WEP & WPA Security lab

**Unit 9 – Wireless security & Availability**

# wep & wpa security lab

**Lab Description:** In this lab your students will use packet captures of wireless 802.11 traffic between a client and access point. Specifically, traffic for both WEP and WPA protocols. The goal is to understand that tools like Aircrack-NG make cracking encryption or brute-forcing passwords in both protocols easy. Cracking the encryption will produce the key used by both the wireless client and access point, while brute-forcing will also attain it. Thus, having the ability to decrypt the traffic and seeing the network traffic.

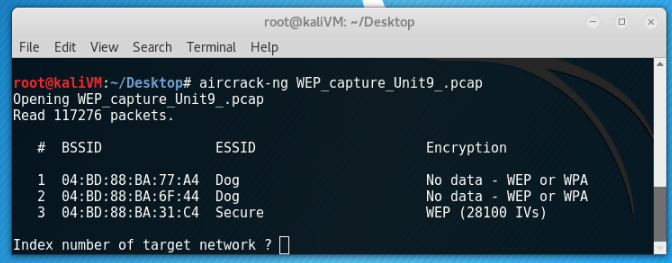
**Lab Environment:** Kali Linux OS w/ Aircrack-NG tool.

**Lab Files that are Needed:** WEP\_capture\_Unit9\_.pcap , WPA\_capture\_Unit9.pcap

### **analyzing pcap**

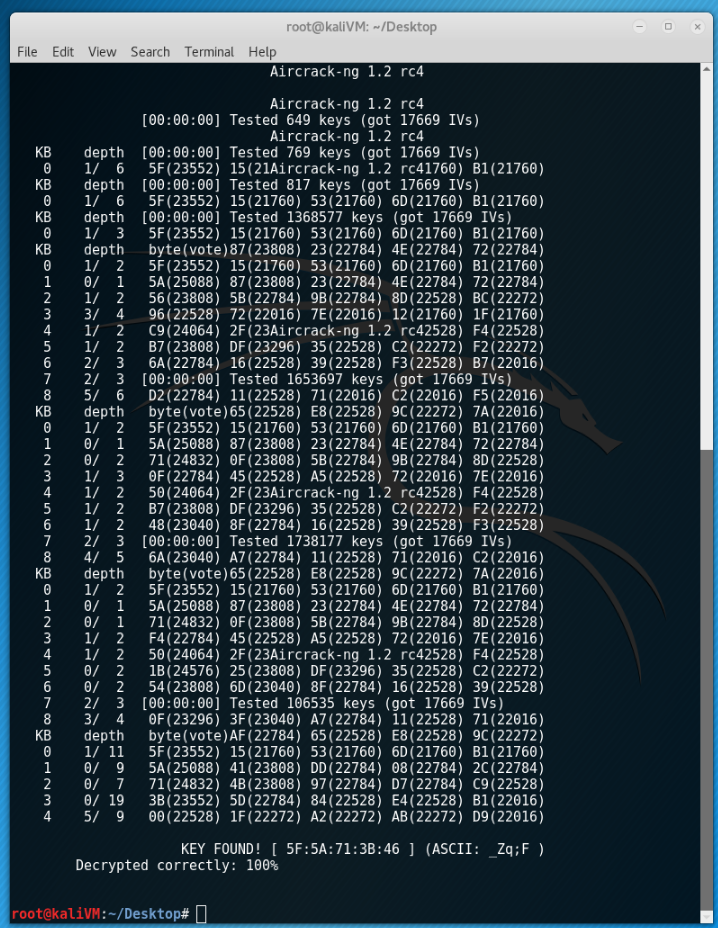
1. What specific frame is needed in order to crack a WPA2 key?
   1. **ANSWER:** Authentication Frame
2. Utilizing the Aircrack-NG tool and the pcap file, crack both the WEP and WPA2 keys.
   1. Screenshot of Aircrack-NG tool and commands to crack the keys.
      1. **ANSWER:**

*Aircrack-NG command (WEP):*

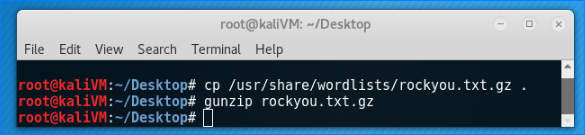


**The Aircrack-NG tool allows users the ability to provide a packet capture containing traffic between a client and access point (a minimum of 5000 packets needed). In theory you would capture the traffic by using a device with a wireless card put in promiscuous mode. Thus allowing it to see wireless traffic meant for other devices (typically wireless cards will ignore traffic not meant for its MAC-Address, in promiscuous mode it will accept all packets). In the case of this lab, a packet capture is provided, the “Secure” network, but your own can be substituted in!**

*Aircrack-NG Results After Network Selection (WPA2):*

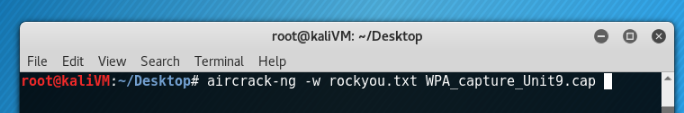


*Attaining Password File:*

**

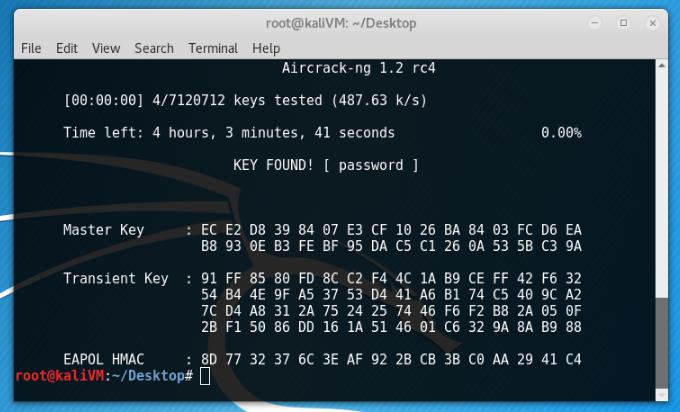
**Kali Linux OS provides a premade password list available for users. In this case you will want to unzip it to your current directory. You can also provide your own password that is tailored to the target, or just a larger list (this will require more computational power and time to complete)!**

*Aircrack-NG command (WPA2):*

**

**The -w flag is used to specify the file containing passwords for brute-forcing. In this case, rockyou.txt provided by Kali Linux OS.**

*Aircrack-NG Results with file selection (WPA2):*

**

* 1. Cracked WEP key: ***\_Zq;F***
  2. Cracked WPA2 key: **password**

**ENCRYPTION RESEARCH**

1. What is the difference between RC4 and AES?
   * **RC4**
     + **Is a stream cipher**
     + **Insecure due to “bit flipping” and weak key scheduling**
     + **Implemented in the WEP protocol**
     + **Favored stream cipher used within 802.11 (and other protocols)**
   * **AES**
     + **Is a block cypher**
     + **NIST & US Government Standard**
     + **Very few detrimental attacks**
     + **Implemented in the WPA/WPA2 protocols**
     + **Modern networks now typically use AES for encryption**
2. Explain the difference between block and stream ciphers.
   * **Stream Cipher**
     + **Converts one character of plaintext into one character of encrypted text**
     + **Faster process time**
     + **Low chance of errors**
     + **Susceptible to insertion attacks**
   * **Block Cipher**
     + **Converts a grouping of characters into one block**
     + **Slower process time**
     + **Higher chance of errors**
     + **More difficult to attack**
3. What other stream ciphers exist?
   * **Types:**
     + **FISH**
     + **A5/1**
     + **SOBER-128**
     + **Etc…**

## What to submit

Screenshots and a description of each part/question in a Word Document or PDF.