VAPT Case Study

For

Banking Industry Client

Client Profile:

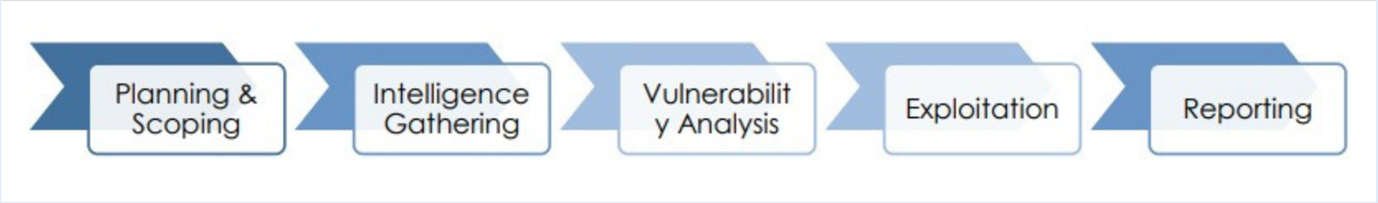
A leading Co-Operative Bank with a robust online banking platform and multiple branch offices in Gujrat. Providing multiple banking solutions.

Challenges Faced by the Client:

- Concerns about the security of network infrastructures across their branches.
- To check potential vulnerabilities in the internal and external networks.
- Ensuring compliance with stringent financial regulations.

Solutions Provided by IBN:

- Network Penetration Testing: Conducted both internal and external network VAPT to identify vulnerabilities and secure the network infrastructure.
- Compliance Check: Ensured all security measures met regulatory requirements.
- Methodology Used:



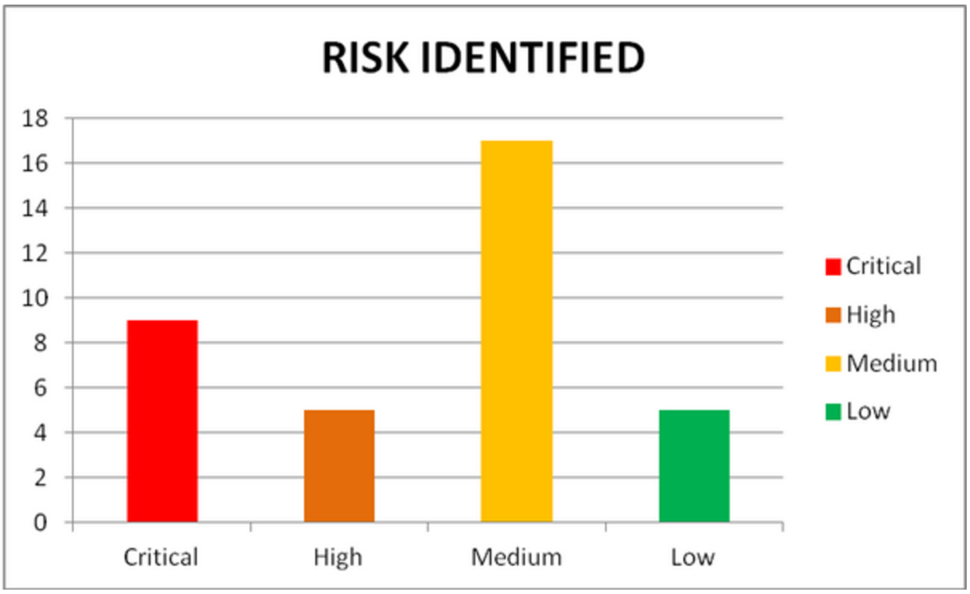
- Technology / Tools Used
  - OWASP Top 10 Standard
  - Nessus Kali
  - Linux Nmap
  - Metasploit
  - Wireshark
  - Custom scripts

- Key Findings

  The VAPT project identified several critical vulnerabilities that could potentially expose the bank to security risks. Some notable findings include:

  - Outdated Software: Numerous instances of outdated software versions were identified, including operating systems, network devices, and web application frameworks. These outdated systems were susceptible to known vulnerabilities that could be exploited by attackers.
  - Weak Authentication Mechanisms: The evaluation revealed weaknesses in the bank's authentication mechanisms, such as weak password policies, inadequate multi-factor authentication, and insufficient session management controls, which could lead to unauthorized access.

  Insufficient Network Segmentation: The internal network lacked proper segmentation, allowing an attacker to move laterally within the network and gain unauthorized access to sensitive systems and data.



- Recommendations and Remediation

  Based on the findings, the VAPT project provided the following recommendations to client:

  a) Regular Patching and Updates: Implementing a robust patch management process to ensure timely updates of all software and firmware across the network and systems, minimizing the risk of known vulnerabilities being exploited.

  b) Strengthening Authentication: Enhancing password policies, implementing multi-factor authentication, and improving session management controls to ensure strong and secure access to the bank's systems and applications.

  c) Network Segmentation: Implementing a proper network segmentation strategy to isolate critical systems and prevent lateral movement in case of a breach.

Benefits Observed from the Client:

- Enhanced security of their internal and external networks.
- Identification and remediation of critical network vulnerabilities.
- Achieved regulatory compliance, avoiding potential fines and penalties.