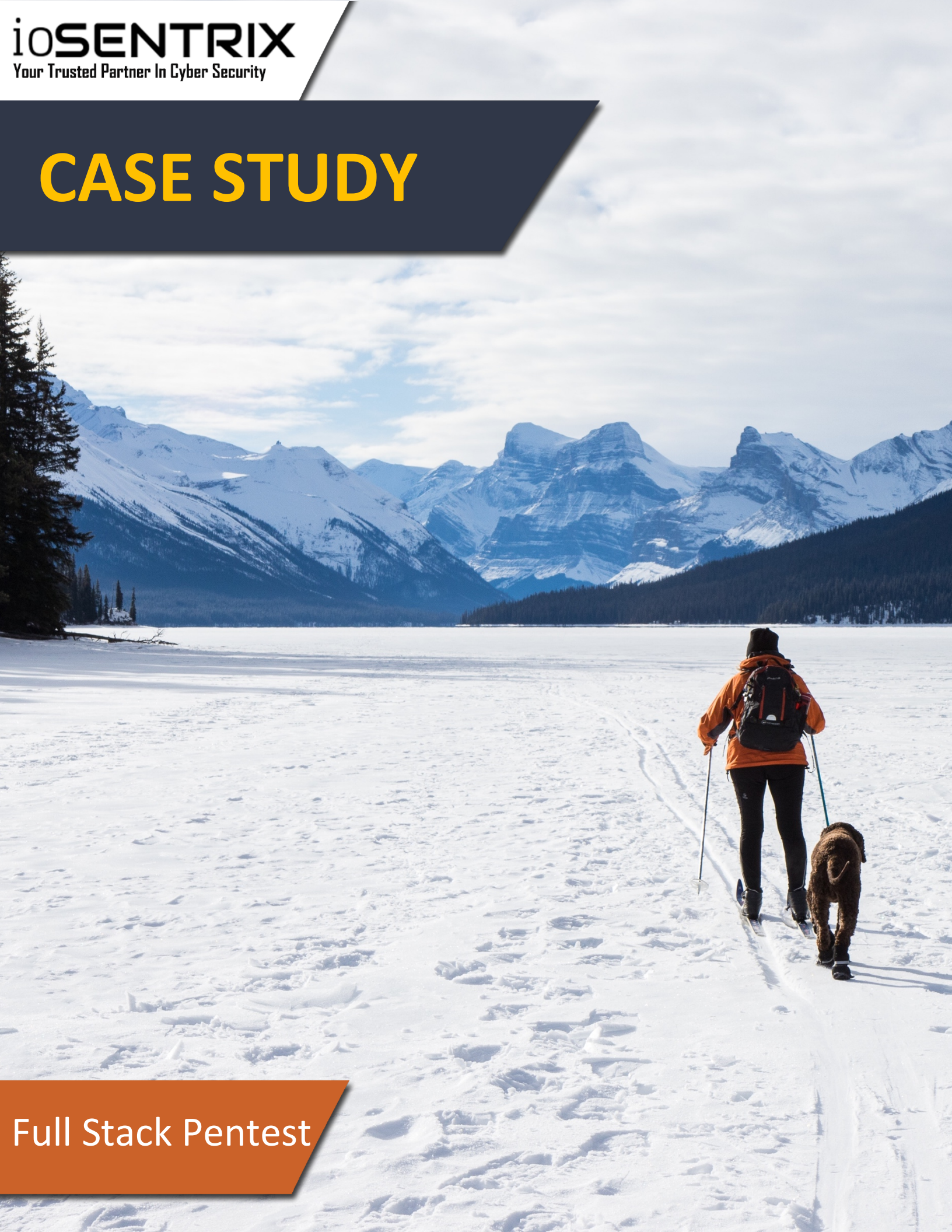
ioSENTRIX
Your Trusted Partner In Cyber Security

CASE STUDY



Full Stack Pentest

Introduction

Today's applications are much complex in nature and consist of several dependencies such as Open Source Software (OSS), libraries, application servers, web-servers, etcetera. A vulnerability at any layer of the technology stack could threaten the security of your application.

In full stack assessment, our experts evaluate all the dependencies that are required by the application to perform its business operation. More specifically, the security of application itself, underlying dependencies such as OSS, libraries and network infrastructure is reviewed to provide comprehensive coverage.

Background

A leading advisory service provider in the US engaged ioSENTRIX to perform a security assessment on their Citrix deployment of a web application prior to “go live”. The web-application was planned to handle legal and financial cases for a variety of different clients. The classification of the information handled by the application was critical; therefore, the app was hosted in an internal locked down (hardened) environment, which was closely monitored by Security Operations Center (SOC). The clients could access the application using Citrix XenApp and XenDesktop, which was exposing only a browser in Kiosk mode to access the internally hosted application.

The Challenge

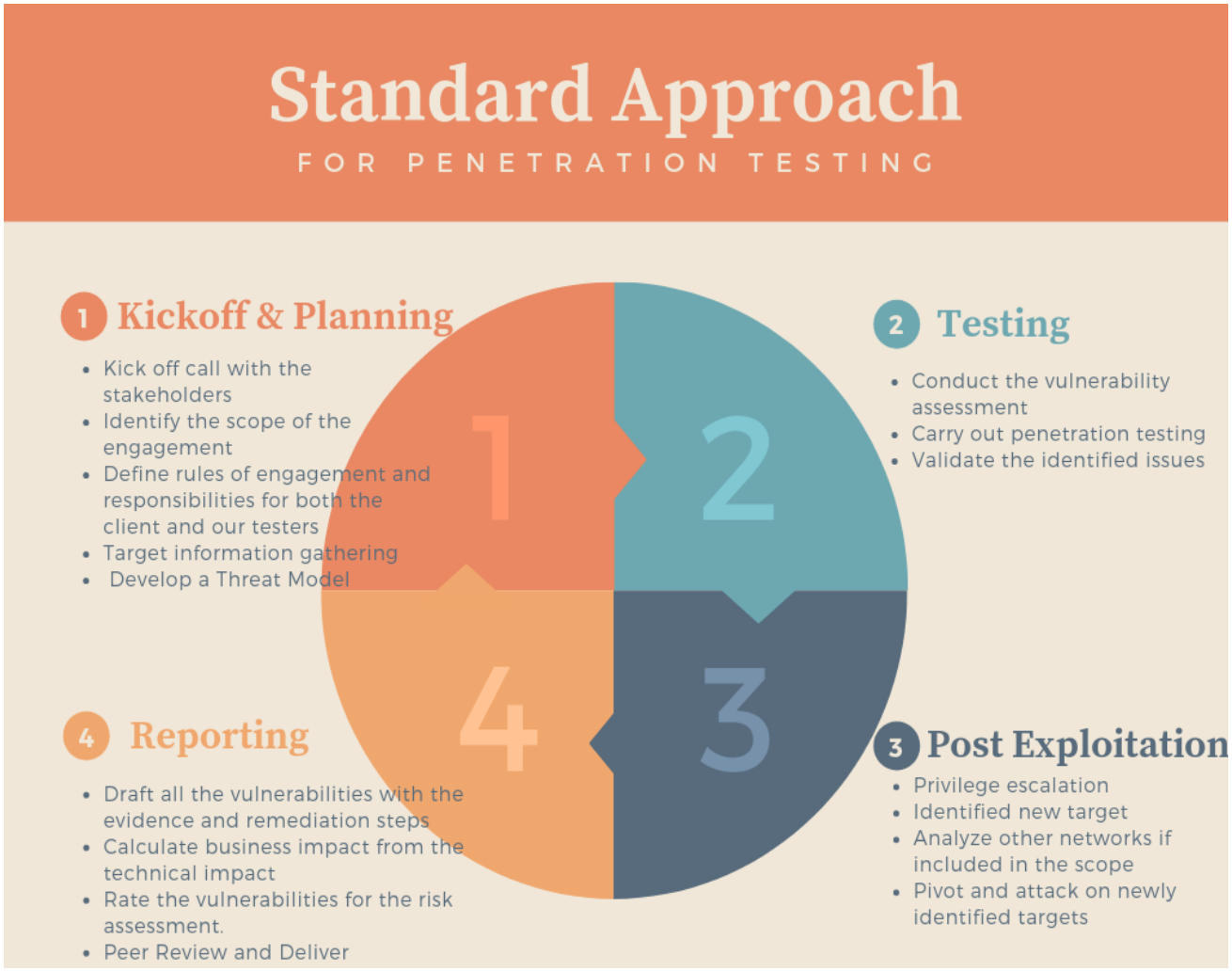
The client was in the challenging situation of not knowing what they don't know -- in terms of risks, they could be vulnerable to.

After consulting with ioSENTRIX, the client understood that the risk is not only about the internally hosted web-application, but also about the infrastructure hosting the Citrix application. Thus, the infrastructure must also be assessed. It had to be explained that a review of the Threat Landscape was essential.

ioSENTRIX educated how a Threat Model could help the client specifically review potential threat agents, attack vectors, and the structure and flow of software components. Additionally, the technology stacks, tier boundaries, and rings of trust could also be reviewed. Therefore, the client agreed to conduct a Full Stack black-box penetration test -- that includes testing the network infrastructure as well as the web application hosted on the internal network.

Our Approach & Process

Figure 1 below depicts our standard approach for Full Stack penetration test



With a team of 2 testers for 3 weeks, we were able to compromise the entire in-scoped network infrastructure and found several issues in the web application as well.

Our testers started by breaking out the restrictions enforced by the Citrix environment. Once they were able to launch the internal utilities such as Explorer or Notepad, they started internal network reconnaissance for further exploitation. During this phase, they discovered several other internally hosted web-applications, which were considered “out of scope”.

In the post-exploitation phase, our testers were successful compromising the system in terms of escalating privileges and obtained unauthorized access to the Domain Controller, as an Administrator.

On the web-application side, our Testers were able to find major vulnerabilities ranging from Cross-Site-Scripting (XSS) to Missing Authorization Checks that would normally protect the access to the critical data.

We concluded with a detailed Report of Findings, which outlined exploitable vulnerabilities details, severity ratings based on NIST standards, evidence and remediation strategies. We also helped the client with risk management support in identifying major vulnerabilities with the most critical/severe ratings for prioritization, given the threat landscape with a 30 day re-test once they are fixed by the client.

The Results

The client benefited in having a better understanding of their risk landscape. Upon receipt of the report, the client reviewed the results with their technical staff and started implementing the recommended remediations. They were pleased with the end results and invited ioSENTRIX to expand the scope of work to review the entire stack to ensure more comprehensive security. In the end, the client was satisfied that they were able to launch the product on time and with the security confidence -- that their customer's data and their infrastructure was secure.

About ioSENTRIX:

ioSentrix LLC is a Security Consulting firm. We provide a wide range of security consulting services to our clients worldwide. Our list of clients spans the fortune 500, large enterprises to small start-ups, financial institutions, and several high-tech companies.

We are an innovative consulting company offering a full range of cyber security services to businesses of all sizes, tailored to meet any budget requirements. We help our clients by identifying, mitigating and preventing vulnerabilities in their software, infrastructure, and cloud.

We offer a comprehensive vulnerability assessment that includes design-review, threat model, penetration test, code review, and open source software security. We've got the necessary tools and the expertise to secure your business so you can focus on growing it.

Learn more about our services at **https://www.iosentrix.com.**

ioSENTRIX LLC.

150 S. Sterling Blvd, Suite 543
Sterling Virginia 20164 (USA)

Sales: 1 (888) 958-0554
Email: sales@iosentrix.com