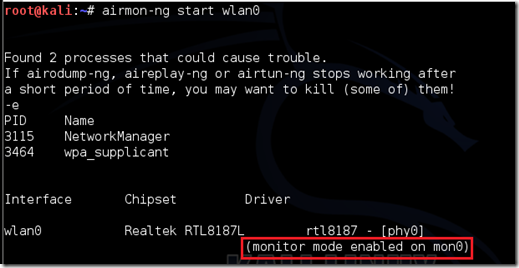
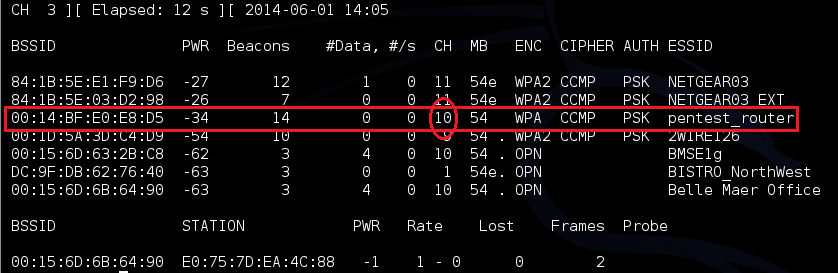
|  |  |
| --- | --- |
| **Angriffsbeschreibung** | |
| **Name:** Zugriffsverletzung WLAN | **Hauptverantwortlicher**: Nikolai Kloß, Eduard Ljaschenko |
| **Ziel des Angriffs**: Zugang zum fremden WLAN | **Gefährdete Personengruppen**: Jeder mit WLAN-Netzwerk |
| **Beispiel eines Angriffsszenarios** | |
| **Benötigten Dinge**:   * Kali Linux VM * Wireless Adapter mit einem Injection/Monitor Mode * Wordlist   Nachdem die Kali Linux VM gestartet wurde, sollte man sich von allen Drahtlosen Netzwerken trennen, ein Terminal öffnen.  Als erstes möchte man sich alle Wireless-Karten anzeigen lassen, die den Monitor Mode unterstützen. | |
| *1 . Schritt:* | |



|  |
| --- |
| Mit dem Befehl **airmon-ng start** gefolgt von dem Namen der Wireless-Karte, aktiviert den benötigten Monitor Mode |
| *2. Schritt* |



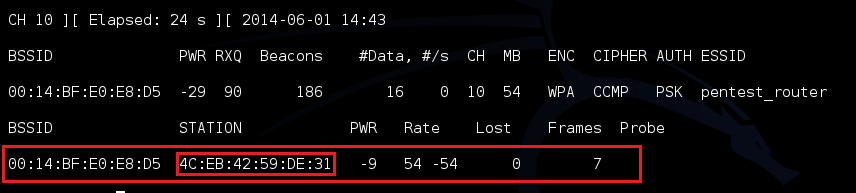
|  |
| --- |
| Mit dem Befehl **airodump-ng** gefolgt von dem Namen des neuen Monitor Interfaces, in dem Fall mon0, werden alle in der Nähe verfügbaren WLAN Netzwerke angezeigt. Für den Angriff ist die BSSID und der Channel von Bedeutung |
| *3. Schritt* |



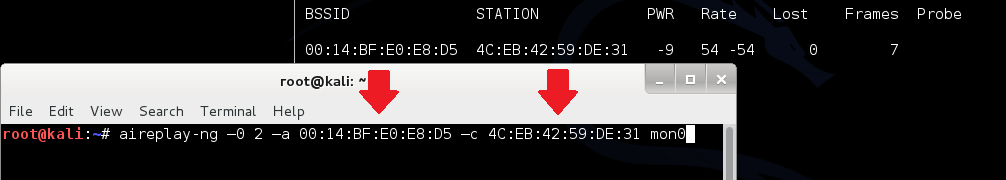
|  |
| --- |
| Nachdem man die BSSID und den Channel erhalten hat, fügt man diese in folgenden Befehl ein:  **airodump-ng -c <channel> --bssid <bssid> -w /root/Dektop/<monitor interface>**  Mit „**-w**“ wird der Dateipfad spezifiziert, an dem alle abgefangenen Vier-Wege-Handshakes gespeichert werden.  In dem Fall wird es auf dem Desktop gespeichert |
| *4. Schritt* |



|  |
| --- |
| Airodump überwacht jetzt das Ziel Netzwerk. Nun steht man vor der Wahl. Entweder wartet man bis sich ein Gerät mit dem Netzwerk verbindet, wodurch der Router gezwungen wird einen Vier-Wege-Handshake auszusenden, den man benötigt um an das Passwort zu gelangen, oder man beschleunigt den Prozess unter der Verwendung des Tools aireplay-ng . Mit dem Tool können Netzwerkgeräte dazu gezwungen werden, sich wieder mit dem Netzwerk zu verbinden, indem deauthentication (deauths) Pakete gesendet werden.  Damit das Funktioniert muss ein anderes schon mit dem Netzwerk verbunden sein.  Im folgendem Bild hat sich ein Gerät mit dem Netzwerk verbunden. |
| 5. Schritt |



|  |
| --- |
| Während Airodump weiterläuft, wird ein weiteres Terminal benötigt, in dem man den folgenden Befehl eingibt.  **aireplay-ng -0 2 -a <router bssid> -c <client bssid> mon0**  Mit „**-0**“ bestimmt man die Anzahl der zu sendenden deauth Pakete  „**-a**“ gibt die BSSID des Routers an. In dem Fall 00:14:BF:E0:E8:D5  „**-c**“ gibt die BSSID des Clients an, zu dem die deauth Pakete gesendet werden sollen, welche unter dem Punkt STATION auffindbar ist. |
| 6. Schritt |



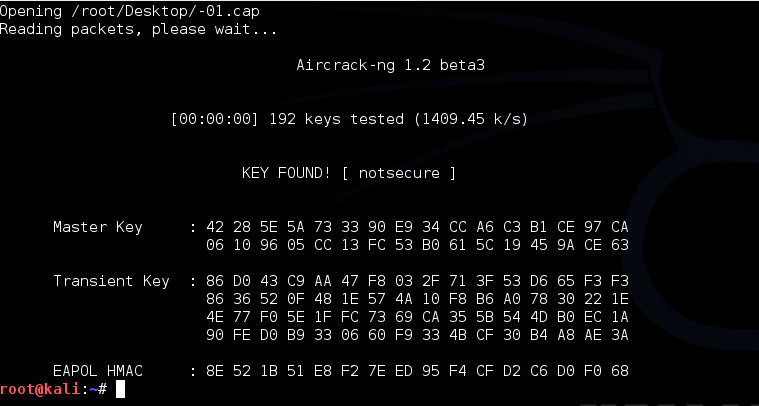
|  |
| --- |
| Bei Eintritt der, in der folgenden Abbildung zusehenden, Nachricht, wurde ein Handshake erreicht und man ist im Besitz des Passworts. |
| 7. Schritt |



|  |
| --- |
| Nun benötigt man die .cap Dateien die mit dem 4. Schritt auf dem Desktop erstellt wurden.  Es wird ein weiteres Terminal benötigt, in dem man den folgenden Befehl eingibt:  **aircrack-ng -a2 -b <router bssid> -w <pfad zur wordlist> /root/Dektop/\*.cap**  „**-a**“ bestimmt die Methode, die aircrack nutzt, um den Handshake zu cracken. (2=WPA).  Ein kompletter Befehl sieht wie folgt aus: |
| 8. Schritt |

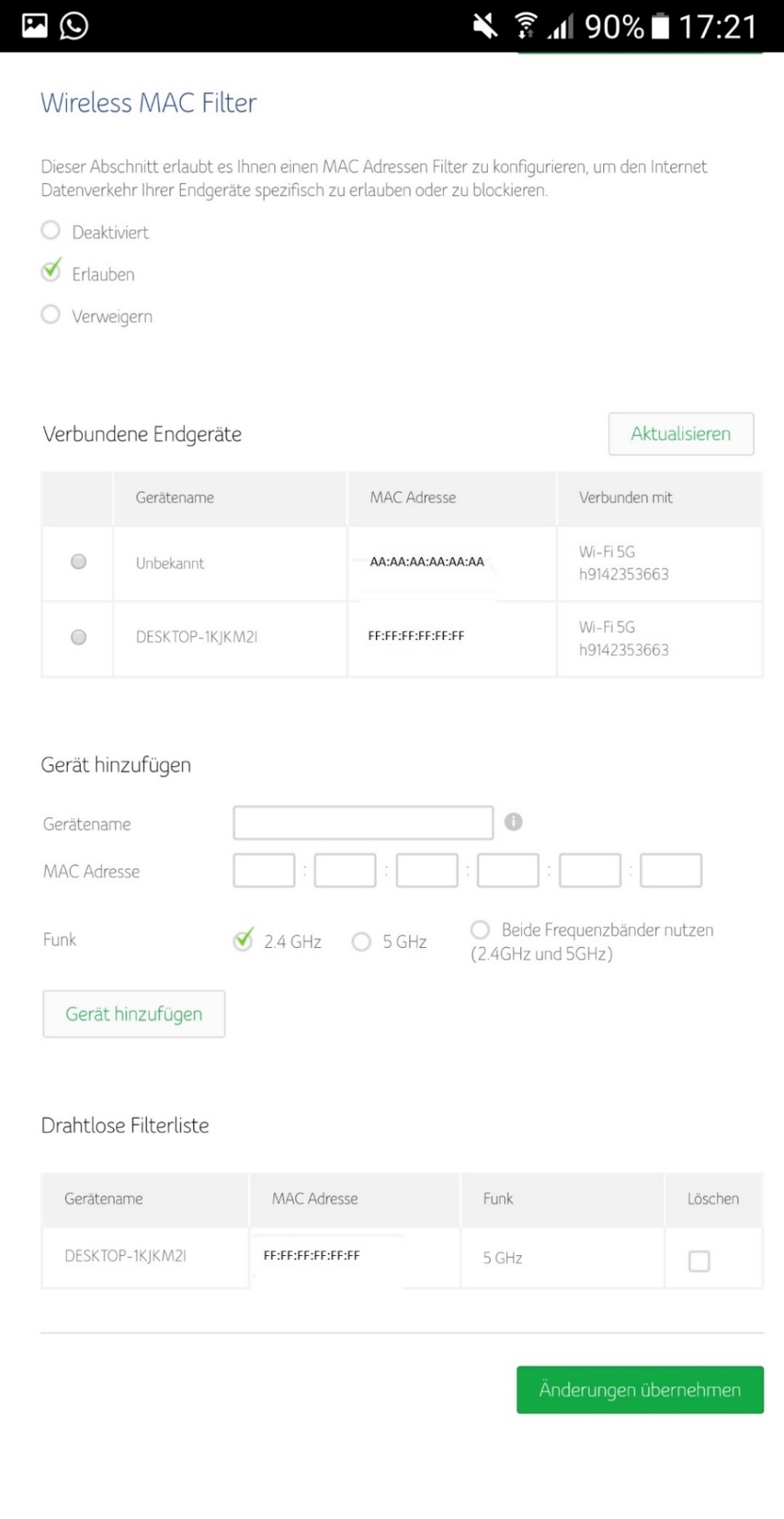


|  |
| --- |
| Nun wird Aircrack-ng versuchen das Passwort zu cracken. Es ist jedoch nur möglich solange die Wordlist das Passwort enthält und kann je nach Größe der Wordlist einige Zeit in Anspruch nehmen.  Ein erfolgreiches Beispiel sieht wie folgt aus: |
| 9. Schritt |

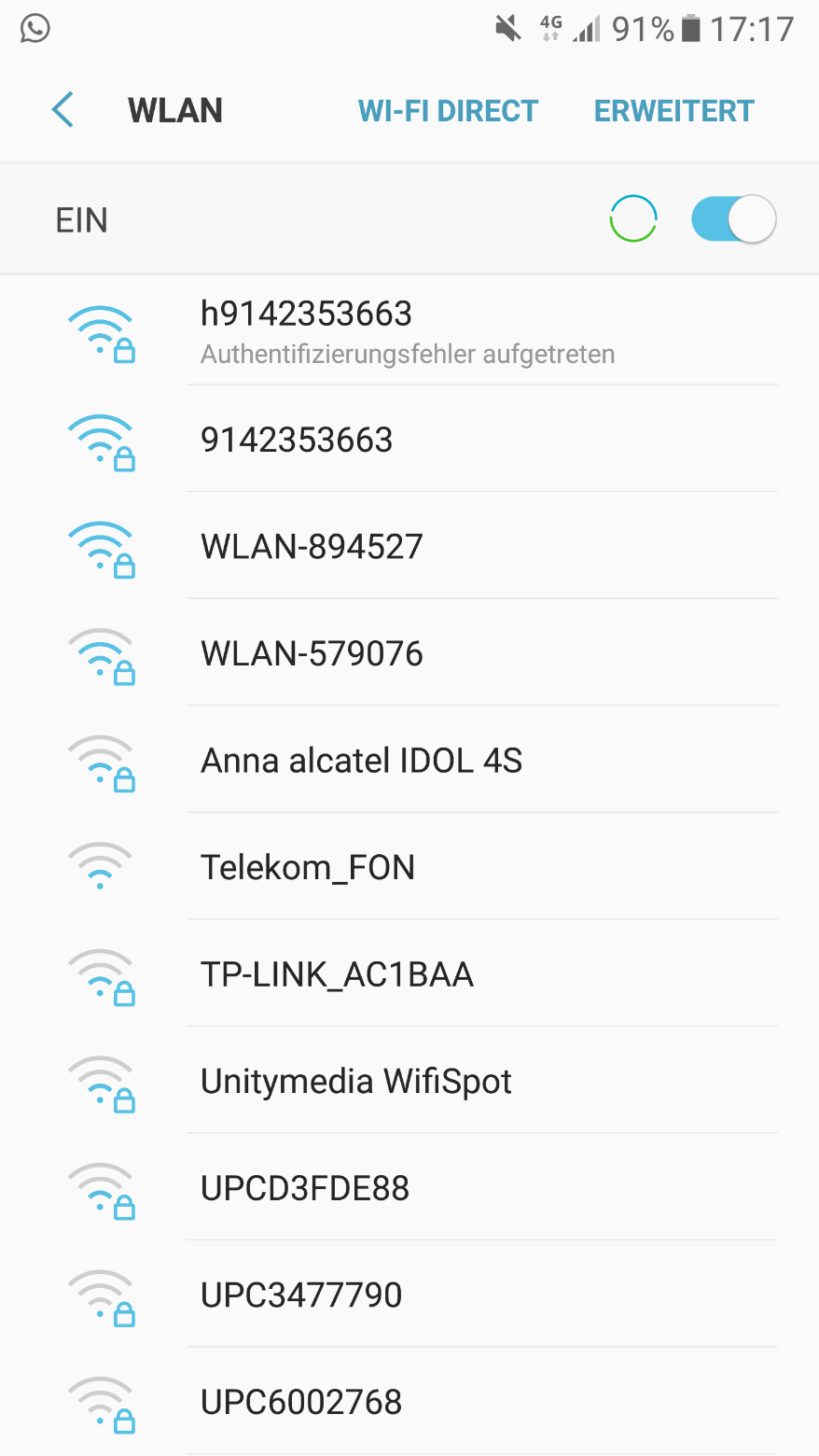


|  |
| --- |
| Schutzmaßnahmen |
| Um sein WLAN Netzwerk vor Angriffen vor Unbekannten zu schützen, sollte man die MAC-Filter-Funktion seines Routers aktivieren. So wäre dem Angreifer nicht mehr die Möglichkeit gegeben, ein Netzwerkpasswort zu Bruteforcen, da es unzulässigen MAC-Adressen unmöglich ist, sich überhaupt zu authentifizieren. |

|  |
| --- |
| *1. MAC-Adressenfilter-Funktion aktivieren* |



|  |
| --- |
| *2. MAC-Adressenfilter-Funktion aktivieren* |



|  |
| --- |
| **Kommentare**:  1:Für das Netzwerk ist nur ein Endgerät mit der MAC-Adresse von „DESKTOP-1KJKM2I“ erlaubt.  2:Jeder Verbindungsversuch zum Netzwerk „h9142353663“, wird mit unzulässiger MAC-Adresse blockiert. |

Zusätzlich:

MAC-Adressen gibt es in 70 Billionen Kombinationen, somit ist es theoretisch möglich eine gültige Adresse zu erraten, um dann daraufhin das WLAN Passwort, ebenfalls zu Bruteforce‘n. Aber durch den Zeitaufwand der hier eine erhebliche Rolle spielt, wird die ganze Prozedur unattraktiv für den Angreifer.

Um die Sicherheit zu maximieren, besteht die Möglichkeit die Anzahl der Zugriffe auf den Router für je eine MAC-Adresse auf bestimmte Versuche pro Zeit zu beschränken. Ebenfalls sollte das WLAN-Zugangspasswort von Zeit zu Zeit geändert werden.