Internal penetration test scoping questions

These are the questions a SilentGrid consultant asks when scoping an internal infrastructure penetration test. Answering them first makes the call shorter and the quote more accurate.

"Not sure" is a fine answer. Working out the unknowns is part of what the scoping call is for.

Questions marked **Sizing** help us prepare an accurate quote.

01 Before any test

What prompted the test, and what date does the result need to meet?

Why we ask: the reason sets the depth and report format, and the date fixes the testing window and any retest.

Will testing run against production, staging or a dedicated test copy?

Why we ask: production needs tighter limits on load, data and timing. A test copy allows more thorough techniques.

When can testing run, and are there change freezes or peak periods to avoid?

Why we ask: the schedule is built around them.

Will you want fixes retested?

Why we ask: retesting is agreed at scoping, so it is scheduled and priced from the start.

02 Internal infrastructure

How many sites, VLANs or subnets, and roughly how many hosts?

SIZING

Why we ask: network size sets how long discovery and testing take.

What is the starting point: a network port with no credentials, a standard domain user, or a standard corporate laptop?

Why we ask: each answers a different question: a rogue device, a compromised account or a stolen laptop.

How many Active Directory domains and forests are there, with what trusts, and is Entra ID connected?

SIZING

Why we ask: trusts and hybrid identity extend the attack paths that need testing.

Which segments should be unreachable from the user network: payment card, operational technology, management?

Why we ask: segmentation testing checks those boundaries specifically.

Is the aim broad coverage of vulnerabilities, or reaching a named objective such as a critical system?

Why we ask: coverage testing and objective-based testing are planned differently.

Can testing run remotely through a testing device or virtual machine, or does it need to be onsite?

Why we ask: remote testing needs a device shipped or a virtual machine deployed before the start date.

Which systems are fragile or must not be exploited? Legacy, medical or operational systems.

Why we ask: they are excluded or tested with care so nothing fails under testing.

Discuss your testing priorities

www.silentgrid.com/contact