

Penetration Testing Scoping Questionnaire

Fill in the sections for the tests you would like quoted and skip the rest. If you are not sure about an answer, leave it blank and we will cover it on the scoping call.

Return the completed form to info@zerodaysecurity.net, or book a free scoping call at zerodaysecurity.net/book-a-free-scoping-call. Every engagement is quoted at a fixed price, agreed in writing before testing starts.

1. About your organisation

Company name

Your name and role

Email

Industry

Preferred testing window or deadline

e.g. "before our SOC 2 audit in March"

What is driving this test?

- | | | |
|--|--|--|
| ☐ PCI DSS | ☐ HIPAA | ☐ SOC 2 |
| ☐ ISO 27001 | ☐ GDPR | ☐ FedRAMP |
| ☐ Customer / vendor request | ☐ Cyber insurance | ☐ After a security incident |
| ☐ Internal security goal | ☐ Other | |

What are your main security concerns?

- | | | |
|--|--|---|
| ☐ Data breach | ☐ Ransomware | ☐ Account takeover |
| ☐ Insider threats | ☐ AI / LLM misuse | ☐ Third-party / supply chain |
| ☐ Other | | |

Which security controls are already in place?

- | | | |
|---|--|--|
| ☐ Firewall | ☐ EDR / antivirus | ☐ IDS / IPS |
| ☐ Web application firewall | ☐ MFA | ☐ SIEM / log monitoring |
| ☐ Other | | |

Have you had a penetration test before?

- ☐ Yes ☐ No ☐ Not sure

If yes, what did it cover and when?

Which tests would you like quoted?

☐ External network☐ Internal network☐ Web application☐ API☐ AI / LLM application☐ Wireless (Wi-Fi)☐ PCI segmentation

2. External Network Penetration Test

Testing of your internet-facing systems, such as firewalls, VPNs, mail and web servers.

How many IP addresses are in scope in total?

Approximately how many of those are live/active?

Are any in-scope systems hosted with a cloud or hosting provider?

☐ Yes ☐ No ☐ Not sure

If yes, which providers?

e.g. AWS, Azure, Google Cloud, a managed host

3. Internal Network Penetration Test

Testing from the perspective of an attacker or compromised device inside your network.

How many active IP addresses or subnets are in scope?

Approximately how many are workstations?

Approximately how many are servers?

Do you use Active Directory or Entra ID?

☐ Yes ☐ No ☐ Not sure

How would you prefer internal testing to be performed?

☐ Remotely (VPN or jump host)☐ Remotely (testing VM on your network)☐ On-site☐ Not sure

How many office or site locations are in scope?

4. PCI DSS Segmentation Testing

Required under PCI DSS v4.0 Requirement 11.4.5 when segmentation is used to reduce PCI scope.

Do you have a Cardholder Data Environment (CDE) that needs testing?

☐ Yes ☐ No ☐ Not sure

How many network segments or zones need segmentation validated?

Is this for a QSA assessment (ROC) or a self-assessment (SAQ)?

5. Web Application Penetration Test

Please describe one application here. For additional applications, use the notes section at the end or ask us for another copy of this page.

Application name and URL(s)

What does the application do, and who uses it?

How many unique dynamic pages or screens?

Count each distinct page type once; 500 product pages built from one template count as one.

How many user roles should be tested?

e.g. customer, staff, administrator

Will you provide test accounts for each role?

☐ Yes ☐ No ☐ Not sure

Which environment will be tested?

☐ Production ☐ Staging ☐ Development

Is there a web application firewall (WAF) in front of the application?

☐ Yes ☐ No ☐ Not sure

6. API Penetration Test

Approximately how many API endpoints are in scope?

What type of API is it?

☐ REST

☐ GraphQL

☐ SOAP

☐ gRPC

☐ Other

Is documentation available?

e.g. OpenAPI/Swagger specification or Postman collection

☐ Yes ☐ No ☐ Not sure

How does the API authenticate?

e.g. API keys, OAuth 2.0, JWT, session cookies

7. AI / LLM Application Penetration Test

Testing of chatbots, copilots, RAG pipelines and AI agents for prompt injection, jailbreaks, data leakage and unsafe tool use.

What does the AI feature do, and who uses it?

e.g. customer support chatbot, internal knowledge assistant, coding copilot

Which model or provider does it use?

e.g. OpenAI, Anthropic, Azure OpenAI, AWS Bedrock, self-hosted

Does it retrieve information from your documents or databases (RAG)?

☐ Yes ☐ No ☐ Not sure

Can it take actions, such as calling tools, APIs or MCP servers?

☐ Yes ☐ No ☐ Not sure

Who can access it?

☐ Public / customers

☐ Employees only

☐ Both

Is a test or staging environment available?

☐ Yes ☐ No ☐ Not sure

8. Wireless (Wi-Fi) Penetration Test

How many locations are in scope?

Does each location use the same wireless setup?

☐ Yes ☐ No ☐ Not sure

How many wireless networks (SSIDs) at each location?

Is there a guest network whose isolation should be verified?

☐ Yes ☐ No ☐ Not sure

Location addresses or general area

Testing is performed on-site at each location.

9. Testing Logistics

When can testing take place?

☐ Business hours

☐ After hours

☐ Any time

Are any systems, techniques or times off-limits?

Main point of contact during testing (name and role)

Their email and phone number

Emergency / after-hours contact, if different

Do you need a summary letter you can share with customers or auditors?

☐ Yes ☐ No ☐ Not sure

Anything else we should know?

Additional applications, special requirements, previous findings you would like re-tested, etc.

10. In-Scope Targets

List IP addresses, ranges, subnets and URLs. You can also send these separately once a proposal is agreed.

External IP addresses / ranges

Internal subnets

Web applications and API base URLs

What happens next

- 1 We review your answers and follow up on anything that needs clarifying.
- 2 On a short scoping call we confirm scope, timing and access requirements.
- 3 You receive a fixed-price proposal in writing. Nothing starts until you approve it.
- 4 After testing you receive an auditor-ready report and a free retest once fixes are in.

Questions? Email info@zerodaysecurity.net or book a free scoping call at zerodaysecurity.net/book-a-free-scoping-call.