S OPS

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

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.
-