Here is a **professionally formatted, sentence-by-sentence breakdown** of your document titled **“203. Cracking Wireless Networks Notes”** in the form of **study notes**. The formatting is intentionally designed for **clear, structured pasting into Microsoft Word** — no excessive spacing, with numbered topic headers, bullet-based explanations, and comprehensive coverage of every key point.

**CompTIA A+ 1102 — Cracking Wireless Networks (Section 203)**

**Professional Study Notes**

**1. Overview of the Lesson**

* The lesson demonstrates how to **crack a WPA2 pre-shared key** using a **dictionary attack**.
* Tools used: **Aircrack-ng suite** including airmon-ng, airodump-ng, aireplay-ng, and aircrack-ng.
* The goal is to simulate an attacker’s process of capturing a **handshake** and using a **wordlist** to crack the key.

**2. Step-by-Step Attack Process Using Aircrack-ng Suite**

**A computer screen with icons and symbols

AI-generated content may be incorrect.**

**2.1 Enable Monitor Mode**

* **Tool**: airmon-ng
* **Purpose**: Sets the wireless adapter into **Monitor Mode**, allowing it to capture all wireless traffic — even if not directed at the device.

**2.2 Locate a Target Network**

* **Tool**: airodump-ng
* **Purpose**: Scans for **WPA/WPA2-enabled networks** and identifies nearby **clients and access points**.
* Captures traffic and writes to a **PCAP file** for offline analysis.

**2.3 Capture Network Traffic**

* **Command structure**:  
  airodump-ng wlan0mon -c [channel] --bssid [MAC] --write [filename]
* **Goal**: Capture handshake between client and access point when they reconnect.

**2.4 Force Client Disconnection (Deauthentication Attack)**

* **Tool**: aireplay-ng
* Sends spoofed **deauth packets** to forcibly disconnect a client from the AP.
* This triggers a reconnection attempt, during which the **four-way handshake** is broadcast and captured.
* **Command structure**:  
  aireplay-ng --deauth 0 -a [AP\_MAC] -c [Client\_MAC] wlan0mon

**2.5 Crack Captured Handshake**

* **Tool**: aircrack-ng
* Uses the **captured PCAP file** and a **wordlist** to perform a **dictionary attack**.
* **Command structure**:  
  aircrack-ng [capturefile.cap] -w [path/to/wordlist.txt]
* Wordlist used in this demo: **rockyou.txt** (over 14 million entries).

**3. Password Cracking Details**

* Demonstrated password: Dr@g0nBr3A+h
  + 12 characters
  + Contains uppercase, lowercase, numbers, and special characters
  + Considered **strong** but **appears in the wordlist**
* Despite its strength, because it's in **rockyou.txt**, the password was cracked in **a few seconds**, at ~830 keys/sec.
* The password was located at ~15,000 entries into the list (less than 0.5% of the list was searched).
* If the password had been later in the file, cracking could have taken **3–4 hours**, or not succeeded at all if it wasn’t in the list.

**4. Key Takeaways and Security Implications**

* **Realism of Attacks**: This attack simulates what a malicious actor could perform using **publicly available tools and lists**.
* **Exam Relevance**:
  + **A+ 1102 exam does not require memorizing commands or attack steps.**
  + Focus is on **understanding vulnerabilities and mitigation strategies**, not execution.
* **Tool Breakdown**:
  + airmon-ng: Enables monitor mode
  + airodump-ng: Scans for access points and clients, writes capture file
  + aireplay-ng: Conducts deauth attacks to capture handshake
  + aircrack-ng: Cracks handshake using dictionary attack
* **Security Recommendation**:
  + Use **strong, unique passwords** that do **not appear in common wordlists**.
  + Length and complexity matter — but **uniqueness** is equally critical.
  + A 14-million-entry wordlist can crack many passwords in seconds if they're common or reused.

**5. Final Notes**

* **Wordlist effectiveness** depends on:
  + Where the password is located in the list
  + Whether it appears at all
* **Strong network security** begins with:
  + Good password hygiene
  + Disabling unnecessary protocols
  + Monitoring for suspicious activity

Let me know if you'd like a **Word or PDF export**, a **flashcard quiz** on this topic, or if you want these notes styled as a **training handout**.