SUCCESS STORY | RED TEAMING

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 their existing flaws and assess the overall security posture. The banks also wanted to know whether their current security controls were robust to prevent/ detect against network intrusions, social engineering and internal attacks on their network and active directory.

The objective of this assessment was to identify potential security gaps in the bank's network, get privileged access to critical infrastructure (Active Directory, Cloud console, Core banking applications) and access company sensitive data (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 employed both external as well as Internal approaches. As a part of External Red Team, Aujas team used a complete Blackbox methodology which meant that the team commenced their assessment without any prior knowledge. During the reconnaissance phase, the team uncovered a vulnerable endpoint within the VPN portal capable of circumventing Multi-Factor Authentication (MFA) by the addition of MFA devices for other users. By leveraging a combination of phishing attacks and compromised credentials sourced from recent security breaches, the team successfully bypassed the MFA controls within the VPN system, thus gaining unauthorized internal access to the client's environment.

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.

Plan

Define Scope, Approach, Objectives, ROE, Boundaries & Limitations

Key activities

- Finalize engagement scope & objectives,
- Finalize communication guidelines, identify the project sponsor
- Establish Rules of Engagement (ROE), boundaries and limitations
- Develop project plan, along with key milestones and periodic reporting timelines

External Red Team

Intel collection , Threat Profiling and Gain Foothold

Key activities

- Perform OSINT reconnaissance, active and passive scans.
- Define threat profile & attack scenarios based on information gathered via OSINT framework
- Initial Access
    1. Social Engineering Attacks – Phishing, Vishing, etc.
    2. Client-Side Attacks
    3. Server-Side Attacks
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion –
    1. Evade and bypass email gateway/ Mail Filter Sandbox, Host/ endpoint controls, security devices/ solution and SOC

Internal Red Team

Gain Access to Critical Assets, Capture Flags & Exfiltrate Sensitive Info

Key activities

- Initial Access
- Internal Recon
- Privilege Escalation
- Defense Evasion – Evade and bypass Host/Endpoint controls, Network security devices/ solutions
- Lateral Movement
- Collection
- Command & Control (C2)
- Objectives –
    1. Gain possible privilege access to critical assets (Crown Jewels)
    2. Capture Flags and Perform data exfiltration to agreed location or C2 machine

Deliverables

Gaps Documentation

Key activities

- Document identified observations/gaps in defense controls/ solutions with artifacts
- Comprehensive report demonstrating the approach and output of each goal
- MITRE ATT&CK Mapping
- SOC Detection and Prevention GAP Analysis
- Provide short-term and long-term recommendations to detect and prevent the attacks
- Lessons Learned
- Report Presentation

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

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**

Unauthorized internal access to the client's environment

- Aujas Team identified user credentials by leveraging a combination of phishing attacks and compromised credentials sourced from recent security breaches .
- They were able to bypass two-factor authentication on the VPN console.

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 Core Banking Application.
- They modified customer details in Core Banking Application.

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

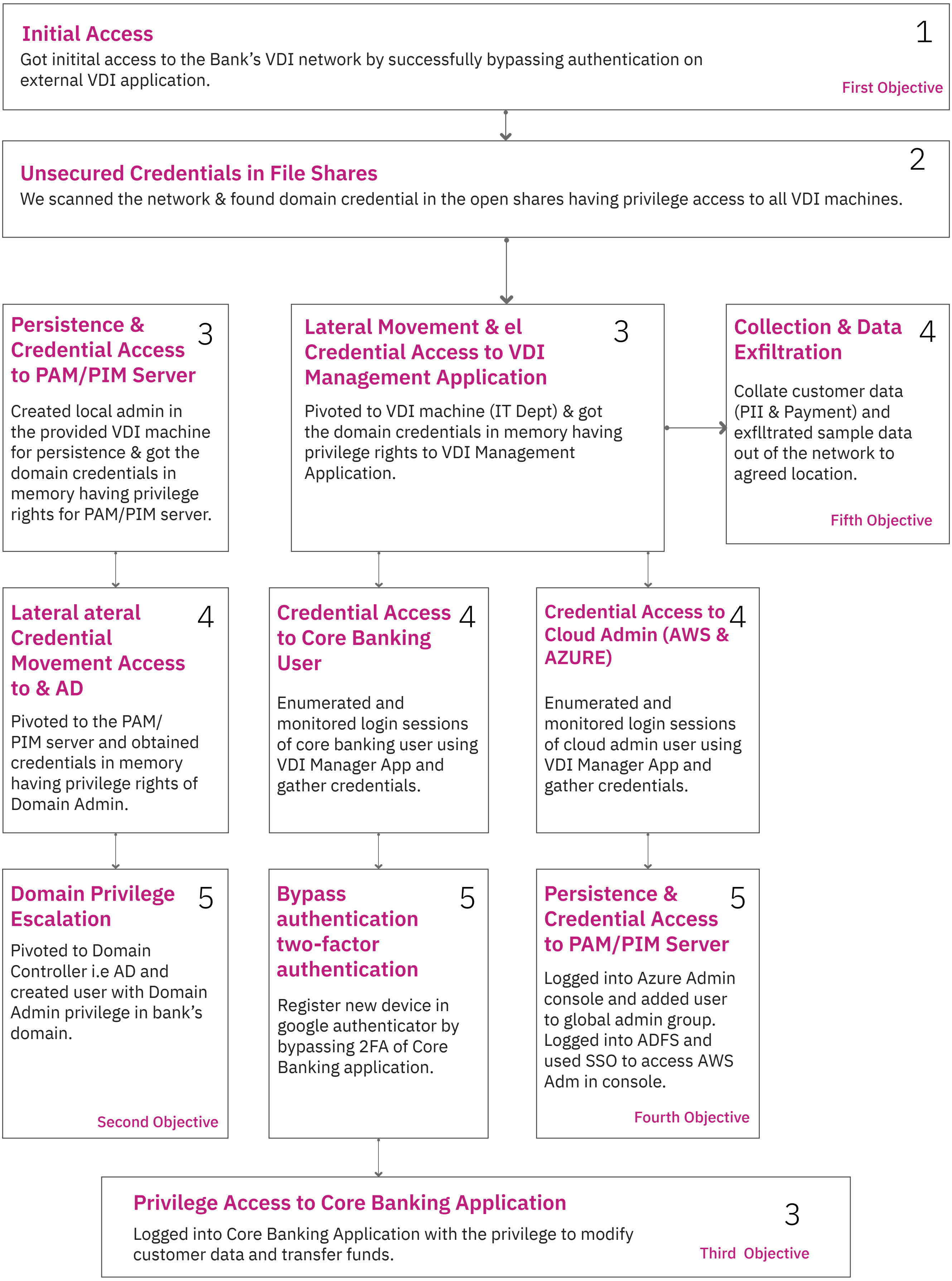
- The team got privileged access to the Bank's Azure and AWS environments.
- They added a rogue Global Administrator to the Azure environment.

Ex-filtrate customer and card information

- The team accessed financial data and PII data ((Aadhar, PAN, Passport, bank statements etc.).
- They exflltrated 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



Initial Access 1

Got initital access to the Bank's VDI network by successfully bypassing authentication on external VDI application.

First Objective

Unsecured Credentials in File Shares 2

We scanned the network & found domain credential in the open shares having privilege access to all VDI machines.

Persistence & Credential Access to PAM/PIM Server 3

Created local admin in the provided VDI machine for persistence & got the domain credentials in memory having privilege rights for PAM/PIM server.

Lateral Movement & el Credential Access to VDI Management Application 3

Pivoted to VDI machine (IT Dept) & got the domain credentials in memory having privilege rights to VDI Management Application.

Collection & Data Exfiltration 4

Collate customer data (PII & Payment) and exflltrated sample data out of the network to agreed location.

Fifth Objective

Lateral ateral Credential Movement Access to & AD 4

Pivoted to the PAM/ PIM server and obtained credentials in memory having privilege rights of Domain Admin.

Credential Access to Core Banking User 4

Enumerated and monitored login sessions of core banking user using VDI Manager App and gather credentials.

Credential Access to Cloud Admin (AWS & AZURE) 4

Enumerated and monitored login sessions of cloud admin user using VDI Manager App and gather credentials.

Domain Privilege Escalation 5

Pivoted to Domain Controller i.e AD and created user with Domain Admin privilege in bank's domain.

Second Objective

Bypass authentication two-factor authentication 5

Register new device in google authenticator by bypassing 2FA of Core Banking application.

Persistence & Credential Access to PAM/PIM Server 5

Logged into Azure Admin console and added user to global admin group. Logged into ADFS and used SSO to access AWS Adm in console.

Fourth Objective

Privilege Access to Core Banking Application 3

Logged into Core Banking Application with the privilege to modify customer data and transfer funds.

Third Objective

About **Aujas Cybersecurity**

Aujas Cybersecurity -An NSEIT Company empowers clients with enhanced security resilience by minimizing the potential for attacks, threats, and risks. We specialize in architecture risk analysis, comprehensive threat modeling, rigorous penetration testing, and secure coding guidelines. By partnering with us, you can strengthen your security defenses and maintain a robust security posture.

For more information, visit us at www.aujas.com or write to us at contact@aujas.com.

Cupertino | Dallas | Jersey City | Ottawa | Riyadh | Dubai | Mumbai | New Delhi | Bangalore

Follow us at: