CASE STUDY

SYNOPSYS®

Red Teaming a Multinational Financial Institution

TABLE OF CONTENTS

Overview

Financial institutions face unique security challenges driven by the highly sensitive data they are trusted to protect and the multi-faceted attack surface they must defend. A red team assessment is a goal-based adversarial activity that requires a big-picture, holistic view of the organization from the perspective of an adversary. This assessment process is designed to meet the needs of complex organizations handling a variety of sensitive assets through technical, physical or process-based means.

Adversarial objectives and strategy

Every red team assessment at Synopsys starts by defining a set of adversarial objectives which influence the testing strategies that are applied and the attack paths that are subsequently followed. Our overall strategy in this assessment was centered on emulating a professional and technically-sophisticated criminal organization with the following objectives:

- Gain access to sensitive customer and business data including PII, PAN and corporate intellectual property.
- Impact the availability of critical business systems, resulting in a direct financial loss for the target.
- Obtain access to the internal corporate network, facilitating longer-term, persistent attacks and data exfiltration.

Getting started

Once we understood the adversary we were emulating, our objectives and our overall strategy that served as a guide throughout, we were able to move into the actual assessment process. Reconnaissance and intelligence gathering were our immediate next steps when attempting to quantify the attack surface of our target. This phase of the assessment is an ongoing activity but serves as the initial base by which scanning, attack path generation and execution is built upon.

In this case, we focused our reconnaissance efforts on several key issues:

- Identifying all possible web and mobile applications, IP addresses, and live hosts/services. Once these were identified, we were able to assess them from an unauthenticated perspective. This included identifying low-hanging fruit vulnerabilities and collecting information that we could later cross-reference to identify relationships between components such as authentication services, routing paths, or authorization frameworks.
- Learning business processes such as the ability to reset a remote employee's password or onboard a new customer to certain systems, followed very specific workflows. We accomplished these workflows in several ways: with intervention from a support representative, interacting with a web application or service, or a combination of the two.
- Gathering information on the primary and satellite offices of the organization. Learning how the network was designed, in order to understand how an attack on a satellite office wielding internal network access could be carried out, allowed us to pivot into the primary network segment designated for the organization's headquarters.

- Collecting information about employees that could facilitate targeted social engineering attacks later in the assessment. The base-level information that was collected included name, phone number, job title, email address and office location. We could use various combinations of this base-level information, depending on the specific attack we leveraged.

Attack path modeling

The following table illustrates a high-level and abstracted version of the composite attack matrix that was generated for this particular Red Team. The matrix highlights several attack paths that we used in relation to compromising customer account information. These composite attacks leveraged a variety of different techniques at different stages. For brevity, only two composite attacks are discussed in detail in the following section.

Motivation	Relevant technical risks	Relevant non-technical risks	Composite attack description
Compromise customer data	• Reflected cross-site scripting • Mail server misconfiguration • Broadly-scoped and unsecured session cookies	• Employees susceptible to emailbased phishing attacks	Described in section 5.1
Compromise customer data	• Framing attacks possible • Mail server misconfiguration • Customer username enumeration	• Application does not perform browser-based fingerprinting for new logins	Enumerate legitimate banking users by email, send them phishing emails from target's mail servers and bring them to a page that frames the primary banking web application, capturing credentials as they are entered
Gain persistent access to internal network	• Administrative VPN service missing two-factor authentication	• Security questions easily identified for organization admins • Phone-based password reset process susceptible to social engineering	Identify administrative users through social media services, learn their possible security answer questions and then use that information to reset a domain password through the help desk hotline. Use this password to access the lone VPN service that did not require two-factor authentication
Gain persistent access to internal network	• Missing network layer authentication	• Physical social engineering at satellite office	Gain physical access to a satellite office and install a persistent remote access device on a live network connection, facilitating further attacks on the internal network
Gain persistent access to internal network	• Reflected cross-site scripting • Outdated software on internal systems	• Employees susceptible to emailbased phishing attacks	Hook user's browser with BEEF cross-site scripting payload and pivot to an older, out-of-date CMS system where a remote, persistent shell can be downloaded
Compromise customer data	• Administration portal accessible from the Internet	• Password reset bypass through the phone • Administrator information collected from social media services	Described in section 5.2
Cause denial of service conditions	• Default password on Tomcat Manager • Outdated version of Apache	• N/A	Bypass authentication to Tomcat Manager with default password, exploit a known denial of service vulnerability in an authenticated page that could bring down a critical sector of services

Leveraging multiple technical vulnerabilities, process weaknesses and testing techniques—all within a single composite attack—allowed us to compromise our adversarial objectives in many ways that a real-world adversary would.

Execution

Building on the reconnaissance efforts and the composite attack paths that were developed, our Red Team started to build and execute each attack, targeting one of our adversarial objectives. Below are two of the composite attacks this Red Team executed.

Phishing with internal resources

Synopsys' Red Team conducted the first composite attack from an Internet-facing perspective. This allowed us to gain access to personal bank account information as well as financial administration applications affecting a much wider user base. During our reconnaissance efforts, we identified a number of promotional sites that were deployed on various subdomains of one of our target's primary top-level domains. Based on our initial analysis, it appeared that the promotional sites had not undergone the same rigorous security processes that many of the higher profile applications had and, therefore, were vulnerable to many basic attacks including reflected cross-site scripting. Leading up to a social engineering component to this attack, Synopsys gathered several hundred employee names and email addresses from various sources on the Internet. During our reconnaissance, we also discovered that the primary banking and administrative portals were using broadly-scoped and unsecured session cookies with the same names as the ones used on the promotional sites.

After we gathered the intelligence needed, we put together a cross-site scripting payload on one of our target promotional sites. The payload captured session cookies that we scoped to the parent domain and posted back to a server we controlled. The payload also re-wrote the returned page to include an authentication form field and some supporting data for a scenario that was described in the phishing email. Once the payload was set up, the team sent the phishing email from a target-owned mail server, exploiting a flaw in the configuration that allowed us to send mail from the server without authentication and attempted to direct the targeted users to the link included.

Once we had a sufficient number of domain credentials and session cookies, we validated that the session cookies worked on both the personal banking application as well as the financial administration application for employees whose role permitted it. When we could, we tested with credentials as well. This administration application allowed the Red Team to actively transfer funds to/from arbitrary accounts as well as drill down into the accounting details of customers in specific regions. This enabled us to accomplish one of the adversarial goals we initially set.

Weaknesses in phone-based password reset process

In the second composite attack, we leveraged Synopsys' role-based social engineering process to compromise employee passwords through the target's phone-based help desk process. We were able to access the help desk in two different ways: through a web-based workflow and by calling a support hotline. Both means of access required the following information to reset the password:

- Employee email address or unique ID
- Answer to only one security question out of a set of five

Interacting with the web-based workflow required an employee's unique ID, which was non-public information, as well as a security question response that matched the stored value exactly. During the course of our assessment, we were unable to learn the unique ID value associated with a specific employee.

Alternatively, a support representative handled the entire phone-based workflow. During our conversation with him, we were able to supplement the unique ID value with an employee's email address to get past the first step. Research into employees on various social media and background investigation services allowed us to learn the answers to many of the security questions for the employees we targeted. When we provided this information during our conversation, the support representative accepted it. Once completing the password reset, the support representative was able to read a temporary password back over the phone. The manner in which the phone-based password resets are handled could be exploited to reset any employee's password in a targeted attack.

We could use this temporary password to change the employee's password to a Synopsys-controlled value as well as authenticate to other external services using LDAP, including the financial administration portal referenced in the first composite attack.

Summary discussion and results

Overall, we found that the distribution of security controls relative to the risk ranking of organizational components—such as high-profile web applications, network segments, and offices—introduced weaknesses that remote adversaries could exploit. However, in many cases, components with a lower risk ranking or perceived risk received much less attention with regards to security, time, and budget. This, in addition to the interconnected nature of the organization, allowed us to build a series of successful composite attacks that leveraged these lower-risk components. Synopsys was able to achieve all of the adversarial objectives outlined at the start of the assessment, including compromising customer account data, gaining persistent internal network access and finding ways to cause denial of service conditions on critical financial services.

The level of access and information that we obtained would have represented a severe breach, financial damages, and harm to the organization's brand and reputation if similarly conducted by a real-world adversary. Each of the risks outlined within this Red Team are real and immediately exploitable by a similarly skilled adversary, given that we operated from the perspective of a remote, technically-skilled, and coordinated black-box adversary.

THE SYNOPSYS DIFFERENCE

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software

SYNOPSYS®
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com