Network Penetration Test: Protecting a Financial Firm's Future

Problem

A financial firm needed to evaluate resilience against malicious intrusion attempts

Solution

Several servers containing critical data were successfully penetrated and compromised

Results

The client identified weaknesses in security, and developed a proactive incident response plan

Overview

Alacer Group was approached by an international finance and development firm to identify and break into high-value, strategic business systems via remote access to simulate a malicious intrusion attempt.

Challenges

We performed benign "white hat" remote penetration testing and compromised several systems, including taking control of servers hosting personal information from clients and employees that would have cost the organization over $500,000 for breach notification mailings alone. We also compromised a database containing strategic information on the organization's financial assets.

Results

We demonstrated conclusively that unless they undertook defensive mitigation, the firm would be exposed to severe risk and injury to its operations, reputation and financial viability. We delivered written and oral reports to help the client thoroughly understand the methodology and implications of the network penetration test, and collaborated with the client's staff to develop immediate steps to mitigate the vulnerabilities reported and to develop an incident response plan to identify and mitigate malicious intrusion in the future.