CASE STUDY

Briskinfosec Secured Wireless Network for A Major Software Organization in The APAC Region

INDUSTRY
Software Sector

STANDARDS
PTES, ISO27001, PCI-DSS

PRIMARY SECTOR
Software

LOCATION
APAC

OFFERED SERVICE
Wireless Security Testing

TYPE OF SERVICES : **Wireless Security Assessment**
for a Leading Software Firm

ABOUT CUSTOMER

Our Stakeholder is one of the leading global information technology, consulting and business processing services Company. They harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help their esteemed customers adapt to the digital world and then make them successful. They have recognized globally for their comprehensive portfolio of services, a strong commitment to sustainability and good corporate citizenship. They have over 160,000 dedicated employees serving customers across six continents. They also discover innovative ideas and connect the dots for building a better future with new horizons.

ASSESSMENT SCOPE

To find the vulnerabilities, Our Stakeholder wanted us to conduct a proactive Penetration test to find out if there any loopholes for hackers to gain access to systems. During the assessment, we only get the access to the router but not the other internal things like the number of people connected to the router and their passwords. We will be testing in the wireless frequency range.

THE SOLUTION

Briskinfosec followed standards like Penetration testing execution standards (PTES) and Payment card Industry Data Security Standards (PCI_DSS) to identify all exposed vulnerabilities in the Website.

Key highlights of the Vulnerability fix are as follows :

- We were able to quickly identify the MAC (Medium access control) address of the client without even connecting to it.
- We could disconnect the client from the router for a certain period. Even after implementing the MAC filter in the router, we were able to perform MAC spoofing and then join the Network.
- We were able to crack the WI-FI password without much strain as the passwords were easily guessable.
- Once we gained access to the Network, we were able to sniff the entire network.
- We performed vulnerability assessment by both automation and manual method of identifying the issues.
- We provided the complete vulnerability fixing document as a reference to your development team.

TECHNICAL SECURITY ASSESSMENT REPORT

Complete security testing was carried out. All the detected issues and the proof of concept (POC) will be covered with detailed steps in a PDF format.

ISSUE TRACKING SHEET

All the identified issues were captured and will the be subjected for the retest review in an XLS format.

WORKFLOW REPORT

Every process was carried out by the entire team without ignorance of anything.

FINAL BUG FIX REPORT

Overview of the entire engagement, the issues identified and the recommendations made to mitigate the same.

CHALLENGES

During a security assessment, there were certain complications that were faced by our security team. Those challenges are elucidated below :

- Sometimes while accessing the requirements, there would be restrictions even after which the customers demand that particular information.
- To make a word list for password cracking, we invested many efforts on Open source intelligence (OSINT).
- Password cracking consumed too much of time.

THE DELIVERABLE

The reports and the remediation information provided were customized to match the Stakeholder's operational environment and development framework. The following reports were submitted to the customer.

Key highlights of the bug fix are cited below :

DAILY STATUS REPORT

This wireless security assessment consumed around 1-2 weeks of time including retest. During the process of testing, issues were identified and we shared all identified issues with corresponding recommendation Fix over mail on a daily basis. Our prospect looked at the given valid report (XLS) and started working the fix right from Day 1 as they need not work laboriously on the last day when the entire report is given by the security team thus making their final assessment report easier for preparation.

CONCLUSION

We advised our Stakeholder on the measures they should take for rectifying the various vulnerabilities in their wireless systems.
For remediation, we educated them about the mandatory processes such as :

- Implementing a captive portal for stronger security.
- Recommending passwords to be the strongest like the combination of alphanumeric Characters.
- Disabling WPS and enabling WPA (2) version as it has strong encryption.
- Removing WEP since they are old versions and easy to crack.

We also worked closely with our Stakeholder for improving policies, procedures and employee awareness programmes for increasing security maturity.

BRISKINFOSEC
TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com