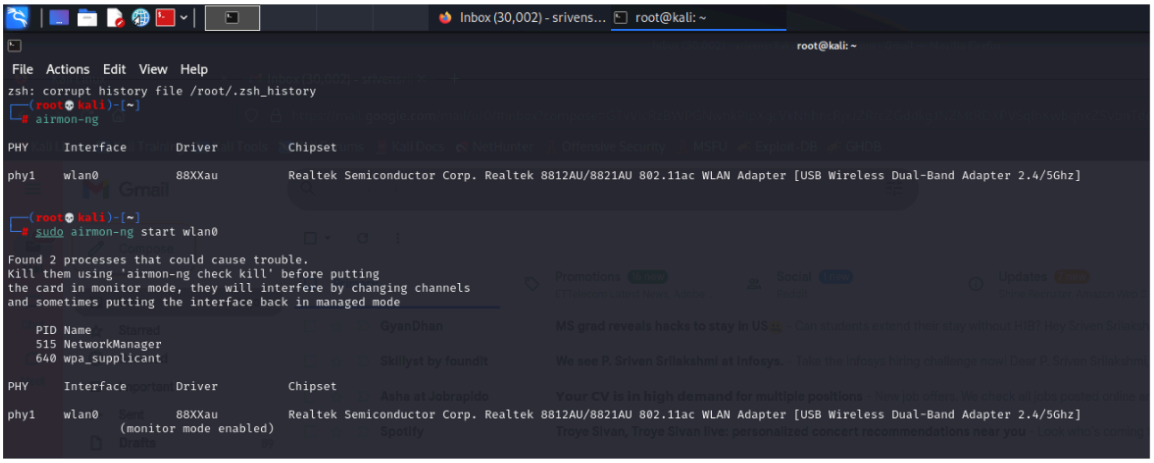
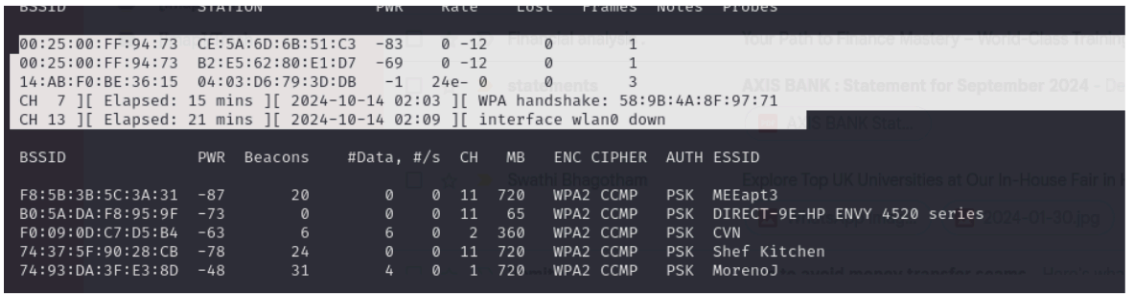
Use the WPA2 handshake captured in the previous lab to attempt cracking the password using a wordlist. This lab emphasizes ethical hacking principles.

WPA2 Handshake Capture and Analysis





Run the following command in your terminal:

aircrack-ng -w /home/kali/wordlist.txt -b 58:9B:4A:8F:97:71 handshake.cap

Interpret Results

- If Aircrack-ng finds the password, it will display it in the terminal.
- Record the time it took and the number of attempts if this information is available.

Report

Importance of Password Strength in Wireless Security

Passwords form the centerpiece in ensuring safety against unauthorized network access in WPA2 wireless security. A good password will reduce the possibility of brute force attacks whereby the length of time it would take for the attacker to guess is extended greatly. A good WPA2 password can be a mix of upper and lowercase letters, numbers, and special characters, much less likely to match any regular wordlist.

Conclusion

This exercise has demonstrated how easy it is to compromise a weak password using simple tools like Aircrack-ng and freely downloadable wordlists. Ensuring that passwords are strong and do not include common words or phases greatly improves the security of the network, discouraging attacks meant to compromise wireless networks through brute-force attacks.