Auditing a Wireless Network for Vulnerability Assessment

1st January 2014   **CASE STUDY**

Client Overview

A client from largest drilling industry based in gulf hired us to conduct the Wireless Network Assessment.

Project & Challenges

The purpose of hiring **Kualitatem** team was to independently audit the wireless infrastructure of client against latest threats. Following were the challenges:

- ➢ Proliferation of Wi-Fi devices
- ➢ Performance and reliability of Wi-Fi was not up to the mark
- ➢ Security of the Wi-Fi network need to be tested
- ➢ Configuration audit against the security baseline

Testing Strategy

To meet the client's goals for the wireless security assessment, Kualitatem security team conducted the test in the following way.

Wireless network of the client was checked against the latest threats:

- ➢ Brute forcing the SSID
- ➢ Establishing a fake access point
- ➢ Man in the Middle attack
- ➢ ARP poisoning, Authentication/Association flooding
- ➢ De-authentication flooding

War driving with high decibels antennas is performed in order to identify the anomalous access points and wireless access point was checked against the industry best information security practices.

Issues Found

The security team performed wireless network attack against client network extensively and identified that there are several **unauthorized access points** in company premises, which were offering free internet facility to its users. It was catchy for the company employees to get connected to it and use it, as company has blocked internet usage for mobile devices.

Outcomes

➢ A full heat map was generated along with signals strength, number of users connected to it, approx. location and few more parameters as evidence for the management.

➢ As remediation, a security awareness campaign was conducted in client premises in which they were given a brief about most the deadly malwares which were active that year.

➢ A practical demonstration of how information can be sniffed on wireless was also shown to the user in order to create awareness of dangers connected to the unknown wireless access points.

➢ Exploitation of access point where weak configuration was in placed was done in controlled manner in order to create awareness among the team about the importance of security baseline document.

➢ Security awareness campaign was conducted along with snapshots of the findings with management permission, was an eye opener for end users.

➢ The whole process was **recorded in form of snapshots** and shared with the client in order to tell the severity of the problems.

THANK YOU FOR DOWNLOADING & READING OUR CASE STUDY

Our Team at Kualitatem has helped refine and fine tune products across multiple industry vertical's in ensuring the quality of their web, mobile and desktop applications.

Our clientele consists of both top tier Global Industry Leader's who are trusted international brand's, as well as Startup's who have a great product on their hands and are looking to introduce the next revolutionary product to the world.

Here are a few of the client's we've helped out:

Google · Microsoft · BBDO NEW YORK · GE Healthcare · GASCO · Dubai Municipality · DP WORLD

So if you're ready to make an impact on your customer's and client', all you have to do is reach out to us to explore options on how we can help you polish your product to make a lasting impact.

Get in Touch   **Explore Our Services**

Kualitatem
QUALITY GROWTH PARTNERS