Red Team Testing - Case Study

Overview

Security Art was engaged by a US Based financial institute which provides retail and commercial banking services in order to perform a full security assessment, herein referred to as a Full Red Team Exercise, on all layers of the institute's operations. These tests involved both physical and digital realms of the institute's activities, offering the institute a unique and comprehensive security overview of their own operations, as perceived and audited by the cyber security experts at Security Art.

The Challenge

The challenges in the path of a large financial institute are manifold; most information on most devices within the institute constitutes as confidential, often falling under well-defined categories such as Intellectual Property (IP), Personal Identifiable Information (PII) or Payment Card Industry Data Security Standard (PCI DSS).

Many functions within this organization perform sensitive actions with the aforementioned data and may be vulnerable to attacks. These attacks range anywhere from identity theft to industrial espionage, from brokering sensitive information to manipulating fiscal transactions, attackers have dozens of ways to capitalize on them for personal gain. Ranging anywhere from lacking physical defense on computing systems to a vulnerable web-application whose database may be jeopardized, attackers have dozens of attack surfaces to choose from. The sheer enormity of banking organizations and their overall attack surface, combined with the wealth of extremely valuable information and financial functions encapsulated within such an institute, make it the proverbial holy grail for both attackers to compromise and security experts to defend.

In employing Security Art's Full Red Team Exercise, our team of security experts aims to:

- Address security requirements and evaluate the risk involved in their viability, modeling potential threats on all potential layers of potential attack
- Deliver an advanced capability to mimic real world attack scenarios, sans the actual risk of being targets of such attacks:
    - Physical attacks on company facilities
    - Personal attacks against employees which may be used as a pivoting point to obtain further access into networks, or manipulated into disclosing sensitive data
    - Cyber-attacks on internet-facing assets such as applications and external networks
    - Cyber-attacks on intranet-facing assets, such as internal and wireless networks
- Provide the client with a robust set of conclusions and industry best practice recommendations derived from the results of this exercise
- Engage in long-term remediation efforts and continued security assessment to ensure a consistent and ongoing business risk monitoring and security posture reinforcement

The Situation

Security Art was engaged by a US Based financial institute to perform a full Red Team exercise on its digital and physical assets, in order to:

- Perform physical security assessments of numerous facilities deemed sensitive by the bank, as well as numerous branches and personnel residence. Physical assessment involved attempting to:
    - Physically infiltrate facilities and gain access to internal devices and networks
    - Breaching any wireless networks in place within the facility or residence of senior executives
    - Delivering custom malware on physical devices to employees
    - Provide an assessment of overall physical security of security countermeasures, from assessing guard behavior and adherence to protocol, to enumerating security cameras and assessing their coverage of approach vectors to mission-critical assets on location.
- Perform Advanced Persistent Threat (APT) evaluation, mimicking scenarios where attackers attempt to map the personal lives, interests and affiliations of employees by gathering open source intelligence (OSINT) on them from social networks and other available data outlets, and leverage this knowledge to directly access employees. The end game of this exercise is to deploy malware within the institute's networks, or encouraging employees to divulge sensitive information to potentially malicious outsiders.
- Perform automated and manual code review on code behind active web, client and mobile applications to provide a clear evaluation of all application layers and potential vulnerabilities, mapping out lacking secure coding policies and standing security issues and providing a manually validated set of results and recommendations.
- Engage all active production web, client and mobile applications in penetration tests
    - Assess environments' security posture in terms of both technical vulnerabilities and business logic flaws
    - Assess all of the platforms within the institute's infrastructure, from web applications to webservers and work environments
    - Provide a thorough set of observations and recommendations from world-leading experts:
        - Short-term tactical fixes for immediate remediation of any outstanding vulnerabilities within the tested environments
        - Long-term strategic policies that will proactively thwart any potential repetition of vulnerabilities discovered during testing

Analysis and Conclusions

The full Red Team exercise executed by Security Art was highly successful and has yielded a significant set of results, highlighting much egregious vulnerability in all realms of testing.

During the physical security infiltration exercise, many protocols in place were breached; namely, access was granted to computers, executive floor and other environments, allowing our experts to obtain photographs of facility internals, as well as attempt to drop custom malware on internal devices. In some cases physical security was circumnavigated, in others, breach incident response was slow and ineffectual, allowing our team to exit without reprimand. The wireless networks at the executives' residence were tested and breached, despite utilizing the WPA2 encryption protocol.

The Advanced Persistent Threat (APT) tests have uncovered the lack of security awareness of many executive level employees, who have disclosed personal information to fictitious forms that impersonate the financial institute, responded to personalized and fraudulent e-mails and downloaded malicious files, all of which were crafted, sent and closely monitored by Security Art.

The penetration testing phase has revealed an overwhelming number of high severity vulnerabilities available within working applications, ranging from a vulnerable web application which may be exploited to disclose its entire backend database to a web server, underlying a sensitive web application, which uses outdated software, allowing Security Art's team to completely compromise and take over the web server and application. Across the board, nearly all sensitive applications were found vulnerable in some way, from allowing customer data theft and manipulation to enabling attackers to lock out massive amounts of users without any prior knowledge or access.

The code review has raised numerous flags regarding repetition of bad practices within the environments tested. While not all bad practices constitute as exploitable vulnerabilities, the continued use of poor security practices was clearly a root cause to the wide array of results provided in the penetration testing.

The independent vulnerabilities discovered during this security assessment were egregious, and lead to one root cause – lacking of adherence to security policies across the board, from the ability to defeat the human factor to the numerous significant flaws found in proprietary technology and assets, which leaves the audited institute vulnerable to attack via any of the attack vectors mapped at the beginning of this exercise. Security Art has provided recommendations for both immediate remediation suggestions and ongoing prevention of such issues via best practice security policies, and will continue to do so in the future.

"...We're very pleased by your work; you've exceeded our expectations in every aspect"

Source: Customer' SVP Security

About Security Art

Security Art is an internationally recognized Cyber Security company, specializing in providing advanced Cyber Security services to customers worldwide.

At Security Art we've concluded and demonstrated that an organization's security posture is derived from its stamina to threat actors which are relevant to its particular line of business, focusing on the attack vectors they typically employ in cyber-attacks and security incidents pertaining to the organization's market vertical.

As such, we execute for our clients Red Team exercises. These exercises are more comprehensive in nature and cover a variety of activities not typically included in standard security assessments.

Following is an example of the content of such a Red Team exercise:

- Collection of open source intelligence (OSINT) and Digital Foot Printing
- Social Engineering
- Ethical Spear Phishing
- APT and Malware Insertion
- Physical Penetration Testing for sensitive locations (HQ, DC, etc)
- Penetration Testing for the Infrastructure including and VPN
- Penetration Testing for Wi-FI networks possibly including the residence of senior executives
- Penetration Testing and Code Review of Application including Mobile applications
- Penetration Testing of Mobile Phones
- Quantify the identified risk to monetary values and provide meaningful deliverables to business executives

Each of the above listed services can be executed individually, in addition we provide a variety of "Blue Team" services, including but not limited to:

- Forensic and Incident Response
- Threat Modeling
- Quantitative Risk Analysis
- Applications and Infrastructure design review
- DDoS Testing and Mitigation
- Secure Development Life Cycle
- Reverse Engineering

For more information please visit our website at www.security-art.com or email info@security-art.com