CLEAR infoSec
An Ana-Data Company

CASE STUDY ON EXTERNAL PEN TEST FOR FINANCIAL INSTITUTION

About the Customer:

Our client is a global institutional fixed income investment management firm, where they focus on building long-term value for their clients. They have their business and operation centers at New York, Chicago, London, Melbourne, & Singapore. Ana-Data was consulted to perform the External Network Penetration Test. After thorough analysis of pre-engagement interactions with senior executives, scope of pen test project was defined and concluded to conduct a network security assessment on 400+ IP addresses.

The Challenge:

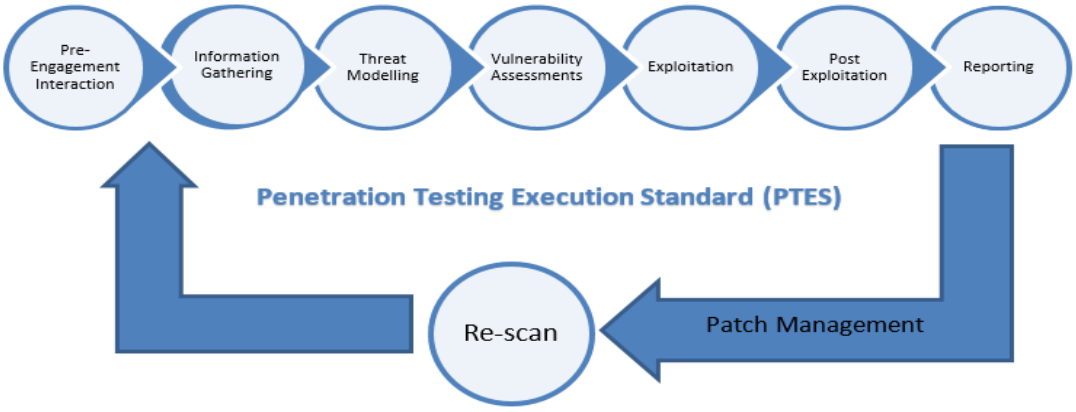
As a part of their security policy and regulatory requirement, our client wanted to assess the vulnerabilities in its external network. Hence, our client consulted Ana-Data to perform the external network penetration test. The test was performed to review and assess their IT security defensive posture. The objective was to determine whether and how a malicious external user could gain unauthorized access to assets and to confirm that the applicable security controls are in place and operating effectively.

The Solution:

After having initial interactions with senior executives, Ana-Data has defined the scope for the pen test. The methodology that was followed for performing Pen Test was Penetration Testing Execution Standard (PTES), which is industry wide accepted methodology which covers everything related to penetration test. The PTES consists of seven phases. We used both automated and manual techniques to simulate a real-world attack against our client's external network environment. Key highlights from the pen test project on our client were:

- ✓ Complete network mapping of the organization.
- ✓ Analyzing the network perimeter and concluding the IPs which fall in DMZ zone.
- ✓ Threat modeling for quantifying the threat factors and attack vectors.
- ✓ Automated scans to analyze the known vulnerabilities existing in the network.
- ✓ Validating the results gathered from the automated scans.
- ✓ Exploiting the vulnerabilities & trying to perform pivot attacks.
- ✓ Enumerating the vulnerabilities and prioritizing them using CVSS Scores.
- ✓ Reporting the vulnerabilities and recommendations for remediation & controls.

Once the first cycle of engagement was completed, and the reports were submitted to the client, a rescan was performed to validate that all the patches were implemented, and recommendations were followed.



The Deliverables:

The reports and recommendations were customized to match with our client's operational environment. The following deliverables were submitted to our client:

- ✓ *Executive Summary:* A brief overview of the pen test project, the vulnerabilities that were discovered and analyzed, and recommendations to remediate those vulnerabilities.
- ✓ *Detailed Technical Report:* Complete comprehensive information about the engagement. The detailed approach, and all the tools, techniques and procedures that were used throughout the engagement. Proof of concepts, and detailed steps of exploitation and threats that were identified. Complete list of vulnerabilities and recommendations and controls for mitigating the identified vulnerabilities.
- ✓ *Re-Scan Report:* Validating if the patches were implemented, and best practices were followed to stay secure.

The Benefits:

Financial industry has been the soft target for both amateur and skilled hackers, it is crucial to prioritize information security along with other business operations. By conducting a thorough external network pen test and identifying the vulnerabilities, Ana-Data, has reduced risk exposure on our client's external network. The other benefits that our client has gained by consulting Ana-Data for their security assessments are listed below:

- ✓ *Reduced Risk factor:* Ana-Data has minimized security risk exposure factor by assessing OUR CLIENT's vulnerabilities and recommending proven methods of remediation, and patches.
- ✓ *List of low hanging fruits:* A list of well-known vulnerabilities existing in the external network was provided with remediation process.
- ✓ *Network Hardening:* Hardening IT environment is an important step in the fight to protect the information and critical assets. Ana-Data recommended a work around to eliminate the attack vectors by patching vulnerabilities and turning off unessential services.
- ✓ *Patch Management:* Patch Management is a complex and never-ending process that isn't easy. Nevertheless, applying vendor security patches regularly is the first step to help harden your environment. Ana-Data reiterated the importance of Patch Management.
- ✓ *Regulatory and Compliance advice:* Ana-Data provided a detailed report which can be used as an input for audits and stay compliant with all the regulations.
- ✓ *Best Practices:* Ana-Data provides with industry standard best practices to be followed to stay secure.
- ✓ *Customized Support:* Ana-Data has provided customized support and assessments based on the client's specifications.
- ✓ *Customer Satisfaction:* The complete pen test engagement was conducted with minimum interruption to the business and by customized process gaining customer satisfaction.

Contact:

E-mail: infosec@ana-data.com
Phone: 551-236-1031
For more details visit: www.clearinfosec.com
For Security bulletin: Subscribe us at www.clearinfosec.com/tib