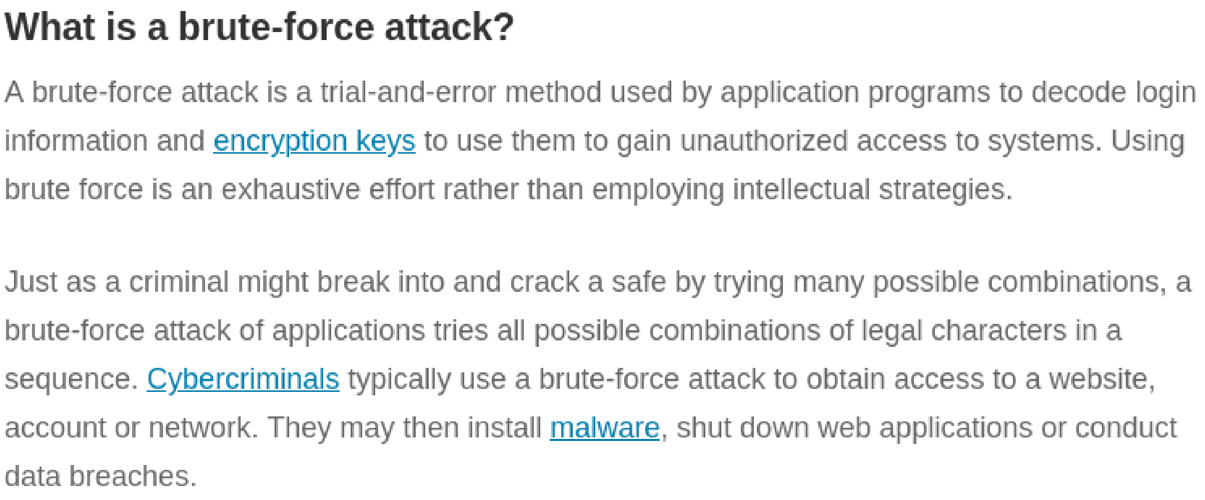
Introduction:

This report provides a comprehensive summary of wireless attacks and Wi-Fi penetration testing techniques based on the content covered in the TryHackMe room "WiFi Hacking 101." The tasks completed in this room offer practical insights into conducting wireless penetration testing, encompassing basic concepts, tools, and methodologies.
https://tryhackme.com/p/Damiano254

Task 1: The basics - An Intro to WPA:

The task familiarizes users with essential terminology and concepts in Wi-Fi security. Notable points include understanding the differences between SSID, ESSID, and BSSID, as well as distinguishing between various authentication standards like WPAPSK/WPA2PSK and WPA2EAP. The task also underscores the significance of capturing the four-way handshake during penetration testing to assess network security effectively.

- **What type of attack on the encryption can you perform on WPA(2) personal?**
    - **Brute force**

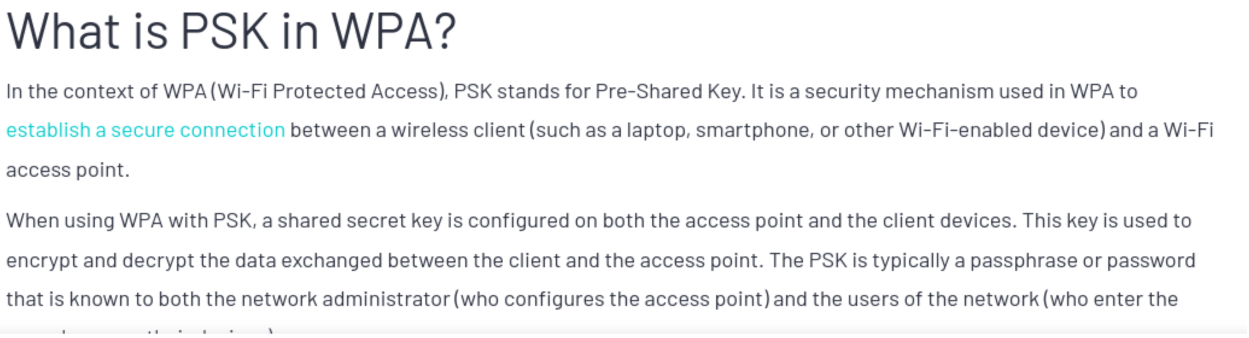


What is a brute-force attack?

A brute-force attack is a trial-and-error method used by application programs to decode login information and encryption keys to use them to gain unauthorized access to systems. Using brute force is an exhaustive effort rather than employing intellectual strategies.

Just as a criminal might break into and crack a safe by trying many possible combinations, a brute-force attack of applications tries all possible combinations of legal characters in a sequence. Cybercriminals typically use a brute-force attack to obtain access to a website, account or network. They may then install malware, shut down web applications or conduct data breaches.

- **Can this method be used to attack WPA2-EAP handshakes? (Yea/Nay)**
    - **Nay**
- **What three-letter abbreviation is the technical term for the "wifi code/password/passphrase"?**
    - **PSK**



What is PSK in WPA?

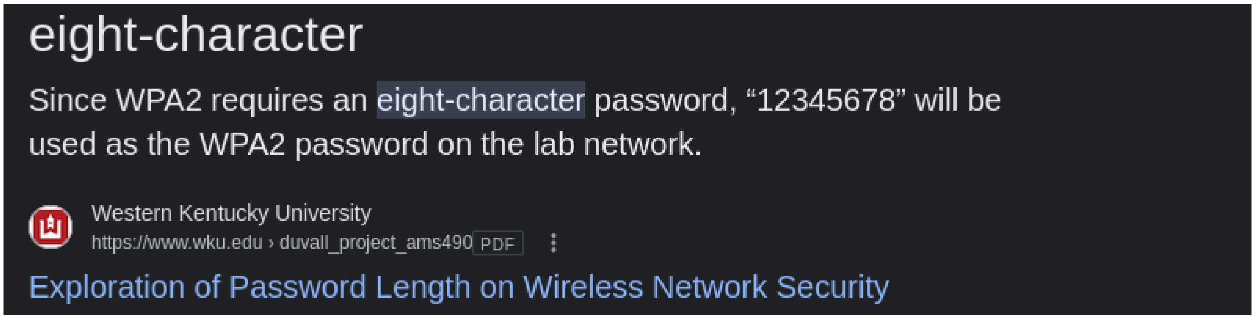
In the context of WPA (Wi-Fi Protected Access), PSK stands for Pre-Shared Key. It is a security mechanism used in WPA to establish a secure connection between a wireless client (such as a laptop, smartphone, or other Wi-Fi-enabled device) and a Wi-Fi access point.

When using WPA with PSK, a shared secret key is configured on both the access point and the client devices. This key is used to encrypt and decrypt the data exchanged between the client and the access point. The PSK is typically a passphrase or password that is known to both the network administrator (who configures the access point) and the users of the network (who enter the

Task 2: You're being watched

Capturing packets to attack: This task delves into the practical aspects of wireless penetration testing, focusing on capturing packets to initiate attacks. Key steps include putting the network interface into monitor mode using tools like Aircrack-ng, checking for interference from other processes, and capturing traffic and Wi-Fi beacons of nearby networks. Special attention is given to de-authenticating devices connected to the target network to capture the four-way handshake effectively.

- **What's the minimum length of a WPA2 Personal password?**
  - **8**



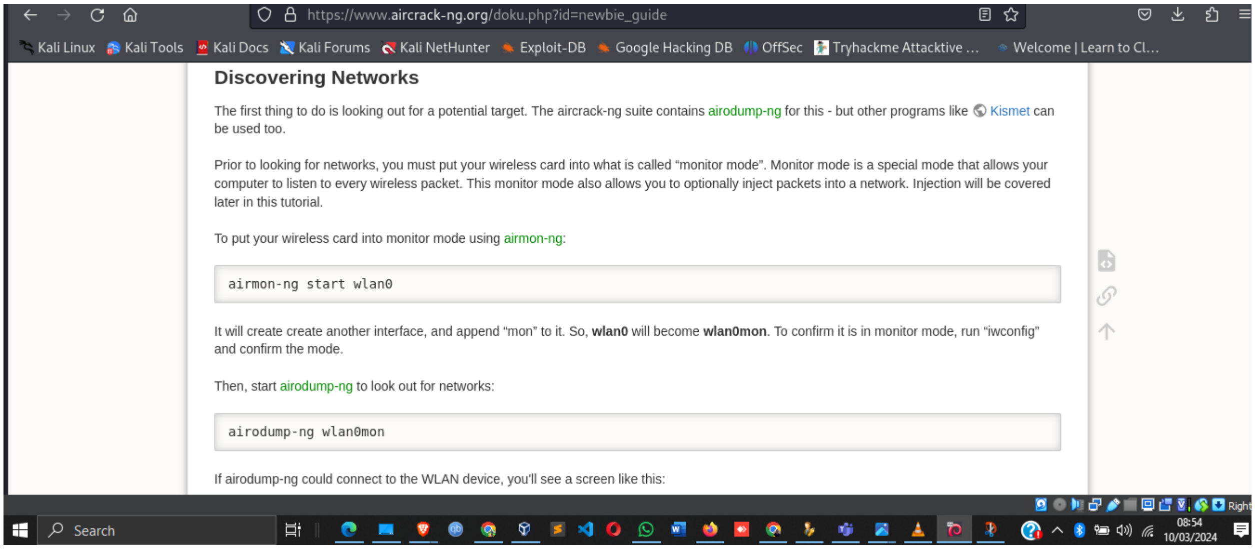
eight-character

Since WPA2 requires an eight-character password, “12345678” will be used as the WPA2 password on the lab network.

Western Kentucky University
https://www.wku.edu › duvall_project_ams490 PDF

Exploration of Password Length on Wireless Network Security

- **How do you put the interface “wlan0” into monitor mode with Aircrack tools? (Full command)**
  - **airmon-ng start wlan0**



Discovering Networks

The first thing to do is looking out for a potential target. The aircrack-ng suite contains airodump-ng for this - but other programs like Kismet can be used too.

Prior to looking for networks, you must put your wireless card into what is called “monitor mode”. Monitor mode is a special mode that allows your computer to listen to every wireless packet. This monitor mode also allows you to optionally inject packets into a network. Injection will be covered later in this tutorial.

To put your wireless card into monitor mode using airmon-ng:

```
airmon-ng start wlan0
```

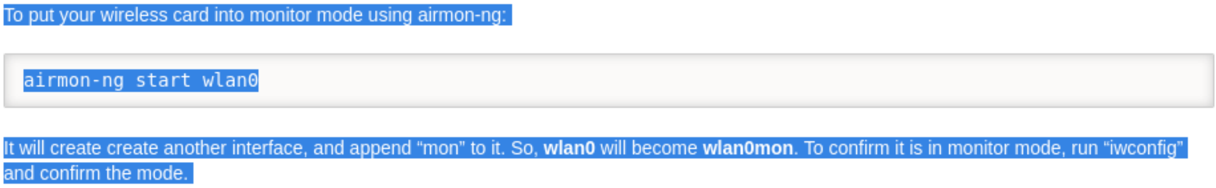
It will create create another interface, and append “mon” to it. So, **wlan0** will become **wlan0mon**. To confirm it is in monitor mode, run “iwconfig” and confirm the mode.

Then, start airodump-ng to look out for networks:

```
airodump-ng wlan0mon
```

If airodump-ng could connect to the WLAN device, you'll see a screen like this:

- **What is the new interface name likely to be after you enable monitor mode?**
  - **wlan0mon**

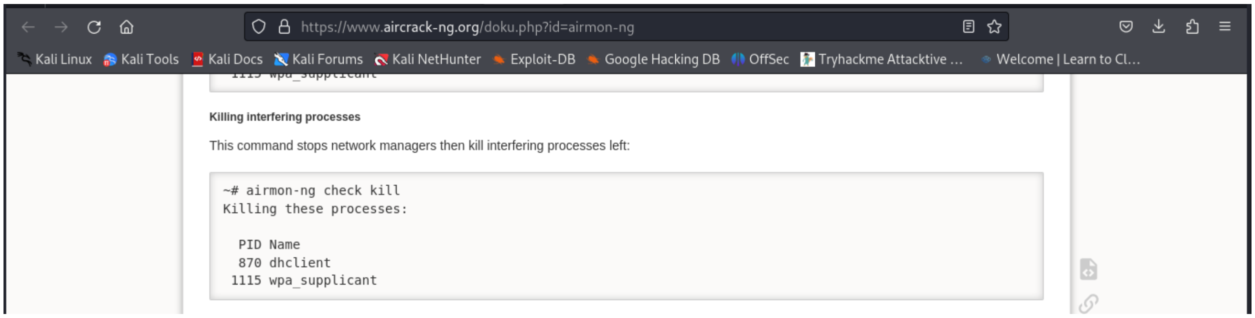


To put your wireless card into monitor mode using airmon-ng:

```
airmon-ng start wlan0
```

It will create create another interface, and append “mon” to it. So, **wlan0** will become **wlan0mon**. To confirm it is in monitor mode, run “iwconfig” and confirm the mode.

- **What do you do if other processes are currently trying to use that network adapter?**
  - **airmon-ng check kill**



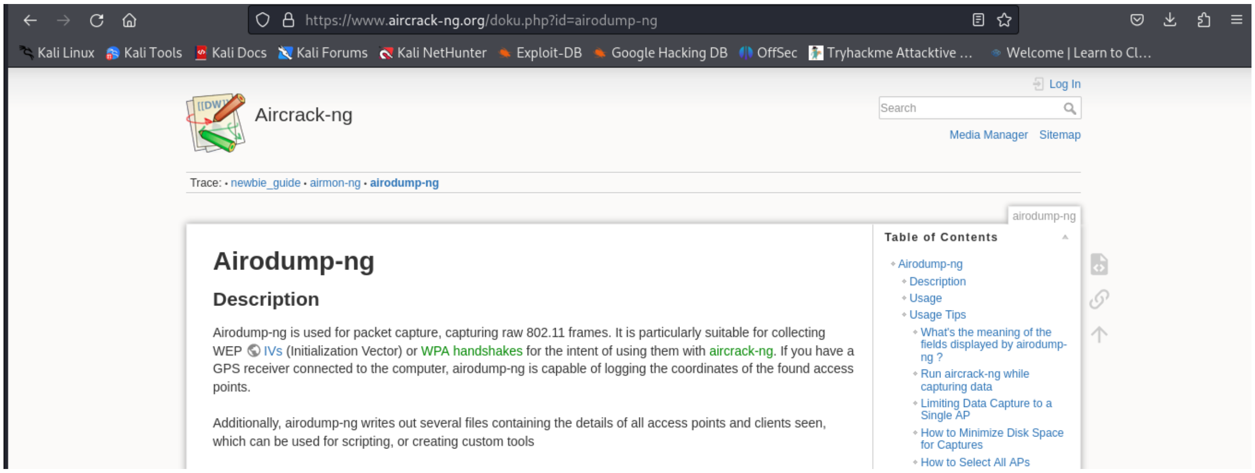
```
 1115 wpa_supplicant
```

Killing interfering processes

This command stops network managers then kill interfering processes left:

```
~# airmon-ng check kill
Killing these processes:

  PID Name
  870 dhclient
 1115 wpa_supplicant
```

- **What tool from the Aircrack-ng suite is used to create a capture?**
  - **airodump-ng**



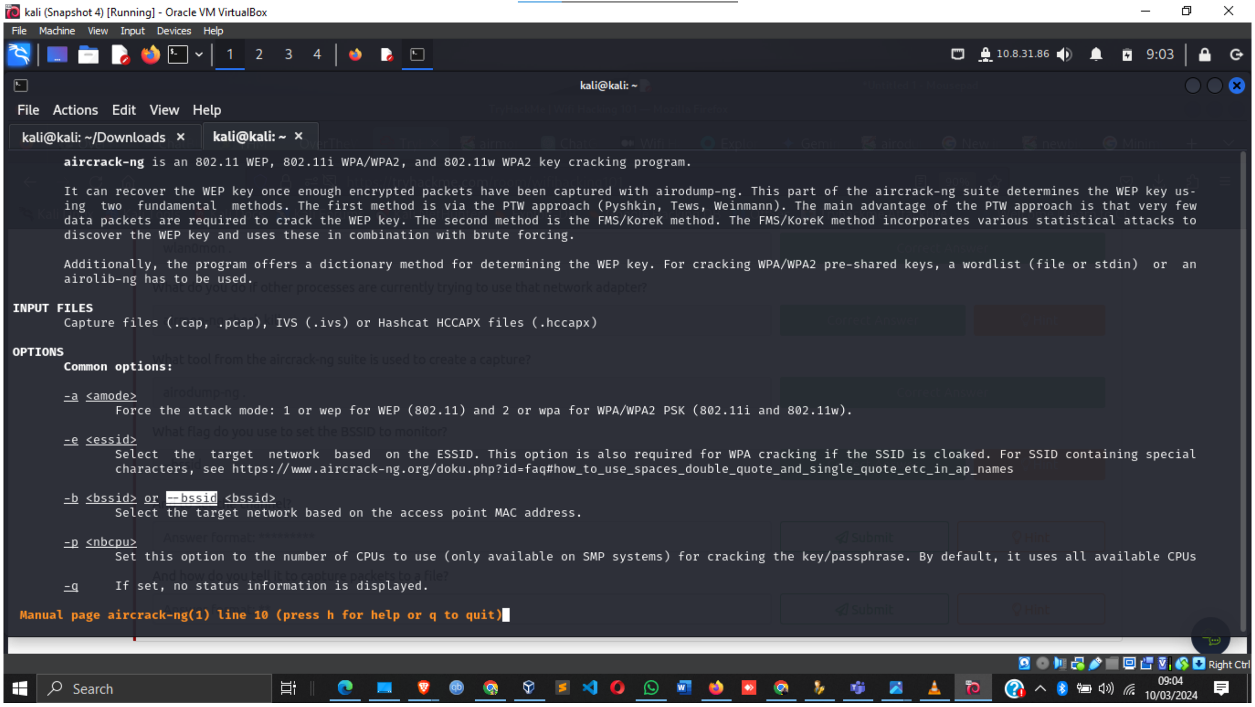
Airodump-ng

Description

Airodump-ng is used for packet capture, capturing raw 802.11 frames. It is particularly suitable for collecting WEP IVs (Initialization Vector) or WPA handshakes for the intent of using them with aircrack-ng. If you have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points.

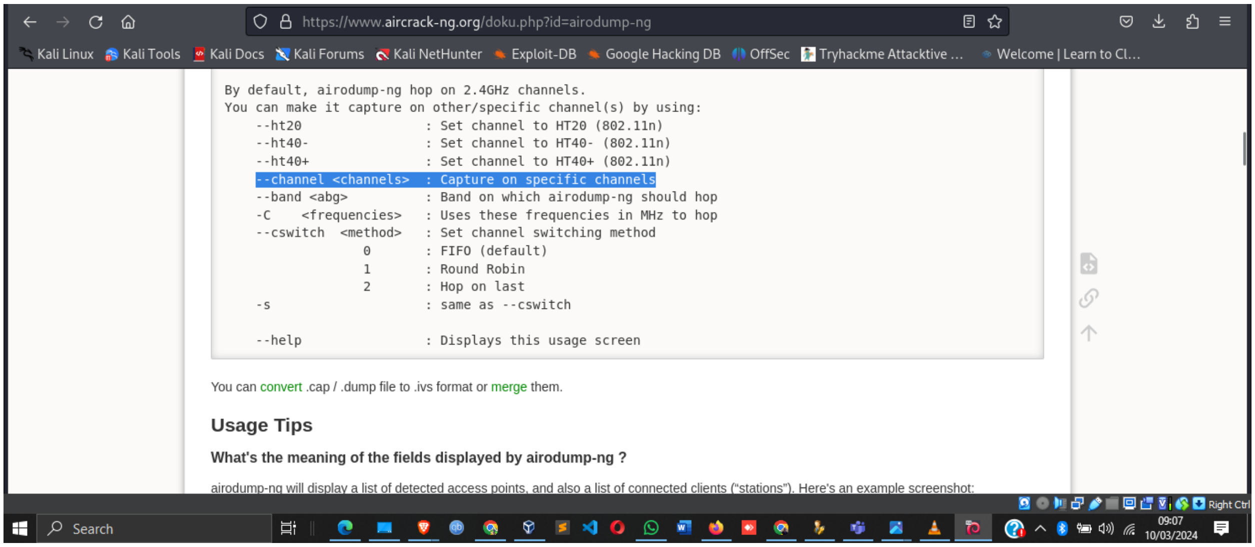
Additionally, airodump-ng writes out several files containing the details of all access points and clients seen, which can be used for scripting, or creating custom tools

- **What flag do you use to set the BSSID to monitor?**
  - **--bssid**


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.31.86
9:03
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads ×
kali@kali: ~ ×
Search
Right Ctrl
09:04
10/03/2024

```
       aircrack-ng is an 802.11 WEP, 802.11i WPA/WPA2, and 802.11w WPA2 key cracking program.

       It can recover the WEP key once enough encrypted packets have been captured with airodump-ng. This part of the aircrack-ng suite determines the WEP key us‐
       ing  two  fundamental  methods. The first method is via the PTW approach (Pyshkin, Tews, Weinmann). The main advantage of the PTW approach is that very few
       data packets are required to crack the WEP key. The second method is the FMS/KoreK method. The FMS/KoreK method incorporates various statistical attacks to
       discover the WEP key and uses these in combination with brute forcing.

       Additionally, the program offers a dictionary method for determining the WEP key. For cracking WPA/WPA2 pre-shared keys, a wordlist (file or stdin)  or  an
       airolib-ng has to be used.

INPUT FILES
       Capture files (.cap, .pcap), IVS (.ivs) or Hashcat HCCAPX files (.hccapx)

OPTIONS
       Common options:

       -a <amode>
              Force the attack mode: 1 or wep for WEP (802.11) and 2 or wpa for WPA/WPA2 PSK (802.11i and 802.11w).

       -e <essid>
              Select  the  target  network  based  on the ESSID. This option is also required for WPA cracking if the SSID is cloaked. For SSID containing special
              characters, see https://www.aircrack-ng.org/doku.php?id=faq#how_to_use_spaces_double_quote_and_single_quote_etc_in_ap_names

       -b <bssid> or --bssid <bssid>
              Select the target network based on the access point MAC address.

       -p <nbcpu>
              Set this option to the number of CPUs to use (only available on SMP systems) for cracking the key/passphrase. By default, it uses all available CPUs

       -q     If set, no status information is displayed.

 Manual page aircrack-ng(1) line 10 (press h for help or q to quit)
```

- **And to set the channel?**
  - **--channel**



```
By default, airodump-ng hop on 2.4GHz channels.
You can make it capture on other/specific channel(s) by using:
    --ht20                  : Set channel to HT20 (802.11n)
    --ht40-                 : Set channel to HT40- (802.11n)
    --ht40+                 : Set channel to HT40+ (802.11n)
    --channel <channels>    : Capture on specific channels
    --band <abg>            : Band on which airodump-ng should hop
    -C    <frequencies>     : Uses these frequencies in MHz to hop
    --cswitch  <method>     : Set channel switching method
                  0         : FIFO (default)
                  1         : Round Robin
                  2         : Hop on last
    -s                      : same as --cswitch

    --help                  : Displays this usage screen
```

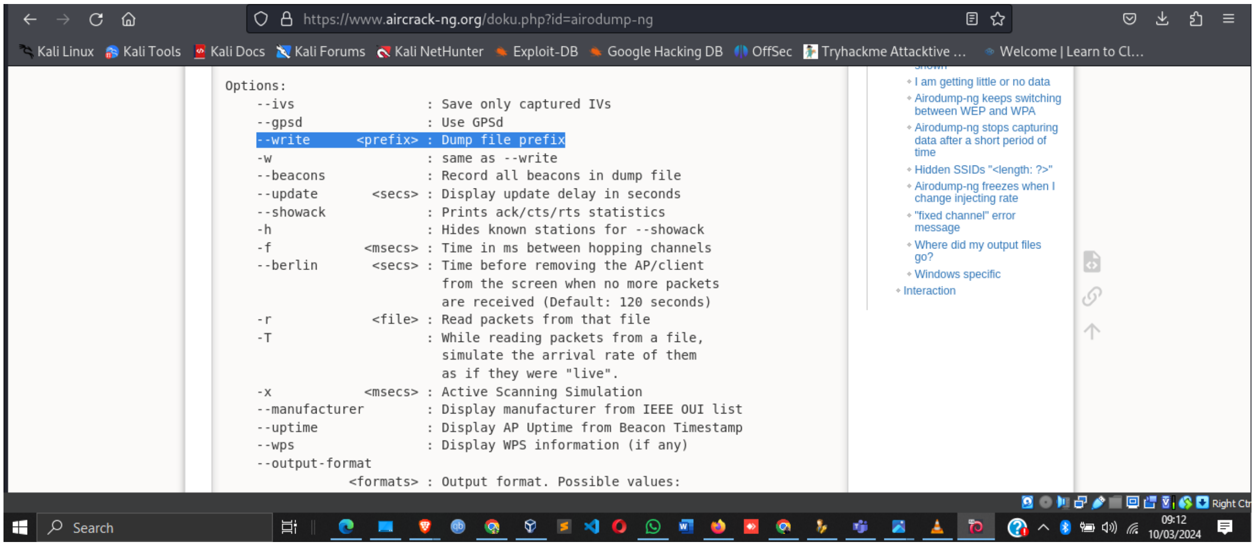
You can convert .cap / .dump file to .ivs format or merge them.

Usage Tips

What's the meaning of the fields displayed by airodump-ng ?

airodump-ng will display a list of detected access points, and also a list of connected clients ("stations"). Here's an example screenshot:

- **And how do you tell it to capture packets to a file?**
  - **-w**

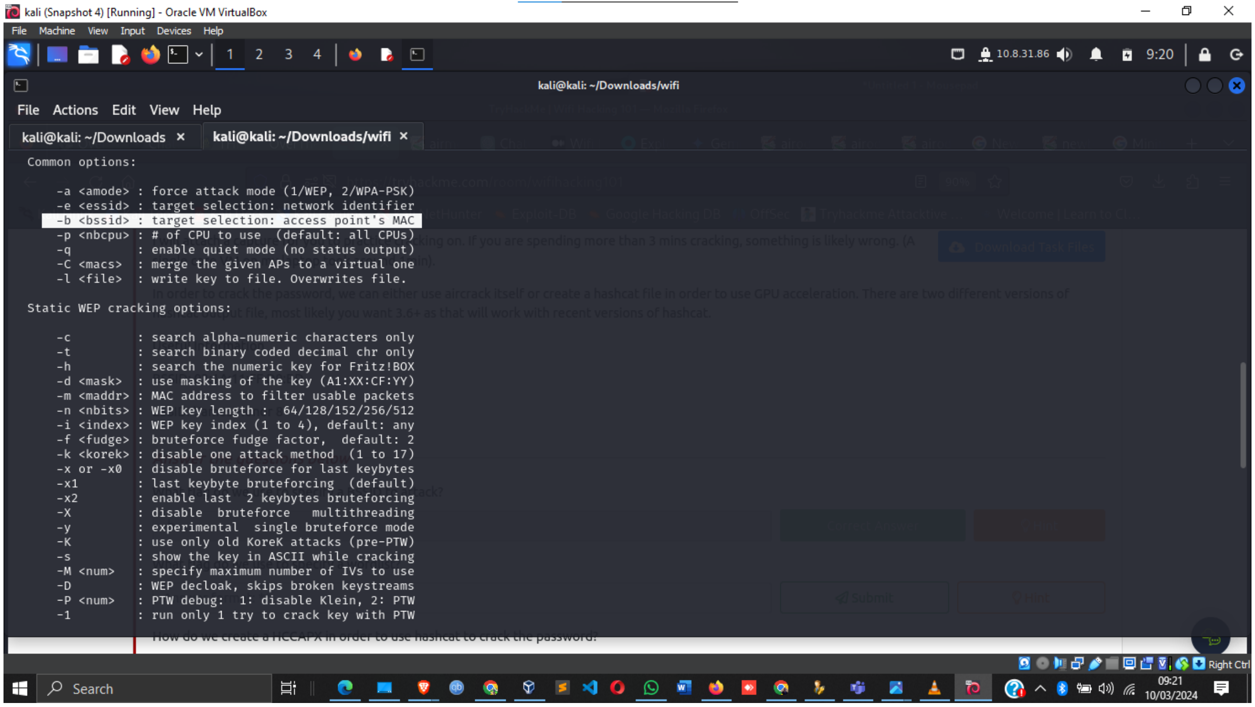

https://www.aircrack-ng.org/doku.php?id=airodump-ng
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Tryhackme Attacktive ...
Welcome | Learn to Cl...
I am getting little or no data
Airodump-ng keeps switching between WEP and WPA
Airodump-ng stops capturing data after a short period of time
Hidden SSIDs "<length: ?>"
Airodump-ng freezes when I change injecting rate
"fixed channel" error message
Where did my output files go?
Windows specific
Interaction
Search
09:12
10/03/2024

```
Options:
    --ivs                 : Save only captured IVs
    --gpsd                : Use GPSd
    --write      <prefix> : Dump file prefix
    -w                    : same as --write
    --beacons             : Record all beacons in dump file
    --update       <secs> : Display update delay in seconds
    --showack             : Prints ack/cts/rts statistics
    -h                    : Hides known stations for --showack
    -f            <msecs> : Time in ms between hopping channels
    --berlin       <secs> : Time before removing the AP/client
                            from the screen when no more packets
                            are received (Default: 120 seconds)
    -r             <file> : Read packets from that file
    -T                    : While reading packets from a file,
                            simulate the arrival rate of them
                            as if they were "live".
    -x            <msecs> : Active Scanning Simulation
    --manufacturer        : Display manufacturer from IEEE OUI list
    --uptime              : Display AP Uptime from Beacon Timestamp
    --wps                 : Display WPS information (if any)
    --output-format
                <formats> : Output format. Possible values:
```

Task 3: Aircrack-ng - Let's Get Cracking:

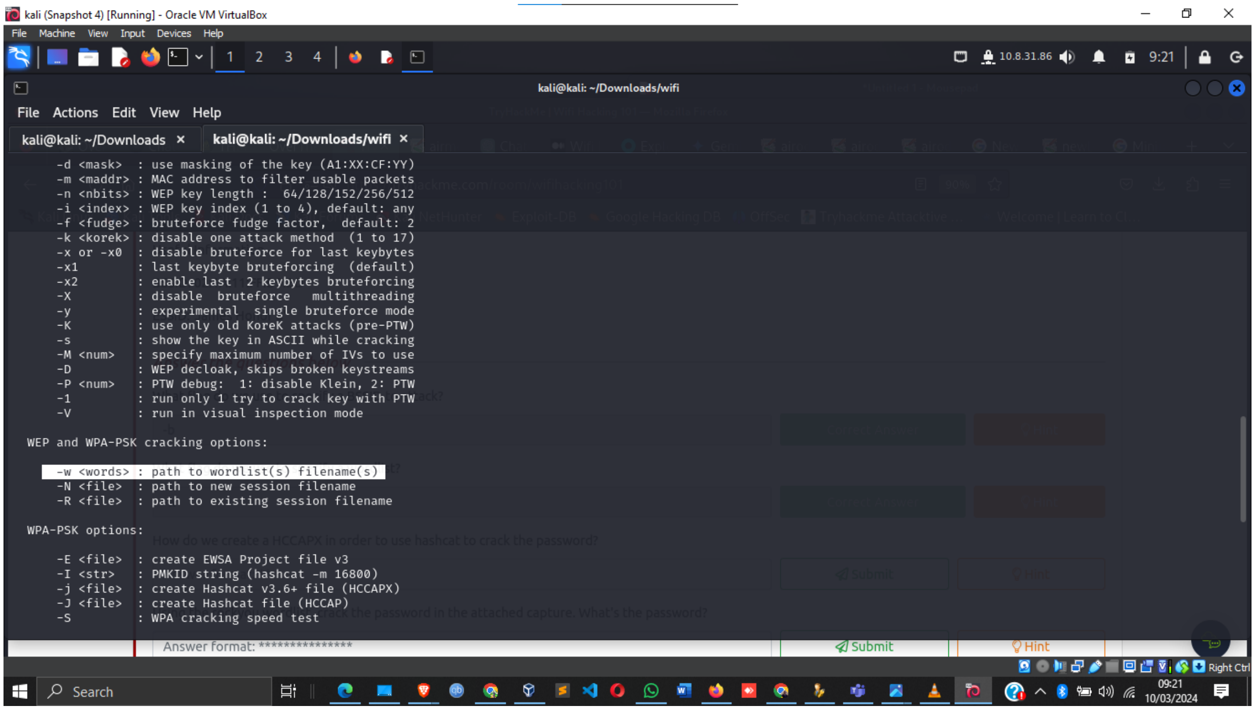
The final task demonstrates the use of Aircrack-ng for cracking Wi-Fi passwords. Users learn to specify the BSSID and wordlist, create an HCCAPX file for hashcat, and crack passwords using tools like rockyou. Emphasis is placed on leveraging GPU acceleration for faster password cracking, highlighting the importance of efficient hardware utilization in penetration testing.

- **What flag do we use to specify a BSSID to attack?**
  - **-b**



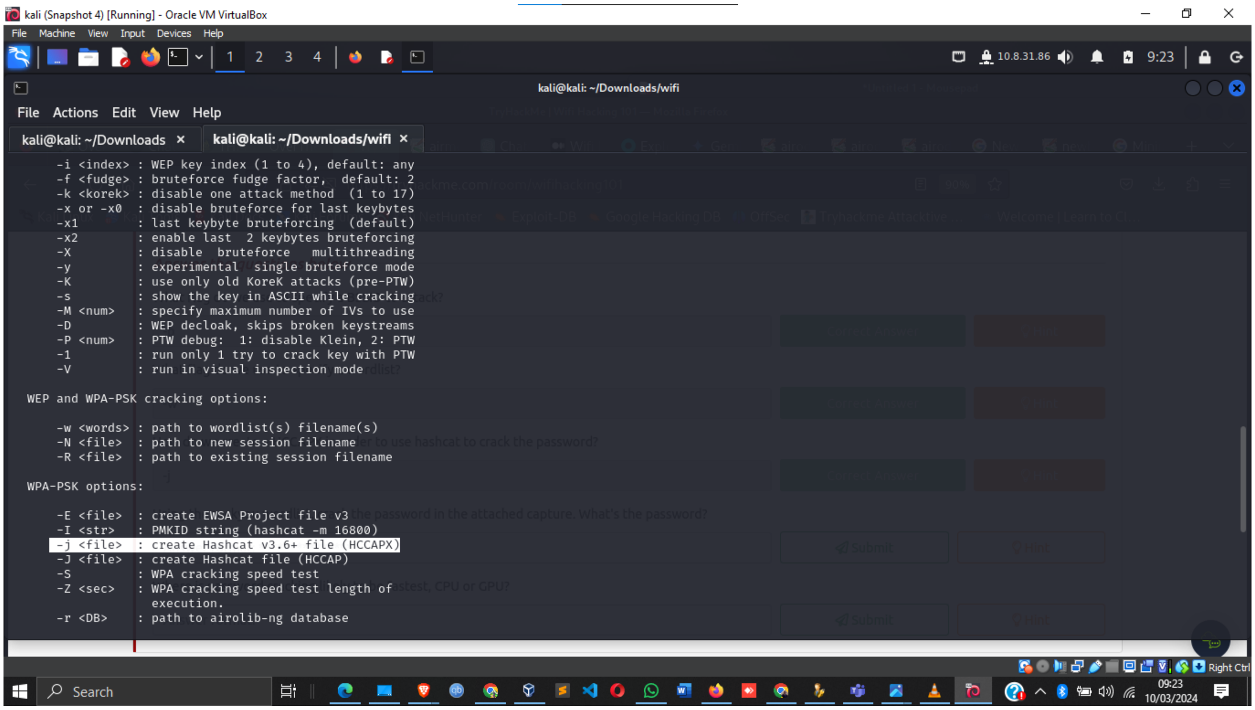
```
  Common options:

      -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 alpha-numeric 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
```

- **What flag do we use to specify a wordlist?**
  - **-w**


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
kali@kali: ~/Downloads/wifi
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~/Downloads/wifi
Answer format: ***************
Submit
Hint

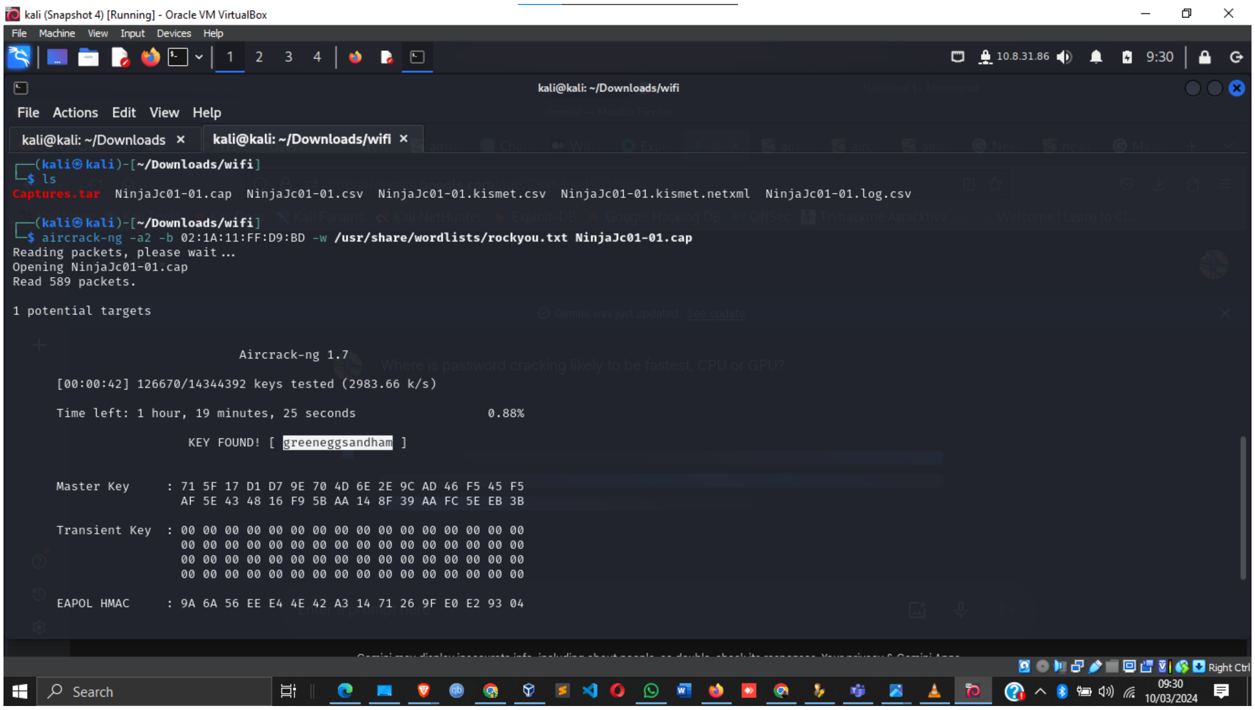
```
      -d <mask>   : use masking of the key (A1:XX:CF:YY)
      -m <maddr>  : MAC address to filter usable packets
      -n <nbits>  : WEP key length :  64/128/152/256/512
      -i <index>  : WEP key index (1 to 4), default: any
      -f <fudge>  : bruteforce fudge factor,  default: 2
      -k <korek>  : 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)
      -S          : WPA cracking speed test
```

- **How do we create an HCCAPX in order to use hashcat to crack the password?**
    - **-j**


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
kali@kali: ~/Downloads/wifi
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~/Downloads/wifi

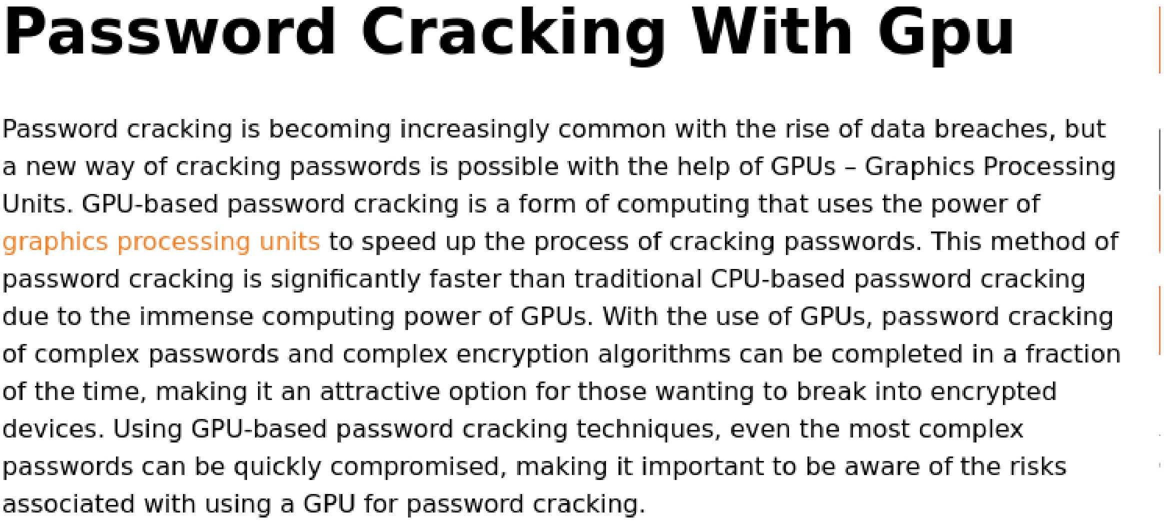
```
      -i <index>  : WEP key index (1 to 4), default: any
      -f <fudge>  : bruteforce fudge factor,  default: 2
      -k <korek>  : disable one attack method  (1 to 17)
      -x or -x0   : disable bruteforce for last keybytes
      -x1         : last keybyte bruteforcing  (default)
      -x2         : 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)
      -S          : WPA cracking speed test
      -Z <sec>    : WPA cracking speed test length of
                    execution.
      -r <DB>     : path to airolib-ng database
```

- **Using the rockyou wordlist, crack the password in the attached capture. What's the password?**
    - **greeneggsandham**


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/wifi
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~/Downloads/wifi
Search
09:30
10/03/2024

```
┌──(kali㉿kali)-[~/Downloads/wifi]
└─$ ls
Captures.tar  NinjaJc01-01.cap  NinjaJc01-01.csv  NinjaJc01-01.kismet.csv  NinjaJc01-01.kismet.netxml  NinjaJc01-01.log.csv

┌──(kali㉿kali)-[~/Downloads/wifi]
└─$ aircrack-ng -a2 -b 02:1A:11:FF:D9:BD -w /usr/share/wordlists/rockyou.txt NinjaJc01-01.cap
Reading packets, please wait ...
Opening NinjaJc01-01.cap
Read 589 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:00:42] 126670/14344392 keys tested (2983.66 k/s)

      Time left: 1 hour, 19 minutes, 25 seconds                  0.88%

                        KEY FOUND! [ greeneggsandham ]


      Master Key     : 71 5F 17 D1 D7 9E 70 4D 6E 2E 9C AD 46 F5 45 F5
                       AF 5E 43 48 16 F9 5B AA 14 8F 39 AA FC 5E EB 3B

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 9A 6A 56 EE E4 4E 42 A3 14 71 26 9F E0 E2 93 04
```

- **Where is password cracking likely to be fastest, CPU or GPU?**
    - GPU

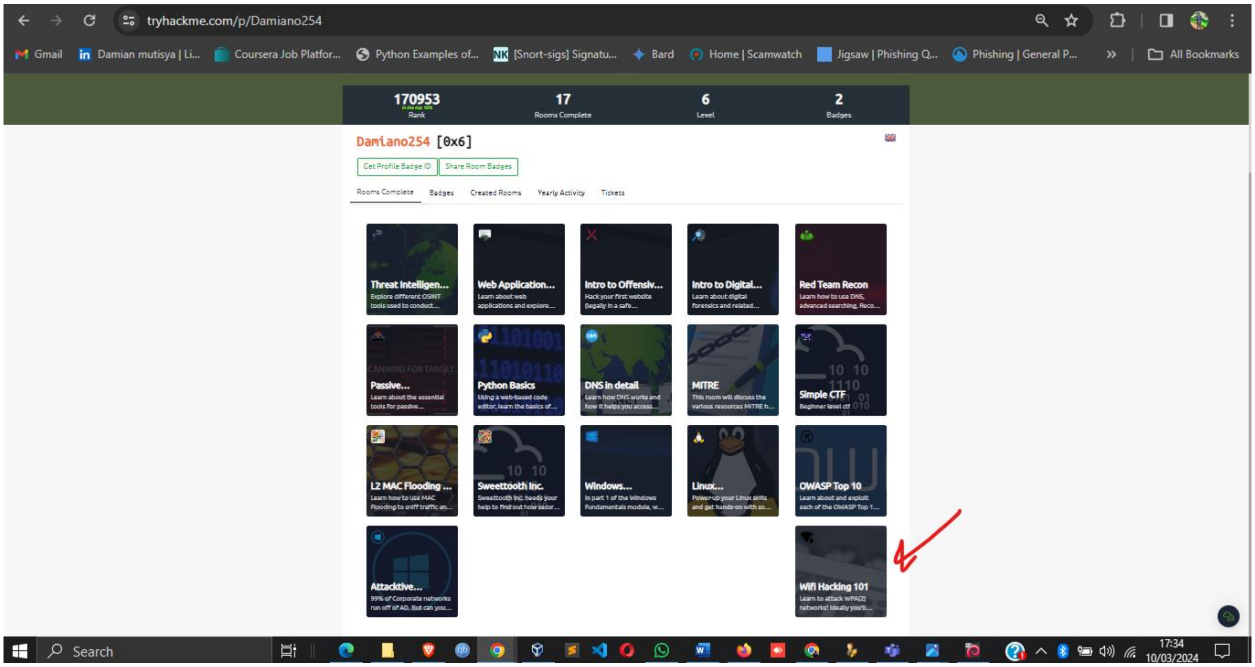


Password Cracking With Gpu

Password cracking is becoming increasingly common with the rise of data breaches, but a new way of cracking passwords is possible with the help of GPUs – Graphics Processing Units. GPU-based password cracking is a form of computing that uses the power of graphics processing units to speed up the process of cracking passwords. This method of password cracking is significantly faster than traditional CPU-based password cracking due to the immense computing power of GPUs. With the use of GPUs, password cracking of complex passwords and complex encryption algorithms can be completed in a fraction of the time, making it an attractive option for those wanting to break into encrypted devices. Using GPU-based password cracking techniques, even the most complex passwords can be quickly compromised, making it important to be aware of the risks associated with using a GPU for password cracking.

Conclusion:

The tasks completed in the "WiFi Hacking 101" room offer valuable insights into wireless attacks and Wi-Fi penetration testing. By combining theoretical knowledge with practical exercises, users gain a solid understanding of conducting security assessments on Wi-Fi networks. Emphasizing the significance of capturing handshakes, utilizing appropriate tools, and leveraging powerful wordlists, the room provides an effective foundation for individuals interested in exploring Wi-Fi security and penetration testing methodologies.



170953 in the top 10% Rank | 17 Rooms Complete | 6 Level | 2 Badges

Damiano254 [0x6]

Threat Intelligen... Explore different OSINT tools used to conduct...

Web Application... Learn about web applications and explore...

Intro to Offensiv... Hack your first website (legally in a safe...

Intro to Digital... Learn about digital forensics and related...

Red Team Recon Learn how to use DNS, advanced searching, Reco...

Passive... Learn about the essential tools for passive...

Python Basics Using a web-based code editor, learn the basics of...

DNS in detail Learn how DNS works and how it helps you access...

MITRE This room will discuss the various resources MITRE h...

Simple CTF Beginner level ctf

L2 MAC Flooding ... Learn how to use MAC Flooding to sniff traffic an...

Sweettooth Inc. Sweettooth Inc. needs your help to find out how secur...

Windows... In part 1 of the Windows Fundamentals module, w...

Linux... Power-up your Linux skills and get hands-on with so...

OWASP Top 10 Learn about and exploit each of the OWASP Top 1...

Attacktive... 99% of Corporate networks run off of AD. But can you...

Wifi Hacking 101 Learn to attack WPA(2) networks! Ideally you'll...