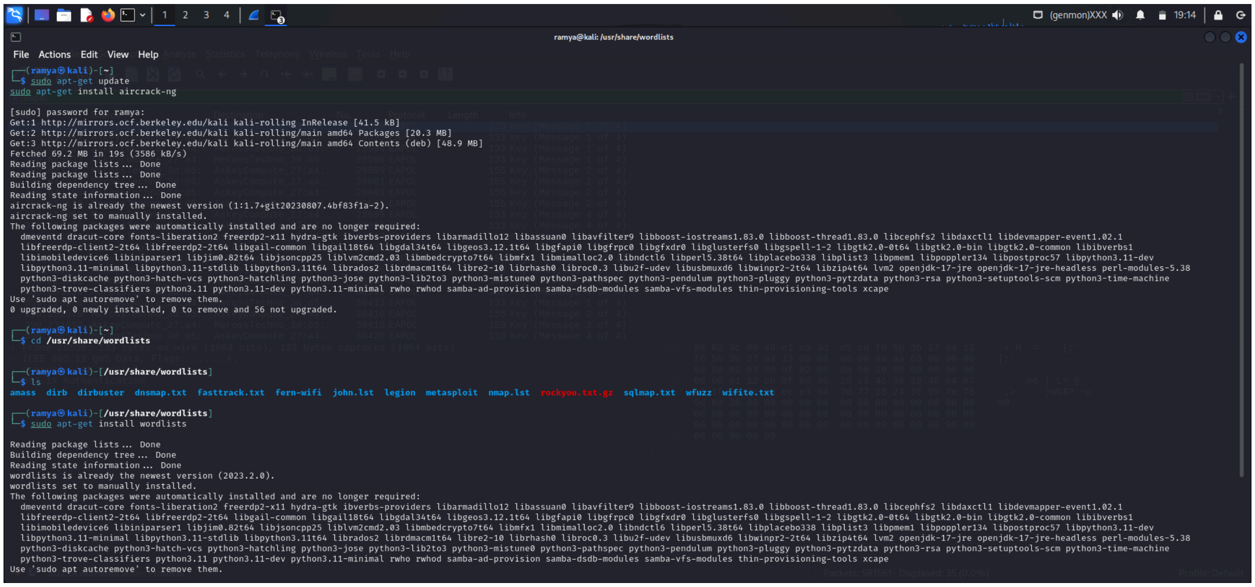
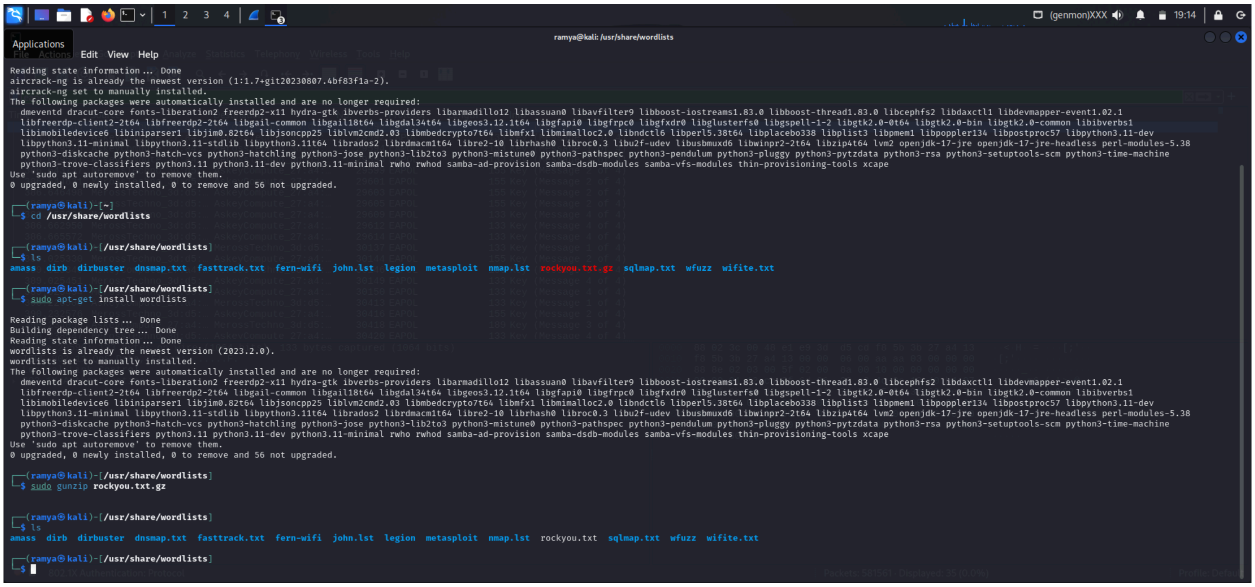
Cracking WPA2 Passwords with Aircrack-ng

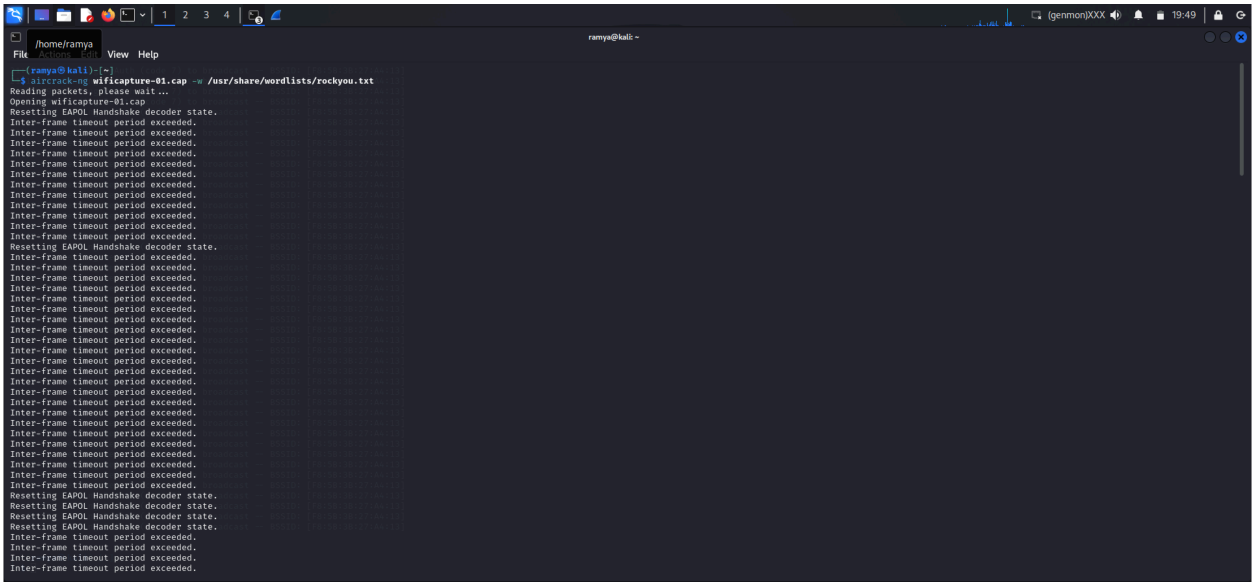
Use the WPA2 handshake captured in the previous lab to attempt cracking the password using a wordlist. This lab emphasizes ethical hacking principles. From this continuously i am doing



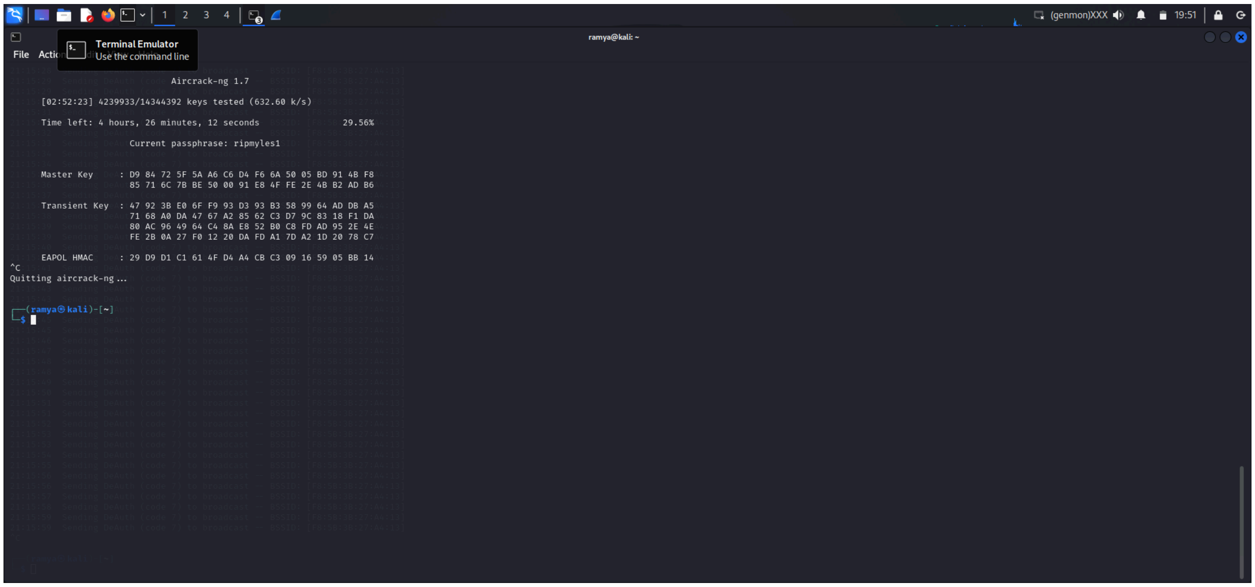
```
┌──(ramya㉿kali)-[~]
└─$ sudo apt-get update
sudo apt-get install aircrack-ng

[sudo] password for ramya:
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 Contents (deb) [48.9 MB]
Fetched 69.2 MB in 19s (3586 kB/s)
Reading package lists ... Done
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
aircrack-ng is already the newest version (1:1.7+git20230807.4bf83f1a-2).
aircrack-ng set to manually installed.
The following packages were automatically installed and are no longer required:
  dmeventd dracut-core fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libarmadillo12 libassuan0 libavfilter9 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libdaxctl1 libdevmapper-event1.02.1
  libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common libgail18t64 libgdal34t64 libgeos3.12.1t64 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin libgtk2.0-common libibverbs1
  libimobiledevice6 libiniparser1 libjim0.82t64 libjsoncpp25 liblvm2cmd2.03 libmbedcrypto7t64 libmfx1 libmimalloc2.0 libndctl6 libperl5.38t64 libplacebo338 libplist3 libpmem1 libpoppler134 libpostproc57 libpython3.11-dev
  libpython3.11-minimal libpython3.11-stdlib libpython3.11t64 librados2 librdmacm1t64 libre2-10 librhash0 libroc0.3 libu2f-udev libusbmuxd6 libwinpr2-2t64 libzip4t64 lvm2 openjdk-17-jre openjdk-17-jre-headless perl-modules-5.38
  python3-diskcache python3-hatch-vcs python3-hatchling python3-jose python3-lib2to3 python3-mistune0 python3-pathspec python3-pendulum python3-pluggy python3-pytzdata python3-rsa python3-setuptools-scm python3-time-machine
  python3-trove-classifiers python3.11 python3.11-dev python3.11-minimal rwho rwhod samba-ad-provision samba-dsdb-modules samba-vfs-modules thin-provisioning-tools xcape
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 56 not upgraded.

┌──(ramya㉿kali)-[~]
└─$ cd /usr/share/wordlists

┌──(ramya㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt

┌──(ramya㉿kali)-[/usr/share/wordlists]
└─$ sudo apt-get install wordlists

Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
wordlists is already the newest version (2023.2.0).
wordlists set to manually installed.
The following packages were automatically installed and are no longer required:
  dmeventd dracut-core fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libarmadillo12 libassuan0 libavfilter9 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libdaxctl1 libdevmapper-event1.02.1
  libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common libgail18t64 libgdal34t64 libgeos3.12.1t64 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin libgtk2.0-common libibverbs1
  libimobiledevice6 libiniparser1 libjim0.82t64 libjsoncpp25 liblvm2cmd2.03 libmbedcrypto7t64 libmfx1 libmimalloc2.0 libndctl6 libperl5.38t64 libplacebo338 libplist3 libpmem1 libpoppler134 libpostproc57 libpython3.11-dev
  libpython3.11-minimal libpython3.11-stdlib libpython3.11t64 librados2 librdmacm1t64 libre2-10 librhash0 libroc0.3 libu2f-udev libusbmuxd6 libwinpr2-2t64 libzip4t64 lvm2 openjdk-17-jre openjdk-17-jre-headless perl-modules-5.38
  python3-diskcache python3-hatch-vcs python3-hatchling python3-jose python3-lib2to3 python3-mistune0 python3-pathspec python3-pendulum python3-pluggy python3-pytzdata python3-rsa python3-setuptools-scm python3-time-machine
  python3-trove-classifiers python3.11 python3.11-dev python3.11-minimal rwho rwhod samba-ad-provision samba-dsdb-modules samba-vfs-modules thin-provisioning-tools xcape
Use 'sudo apt autoremove' to remove them.
```



```
Reading state information ... Done
aircrack-ng is already the newest version (1:1.7+git20230807.4bf83f1a-2).
aircrack-ng set to manually installed.
The following packages were automatically installed and are no longer required:
  dmeventd dracut-core fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libarmadillo12 libassuan0 libavfilter9 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libdaxctl1 libdevmapper-event1.02.1
  libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common libgail18t64 libgdal34t64 libgeos3.12.1t64 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin libgtk2.0-common libibverbs1
  libimobiledevice6 libiniparser1 libjim0.82t64 libjsoncpp25 liblvm2cmd2.03 libmbedcrypto7t64 libmfx1 libmimalloc2.0 libndctl6 libperl5.38t64 libplacebo338 libplist3 libpmem1 libpoppler134 libpostproc57 libpython3.11-dev
  libpython3.11-minimal libpython3.11-stdlib libpython3.11t64 librados2 librdmacm1t64 libre2-10 librhash0 libroc0.3 libu2f-udev libusbmuxd6 libwinpr2-2t64 libzip4t64 lvm2 openjdk-17-jre openjdk-17-jre-headless perl-modules-5.38
  python3-diskcache python3-hatch-vcs python3-hatchling python3-jose python3-lib2to3 python3-mistune0 python3-pathspec python3-pendulum python3-pluggy python3-pytzdata python3-rsa python3-setuptools-scm python3-time-machine
  python3-trove-classifiers python3.11 python3.11-dev python3.11-minimal rwho rwhod samba-ad-provision samba-dsdb-modules samba-vfs-modules thin-provisioning-tools xcape
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 56 not upgraded.

┌──(ramya㉿kali)-[~]
└─$ cd /usr/share/wordlists

┌──(ramya㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt

┌──(ramya㉿kali)-[/usr/share/wordlists]
└─$ sudo apt-get install wordlists

Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
wordlists is already the newest version (2023.2.0).
wordlists set to manually installed.
The following packages were automatically installed and are no longer required:
  dmeventd dracut-core fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libarmadillo12 libassuan0 libavfilter9 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libdaxctl1 libdevmapper-event1.02.1
  libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common libgail18t64 libgdal34t64 libgeos3.12.1t64 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin libgtk2.0-common libibverbs1
  libimobiledevice6 libiniparser1 libjim0.82t64 libjsoncpp25 liblvm2cmd2.03 libmbedcrypto7t64 libmfx1 libmimalloc2.0 libndctl6 libperl5.38t64 libplacebo338 libplist3 libpmem1 libpoppler134 libpostproc57 libpython3.11-dev
  libpython3.11-minimal libpython3.11-stdlib libpython3.11t64 librados2 librdmacm1t64 libre2-10 librhash0 libroc0.3 libu2f-udev libusbmuxd6 libwinpr2-2t64 libzip4t64 lvm2 openjdk-17-jre openjdk-17-jre-headless perl-modules-5.38
  python3-diskcache python3-hatch-vcs python3-hatchling python3-jose python3-lib2to3 python3-mistune0 python3-pathspec python3-pendulum python3-pluggy python3-pytzdata python3-rsa python3-setuptools-scm python3-time-machine
  python3-trove-classifiers python3.11 python3.11-dev python3.11-minimal rwho rwhod samba-ad-provision samba-dsdb-modules samba-vfs-modules thin-provisioning-tools xcape
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 56 not upgraded.

┌──(ramya㉿kali)-[/usr/share/wordlists]
└─$ sudo gunzip rockyou.txt.gz


┌──(ramya㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt

┌──(ramya㉿kali)-[/usr/share/wordlists]
└─$ 
```



```
┌──(ramya㉿kali)-[~]
└─$ aircrack-ng wificapture-01.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait ...
Opening wificapture-01.cap
Resetting EAPOL Handshake decoder state.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
```



```
                              Aircrack-ng 1.7

      [02:52:23] 4239933/14344392 keys tested (632.60 k/s)

      Time left: 4 hours, 26 minutes, 12 seconds                 29.56%

                       Current passphrase: ripmyles1


      Master Key     : D9 84 72 5F 5A A6 C6 D4 F6 6A 50 05 BD 91 4B F8
                       85 71 6C 7B BE 50 00 91 E8 4F FE 2E 4B B2 AD B6

      Transient Key  : 47 92 3B E0 6F F9 93 D3 93 B3 58 99 64 AD DB A5
                       71 68 A0 DA 47 67 A2 85 62 C3 D7 9C 83 18 F1 DA
                       80 AC 96 49 64 C4 8A E8 52 B0 C8 FD AD 95 2E 4E
                       FE 2B 0A 27 F0 12 20 DA FD A1 7D A2 1D 20 78 C7

      EAPOL HMAC     : 29 D9 D1 C1 61 4F D4 A4 CB C3 09 16 59 05 BB 14
^C
Quitting aircrack-ng ...


┌──(ramya㉿kali)-[~]
└─$ 
```

The process is completed without finding a matching password in the wordlist. Possible reasons may be for the failure:

1. The **wordlist** used (`rockyou.txt`) did not contain the password.
2. The password may be **too complex or uncommon** for the wordlist to include.
3. A **strong password** with sufficient length and complexity increases the difficulty of brute force attempts.

Report:

Wi-Fi networks are protected by the security standard WPA2. The WPA2 password's strength is essential for protecting the network from intrusions, particularly brute force assaults, in which the attacker attempts a large number of passwords before figuring out the one that works.

The Significance of Strong Passwords

A secure password:

Hard to Guess: Attackers find it challenging to break using standard methods.
Complexity and Length: It is more difficult to crack longer passwords that contain a combination of letters, numbers, and symbols.
Defense Against Assaults: A strong password makes it difficult for hackers to break the WPA2 handshake if they manage to record it (during the connection procedure).

The Protection of Robust Passwords against Brute Force Attacks

In a brute force approach, every conceivable combination is tried until the one that works is discovered. A strong password can assist in the following ways:

More possibilities: Longer, more complicated passwords are more difficult to break since they contain a greater number of potential possibilities.
Takes More Time: Even with sophisticated computers, it takes a lot longer for attackers to figure out a strong password.
Stops Simple Cracking: Using pre-made lists of popular passwords, weak passwords may be swiftly broken. It is far more difficult to guess a strong password.

In conclusion

To keep hackers out of your Wi-Fi network, you must have a strong WPA2 password. Stronger passwords are more difficult for hackers to crack, increasing the security of your network.