Cyber Security Case Study

Banking web application portal

Task Title	**Penetration testing of a banking web application portal**
Industry Vertical	Finance (Banking)
Industry Details	• Co-operative bank.Online customer base > 10000 Famous and wealthy bank in India's co-operative banking regime
Location	Mumbai (India)
Time to solution	1 month

Business Situation

The co-operative private bank provides e-banking and e-commerce facilities to multiple end customers and multiple banking and payment gateway industries all over the country. Web based e-banking portal is deployed and being heavily used, with an availability of 24x7x365. Customers perform transactions such as account checking, money transfer, e-bill payment, mobile payment etc.

Bank wanted to perform web penetration test, patch deployment test, and other few tests enforced as a pre-requisite by RBI (Reserve Bank of India). Bank also wanted to perform black hat and gray hat testing to protect from external and internal attacks. SecMyIT was approached to suggest right strategy to address these concerns, and perform tests and produce results.

SecMyIT's Solution

- SecMyIT had a kickoff meeting with firm's senior management and a series of meetings with IT management and technology staff to understand web portal design.
- It was suggested that the network components protecting web infrastructure should also be pentested.The components were, a router, firewall, intrusion detection system, L3 switches.
- A series of non-intrusive tests were performed to gather information and perform technical
- reconnaissance.
- Based on the information gathered, appropriate tools were selected and a series of deep-dive tests were performed on the network and web infrastructure. Logs were captured.
- A separate set of scanning and penetration tests were performed targeting the network components mentioned above.
- Specific critical web vulnerabilities such as code-red, sql injection, XSS attack, AJAX attack etc, were performed too.
- Finally, two intrusive attacks were performed during off-business hours. Those were "Password bruteforce attack" and "Denial of Service attack".
- Elaborate log processing was performed and a report with all severity 1, 2, 3 vulnerabilities and the corresponding suggestions to fix, was created.
- Bank management was informed about maintaining the confidentiality of the report
- A tactical and strategic patch deployment schedule was provided, to segregate "Must patch
- immediately" and "Should patch eventually" lists of missing patched.
- Report was signed-off by the bank's IT management.

Benefits

- Banks web portal infrastructure was thoroughly tested, which helped bank's management gain confidence to advertise the portal further to multiple customers.
- As an outcome of penetration test, the banks money transaction process was revamped to strengthenaudit trails and security. A new firewall was deployed to shut the denial of service attack at the door step.
- A professional pen-test report helped bank create IT audit policies and standard operating procedures. This further led to getting RBI approval for increased business

Learn More About us at :
www.secmyit.com

For Further Information, Please Contact
contact@secmyit.com