Collaboration and Communication

Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant

Typical Communication During a Pentest

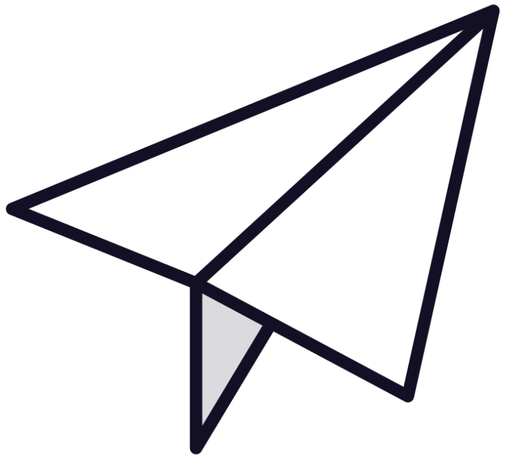
Before the Pentest

- Validate the plan and scope
- Validate Rules of Engagement (ROE)
- Validate test dates

During the Pentest

- Notify pentest start
- Dealing with unknowns
- Notify critical vulnerabilities
- Notify signs of intrusion
- Notify mistakes/changes
- Notify pentest finish

Notify Start and End



Notifying the client when the pentest is about to start and when the tests are completed

The client can correlate with any outages or instabilities

Commonly done by email

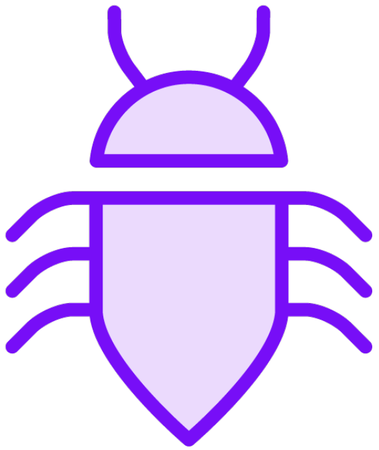
Dealing with Unknowns

Contact the client with any questions or to validate any out-of-the-scope actions

Examples:

- Request additional accounts for a website
- Ask about an unexpected server in the IP range
- Validate if you can create an admin account in the server

Dealing with Critical Vulnerabilities



Some clients might request you to inform in case of critical vulnerabilities

Contact the client with details about the vulnerability and proof of exploitation

Validate the vulnerability before alerting people

Examples:

- SQL Injection on a public-facing server
- Default credentials on a public-facing server
- etc.

Communicating Illegal Activities and Data Breaches

It’s not uncommon to find signs of exploitation, specially in public facing servers

Common signs:

- Malware running on the server
- Command-and-control activity
- Backdoor users, services, or scheduled tasks
- Data exfiltration packs

Stop everything and communicate your client

Do not try to fix anything

Communicating Your Mistakes

Mistakes will happen

Be honest to your client, communicate your mistakes, and propose solutions

Common mistakes:

- Attacking the wrong server
- Modifying/deleting data
- Causing denial of service

Globomantics Scenario: Data Breach Found

Communication Considerations

Stakeholder Alignment

Ensures that both client and testers are aligned and have the same expectations

- IT, security teams, business units, etc.

Formalize everything in writing

Ensure that the scope and risk are understood and approved

Remember that not every stakeholder is a technical person

Peer Reviews

Ensures you are not missing critical steps

Ensures your findings are concise and meaningful

Ensure the proper severity is being set

Root Cause Analysis

Understand the underlying issues that led to a vulnerability

Helps the client to understand the finding

Helps to identify long-term solutions

Example:

- Database vulnerable to remote code execution
  - Missing patch
    - Lack of a patching process

Classifying a Vulnerability

Severity

How quickly it should be fixed

Impact

What will happen to the business

Risk

Impact and likelihood

Business Impact Analysis

Maps the discovered vulnerabilities to actual business risks

- Disruptions, loss of revenue, damage to reputation, etc.

Helps business stakeholders to understand the impact of a vulnerability

- More likely to get proper funding for security

Goal Reprioritization

Adjusting the focus of the test based on the findings observed in the environment

- Example: finding legacy servers

Critical vulnerabilities might shift the test priority of clients

Communications After a Pentest

Informing the Client

Communicates the client about the end of the tests

In some cases, provide a quick overview of what was found before the final report

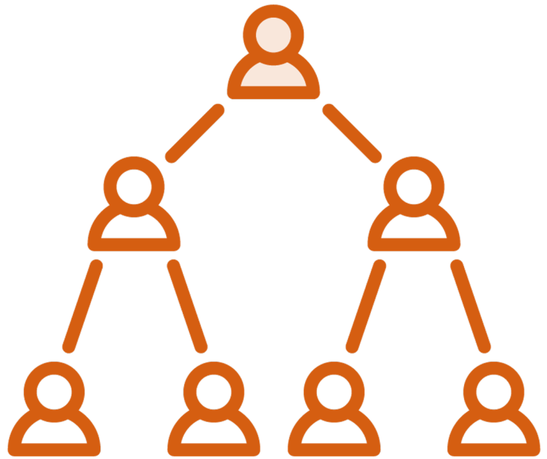
Peer Review

The findings and methodologies are reviewed by another pentester

Ensure quality control across reports

Usually performed by a senior team member

Escalation Paths

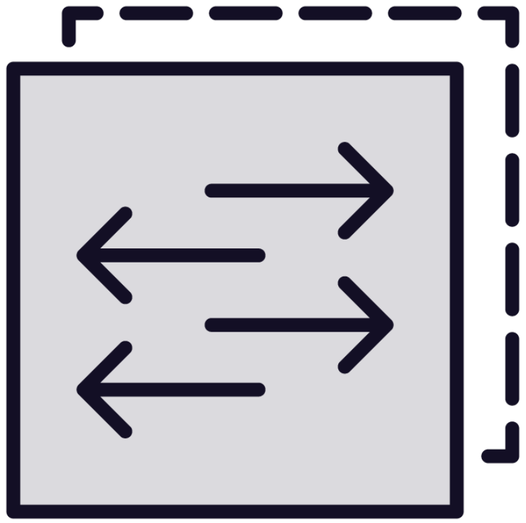


In case critical vulnerabilities or data breaches are observed, the escalation path should be followed

Only communicate the required stakeholders

Do not inform every single person on the client side

Secure Distribution



Distributing the information to the client on a secure channel

- Example: Encrypted communications portal

Avoid using insecure communication for the details of findings

- Emails, FTP, SMS messages

In some cases, might require encrypting the actual reports

Client Acceptance

The formal process where the client reviews and approve the report

Ensures that the client agrees with the results and recommendations

Clients might raise questions about the test and request changes to the report

Up Next:

Reporting