Strategi ujian penembusan:

Ujian ini mensimulasikan tindakan dan prosedur penyerang sebenar dengan sangat mengehadkan maklumat yang diberikan kepada orang atau pasukan yang melakukan ujian terlebih dahulu. Biasanya, mereka hanya boleh diberi nama syarikat itu. Kerana ujian jenis ini memerlukan banyak masa untuk peninjauan, kosnya boleh menjadi mahal

Ujian ini melakonkan serangan dalaman di belakang *firewall* oleh pengguna yang dibenarkan dengan keistimewaan akses yang biasa. Ujian semacam ini berguna untuk menganggarkan berapa banyak kerosakan yang boleh disebabkan oleh pekerja yang tidak puas hati.

Ujian disasarkan dilakukan oleh pasukan IT organisasi dan pasukan ujian penembusan yang bekerja bersama. Ia kadang-kadang dirujuk sebagai pendekatan "lights-turned-on" kerana semua orang dapat melihat ujian dijalankan.

Ujian penembusan jenis ini menyasarkan pelayan atau peranti luaran syarikat yang termasuk pelayan nama domain (DNS), pelayan e-mel, pelayan Web atau *firewall*. Objektifnya adalah untuk mengetahui sama ada penyerang luar boleh masuk dan sejauh mana mereka dapat masuk selepas mereka mendapat akses.

Dalam ujian penembusan jenis ini, hanya satu atau dua orang di dalam organisasi mungkin menyedari ujian dijalankan. Ujian ini boleh digunakan untuk menguji pemantauan keselamatan dan identiti kejadian organisasi serta prosedur tindak bala