# Penetration test scoping

## What is penetration testing

Penetration testing is the process of identifying security gaps in an organisation’s systems environment that could be exploited by adversaries and harm the organisation. The penetration testing team uses a number of technical and non-technical approaches to identify these gaps.

These techniques can include social engineering to compromise user accounts, using manual and automatic scanning tools., and using manual coding techniques like simulated malware. And testing exploits for web applications, on-premises applications, and systems infrastructure.

Testing is performed by very skilled cybersecurity professionals with the capability to simulate a hacker that would be trying to break into and get access to your systems and valuable data.

## What is penetration test scoping

Penetration testing can be very broad or specific and can target specific sensitive systems that house critical data for an organisation. These days most IT environments are complex and included areas such as wired and wireless networks, systems infrastructure, on-premises data centres, cloud computing, local and web applications, access control systems, databases and many other systems and environments.

Engaging a penetration testing organization can be expensive the service you hire may deliver inconsistent results. It is important the test covers correct areas and requirements and that the proposals provided by penetration test organisations are compared accurately, in other words, proposals can be evaluated by comparing “apples with apples”.

## User case – scenario

An organisation has performed a number of cybersecurity improvements covering its systems, infrastructure and IT environment in general. Although the organisation’s executives are happy these works have taken place and feel somewhat more comfortable with the risk mitigation the project was able to achieve, they are concerned that there may be still gaps in their cybersecurity environment which could potentially expose them to adversaries.

The thought of engaging a professional penetration testing organisation to ensure they test their defences, identify issues and provided recommendations with priorities.

They approached a few reputable organisations requesting a quote for a penetration test. Quotes came back all over the place with various price points varying from $20,000 to $110,000 to perform various penetration test works. In addition, the proposals listed several technical elements that they did not fully understand. The executives quickly concluded that they could not compare quotes on offer and were not sure if they were going to cover the desired outcomes of a penetration test. They decided therefore to get the assistance of a professional cybersecurity consultant that could assist them to write the desired scope and assist them to evaluate the returned proposals from a procurement process.

A professional cybersecurity consultant is important to get the right outcomes for the organisation, however, the executives don’t know whom to approach and how to engage someone. Consultancy can also get expensive, and the organisation has limited funds and resources.

Where Fortify can help

Fortify is a not-for-profit organization with cybersecurity expertise, resourced by volunteer professionals. We provided Cybersecurity advisory services at minimal, or at no cost, to assist organizations such as yours that have limited resources.

Fortify will provide a self-assessment guideline and questionnaire so you can assess your requirements in this area.

* Our consultants will write the scope for testing which will include:
  + Network size specifications
  + Public-facing websites
  + Number of applications
  + Internal Penetration Test
  + External Penetration Test
  + Wireless Penetration Test
* We will assist you by writing the procurement documentation
* Once the proposals from vendors are returned our consultant will provide guidance to the evaluation process until a penetration test organisation is engaged.
* Post penetration test and report, our consultant will provide an implementation plan for the organisation to follow and close cybersecurity gaps.

How to engage with Fortify

There are a few simple steps to follow in engaging our services

1. Go to the website: fortify.com.au
2. Register your organization
3. Read the guidelines and start to complete the self-assessment questionnaire. Please allow 50 minutes to complete the questionnaire as some areas may be complicated and require some careful thought
4. If you required assistance to complete the questionnaire, please submit a request via the “require assistance” button or go to fortify.com.au/assistance.

# Part B – the Process

Once the organisation registers with Fortify, the following the process is as follows:

1 – Organisation to completed questionnaire regarding penetrations testing knowledge.

|  |  |  |  |
| --- | --- | --- | --- |
| Questions to be answered by Organisation | Yes or No answer | Maturity Level Analysis | Maturity Level result |
| Q 1 – We understand the importance of penetration testing assessments and why they are conducted. | YES/NO | If Q 1 to Q 4 = Yes then Maturity Level 1 |  |
| Q2 – Our organisation’s professionals have knowledge of various penetration testing techniques such as Network service, Web application, Wireless, Social Engineering, and Physical penetration testing. | YES/NO |
| Q3 – Our IT department follows standard approaches to design and execute penetration testing activities / processes. | YES/NO |
| Q4 – Our organisation can analyse and understand penetration testing processes, results / reports, issues and risks. | YES/NO |
| Q5 – Our organisation is able to research / investigate attack techniques and present recommendations to prevent and/or defend against them. | YES/NO | If Q 1 to Q 7 = Yes then Maturity Level 2 |
| Q6 – Our organisation has the ability to produce test scripts, use tools, and implement test packs to test new or existing networks, systems, and applications. | YES/NO |
| Q7 – Our organisation’s IT has knowledge and understanding of Intrusion Detection / Prevention systems, routing, and firewalls. | YES/NO |
| Q8 – We can implement NEW approaches to penetration testing and contributes to security testing standards. | YES/NO | If Q 1 to Q 10 = Yes then Maturity Level 3 |
| Q9 – We have the expertise in at least one Operating System (knowledge in password locations, services management, log file locations etc). | YES/NO |
| Q10 - We can assess third-party pen tester's development and testing capabilities and manage relationships in regard to penetration testing. | YES/NO |

2- The data form the questionnaire is analysed and a suitable volunteer consultant is appointed to assist the organisation.

Data matching example:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Survey questionnaire questions | Maturity Level Analysis | Maturity Level result | Volunteer 1 Skill level 0 to 3 | Volunteer 2 Skill level 0 to 3 | Volunteer 3 Skill level 0 to 3 |
| Q1 | If Q 1 to Q 10 = Yes then Maturity Level 3 |  | 3 | 1 | 2 |
| Q2 | 1 | 0 | 3 | 1 |
| Q3 |  | 2 | 2 | 2 |
| ~ |  |  |  |  |
| ~Q10 |  |  |  |  |

3 – Legal documents are signed by the organisation, the consultant and Fortify including Non-Disclosure Agreements (NDA).

4 – The consultant performs analysis of the organisation’s environments and provided a high level view including a wide price range for penetration testing. This will ensure that the penetration test activity is well understood by the board and executive and there are funds allocated for the works to commence.

5 – Once the activities and funds are approved by the board, the consultant commences to write the penetration test scope based on Fortify’s template. Template extract as per below (for details please see attachment xx):

|  |  |  |
| --- | --- | --- |
| Penetration Test Activity | Scope Details | Scope Answers |
| Internal Penetration Test | How many live servers/devices are in scope? |  |
| How many subnets are in scope? |  |
| How many IP addresses are in scope? |  |
| unauthenticated testing | Guest access yes/no |  |
| authenticated testing | Type of account, guest, staff, elevated account. Name the accounts to be tested |  |
| Internal application testing | specific internal applications in scope - list applications |  |
| External Penetration Test | how many live servers/devices are in scope for external penetration testing? |  |
| How many subnets/IP addresses |  |
| Wireless Penetration Test | How many SSIDs are in scope |  |
| Are separate staff/public wireless networks used? |  |
| Web Application Penetration Test (Web-facing sites pen test), (Scan, find and test) | Are there any specific external web applications in scope for additional authenticated penetration testing? If so, what are they and is testing to be conducted as a guest, staff member or both? |  |

6 – Once scope is written, the Fortify consultant, will assist the organisation in the procurement process to find an appropriate vendor. Fortify may also provide penetration test services, however responding to the scope must be done and be equivalent to the quality of any external vendor.

7 – Once proposal are received, the Fortify consultant will assist the organisation in the evaluation process to find the successful vendor.

8 – The Penetration test will commence and the vendor will complete and produce a report that covers finding, gaps, recommendations and priorities.

9 – The Fortify consultant will read the report and provide a summary analysis, recommendations and an implementation plan for fixing gaps to the board for approval.

10 – Engagement closure report is produced and accepted by the organisation as the end of this engagement.