CASE STUDY

Briskinfosec secured
Network for A Largest Software Sector that is of Global Presence

INDUSTRY
Software Sector

STANDARDS
PTES, SANS, PCI DSS, ISO 27001, NIST

PRIMARY SECTOR
Software

LOCATION
Worldwide

OFFERED SERVICE
Penetration Test
Security Assessment

TYPE OF SERVICES : **Network Security Assessment**
(for One of the Leading Technology Consultant)

ABOUT CUSTOMER

Our Stakeholder is a world-wide leader in next-generation technology and consulting technologies. With magnanimous experience in management and technology, they rightly guide their customers through their digital journey. Their ever learning agenda enhances incessant improvement through building and transferring digital skills, expertise, and ideas from innovation ecosystem. They have more than 10000 employees in the organization.

ASSESSMENT SCOPE

Our Stakeholder wanted us to perform Network penetration testing from both external and internal aspects. So our assessment scope can be distinguished into two testing aspects as internal and external testing.

FOR INTERNAL TESTING

Through this testing process, we can get connected to their internal Network and then scan the given target systems. At the same time, we should also remember that scanning intensely the important systems shouldn't result in the crashing of that system as there may be so much of important processes connected with it.

FOR EXTERNAL TESTING

Through this testing process, we will be given only with one IP address and with that assigned IP address, we have to perform the scans and then detect vulnerability. After figuring out the vulnerabilities, we also perform the OPEN SOURCE INTELLIGENCE (OSINT) report about the given target.

THE SOLUTION

By using BriskInfosec frameworks, the security team successfully completed the Host Level Security bug fix and recommended best practices using the Penetration Testing Execution Standard (PTES).

Key highlights of the bug fix are as below :

- We encountered some serious issues related to SSL attacks, Weak encryptions, Captured NTLM Hashes to crack passwords, SMB login default credentials issues were identified and fixed by the Network Team.
- Security-related patches for the operating system was not deployed properly.
- We came across presence of Trojans and backdoor.
- Unnecessary protocols were enabled.
- Host-Level firewall rules were weak and we found some suspicious file existence.

DAILY STATUS REPORT

This Network security assessment consumed around 1-4 weeks of time including retest. During the process of Network security assessment, issues like False positives and many others were identified. Then we shared all the 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

TECHNICAL SECURITY ASSESSMENT REPORT

At the end of security assessment, we identified whopping number of security vulnerabilities and then documented the technical security assessment report with proper POC and also we shared the same over protected PDF.

ISSUE TRACKING SHEET

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

FINAL BUG FIX REPORT

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

CHALLENGES

During Network security assessment, there were certain complications that were faced by our security team.

Those challenges are elucidated below :

- There were many false positives identified during Automation and they were verified with manual testing methods like Network mapper (nmap).
- Because of those kind of issues, we had to correct them which consumed too much quantity of time.
- Sometimes while accessing the strictly configured server, there would be restrictions and complications to access it.
- If a particular server is too strictly configured, then nothing lucrative can be done.

THE DELIVERABLE

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

Key highlights of the bug fix are as below :

- During external testing, certain sites and certain scans will be restricted by the firewall because of which continuity goes for a toss.

But with sheer grit and perseverance, Briskinfosec successfully alleviated the Stakeholder's risk.

RISK BENEFITS

BriskInfosec diminished security risks by assessing the customer's infrastructure vulnerabilities and recommending solutions with proven methods for security enhancement.

COST SAVINGS

BriskInfosec suggested cost-effective measures based on the customer's business requirements that would ensure security and continuity of the business.

CUSTOMER SATISFACTION

Host Level Security Penetration testing was conducted with minimum interruption and damage across customer systems for identifying security vulnerabilities, impacts and its potential risks.

SUPPORT

We provide 1year support with periodic security assessment.

CONCLUSION

After the completion of our Network penetration testing, we advised the Stakeholder on the measures they should take for rectifying the various vulnerabilities in their systems. For remediation, we educated them about the mandatory processes like

- Completely scanning their systems on a regular basis.
- Emphasizing log monitoring to be done in a consistent manner.
- Implementation of DMZ (Demilitarized zone).
- Implementation of Network firewall.
- Implementation of IDS (Intrusion detection systems) and IPS (Intrusion prevention system).
- Implementation of Network device Fire wares that must be patched flawlessly.

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

BRISKINFOSEC

TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com