A read team assessment is done to find as many vulnerabilities as possible in a system. It is generally accomplished with lateral thinking, trying various attacks and considering how to bypass certain defences.   
Here are some best practices to ensure that both the customer and Red Team have a good assessment experience.

**Take the Time to Plan**

Take out the time to plan operations in advance. Though the details of a certain engagement depend upon the environment of the customer, it’s a good practice to proactively plan for potential attacks. By planning initial phases and roles, red team can ensure that the customer gets detailed test during the engagement.

**Document the Plan**

Once done with planning the assessment, always draft a mutually signed document that outlines rules of engagement. Discuss potential attack vectors with customer and get approval for any tactics you plan to use. This is important to prevent legal liabilities later on.

**Use Different Methods**

A hacker can use different methods to conduct the same attack with the help of different techniques and tools. Keeping the test as realistic as possible, mix up your assessment instead of going through a checklist of using same tools and techniques.

**Choose Your Tools Carefully**

When conducting a Red Team assessment, you can conduct various tests with different tools. You can make a choice between tools and techniques using a variety of factors such as efficiency and familiarity.

However, you must consider some important factors when making the choice. One factor is the assessment’s impact on the customer’s system and network. Sometimes, a system that is unstable is brought down due to certain tests or tools. Wherever possible, your red team should use tools that limit this possibility.

**Record Everything**

When conducting a red team assessment, always keep a detailed record of everything. This is beneficial for both the customer and red team members. On the customer’s part, it benefits them with understanding the assessment narrative from the beginning till the vulnerability exploitation. On the team’s part, it helps them figure out the problem if something goes wrong.

**Provide Quantifiable Value**

The results of red team assessment typically include a list of vulnerabilities discovered and the recommendations for corrections. However, to fully satisfy the customer and improve the probability of repeat business, you must provide something of measurable value to the customer. This could be providing additional information, such as demonstrating that your team tested potential attacks of high probability and severity.

All red team assessments are unique and may require different tools and tactics. However, it’s always advisable to follow best practices. Our red team at Aardwolf ensures that all best practices are followed in order to provide maximum value to the customer. To get a quote, get in touch with us today.