novacoast

SECURITY ASSESSMENT

Case study:
Internal infrastructure

Industry	Business	Company size	Reason for assessment
Medical	**Public Hospital**	**10,000+**	**Routine penetrations testing for HIPPA compliance**

Situation: Small misconfigurations lead to big internal network breaches

Today, many organizations deploy numerous technologies to function effectively. As new hardware and software is introduced—from appliances, to business and productivity software, and operating systems—the potential to misconfigure access and permissions settings increases. Even simple misconfigurations can lead to expansive breaches.

Read how one hospital partnered with Novacoast in a routine penetration test, exposing a simple JMX Server misconfiguration that allowed full domain access.

Novacoast assessment: Internal infrastructure

As part of an internal infrastructure assessment, the Novacoast team deployed a testing node. Selecting a regular user segment—a role reflecting the lowest possible access and permissions settings—they were able to test the strength of the system, mimicking the likely scenario of an external breach. No other authentication was provided.

Solution: Gained access to internal network with leaked software

The Novacoast team discovered a server running a misconfigured Java JMX agent that didn't require authentication. With entry to the machine, the team was able to apply post-exploitation techniques to obtain full domain administrator privileges.

Outcome: Short-term remediation, long-term security strategy

This case study demonstrates how inconspicuous configuration missteps can lead to compromising an otherwise secure network. Ultimately, the Novacoast team delivered an actionable, short-term remediation solution and long-term strategy to help the hospital increase network security as their data management and protection needs matured.

Routine pentests with Novacoast can help your team gauge security posture strength and identify opportunities to improve.

Ask yourself—are your systems reliably secure?

- ✔ Are there strong password policies in place?
- ✔ Are your employees' credentials securely managed?
- ✔ Do you have 24/7/365 access and behavior monitoring?
- ✔ Is MFA enabled on all critical services?