

Questions Regarding a Penetration Test (PT)

The following questions will help you create a bid for a Penetration Test that more precisely meets the needs of the customer.

What is the Goal of the PT?

- Statement about the level of security
- Budget allowance
- Improve awareness / Know-how transfer
- Spot-test of the IT infrastructure
- Test escalation during an attack
- Compare current situation with security guidelines

Is a Security Review more meaningful than a PT?

Efficiency and thoroughness is greater, since it involves an attack on the configuration of the system, examination of the source code, interview with developers, administrators, etc.

- Is a spot test or a thorough security overview required?
- Phase 1 as a Penetration Test, Phase 2 as a Security Review?

How should the PT be carried out?

- Only from the outside, or also from within the Intranet or in a DMZ
- With a remote access laptop (simulation of a stolen laptop)
- In phases (1. from outside, 2. in the DMZ, 3. in the Intranet)

State of Knowledge (Blackhat/Whitehat)?

The more information that is known, the more precision can be applied to the tests. Without information we can demonstrate what an attacker could find out within a particular time frame.

- Should IP-ranges/domain names be discovered or will these be made known?
- Is there a list of telephone numbers, also special numbers?
- Topology of the Internet connections
- Products used
- Technologies applied
 - client-side (if possible with analysis)
 - server-side

Depth of the PT?

- Only vulnerability scanning?
- Use of vulnerabilities (attempted break-in)?
- Launch Denial Of Service?

What it is about?

- E-Business application (diverse components, source code, technologies, etc.)
- Webserver/Mailserver/DNS/FTP
- Firewall environment
- Entire Internet connection
- Perimeter scans
- Intranet scans
- Dial-in modems
- Connections to third-party companies
- Social engineering
- Inside-out attacks (Trojans/virii)
- VPN / remote access
- What is the correct spelling of the products / projects

How many systems / components are to be tested?

- How many systems are to be tested or scanned?
 - Number of servers
 - Number of applications
 - Size of the IP range

Is Social Engineering allowed?

- Physical presence (E.g. as electrician)?
- Telephone information regarding infrastructure?
- Send CD-ROM with a Trojan?
- Send email with a Trojan?

Which attacks do they want to prevent?

- Springboard attacks
- Reading, changing or destroying data
- System outages
- Abuse of resources for third parties (E.g. as platform for pornography)

What do they want to protect?

- Number of systems
- Assets (data, documents, accounts, etc.)

Against whom do they want to protect themselves?

- Attacks by anonymous users
- Attacks from „normally“ registered users
- Attacks by script kiddies, joy riders, white collar criminals

From where do they expect an attack?

- Attack from outside (Internet, telephone, X25, wireless, Bluetooth)
- Attack from suppliers (rented line, feeds)
- Attack from insiders (own employees, external consultants, Trojans)
- Attack from a DMZ (scenario hacking)
- Attack via administration-workstations
- Attack via backup facilities

Time frame of the tests?

- When is the test planned?
- Are there dependencies (new implementations, changes in infrastructure)?
- When do we have the time?
- When is it feasible to carry out the tests (blocked times)
- When would a provider allow tests?
- Are the systems stable and available at this time (maintenance window)?

Who runs the System / Infrastructure?

- Has the owner of the infrastructure been informed and have they agreed?
- Do the clients run the infrastructure themselves?
- Is the client present during the tests and looking over your shoulder (training of their staff, explanations) or can Compass work autonomously?

In which language should the documentation be?

English or German?

- Bid
- Report

Structure of the documentation?

- Is a certain fragmentation required? Key words listing to some departments, not all allowed to read everything (instructions for hacking)?
- Are there customer-specific Do's and Don'ts?



Who is the contact / contractual partner?

- Names
- Correct spelling of the company name
- Especially for holding companies: for which sub-area are we conducting tests?
- Telephone
- Email
- Mobile, FileBox
- Address (value-added tax-able), billing address

How large is the Budget?

- Determines the scope of a penetration tests