Ethics

- Rules of Engagement (ROE)
- Hacker Categories
- Scopes

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.

Hacker Categories

Hat Category	Description	Example
White Hat	These hackers are considered the "good people". They remain within the law and use their skills to benefit others.	For example, a penetration tester performing an authorised engagement on a company.
Grey Hat	These people use their skills to benefit others often; however, they do not respect/follow the law or ethical standards at all times.	For example, someone taking down a scamming site.
Black Hat	These people are criminals and often seek to damage organisations or gain some form of financial benefit at the cost of others.	For example, ransomware authors infect devices with malicious code and hold data for ransom.

Scopes

Black-Box Testing

This testing process is a high-level process where the tester is not given any information about the inner workings of the application or service.

The tester acts as a regular user testing the functionality and interaction of the application or piece of software. This testing can involve interacting with the interface, i.e. buttons, and testing to see whether the intended result is returned. No knowledge of programming or understanding of the programme is necessary for this type of testing.

Black-Box testing significantly increases the amount of time spent during the information gathering and enumeration phase to understand the attack surface of the target.

Grey-Box Testing

This testing process is the most popular for things such as penetration testing. It is a combination of both black-box and white-box testing processes. The tester will have some limited knowledge of the internal components of the application or piece of software. Still, it will be interacting with the application as if it were a black-box scenario and then using their knowledge of the application to try and resolve issues as they find them.

With Grey-Box testing, the limited knowledge given saves time, and is often chosen for extremely well-hardened attack surfaces.

White-Box Testing

This testing process is a low-level process usually done by a software developer who knows programming and application logic. The tester will be testing the internal components of the application or piece of software and, for example, ensuring that specific functions work correctly and within a reasonable amount of time.

The tester will have full knowledge of the application and its expected behaviour and is much more time consuming than black-box testing. The full knowledge in a White-Box testing scenario provides a testing approach that guarantees the entire attack surface can be validated.