Rules of Engagement (ROE)

The ROE is a document that is created at the initial stages of a penetration testing engagement. This document consists of three main sections (explained in the table below), which are ultimately responsible for deciding how the engagement is carried out. The SANS institute has a great example of this document which you can view online here.

Section	Description
Permission	This section of the document gives explicit permission for the engagement to be carried out. This permission is essential to legally protect individuals and organisations for the activities they carry out.
Test Scope	This section of the document will annotate specific targets to which the engagement should apply. For example, the penetration test may only apply to certain servers or applications but not the entire network.
Rules	The rules section will define exactly the techniques that are permitted during the engagement. For example, the rules may specifically state that techniques such as phishing attacks are prohibited, but MITM (Man-in-the-Middle) attacks are okay.

Revision #1
Created 2023-02-11 20:39:04 UTC by Fettlaus
Updated 2023-02-11 21:16:51 UTC by Fettlaus