HackHunter **Vision** case study:

Enumerating WiFi networks with continuous monitoring

HackHunter Vision continuous monitoring trial #1

An ASX-listed technology company wanted to assess the security of their WiFi environment over a period of time. They wanted accurate visibility and to know what WiFi was in their environment. We also wanted to use this trial to improve the HackHunter technology and refine our algorithms to reduce false positives.

We installed 4 HackHunter Vision continuous monitoring sensors with hosts (Raspberry Pi) in their office for a period of 6 months.

Alerts were configured to be sent to specified staff members by email when unauthorised and potentially malicious WiFi was detected.

So what happened?

The office is located on one of the busiest arterial access roads to Melbourne's CBD, and, as a result, thousands of vehicles pass within metres of the office daily.

This resulted in hundreds of false positives every day, as we discovered that misconfigured hot-spots are quite common!

© HackHunter 2020

Through gradual refinement of our detection algorithm we reduced these false positives to nil.

With false positives removed, and confident that we were only picking up the access points that our customers should be concerned about, we progressed to our second Vision continuous monitoring trial to see what our technology was really capable of.

HackHunter Vision continuous monitoring trial #2

A retail food franchisor wanted to assess the security of the WiFi environment at a Franchisee site over a period of time. We installed a HackHunter Vision continuous monitoring sensor with host (Raspberry Pi) at the Franchisee site, located at one of the major railway stations in Melbourne's City Loop, for a period of 24 days.

So what happened?

- Over 6.5 million individual access point beacons were captured and analysed for suspicious behaviours using our templates, and 297 were determined to be suspicious.

Note: An access point beacon is generated by a WiFi device to announce its presence in the area. Any beacons in the area that weren't the franchisee's network were unauthorised and potentially malicious.

- Over 1.7 million WiFi packets were captured and analysed.
- A number of vulnerabilities that could be easily exploited were identified, including 33 deauthentication attacks, which can effectively block WiFi from being used by disconnecting devices from the WiFi router.

Through this series of field trials the HackHunter Vision continuous monitoring technology was refined and improved and our partners gained unparalleled, in-depth insight into their WiFi network.

Product Enquiries

HackHunter Vision sensors can be customised for use in any environment and to detect and locate any role, from basic signal analysis to drone hunting. Contact us at info@hackhunter.io or call +61 3 8669 2090 for more information.

© HackHunter 2020