HackHunter Pursuit case study:

Rogue access point audit with an ASX 50 company

An ASX 50 company wanted to see how the HackHunter Pursuit portable WiFi tracker rated against its current method of detecting and locating unauthorised WiFi.

Their Existing Method

- A laptop running Kali Linux and Aircrack-ng with an Alfa antenna; and
- A Netscout WiFi Analyser.

The Trial

Our CTO Mike Thompson walked the floors of 3 buildings over 3 days with the Pursuit tracker, side-by-side with their two-man team using the laptop and WiFi analyser.

Their Method

On each floor the team member operating the laptop would:

- From one corner of the floor, see which unauthorised WiFi access points (APs) were picked up by the laptopRepeat for the other 3 corners of the floor
- Select 4 – 5 APs to locate and investigate

- Cut and paste these APs to a spreadsheet (with one hand while holding the laptop with the other)
- Tell the other team member with the WiFi analyser which APs to find
- When the APs were found, investigate them and record the results in the spreadsheet.

On each floor the team member operating the WiFi analyser would:

- Carry the heavy WiFi analyser on a lanyard around his neck
- Change batteries every 90 minutes from the huge bag of heavy batteries he lugged around
- Attempt to track down the selected APs by following the signal strength in a spiral pattern, narrowing down the location of the AP through trial and error.

The HackHunter Method

On each floor Mike would:

- Point the 250g hand-held Pursuit tracker to the 4 cardinal points to find the direction of the AP
- Walk towards it
- Continue the process until the AP was located, to within a few centimetres.

So what happened?

The HackHunter Pursuit tracker was 300% more effective, finding the APs first by a wide margin, except in the few cases when the WiFi analyser was right next to the AP and the Pursuit tracker was on the other side of the floor when tracking started.

Our Pursuit tracker alerted that there were 3 potentially malicious APs:

- Under the floor, which the WiFi analyser didn’t even register as it only operates on the horizontal plane
- A suspicious unknown person
- A device hidden in a bag switched off remotely on approach.

We were even able to do something the laptop and WiFi analyser couldn’t do at all – tell the difference between unauthorised and malicious WiFi.

The HackHunter Pursuit tracker was so much easier to use (lightweight, single-hand use and 10.5 hours with no battery change) that the team member operating the heavy WiFi analyser asked to swap!

Through this trial we proved that HackHunter Pursuit is significantly more effective than the existing method of performing rogue access point audits, finding rogue access points quicker, easier and more accurately, saving time and money.

Product Enquiries

The HackHunter Pursuit can be customised for any role, from basic signal analysis to drone hunting. Contact us at info@hackhunter.io or call +61 3 8669 2090 for more information.