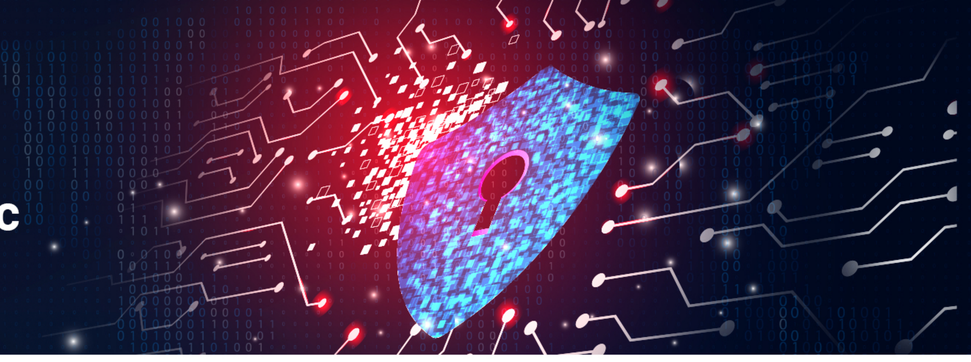
Red Team Assessment to identify security gaps and understand threat exposure levels of a large banking corporation in Asia Pacific



One of APAC's region's leading regulatory body released a mandate that every bank under its jurisdiction must undergo Red Team Assessments for all critical systems facing the internet. These assessments can help banks identify vulnerabilities and business risks, assess cyber defense efficacy, and evaluate existing security controls by simulating attacker's objectives and actions.

The Challenge

It was time the bank performed the Red Team Assessment to gain better understanding of any existing flaws such as open ports, misconfigured SSLs, leaky S3 buckets, and XSS vulnerabilities. The bank also wanted to know whether their current security controls could withstand network intrusions, social engineering phishing, and DDoS attacks.

The objective of this assessment was to identify potential security gaps in the bank's network and get privileged access to critical infrastructure (Active Directory, Finacle, TI Plus, Swift, Financial, and PII Data).

Strategy Design & Solution Approach

The Red Team Assessment leveraged the adversarial attack emulation in adherence to industry standard MITRE ATT&CK framework. The framework is similar to Advanced Persistence threats (APT) observed in millions of attacks that led to cyber breaches worldwide.

The red team assessment performed for the Bank was an "Assume Breached" scenario that simulated targeted attacks through the tools, techniques and procedures used by real world adversaries. For this assessment, Bank provided Aujas with two low privilege domain user accounts having VDI access to the internal network. The assessment followed a stealthy, evasive approach to meet the defined goals and objectives.

Scope Definition, Develop Approach, Set Objectives, Rules of Engagement & Boundaries

- Fix engagement scope, objectives & communication guidelines
- Identify the project sponsor
- Establish Rules of Engagement & boundaries
- Develop project plan, along with key milestones and periodic reporting timelines

Conduct Red Team Assessment to Access Critical Assets, Capture Flags & Exfiltrate Sensitive Data

- Internal reconnaissance
- Privilege escalation
- Defense evasion – evade and bypass host/endpoint controls, network security devices/solutions
- Command & Control (C2)
- Lateral movement
- Collection & data exfiltration
- Target goals & scenarios for the exercise are as below:
  - Compromise the Active Directory with possible highest privileged account
  - Once the payment system is accessed perform a transaction
  - Access VPC servers or compromise VPC Admin to make configuration changes to VPC
  - Ex-filtrate customer and card Information

SOC Gap Analysis

- Perform SOC gap analysis to evaluate detection (Missing Security Alerts) uncovered during Red Team attacks

Documentation

- Document identified observations & gaps in defense controls & solutions and SOC detection capabilities
- MITRE ATT&CK dashboard
- Provide short-term and long-term recommendations to mitigate
- Document lessons learnt

Outcomes for a valuable difference

Mitigation of existing risks

Evaluated effectiveness of existing security controls and solutions to further optimize and fine tune them to mitigate risks. Got a deeper understanding of the risk levels of the most critical assets in the organization.

Threat detection & response capability assessment

Evaluated the detection and response capabilities of Blue Team to improve the Security Operations Centre (SOC) maturity. Uncovered serious security flaws that would not been detected with traditional penetration tests.

Security posture improvement recommendations

Provided an evidence-based risk profile to senior management and gave recommendations to improve the overall security posture to maximize return of security investments.

Objectives achieved as part of the solution framework

Compromise the Active Directory of the highest privileged account

- Aujas Red Team experts compromised the highest privilege account: Domain Administrator account.
- They added a rogue Domain Administrator in the Bank's domain.

Upon accessing payment systems modify customer data & perform a transaction

- The team bypassed the two-factor authentication mechanism of TI Plus and Finacle applications.
- They modified customer details in TI Plus application.

Access VPC servers, ensure compromise of VPC Admin & make configuration changes to VPC

- The team got privileged access to the Bank's Azure and AWS environments.
- They added a rogue Global Administrator to the Azure environment.

Ex-filtrate customer and card information

- The team accessed financial data (customer transaction details, statements, account balances) and PII data (Aadhar card, PAN card, Passports, Account Numbers, Customer relationship numbers, beneficiary and nominee details, name, address, telephone, Email Ids, etc).
- They exfiltrated dummy data externally to the Aujas controlled Command and Control server.

Solution Highlights

The high-level description of the attack path to complete the assessment objectives is demonstrated below