PROELIANS

PROACTIVE CYBER SECURITY

Assumed Breach Assessment

Assumed Breach assessments are designed to simulate controlled and realistic cyber attacks and test your ability to protect your most critical assets.

With a foothold inside your internal infrastructure **Proelians** will perform stealth attacks to gain access to the predefined targets. This service will help you in identifying vulnerabilities and assess the detection and response capabilities of your Blue Team.

Why would you benefit from an Assumed Breach assessment?

The main benefits of conducting a red team assessment are:

- Identify whether your most critical asset is vulnerable to cyber attacks
- Assess your Blue Team to detect, respond and prevent cyber attacks
- Uncover unconventional vulnerabilities that would not be typically identified with traditional penetration tests
- Provide an evidence-based risk report to directors, senior-level management or stakeholders

Our Methodology

Scoping

Proelians will define with you the rules and the boundaries of the Assumed Breach assessment, also ensuring all your requirements are carefully considered.

Execution

Red team assessment pursues a stealthy and dynamic attack path in the attempt to compromise the predefined targets through the following stages:

- **PERSISTENT ACCESS** Establish a reliable and stable command and control channel by compromising multiple systems
- **PRIVILEGE ESCALATION** Obtain the highest level of privileges in systems or applications
- **LATERAL MOVEMENT** Move and compromise predefined target applications or systems that hold critical or sensitive asset
- **DATA EXFILTRATION** Transfer critical or sensitive asset out the organisation's boundaries

Delivery

When the Assumed Breach assessment is complete, Proelians will provide a report containing the following sections:

- Executive summary for directors, senior-level management or stakeholders
- Exploitation path scenarios for post-assessment analysis
- Technical recommendations for fixing discovered vulnerabilities
- Strategic recommendations for long-term improvement
- Indicator of compromises mapped to the ATT&CK framework for Blue Team investigation

Along with your report, Proelians will present the results in a post assessment briefing which gives the opportunity to discuss the findings and recommendations.

In addition to the above, Proelians will provide the Blue Team access to the Red Team's Security Information and Event Management (SIEM) console. Unlike the report, this SIEM console would give much more visibility to the Blue Team when auditing logs of all activities performed during the assumed breach assessment.

Proelians can also assist Blue Team with the following tasks:

- Review of the audit logs and alerts to check if there are any trace of the activity performed by Proelians
- Assist your SOC or Blue Team to configure alerts in order to detect these attacks
- Test the newly configured alerts by re-running the attack scenarios of the assumed breach assessment

Why Proelians ?

We are not just another independent security firm. With more than 10 years of experience in Cyber security our commitment is to provide top-quality services that meet your expectations. If you are willing to try us, feel free to contact us and we will get back to you as soon as possible.

Flexible - Trusted - Secure - Unconventional