## CYBER ATTACK SIMULATION – Red team

Red Team services provide clients with a realistic understanding of the key cyber security threats and gaps they are facing, as well as the mitigation and response capabilities they possess. Rather than testing a single system and/or application, Red-Team activity tests the weakest paths in the organizational network. In most cases it is the most cost-efficient way to verify the company’s resilience to a real life cyber attack.

## Describe our Service

## Comsec’s red team provides its clients with realistic cyber-attacks against people (if needed), processes, and technologies. Throughout the course of this exercise, the Red Team engages controlled cyber-attacks against the client’s corporate network to test the entire ecosystem and see how and when one security solution reacts to another– as the goal is to breach the perimeter, gain control over predefined marks and exfiltrate them in case of need.

## Goals

**Breach the Perimeter** – Attack from outside the organization’s facilities, getting inside.

**Lateral Network Movement** – Attack from within the organization’s network and try to move laterally over the network to reach headquarters with elevated network rights.

**Capture the Flag** – Establishing access rights into servers, preferably with Domain Administrator rights.

## Attack levels

The research and exercises are conducted based on a predetermined attack profile. There are four defined levels of attack in which research and execution can take place with different resources. Each level has its own limitations and attack techniques:

1. An attacker who only requests anonymity and needs the cheapest possible access attempts to access systems using open source software. The attacker will be looking for standard vulnerabilities that can be implemented quickly on many servers at once.

2. A novice hacker where a limited budget is available to gain access to the networks of the party under consideration. The attacker will focus more on a specific target and has a focused goal.

3. A professional hacker who works alone, but has professional resources and knowledge to deploy his own exploits against the organization. Specific attacks such as the use of proper written exploits of Social Engineering attacks are used to achieve the goal.

4. The hacker-for-hire. Multiple hackers are hired by an organization to try and breach the external perimeter. The greater the value of the hack, the more resources are used during the attack.

## Why Comsec

Comsec offers a unique approach to Red Teaming services by combining proven work experience and a result-oriented attitude with an arsenal of creative intelligence gathering, infiltration, and attack techniques.

By tailoring the Red Team activity to the client, Comsec is able to accurately identify the most relevant cybersecurity threats and provide the client with pragmatic insights into risk and feasibility. This process also demonstrates to the client their ability to detect and react to threats, and exposes gaps in mitigation techniques and security infrastructure.

While the traditional approach to Red Teaming only focuses on the technical aspects of cybersecurity, Comsec utilizes its renowned ability to analyze business and legal-level threats, risks, and perspectives in security in order to craft a unique and all-encompassing cybersecurity image for clients.

## Consumer Problems

As most of the organizations are taking actions to secure their applications and networks as part of their security policy by conducting penetration tests, they might get a partial overview regarding their readiness to a real world attack performed by a group of hackers. The actual reason for that, is because penetration tests are usually limited in scope and resources and therefore present only the impact against a certain application or system.

The clients may face several limitations that impacts overall security level of the organization:

• Limited insight into cybersecurity threats facing the organization

• Security solutions with unproven efficiency

• Untrained SOC team

• Lack of understanding of the exposure level of the organization

• Lack of insight into the security level of current infrastructure

• Weak business case for various goals such as SOC team improvement/installation, IT maintenance, organizational-level upgrades, etc.

Comsec’s red team services can validate all of the above and provide specific recommendations to mitigate the risks and improve the overall security level in the organization.

## About the Team

Comsec has a variety of Cyber security professionals with different skill sets and experience in conducting red team activities. We act as a real hacking team with full transparency to the POC at the client, to get access to the most valuable assets of our clients.