External penetration test scoping questions

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

"Not sure" is a fine answer. The scoping call helps resolve unknowns.

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 External infrastructure

How many IP addresses, ranges and domains are in scope?

SIZING

Why we ask: this is the main driver of external testing time.

Should testing also find assets you have not listed: subdomains, forgotten hosts, cloud services?

Why we ask: unlisted assets are often the weakest, but ownership has to be confirmed before they are tested.

Which services face the internet: VPN, remote access, email, web portals, file transfer?

Why we ask: remote access gateways are among the most targeted systems on any perimeter.

Are any hosted by a cloud provider, CDN or other third party?

Why we ask: some providers need notice, and ownership must be confirmed.

Should password spraying against exposed logins be included, and what is the lockout policy?

Why we ask: spraying finds weak passwords, but can lock staff out if the policy is not known.

Is there filtering such as an intrusion prevention system or geo-blocking, and should testers be allowed through?

Why we ask: it decides whether the test measures the service or the filter in front of it.

Discuss your testing priorities

www.silentgrid.com/contact