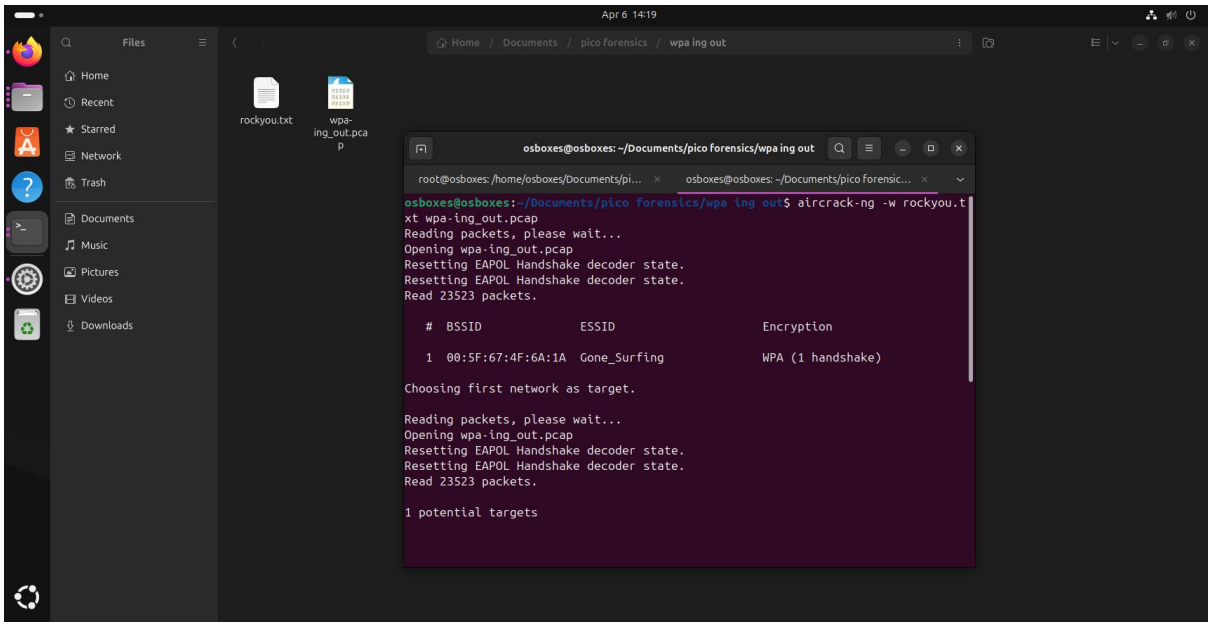
I thought that my password was super-secret, but it turns out that passwords passed over the AIR can be CRACKED, especially if I used the same wireless network password as one in the rockyou.txt credential dump. Use this 'pcap file' and the rockyou wordlist. The flag should be entered in the picoCTF{XXXXXX} format.



aircrack-ng -w rockyou.txt wpa-ing_out.pcap

Reading packets, please wait...

Opening wpa-ing_out.pcap

Resetting EAPOL Handshake decoder state.

Resetting EAPOL Handshake decoder state.

Read 23523 packets.

BSSID ESSID Encryption

1 00:5F:67:4F:6A:1A Gone_Surfing WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...

Opening wpa-ing_out.pcap

Resetting EAPOL Handshake decoder state.

Resetting EAPOL Handshake decoder state.

Read 23523 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:01] 1363/10303727 keys tested (2289.18 k/s)

Time left: 1 hour, 15 minutes, 0 seconds 0.01%

KEY FOUND! [mickeymouse]

Master Key : 61 64 B9 5E FC 6F 41 70 70 81 F6 40 80 9F AF B1

4A 9E C5 C4 E1 67 B8 AB 58 E3 E8 8E E6 66 EB 11

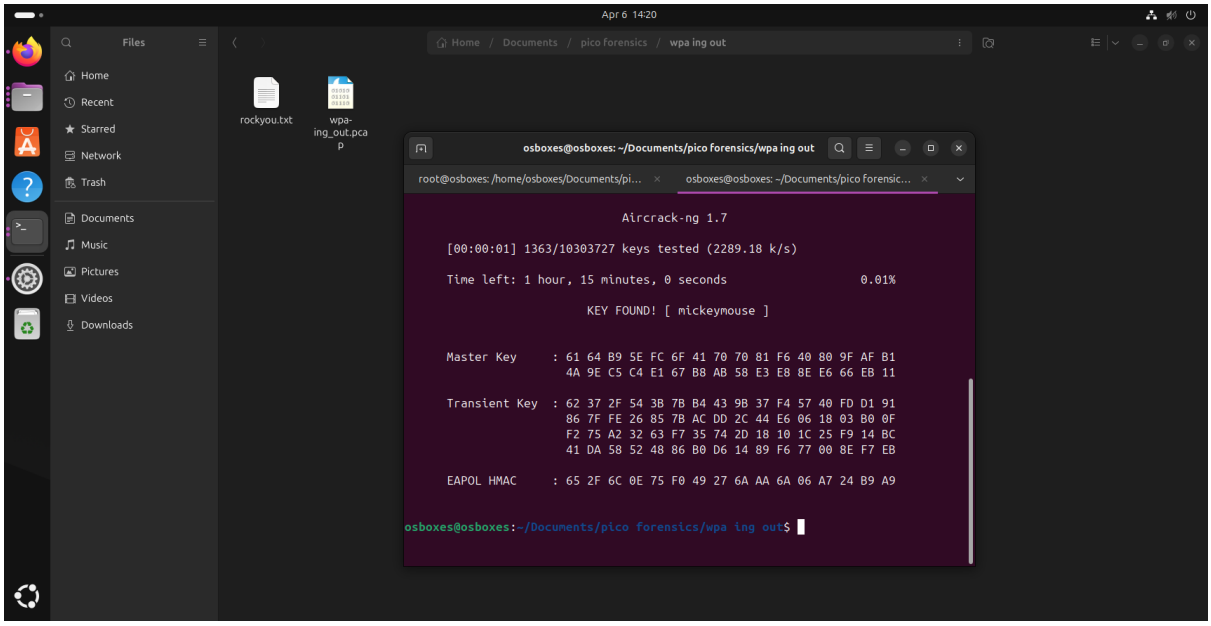
Transient Key : 62 37 2F 54 3B 7B B4 43 9B 37 F4 57 40 FD D1 91

86 7F FE 26 85 7B AC DD 2C 44 E6 06 18 03 B0 0F

F2 75 A2 32 63 F7 35 74 2D 18 10 1C 25 F9 14 BC

41 DA 58 52 48 86 B0 D6 14 89 F6 77 00 8E F7 EB

EAPOL HMAC : 65 2F 6C 0E 75 F0 49 27 6A AA 6A 06 A7 24 B9 A9



The answer is picoCTF wrapped around the key discovered