Wireless penetration test scoping questions

These are the questions a SilentGrid consultant asks when scoping a wireless network 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 Wireless networks

How many sites and buildings, and which networks: corporate, guest, devices, hidden?

SIZING

Why we ask: each site and network is assessed on location.

How do corporate devices connect: a shared key, certificates (EAP-TLS), or domain credentials (PEAP)?

Why we ask: networks that accept domain passwords are open to evil twin credential capture. Certificate-based networks are not.

Should isolation between guest and corporate networks be tested?

Why we ask: a guest network that reaches internal systems is a common and serious finding.

Are rogue access point and deauthentication testing allowed, and when?

Why we ask: deauthentication disconnects real users, so it needs approved timing.

If access is gained, should testers pivot into the internal network?

Why we ask: it shows what an attacker in the car park could reach.

Discuss your testing priorities

www.silentgrid.com/contact