Penetration Test Scoping Document Crib Sheet

This document defines the key questions and issues that should be raised during a scoping meeting for a Penetration Test.

- Non-Disclosure Agreement (NDA)
- Point(s) of Contact (POC) for Security Test
- Start date of test and stop date / duration of test
    - When testing is allowed, for example 9am to 6pm (Monday – Friday)
- Systems/Networks/APIs and Applications that are in scope for the test
    - This there are White-listing and Black-listing of all system that fall within scope of the test?
    - What systems/networks/API and Applications are directly out of scope?
    - What systems are a priority to be tested?
- Do you own all the hardware/infrastructure that is to be test?
    - If not (such as with cloud services) do you have permission from the system owners for the test to be conducted.?
- Required Authorization
    - This must be provided on written form
- Key legislation to be covered:
    - Computer Misuse Act
    - Data Protection Act /GDPR
        - Do any of the systems to be tested contain Personal Identifiable Information (PII)
    - Investigative Power Act
    - Human Rights Act
- Acceptable Usage Policy
    - The ability to exploit back systems
    - The ability to install software/applications
    - The ability to create users
- What format does the final report take and what information do they want contained in the report
    - How should vulnerabilities be identified and scored (CVE, CWE and CVSS)
    - What form would they like the final report to take?
- During the test do they want daily wash-up meetings and if so what areas/topics would they like these meeting to covers
- Have the following people that the test may affect been made aware of the test
    - The users if of the system
    - The administrators of the system
    - The owners of the system
    - Any other stakeholders in the system
- For those systems to be tested has the data on these systems been recently back up.
- If an intrusion/data breach is detected how would they like it to be reported
    - Do they have an incident response policy?
    - Do they have a data breach policy?
- How are we to connect to the network to be tested
    - Ethernet – Static/DHCP IP
    - WIFI networks – Please specify SSID
- Are they any access codes/usernames/password that they would like us to use as part of the test?