**SETTING UP PENETRATION TESTINNG**

Table of Contents

[1. Introduction 3](#_Toc62557860)

[2. Pre engagement process 3](#_Toc62557861)

[2.1. Scope of the test 3](#_Toc62557862)

[2.2. Pricing 3](#_Toc62557863)

[3. Information gathering 4](#_Toc62557864)

[4. Threat modelling 4](#_Toc62557865)

[5. Vulnerability analysis 4](#_Toc62557866)

[6. Exploitation 4](#_Toc62557867)

[7. Post exploitation 4](#_Toc62557868)

[8. Reporting 4](#_Toc62557869)

# Introduction

The purpose of the report is to build up a solution to conduct penetration test on the organization level. The main target will be an IP by which we can search for the machines which are providing services and through scanning, finding the vulnerabilities and afterwards if required, exploiting those vulnerabilities. The timeframe for penetration testing for an organization varies and cannot be considered to be a full security audit because the system testing could change the behavior after testing.

The vulnerabilities found during test out of them some of them are selected by an organization to get them checked and fixed. The process might be costly and every organization might not able to allocate resources for fixation.

***Purpose:*** The purpose of penetration testing is either to aware the higher authority of the security issues or to check the system capabilities for getting response in case of any attack.

# Pre engagement process

Before conducting the penetration test, a meeting should be called to get the idea of the project and working out the scope of the test and the objective. The results of the test should be discussed as sometimes the outcome contains no clear results because purpose might be demonstration of the vulnerabilities which are exploitable and exists within the organization’s network. The form in which the results of the outcomes are showed should also be discussed with the organization.

## Scope of the test

The most important step in the pre-engagement is defining the scope which specifically defines what is to be tested. The scope of penetration test depends upon identifying the machines, systems and network, optional requirements and the staff involved.

### Scoping Meeting

It is also possible to have further meetings after the contract has been signed and situation may occurs where the scope-related topics are discussed before the scope but afterwards required to work upon so a non-disclosure agreement should be signed before any in-depth scoping discussions occur.

The goal of the scoping meeting is to discuss what will be tested. The range of IP addresses should be discussed to know which of them are in the engagement process. It must be verified that the client own all the components as involving the target environments: DNS server, email server, actual hardware there web servers run on and their firewall/IDS/IPS solution.

### Pricing

Pricing depends upon the time of the pen-testers involved. As an example, a customer requests that one hundred IP addresses be tested for the price of $100,000. This means that the customer is offering $1,000 per IP address tested. However, this cost structure only remains effective at that volume. A common trap some testers fall into is maintaining linear costs throughout the testing process. If the customer had only asked for one business-critical application to be tested at the same pricing structure ($1,000), while the tester will still be only attacking a single IP, the volume of work has increased dramatically. It is important to vary costs based on work done. Otherwise, a firm can easily find themselves undercharging for their services, which motivates them to do a less than complete job [1].

Hence, pricing structure should be defined properly because same structure cannot work for both of the above-mentioned example. Moreover, the client may not understand the proper scope of the test so it is the responsibility of the pen-tester to make the client satisfied for territory of the test and the difference between the single application test and the test where client provides wide range of IP’s to test.

### Goal

Every penetration test should be goal-oriented which is to test and identify the specific vulnerabilities which could result in compromising the business or mission objectives of the client. It is not only to find un-patched systems but to identify the risks that could adversely impact the organization.

## Metrics for Time Estimation

The time estimation depends on the expertise of the tester and whatever the time frame decided it better to add a padding of 20% to total time which acts as a backup as in scenarios continuous failure to scanning the target may lead to overtime. Also, it is possible that the network segment may go down or the founded vulnerability may results into involving many levels of management to address. Both of such events are time consuming and significantly could impact the original time which is why 20% added.

Another important component of penetration testing metrics is that to have definitive dead date of the project. The beginning and the end of the project is very important. A signed statement of work specifying the work and the hours required to complete all the goals and milestones.

## IP Ranges and Domains

Before starting a penetration test, all the targets must be identified. The target must be obtained from the client in the initial phase. Targets can be in the form of IP addresses, network ranges, or domain names by the customer. Moreover, it is also important to define that if there is any firewalls, IDS/IPS or networking equipment between the tester and the final target and as they are or not part of the scope. As, in some instances target only provides with the details of the name of the organization and expects the tester to identify the rest on their own. Also, check the IP’s provided to make sure whether they are valid and owned by the client itself or not because these could lead to severe legal consequences.

## Dealing with the Third Parties

It is also observed that sometimes the client do not tell or forget to tell about the third involved so which means testing a service or application being hosted by the third party. In recent years, cloud services are widely implemented everywhere and it is need of today to let those third party know or seek permission from them for testing. Failing to take permissions will possibly bring us in front of law.

## Cloud Services

Testing cloud services may incur an issue of that data from multiple organizations are stored on one physical medium. The cloud services providers needs to be alerted to the testing and needs acknowledge that the test is taking place and granting permission to testing organization to test. Moreover, security contract should be there that can be helpful in the event of finding security vulnerability which could impact the other cloud customers. Also, the cloud providers have specific procedures for penetration testers to follow, and may require request forms, scheduling or explicit permission from them before testing can begin.

## ISP

The ISP terms and conditions should be consider before launching any attack because in many commercial situations the ISP will have specific conditions for testing. In certain situations, the ISP may block the traffic which is considered malicious. The client may approve the risk but it must be always communicated before the beginning. Web hosting with the third parties, the scope and timing of the test needs to be clearly communicated with web hosting provider.

## Incident Reporting Process

It is important to discuss the organizations incident response capabilities before the start of the engagement process. The penetration test is not just about testing the environment but to check the capabilities of the incident response team. If an entire engagement process can be completed without the target’s internal security teams ever noticing, then it means there is a big major gap in the security posture. Also inform some from the incident team about the test so the incident team does not start to call every member.

## Rules of Engagement

As the scope defines what will be tested, the rules of engagement defines how that testing is to occur. A sample of rules of engagement is provided in the *appendix Rules of Engagement*.

# Information gathering

# Threat modelling

# Vulnerability analysis

# Exploitation

# Post exploitation

# Reporting

# Appendix

## Rules of Engagement

Company-ABC takes the security of our guests and colleagues very seriously. Company-ABC hopes to raise its already high level of security standards, as well as learn from and collaborate with highly skilled Pentesters at Herts Cyber Security Ltd. in order to keep our businesses and customers safe.

By taking this Pentesting project of Company-ABC you agree to follow all of the requirements below.

### 1.      SLA

* Duration: W1 – W 15
* Produce a comprehensive Pen test report as specified in **Table 3** and Activity narrations as specified in **Table 4**

### 2.      Disclosure Policy

Do not discuss this program or any vulnerabilities (even resolved ones) outside of the program without express consent from the undersigned.

### 3.      Pentesting Rules

* Do not collect any personally identifiable information, authentication information, or credit card information from Company-ABC guests.
* Do not destroy or alter discovered data.
* Do not inappropriately store Company-ABC information in public locations.
* Do not intentionally harm guests as well as their experience.
* Do not publicly or privately disclose any vulnerabilities belonging to Company-ABC - existing or remediated - to anyone other than the undersigned.
* Contact undersigned about questions regarding vulnerabilities or any issues.
* Current Company-ABC employees and contractors should not be participated in this pentest.
* You cannot participate in this pentest if you have been an employee or a contractor of Company-ABC in the past six months.
* Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue will not be accepted.
* Social engineering (e.g., phishing, vishing, smishing) is prohibited.
* Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.
* Limit automation/rate scraping to 100 requests per minute.
* Remove all changes you have made during the pen test.

### 4.      Submission Requirements

* All reports must be submitted through the Herts Studynet platform.
* Consolidated Pentest report must meet Task 4 requirements.
* Attack Narrative reports must meet Task 5 requirements.

### 5.      Testing Requirements

**Test Accounts**

**Create** Company-ABC **test accounts to these specifications:**

* First name: < Company-ABC > (for multiple accounts - <handle>one, <handle>two, etc.).
* Last name: "**Test**".    
    
  Reservation Requirements    
    
  **If you must create bookings for testing purposes, follow these rules:**
* Test bookings should be made four months into the future at a minimum.
* All test bookings should be cancelled **as soon as possible**.
* Do not book London or Melbourne properties for testing purposes.
* If possible, add "Herts Pen Test" to the comments of bookings.

### 6.      In Scope

**Assets**

* Company-ABC.com (no subdomain).
* [www.Company-ABC.com](http://www.Company-ABC.com) (no additional subdomains).
* world.Company-ABC.com (no additional subdomains).
* assets.Company-ABC.com (no additional subdomains).    
    
  **Vulnerabilities**
* Authentication bypass.
* Back-end system access via front-end systems.
* Business logic bypass resulting in financial gain to an attacker (e.g., forced rate change).
* Container escape.
* Discovery of Company-ABC data on other  storage services.
* Highly creative means of automating account checking or rate scraping (e.g., botting).
* Highly creative means of discovering origin IP.
* Highly creative means of spoofing email messages.
* Other systems that may host Company-ABC information.
* SQL Injection.
* Cross-Site Request Forgery.
* Exploitable Cross-Site Scripting.
* Web Application Firewall (WAF) bypass.
* Any other, which are not out of scope.

### 7.      Out of Scope

**Assets**

* Any Company-ABC not specifically listed as in-scope.
* Company-ABC and Herts properties and their physical and networks infrastructure.
* Company-ABC and Herts corporate information systems.
* Third-party companies that perform business transactions for Company-ABC and/or Herts employees and contractors.    
    
  **Vulnerabilities**
* Vulnerabilities without discernible impact on Company-ABC IT systems or guest privacy.
* Attacks requiring physical access to a user’s device.
* Attacks requiring physical access to a Company-ABC employee, contractor or guest device.
* Autocomplete on web forms.
* Clickjacking, unless an effective exploit can be demonstrated.
* Client browser vulnerabilities.
* Denial of Service attacks on Company-ABC infrastructure.
* Limited content reflection or content spoofing.
* Missing best practices.
* Password and account recovery policies.
* Password policies, i.e., complexity.
* Phishing or spear phishing attacks.
* Rate-limiting issues.
* Reports originating from automated tools or scanners (e.g., Burp, Acunetix, WebInspect).
* Self-exploitation.
* Social engineering attacks.
* Software version disclosure.
* SSL / TLS best practices.
* Vulnerabilities that cannot be reproduced.
* Clickjacking on pages with no sensitive actions.
* Unauthenticated/logout/login CSRF.
* Attacks requiring MITM or physical access to a user's device.
* Previously known vulnerable libraries without a working Proof of Concept.
* Comma Separated Values (CSV) injection without demonstrating a vulnerability.
* Missing best practices in SSL/TLS configuration.
* Any activity that could lead to the disruption of our service (DoS).
* Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS

### 8.      SQL Injection Policy

* Do not alter any data.
* Do not change or interrupt server or database functionality.
* Do not destroy any data.
* Do not read or save sensitive data belonging to guests other than yourself.
* Blindly counting rows and columns of databases is permissible.
* Generating outbound DNS requests is permissible.
* Listing database names and columns is permissible.
* Logic responses are permissible.

### 9.            Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Thank you for helping keep Company-ABC Hotels and our users safe!