



Project Objectives

- Determine if the level of internal controls in place at the service provider sufficiently mitigated key risks, most notably the exposure of confidential client data.
- Determine if a malicious internal user could gain unauthorized access to sensitive financial data.
- Determine if a malicious employee of the service provider could gain unauthorized access to sensitive financial data.
- Determine if another bank, hosted by the same service provider, could gain unauthorized access to sensitive financial data.
- Determine the security of the application from the perspective of a malicious user on the Internet.

CASE STUDY

Pivot Point Security Reveals Holes in Hosted Fund Transfer Application

Pivot Point Security receives a call from a major international bank to conduct an Ethical Hack on a key Fund Transfer application hosted by a third party. The weaknesses that were uncovered shocked and surprised both the client and PPS.

The Phone Call

We received a call from an Information Security engineer at a major international bank, who we will refer to as Bank Client (BC) from this point forward. An industry colleague that frequently worked with us in support of our projects (and vice versa) on network and security architecture referenced them to us.

Strangely, the character of the phone conversation was one of a direct and immediate call-to-action even though we had never met this client prospect. He cited some concerns regarding the security of an application that was hosted by a third party on their behalf and wanted to know soon we could come on site and perform an Ethical Hack against the application.

Further affirming our impression that this was an imperative matter for this customer, they requested our Ethical Hacking team on site at their location only three days after we received the Monday call.

Kick Off

Judging from the high level titles of the individuals (Chief Information Security Officer, Chief Information Officer, and Sr. VP Auditing) at the kick-off meeting, we quickly surmised that their concerns were of a significant nature. Interestingly, they would not detail any specific concerns and we spent the better part of the two hour meeting discussing their business environment and the critical role of the application under review. We quickly began to understand that the application we were looking at processed billions of dollars of transactions on a daily basis. Since the application and supporting systems include interfaces to Federal Reserve Banks, we were advised that we could not begin Penetration Testing until after 6:30 PM. We accepted an invitation to grab a bite for dinner with the Chief Information Security Officer and

some of the other key team members on the project.

Following our return from dinner, the rapidity of events that started the engagement startled us—within 10 minutes we were the Domain Administrator for the seven hosted devices that comprised the ASP-hosted solution. Five minutes after that we gained control of the application and database with critical customer data, effectively enabling us to transfer \$500 million between accounts. And ten minutes after that, we were on an emergency conference call with BC executives to go over next steps following such startling revelations.

The Means to an End (Game)

The Terminal Services application's login screen allowed the option of local authentication from the drop down instead of network authentication. This was the first indication that the level security of the application might not be adequate given its significance and value to BC as local user accounts usually aren't subject to network security policies. We quickly discovered that this was only the tip of the proverbial iceberg, further uncovering:

- The user of weak passwords which we guessed on our second attempt—the combination "administrator"/"ASP" (where ASP was the name of the ASP)
- This weak username/password combination was persistent on every device on BC's hosted segment

The eventual goal of most network intrusions is the application database where the most valuable data to the organization is stored. With the egregious lack of security across the BC's hosted segment, we moved on to the database and tried an equally weak password guess on BC's hosted database. Regrettably, we were correct—the default MS SQL username "sa" and blank

password field allowed us to gain entry and access to the literal jewels of their systems--the bank records of foreign Republics, huge corporations and even international royalty.

Quickly reaching the most valuable BC asset in the hosted infrastructure, we paused our work and reported back to the BC project liaison to immediately let them know of our findings and their potential impact.

During the conference call with BC Executives, the client posed a vital question--"Could one of the ASP's other clients compromise their infrastructure, access their client data, and gain the ability to transfer funds, in the same way that the Pivot Point Security Ethical Hacking team did?"

There was no question that testing this theory was of the utmost importance to the overall impact of the engagement--providing the maximum value to BC on the risks associated with a maliciously intended user inside and outside of their hosted funds application. However, this was a risk that could not be substantiated without considering the potential legal implications of the effort. We quickly convened a second conference call, which would include BC counsel and our counsel. After considerable discussion with our respective attorneys, we reached a consensus that we would continue the ethical hack to ascertain whether another bank could potentially take the same actions that we did, but that we would make every effort practical to ensure that we did not breach another client's confidentiality.

"In short order, we had confirmed that a malicious individual at any one of the dozens of banks hosted by the ASP could connect into another bank's fund transfer system and move hundreds of millions of dollars across banks and accounts."

Two for the Price of One

Resuming our ethical hack, we attempted to enumerate other banking clients on the ASP's network, but quickly discovered that all we could do was ping them. The ASP had done a good job of segregating their clients from each other. We did confirm the existence of dozens of duplicate networks for other large banks on the ASP network.

One of our team members came up with a potentially clever workaround--by writing and deploying a simple Netstat script, we could monitor active TCP connections and their respective ports from our console. From this, we hoped that we may catch a connection in progress. After an hour, we

noticed a connection coming into one of the boxes from an unfamiliar IP address. Attempting to telnet to the IP did not succeed, which indicated a good practice of not allowing unsecured connections to critical assets. But, our following attempt to connect to the same IP via a secure shell (SSH) yielded a username /password prompt.

We paused briefly, wondering if it were possible that the level of security on this segment was as loose as the ones we previously controlled on the BC segment. Unfortunately, "administrator"/"ASP" provided us with root privileges on the box. The box we had gained access to was running an open source network monitoring tool that was monitoring all of the ASP's clients. We connected via SSH again to another bank's network and ascertained the same weak "administrator"/"ASP" combination was in use on the systems on their hosted domain as well.

In short order, we had confirmed that a malicious individual at any one of the dozens of banks hosted by the ASP could connect into another bank's fund transfer system and move hundreds of millions of dollars across banks and accounts. Reaching this end point, we ceased testing and began preparation of our report to BC executives.

During the audit readout meeting we encountered one final surprise; the ASP had provided BC with a "clean" SAS-70 Type II Audit Report issued by a prestigious CPA firm. Accordingly, BC had felt confident that their clients' data would be well protected by the ASP.

Take Away

Our client was very pleased with our efforts on their behalf, but anxious with regards to the level of risk that the application presented. Their Internal Audit team planned a follow-up audit of the ASP, and requested that we substantiate the changes to the control environment via another Ethical Hack at some point in the future.

Validating that a provider (particularly a provider handling high value and trusted client data) is adhering to your company's specific needs is vital to achieve and maintain compliance in today's increasingly regulated business environment. Unfortunately, scenarios such as the one described in this case study are commonplace and expose many organizations to unseen risks.

As a result of our work with BC, the most significant risks have been mitigated, and the client and ASP are jointly working together to move the overall security posture of the application to an appropriately high level.



ABOUT PIVOT POINT SECURITY:

Achieving, and more importantly maintaining, a "reasonable & appropriate" security posture in today's environment requires a new approach. We approach IT Security as a business issue and focus on IT Governance, appropriate balance of key elements (people, process, & systems) and objectives (risk, cost, usability, and performance), strong control environments, and ongoing monitoring capabilities. Those safeguards are the hallmarks of today's best security architectures and the strength of Pivot Point Security.

Pivot Point Security is the premiere provider of information security auditing, penetration testing, enterprise security management, vulnerability assessment and mitigation services and solutions in the NY / NJ / PA metro area.

Clients (small business through international corporations) benefit from our Internal Control oriented approach to Information Security and our assistance with complex issues including Sarbanes Oxley, HIPAA, and SAS-94.