeit in Tagen	laufzeit in jahren	
5	ja	ja	10	3,5		
6	ja	ja	10	219,1		
7	ja	ja	10	13586,5	37	
8	ja	ja	10	842362	2307	
Länge	A,B,C	a,b,c	Zahlen	Zeichen	Laufzeit in Tagen	Laufzeit in jahren
5	ja	ja	10	20	14,3	
6	ja	ja	10	20	1172,8	3,2
7	ja	ja	10	20	96175	263,4
8	ja	ja	10	20	7886350	21606

Abb.12

7.Quellenverzeichnis

1. Stefan Luber, Peter Schmitz(03.09.2018) Definition Wired Equivalent Privacy (WEP)/ Was ist WEP https://www.security-insider.de/was-ist-wep-a-742205/ geöffnet am 17.04.2019
2. Damon Dransfeld (28.03.2013)RC4 Verschlüsselung Grundlagen http://www.tacticalcode.de/2013/03/rc4-verschlusselung-grundlagen.html geöffnet am 17.04.2019
3. (03.07.2018)Wired Equivalent Privacy https://de.wikipedia.org/wiki/Wired_Equivalent_Privacy geöffnet am 12.04.2019
4. Stefan Luber, Peter Schmitz Definition PSK (Pre-shared Key) Was ist ein Pre-shared Key (PSK)? https://www.security-insider.de/was-ist-ein-pre-shared-key-psk-a-792430/ geöffnet am 13.04.2019
5. Peter Riedlberger , Peter Schmitz(13.09.2007) WEP: Funktionsweise, Schwachstellen, Exploits WEP bietet keinerlei Schutz fürs WLANhttps://www.security-insider.de/wep-bietet-keinerlei-schutz-fuers-wlan-a-92868/ geöffnet am 11.04.2019
6. Andreas Sebayang (05.04.2007) WLAN: WEP in weniger als einer Minute knacken Forscher optimieren Angriffe auf drahtlose Netzwerke mit WEP-Verschlüsselung https://www.golem.de/0704/51549.html geöffnet am 11.04.2019
7. (16.04.2019) Wi-Fi Protected Access https://de.wikipedia.org/wiki/Wi-Fi_Protected_Access geöffnet am 11.04.2019
8. Stefan Luber, Peter Schmitz (04.09.2018) Definition Wi-Fi Protected Access (WPA) Was ist WPA? https://www.security-insider.de/was-ist-wpa-a-742206/ geöffnet am 11.04.2019
9. (17.11.2006) MIC (message integrity check) https://www.itwissen.info/MIC-message-integrity-check.html geöffnet am 11.04.2019
10. (16.04.2019) Wi-Fi Protected Access https://de.wikipedia.org/wiki/Wi-Fi_Protected_Access geöffnet am 12.04.2019

11. WPA2 - WiFi Protected Access 2 / IEEE 802.11i https://www.elektronik-kompendium.de/sites/net/0907111.html geöffnet am 15.04.2019
12. Rainer Schuldt Schwere Sicherheitslücke bei vielen Routern entdeckt https://www.computerbild.de/artikel/cb-Aktuell-Sicherheit-WPS-Luecke-bei-WLAN-Routern-7012708.html geöffnet am 20.04.2019
13. Deckblatt “WLAN-Symbol“ https://cdn.pixabay.com/photo/2014/12/05/13/51/wlan-558025_960_720.png geöffnet am 20.04.2019

8.Versicherung der selbständigen Erarbeitung

Ich versichere, dass ich die vorliegende Arbeit einschließlich evtl. beigefügter Zeichnungen, Kartenskizzen, Darstellungen u. ä. m. selbstständig angefertigt und keine anderen als die angegebenen Hilfsmittel benutzt habe. Alle Stellen, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen sind, habe ich in jedem Fall unter genauer Angabe der Quelle deutlich als Entlehnung kenntlich gemacht.

_____, den _____

(Ort) (Datum)

_____

(Unterschrift)