

Case Study: Penetration Test

Industry Sector: Finance

The finance sector has largely championed the increasingly interconnected business world. The need for the facilitation of business-to-business (B2B) and business-to-customer (B2C) commerce, rapid transfers of business intelligence and remote access working has resulted in an ever increasing number of systems, portals and services situated on the publicly-accessible Internet.

Regular system and network security assessments that provide the highest levels of assurance are critical for an organisation seeking confidence in its perimeter defences. IRM adds value to the penetration testing process by providing deeply technical business consultants who deliver findings in terms of the necessary business impact analysis to the information security managers charged with ensuring those defences.

Case #1 – A weak link in the chain

IRM performed a penetration test against all externally accessible network infrastructures belonging to a global leader in online market trading; including an examination of corporate websites hosted within the target network ranges.

The penetration test began with an identification of all target hosts within the network ranges, along with a vulnerability assessment of services running. IRM identified a number of process failures related to patch management and server hardening, all of which were included in the final report.

Following this stage attention was turned to the regional corporate websites hosted within the various network ranges. Upon initial inspection all appeared in order – there were no exceptions raised in response to malicious input to login forms, no cross-site scripting seemed to occur and no useful information appeared in the pages presented. However, a more thorough inspection revealed that an input verification issue within one of the many login forms of the various corporate websites presented an opportunity for SQL injection.

Although the typical error messages associated with SQL injection were absent when submitting malicious input, IRM utilised blind SQL injection techniques to execute system level commands through the inadequately configured database server. IRM consultants were able to upload tools that allowed them to circumvent firewall restrictions and gain graphical desktop access to the server remotely, with full administrative privileges.

IRM was then able to exploit trust relationships within the DMZ hosting the database server and a remote office location due to the fact that weak passwords were replicated between the two sites. This allowed the consultants to obtain *domain administrator* access to a remote office belonging to the client. Through exploitation of a further trust relationship from the remote location IRM consultants gained access to the organisation's main corporate domain and a number of file servers holding compliance related data and board meeting minutes.

IRM successfully demonstrated that the unauthorised access provided by a single poorly configured system on the Internet could provide a malicious and motivated attacker with the ability to gain wholesale access to a vast number of corporate systems and the sensitive data stored upon them from within the organisation.

The findings allowed our client to rectify issues within their web applications and also prompted a formal risk assessment of the control weakness surrounding the trust relationships within the globally disparate infrastructure.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.