RED TEAMING

“Stay Ahead of Threats with Our Red Teaming Service”

Introduction

Noventiq is a leading global solutions and services provider in digital transformation and cybersecurity. We help organizations to transform and operate efficiently and securely in an increasingly digital economy. We are committed to delivering for our customers wherever they are using our globally accumulated knowledge and proficiency.

Red Teaming is a full-spectrum, adversarial simulation exercise aimed at evaluating the effectiveness of an organisation’s security program. Unlike standard security checks, Red Teaming involves mimicking real-world attackers' tactics, techniques, and procedures under controlled conditions to test how well a system can withstand an attack from a motivated adversary. IT can uncover vulnerabilities in physical, digital, and human security elements and provide actionable insights to enhance the organisation's security strategies and responses.

HOW RED TEAMING DIFFERS FROM VA/PT

- **Scope and Depth:** While traditional assessments like VA/PT focus on specific systems or applications, Red Teaming is broader, assessing the organisation’s resilience against attacks across all vectors.
- **Real-World Attack Simulation:** Red Teams use techniques that mirror actual attacker behaviour, creating realistic scenarios that test the organisation’s defences as they would occur in the real world.
- **Strategic Perspective:** Red Teaming is as much about understanding the organization’s strategic response to incidents as it is about finding specific vulnerabilities. It looks at the bigger picture, including how well policies, procedures, and controls work together.
- **Objective-Driven:** Red Teaming is goal-oriented, often with specific objectives such as gaining access to high-value targets, which differ from the more vulnerability-focused goals of VA/PT

TYPICAL RED TEAMING OBJECTIVES

COMPROMISING KEY BUSINESS PLATFORMS
Compromising and gaining access into key business platforms such as CRMs, Back-Office Platforms, Management Portals, etc.

CXO MAILBOX
Accessing & leveraging emails of top management

LAN ACCESS
Gaining access into the corporate network

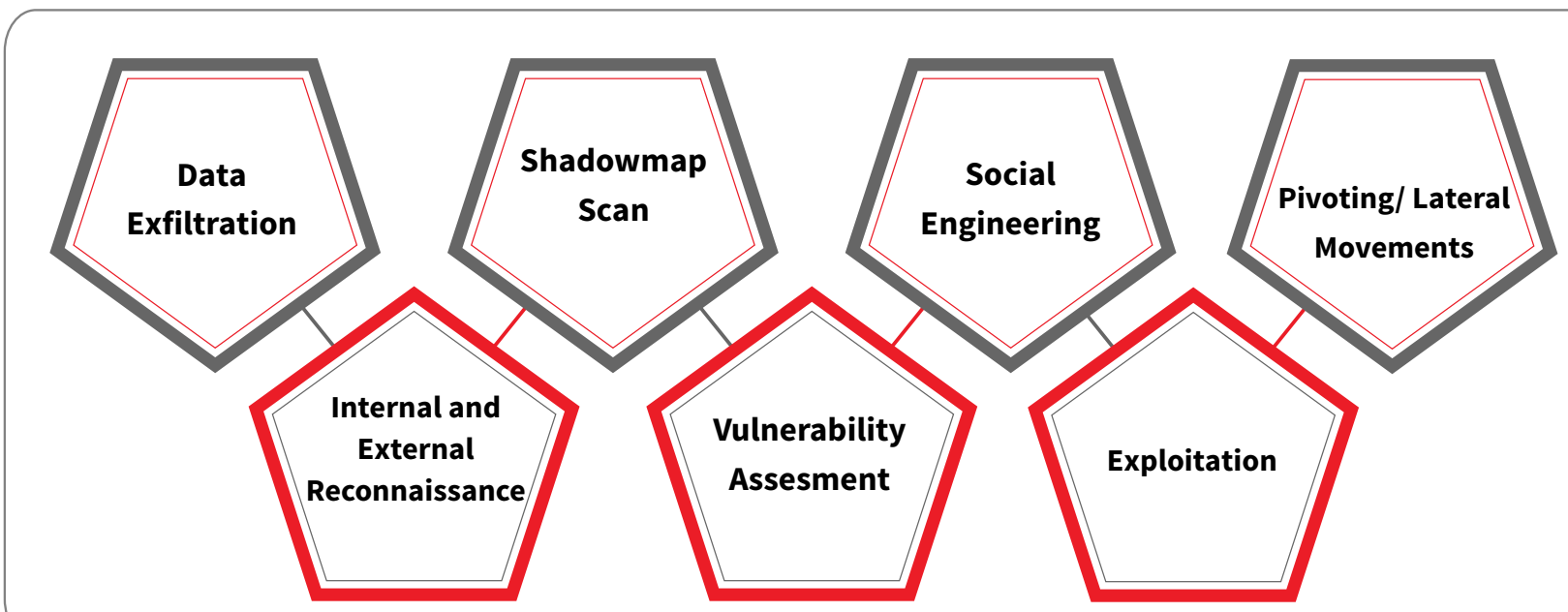
INTELLECTUAL PROPERTY
Gaining access to proprietary source code, designs, plans and other highly confidential corporate data.

EMPLOYEE ACCOUNTS
Compromising employee accounts to key portals

COMPROMISE CLOUD
Gaining access to AWS & Azure keys, buckets, etc

ACTIVE DIRECTORY
Compromising AD administrative credentials

THE RED TEAMING PROCESS



BENEFITS OF RED TEAMING

- **Holistic Discovery of Security Vulnerabilities:** Red Teaming uncovers hidden weaknesses across the organisation's security infrastructure that automated tools or routine checks might miss.
- **Real-World Scenarios:** By simulating real attack scenarios, Red Teaming identifies exploitable vulnerabilities rather than theoretical risks.
- **Comprehensive Coverage:** It assesses technical flaws andorganisational and human factors that attackers could leverage.
- **Response Efficacy:** Red Teaming tests the organisation's incident response plan in action instead of only in theory, highlighting areas for improvement.
- **Team Readiness:** It evaluates whether the incident response team can detect and respond to an attack quickly and effectively.
- **Security Control Efficacy:** Red Teaming offers a reality check for the effectiveness of existing security controls against sophisticated attack strategies.
- **Continuous Improvement:** The feedback loop from Red Teaming informs continuous improvement cycles for security controls, ensuring they evolve to counter new threats.

NOVENTIQ
Global expertise, local outcomes

https://noventiqgcc.com

Noventiq Bahrain
Phone: +973 77080711 - eMail: bahrain@noventiq.com

Noventiq Oman
Phone: +968 24-66-7714 / +968 79130016 - eMail: oman@noventiq.com

Noventiq Saudi Arabia
Phone: +966 55 136 7783 - eMail: SaudiArabia@noventiq.com

SCAN ME