Proof-of-Concept Report:-

Tool Name:

aireplay-ng and aircrack-ng

Description:

aircrack-ng is a complete suite of tools for assessing Wi-Fi network security.
aireplay-ng is a component of this suite, specifically used to inject packets and perform replay attacks to capture necessary data (like WPA/WPA2 handshakes) for cracking wireless keys.

What Is This Tool About?

These tools are primarily used for **wireless penetration testing**, focusing on capturing, analyzing, and cracking Wi-Fi security protocols.

- aireplay-ng is used to **force deauthentication** or replay ARP packets.
- aircrack-ng is used to **crack WEP/WPA-PSK keys** using captured handshake data.

Key Characteristics / Features:

1. Packet injection and replay
2. Deauthentication attack support
3. WPA/WPA2 handshake capture
4. Dictionary and brute-force key cracking
5. Real-time capture and cracking status
6. Works on 802.11 a/b/g/n/ac networks
7. Supports WEP, WPA, WPA2 protocols
8. Runs on Linux, Windows, macOS, OpenBSD
9. Integrates with airmon-ng and airodump-ng
10. Channel hopping and filter options
11. Compatible with many wireless chipsets

12. Fast cracking with CPU/GPU optimizations
13. Can detect rogue APs or evil twins
14. Fully CLI-based with automation scripts
15. Used in Kali Linux and other pentesting distros

Types / Modules Available:

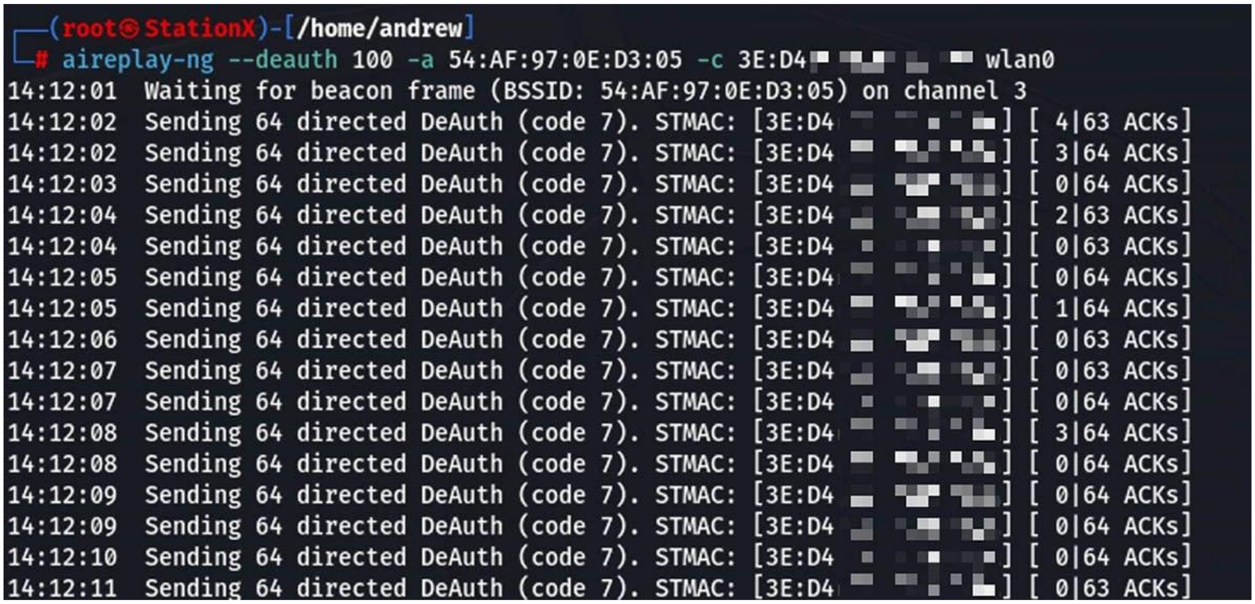
- aireplay-ng: Packet injection tool
- aircrack-ng: Key cracking engine
- airodump-ng: Packet capture tool
- airmon-ng: Monitor mode setup
- airdecap-ng: Encrypted packet decoder
- packetforge-ng: Packet crafting module

How Will This Tool Help?

- Captures encrypted traffic and handshakes
- Performs deauthentication to speed up key capture
- Cracks wireless encryption to test network robustness
- Detects and exploits weak Wi-Fi implementations
- Supports security audits of corporate and public Wi-Fi

Proof of Concept (PoC) Images:

Aireplay-ng forcing deauthentication



```
┌──(root㉿StationX)-[/home/andrew]
└─# aireplay-ng --deauth 100 -a 54:AF:97:0E:D3:05 -c 3E:D4[redacted] wlan0
14:12:01  Waiting for beacon frame (BSSID: 54:AF:97:0E:D3:05) on channel 3
14:12:02  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 4|63 ACKs]
14:12:02  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 3|64 ACKs]
14:12:03  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|64 ACKs]
14:12:04  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 2|63 ACKs]
14:12:04  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|63 ACKs]
14:12:05  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|64 ACKs]
14:12:05  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 1|64 ACKs]
14:12:06  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|63 ACKs]
14:12:07  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|63 ACKs]
14:12:07  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|64 ACKs]
14:12:08  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 3|64 ACKs]
14:12:08  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|64 ACKs]
14:12:09  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|64 ACKs]
14:12:09  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|64 ACKs]
14:12:10  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|64 ACKs]
14:12:11  Sending 64 directed DeAuth (code 7). STMAC: [3E:D4[redacted]] [ 0|63 ACKs]
```

15-Liner Summary:

1. Used for Wi-Fi security testing
2. Captures WPA/WEP handshakes
3. Supports multiple attack modes
4. CLI-based, ideal for scripting
5. Cracks keys using wordlists
6. Real-time status updates
7. Works with monitor mode interfaces
8. Portable across platforms
9. Supports replay and deauth attacks
10. Widely used in security assessments
11. Compatible with most Wi-Fi chipsets
12. Cracks WEP in minutes
13. Performs dictionary or brute-force

14. Supports fake authentication attacks

15. Open-source and maintained

Time to Use / Best Case Scenarios:

- During red team wireless engagements
- To test password strength on WPA/WPA2
- When auditing public Wi-Fi deployments
- To confirm correct segmentation in networks
- During compliance audits of wireless networks

When to Use During Investigation:

- Analyzing rogue access points
- Testing if WPA handshake leaks exist
- During pen-testing engagements
- Forensics of wireless breach attempts
- Post-exploitation Wi-Fi lateral movement

Best Person to Use This Tool & Required Skills:

Best Users:

- Penetration Testers
- Network Security Engineers
- Wireless Forensics Analysts

Required Skills:

- Linux CLI proficiency
- Understanding of Wi-Fi protocols (802.11)
- Knowledge of encryption types (WEP/WPA/WPA2)

- Ability to interpret packet captures
- Familiarity with aircrack-ng suite and drivers

Flaws / Suggestions to Improve:

- Requires compatible wireless chipsets
- GUI version would benefit non-technical users
- WPA3 support still limited
- High battery usage on laptops
- Needs better error handling on unsupported drivers

Good About the Tool:

- Very powerful for Wi-Fi security auditing
- Fast, scriptable, and modular
- Free and open-source
- Popular in security certifications (OSCP, CEH)
- Continuously updated by the community
- Excellent documentation and community support