Requirements for Network Penetration Tests

1. The **list of IP blocks and/or addresses** to be tested.

2. If there are known fragile devices, we would need you to indicate them. Such devices would normally be encountered only in internal networks. Typical examples are very old network devices and voice recording systems.

3. If the target network is an internal network segment that is not accessible from the internet, then we should either be provided with **access to the internal network** (E.g.: via VPN) or should be provided with a PC located in the internal network, with at least 4 Gigabytes of RAM (preferably 8). Any remote desktop solution installed on the PC would be ok for us (E.g.: TeamViewer)

4. Normally, our tests also involve **brief brute-force attacks** against any available services, such as SSH, FTP or RDP. If you prefer this to be out of scope for any or all of the IPs/IP ranges, then please let us know. Systems that have an account lock-out policy should be considered to be out of scope.

5. If no special access arrangements are needed (access via VPN or remote desktop application), then all of our test packets by default would come from **our static IP address**, which we will declare before the test commencement. This aims to help you track our activities and differentiate our test activities from any real-world attacks.

6. The internal **IT Security and IT Operation teams should be notified** about our tests and IP addresses and also, please request that they add our IP to the white list of the security products (E.g.: Firewall, WAF, IPS/IDS). This would help us perform all the test scenarios in a more manageable time frame.

7. If you are using a **hosting provider** for some/all of your servers, please note that your hosting provider(s) may require you to **notify them** a few days before the commencement of the penetration test. Please check with your hosting provider if they have such a requirement (Usually referred to as "Penetration testing policy").