CALIAN
Confidence. Engineered.

Purple Team Exercise

A simulated attack conducted by an ethical hacker aiming to identify vulnerabilities based on pre-defined scenarios mimicking real-world compromised assets.

Objectives

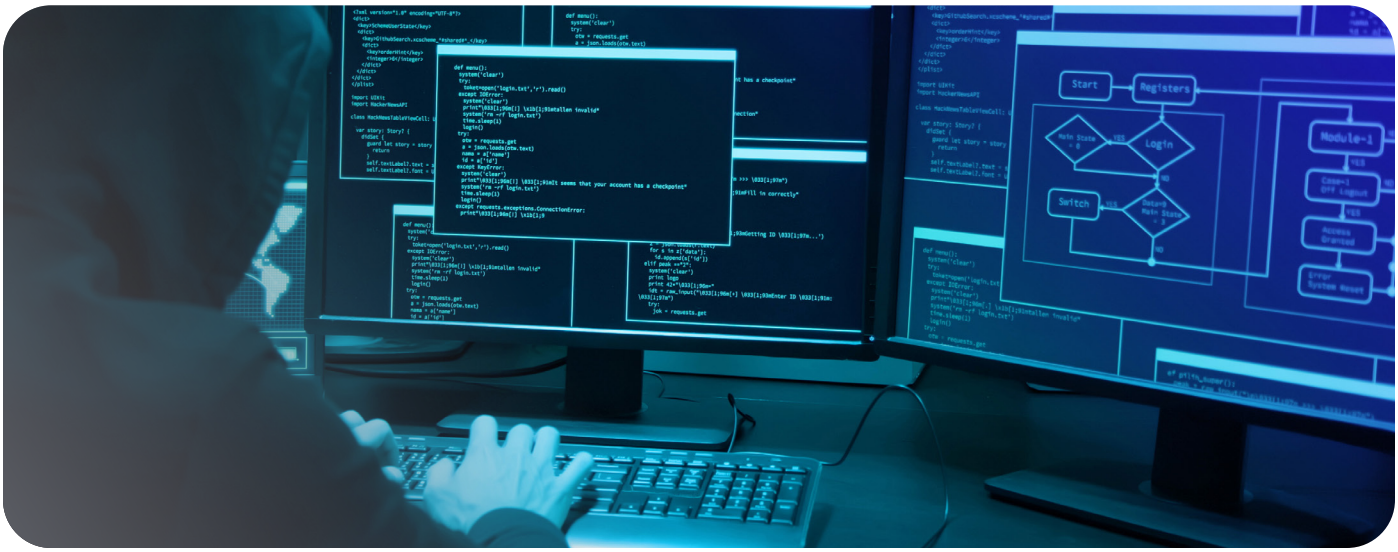
If an internal desktop is compromised by a threat actor through a phishing/vishing scam, how far can the threat actor go? This exercise:

1. Identifies the effectiveness of the security controls locally installed and whether they can prevent bypassing and evasion tactics
2. Validates the robustness of the security on the network if it can prevent lateral movement from a compromised asset
3. Tests the effectiveness of the endpoint protection to prevent successful privilege escalations
4. Tests the effectiveness of the monitoring solutions and blue teams in detecting and preventing malicious attempts

Outcomes

The results of this exercise:

1. Provide visibility and awareness of the exploitation paths in the environment under the assumption of a compromised account/asset, and an evaluation from a measure of the impact of possible breaches of this nature
2. Help internal teams address the gaps in security systems and enhance their configuration for more efficient prevention
3. Support the SIEM configuration, and the company's detection and prevention response program for more efficient incident response technologies



Scope of service

The test's starting point is an assumed breach involving credentials and a workstation. An adversarial team resource will try to vertically escalate privileges on this asset applying bypassing tactics to evade security. Many other use cases can be defined based on the customer's infrastructure model, some examples are:

1. User working remotely
2. Application servers accessed by different user roles
3. VDI portals

Out of scope for this delivery:

Remediation support

Deliverables:

1. A report with an executive summary, the enumeration and exploitation attempts detailed
2. Recommendations for each flaw identified with the principles that can be applied to all security vendors
3. A walkthrough session with the technical team to review the results and lessons learned
4. Requirements:
5. Define the use cases (recommended defining at least two)
6. Access to the targeted systems

calian.com/**itcs**
For more information, contact: itcs@calian.com

calian.com | info@calian.com | 1.877.225.4264 |

Contract Service: Adversarial Simulation – Assumed Breach Assessment

Duration: 2 weeks+, depending on the scope

Technical Level: L3 security specialist, certified ethical hacker