Limitations and assumptions:

Assumptions:

A pen test should be able to find our any potential vulnerability, from unauthorised access to any malicious activity. The test should cover every system, from frontend to backend server, but also the API of the web site, to expose any vulnerability and security breach.

A pen test should also cover different aspects of security testing and simulation.

Limitation:

Limitation of time: Pen Test will only be carried out for a limited of time. And we only can produce result at a specified period. In fact, attacker would attack a system at any time, anywhere.

Limitation of Scope: Although we are trying to do every known security intrusion and breach tests, but we cannot test everything, especially those unknown security attack methodology from any attacker.

Limitation of access: A pen test is restricted to a target environment, but not every production area of the network.

Limitation of methods and skill sets: A pen test is restricted to use a specific set of methods and skills, to avoid any downtime or system crash of the production network.

Reference:

Aaron, C (2020) *Major Limitations of Penetration Testing You Need to Know,* Available at: *https://www.cypressdatadefense.com/blog/limitations-of-penetration-testing/* (Accessed: 27th May 2021).