# Scoping & Technical Environment Questions

## Engagement Type

Will this be a clear box (information shared in advance) or black box (no prior knowledge) assessment?

Clear box is typically faster, cheaper, and more thorough.

If black box: skip ahead to authorization, contact, and logistics questions.

Is social engineering in scope?

Social engineering bypasses security control by manipulating people rather than technologies. It is a primary tool in all hacker’s toolboxes. Unlike traditional hacking, it exploits human trust rather than software flaws, and is often relied on for initial access to computing resources.

Including social engineering as an element of your pen test reveals how susceptible your people and processes are—not just your technologies. It helps uncover real-world attack paths that purely technical testing would miss.

Phishing (email, text messaging, etc)?

Voice phishing (vishing - phone calls)

In-person (showing up for an appointment, or as an ISP rep, etc.)

For social engineering, execs and staff are in-scope by default, to be amended within the SoW

Family members and others to be specifically included or excluded

This holistic approach reflect real-life attackers’ workflows and exposes how your group can best defend against these attacks.

CrowdStrike’s 2025 Global Threat Report highlights that vishing (voice‑based social engineering) and other social engineering tactics to steal credentials surged 442% in the second half of 2024—a massive escalation in how adversaries exploit human trust.

https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0

Verizon’s 2025 Data Breach Investigations Report (DBIR) lists threat actor motives for social engineering were 55% financial and 52% corporate espionage.

<https://www.verizon.com/business/resources/Tbd4/reports/2025-dbir-data-breach-investigations-report.pdf>

## Environment & Architecture

What is the network architecture for:

Corporate HQ

Executives’ residences

What network hardware brands/models are used at:

HQ

Executive homes

What security controls are in place? (HQ + homes)

IDS/IPS (intrusion detection system/intrusion prevention system), network firewalls, host-based firewalls, etc.

Endpoint protection (on servers and workstations)

Managed detection and response (MDR)?

Are there IoT or smart devices at the executive homes on the same networks they use for work (e.g., smart TVs, security cameras, HVAC)?

## Scope of Infrastructure

What are the IP ranges we are permitted to test?

How many on-network devices:

Servers

End-user workstations

Mobile devices (BYOD policy?)

Total endpoints across all sites

How many user accounts exist in:

Active Directory / LDAP

Cloud IAM (e.g., Okta, Azure AD)?

How many physical locations are in scope (HQ, exec homes, others)?

Do execs connect differently than regular remote workers?

How do work-from-home employees connect (VPN, ZTNA, etc.)?

## People & Authorization Questions

Who will provide written authorization for the pen test?

(This is essential for liability and legal clearance, i.e. our "get out of jail free card".)

Who is the daily contact during the engagement?

For scope clarifications, change control, and reporting anomalies

Which employees will know the test is happening?

Will they inform teams prior to the engagement?

# Methodology & Logistics Questions

Do you have a preferred timeline or hard deadline?

Are there blackout dates/times for testing (e.g., executive travel, critical ops)?

Have you had pen tests previously at:

HQ

Exec homes

If yes: can we see prior statements of work and reports?

Is physical security in scope?

At HQ?

At executive homes?

Is wireless profiling in scope?

Passive scan during business hours?

After-hours scanning with APs off?

Active spectrum scan (adds ~$5K in hardware/license costs)

Are cloud services made accessible to off-network devices such as mobile phones (e.g., GitHub, Jira, ServiceNow)?

Do execs use any cloud services for company work (e.g. Dropbox, Box, Gmail, etc.)?

Are these in scope?

Is the home router/modem managed by the company or by the ISP/resident?

# Shadow/Strategic Discovery Questions

These are for you only—please don’t ask directly, but if you can suss out answers, they’ll help me tailor the approach and report tone.

What’s driving this test—compliance, incident response, risk management, or something else?

Is there a pending audit or third-party certification (e.g., SOC 2, ISO 27001)?

What would make this pen test “valuable” in their eyes—tech findings, compliance checkboxes, political cover, executive peace of mind?

Who will read the report: IT staff, execs, legal/compliance?

For pen testing at company HQ and at exec’s homes, here are some options. Each location (HQ, each exec’s home) can have its own option. Unless physical security is in scope, I recommend option 1; this allows me to work each site in parallel and puts the least burden on execs and their staff. If physical is in scope, we could still go with option 1, and I would install the Raspberry Pis while I’m at each location:

| **#** | **Approach** | **Summary** | **Logistics** | **Cost** | **Depth of Coverage** | **Privacy Impact** | **Ideal When…** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **Fully Remote via Shipped Raspberry Pi** | Ship Raspberry Pi, exec/staff plug it into network and power, I access remotely over VPN | Ship + remote access setup | $$ | High (internal scans, active/passive recon) | Low-Med (exec plugs in device) | Moderate trust, tech-savvy staff available |
| **2** | **Fully On-Site Testing** | I visit each site and test in person | Travel + coordination | $$$$ | Very High (physical security, RF, social vectors) | High (I’m in their house) | High sensitivity targets, no tech support available |
| **3** | **Drop-In Kit + Drive-By Access** | I ship a Pi and battery rig, then access from nearby (e.g., parked car) | Courier + brief local presence | $$$ | High (Wi-Fi attack surface, passive recon, sniffing) | Med (I’m near but not inside house) | RF-focused, minimal intrusion needed |
| **4** | **Hybrid: Remote Consult + Shipped Device** | Initial scan done remotely, then deeper follow-up via Pi plugged in by exec | Consult + ship device | $$ | Medium-High | Low-Med | Gradual trust-building or phased engagement |