PRACTITIONER RESOURCE

Checklist for Preparing for a Penetration Test Scoping Call

Define business objectives, authorized targets, operating constraints and expected reporting before agreeing the scope of a test.

Edition 2026-11-03 · Updated November 3, 2026 · miami-computer-forensics.com/guides/penetration-test-scoping/

The first scoping call should establish what the business needs to learn and the boundaries within which testing can safely occur. A count of IP addresses or a list of domain names is only the beginning. The team also needs authority, operating constraints, third party permissions, relevant identities and a clear description of the result the organization expects to use. NIST's testing guidance treats planning and analysis as part of the assessment process, not as paperwork added after testing. [1]

State the business objective and the intended audience

Explain whether the work supports a customer requirement, a regulatory obligation, a transaction, a new release, remediation verification or another decision. Identify who will use the result and what evidence they need. A vulnerability scan, a penetration test, an application review and an OT assessment answer different questions. Bring the exact contractual or regulatory wording, because the request defines what the report must show.

Bring the requirement or request that prompted the work, together with the intended completion date and any review meeting. Ask which deliverables are needed: executive findings, technical reproduction detail, remediation guidance, a retest account or a scoped attestation. Agree any assurance wording after the scope is set, so it matches the work performed.

Inventory the targets and the owners who can authorize them

List the network ranges, domains, applications, APIs, cloud environments and other proposed targets. Identify their business and technical owners and distinguish production from development or test. Include externally hosted and third party systems, even when your organization uses them daily. Confirm what the owner and provider permit for each target and record the approval.

For applications, describe the main functions, account roles, authentication process, sensitive workflows and important integrations. State whether source code, documentation or test accounts can be provided through a secure arrangement. Record significant exclusions and why they matter. A small target list can carry a complex authorization model or a high consequence business function.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Describe operating and safety constraints

Identify services that cannot be interrupted, testing windows, change freezes, monitoring arrangements and systems that require a different method. Call out OT, industrial control, medical, safety or physical process dependencies. We scope those systems with their owners under a separately approved assessment approach and operational stop conditions. [2]

Define who can stop the test, how that person will be reached and who can authorize resumption. Agree on the handling of an unexpected outage or a suspected active compromise discovered during testing. Identify backups and recovery arrangements relevant to the proposed work. The rules of engagement, not the time window, define which techniques are authorized.

Prepare identities, access and rules of engagement

Identify the account roles that may be needed, their approval owner and the supported way to deliver credentials. State whether MFA, conditional access, federated identity or device restrictions affect test access. Passwords, tokens, keys and privileged connection details travel through the secure delivery method agreed on the scoping call.

Discuss permitted techniques and prohibited actions explicitly. The rules of engagement should address the target boundary, test sources, timing, escalation, data handling and evidence needed to demonstrate a finding. Clarify whether exploitation, privilege escalation, social engineering, data access or source code review is included. Each one is listed explicitly in the written scope. [3]

Explain prior findings and relevant changes

Identify earlier reports, known unresolved weaknesses, recent incidents and material changes to the environment. Record the dates and scope of prior work so the assessor can distinguish a retest from a new assessment. A previous report focuses the conversation, and current testing shows the current state.

Describe planned releases, migrations or significant provider changes that could invalidate a test's assumptions. Ask whether testing should occur before or after the change and whether follow up work will be needed. If the team wants a comparison over time, agree on what can be compared and what differences in scope or access must be explained.

Agree on evidence, reporting and secure communication

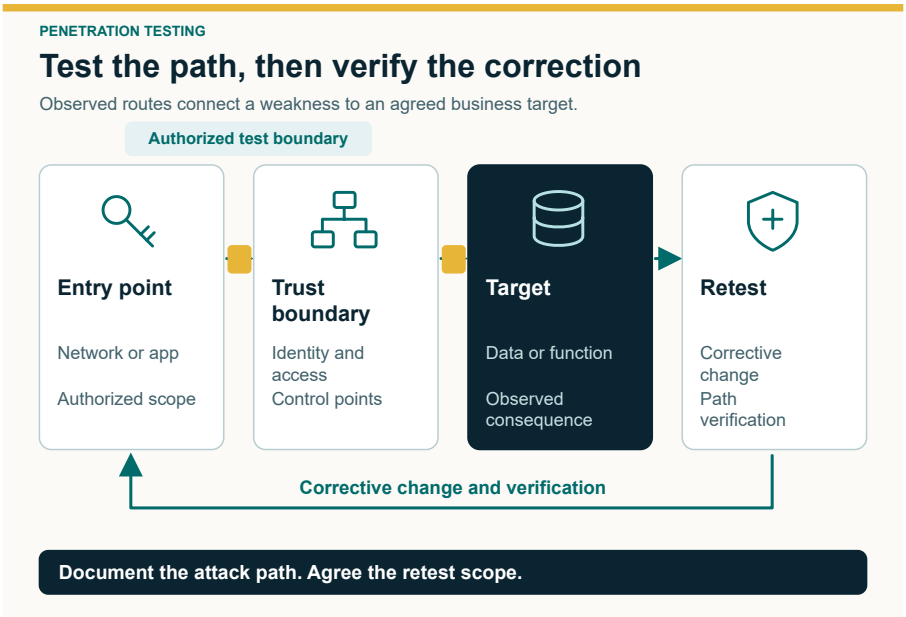
Identify the people authorized to receive findings and the severity of issues that require immediate notice. Discuss how sensitive evidence will be minimized and shared. A finding demonstrates the relevant consequence within the approved scope, and testers collect only the data needed to prove it.

Before the call ends, confirm the remaining inputs needed for a written scope, the owner of each input and the decision date. Ask how the report will distinguish validated findings, unconfirmed observations and untested areas. Record the arrangements for remediation discussion and any retest. A successful engagement gives the business a supported account of the tested conditions, business impact and practical next steps.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Put Your Scope in Front of a Senior Operator

Bring the target list, the requirement behind the test and your operating limits to a free scoping call with a senior GDF operator. On that first call we recommend the testing depth, confirm the rules of engagement and set out the timeline, the deliverables and the retest. Call (786) 219-1210 or the 24/7 hotline at (800) 868-8189, or write to info@evestigate.com. To keep preparing, browse the cybersecurity guide library.



How testing moves from exposure to access to a validated finding.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Information Gathering Q&A Checklist

Complete this record with the system owners and the person sponsoring the test. Mark unknown answers plainly, and record who confirmed each answer and when.

Leave passwords, keys and tokens off this record. Note who controls each credential and how it will be delivered securely, and keep the completed record with the test sponsor.

Who sponsors the test, and who can authorize each target?

Name the executive sponsor, the technical owner of each target and the person who can sign the authorization. Where a provider hosts a target, record who at the provider grants permission and how.

Answer:

Owner, source, date and unresolved questions:

What decision will the report support, and who will read it?

Record the customer requirement, regulation, transaction, release or remediation decision behind the test, the readers of the report and the date they need it.

Answer:

Owner, source, date and unresolved questions:

Which third party hosts, cloud providers or managed services must approve testing?

List each provider, the testing policy that applies and any notice or approval it requires, with the contact who confirms it.

Answer:

Owner, source, date and unresolved questions:

Which account roles and test credentials will testers need?

List the roles to test, the approver for each test account, the MFA or device restrictions that apply and the secure method for delivering credentials.

Answer:

Owner, source, date and unresolved questions:

Which techniques are in scope, and which are excluded?

Record whether exploitation, privilege escalation, social engineering, data access, denial of service or source code review is included, and the reason for each exclusion.

Answer:

Owner, source, date and unresolved questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

What prior reports, open findings and recent changes should testers know about?

Identify earlier reports with their dates and scope, unresolved findings, recent incidents and planned releases or migrations that could change the results.

Answer:

Owner, source, date and unresolved questions:

Who receives urgent findings, and how?

Name the people authorized to receive findings, the severity that triggers immediate notice and the secure channel for sharing evidence.

Answer:

Owner, source, date and unresolved questions:

Which networks, applications, APIs and cloud environments can your organization authorize?

Identify third party ownership and permission requirements.

Answer:

Owner, source, date and unresolved questions:

What are the testing window, stop conditions and escalation contacts?

Identify any OT, safety or production dependency requiring a separate approach.

Answer:

Owner, source, date and unresolved questions:

Primary sources and further reading

Sources checked November 3, 2026.

1: NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (September 2008)
https://csrc.nist.gov/pubs/sp/800/115/final

2: NIST SP 800-82 Revision 3, Guide to Operational Technology (OT) Security (September 2023)
https://csrc.nist.gov/pubs/sp/800/82/r3/final

3: NIST rules of engagement glossary
https://csrc.nist.gov/glossary/term/Rules_of_Engagement

Talk to a Senior GDF Security Lead

Bring this checklist to a free scoping call. We review your answers, confirm the systems and operating limits that matter and set out the testing depth, the timeline and the deliverables.

Miami office: (786) 219-1210 · **24/7 hotline:** (800) 868-8189 · **Email:** info@evestigate.com

miami-computer-forensics.com

© 2026 Global Digital Forensics, Inc. All rights reserved.