**Introduction**

Penetration testing/Pen test is a part of the security plan that aims to measure the effectiveness of protection in place (Crest, n.d.). In more details, the objective of penetration testing is to find out the vulnerabilities and attack vectors on a(n) network/system/asset that can cause a security threat. There are several types of penetration testing exist such as network, web application, IoT. This analysis plan consists of the various steps and procedure that are going to take place for penetration testing on a given system.

As to complete the penetration testing, various tools and techniques are used. These tools and techniques involve both automation, and manual types, to ensure the maximum level of testing. In some cases (Aditya, 2017), after using automated tools, the results will be verified by manually trying to exploit them. This approach ensures the maximum level of effectiveness in penetration testing. As a conclusion, the result of the penetration testing focuses on finding out the vulnerabilities that pose a security threat to the business, and to provide remedies for the findings.

**Case Analysis**

For the given case, all the six phases of penetration testing need to be done. Furthermore, as it is mentioned that five flags have been hidden inside the system all the flags will be found by exploiting the vulnerabilities.

Gaining the root privileges will remain as a high-level priority and this will be done by using appropriate techniques. Also, as it is mentioned to look for security violations, the penetration testing focuses on the security violations recorded on the system. These violations may include using week credentials, sharing user credentials. The whole testing will be documented according to each phase starting from scanning.

**Processes and phases**

Penetration testing involved standard phases (Shon Harris. Allen Harper. Chris Eagle. Jonathan Ness., 2008). Starting from a pre-engagement phase which involves penetration testing planning documentation, continuing to information gathering phase which involves collecting information about the target through various sources, then going ahead to threat modelling which involves the finding of assets with most likely to get attacked, then moving forward to vulnerability assessment which involves the usage of tools to identify the vulnerabilities, then proceeding forward to exploitation phase which involved trying to gain the advantage over the target by using the results from previous vulnerability assessment phase. Right after the exploitation phase, post-exploitation phase comes which involves performing various activities on the compromised system such as enumerating users, services.

Once all the technical phases are over, reporting/documentation phase comes in. This phase involves the documentation of the whole test starting from the scope statement, it consists of all the findings, actions performed, evidence of exploitation, and remedies/suggestions.

**Methodology**

In penetration testing based on the tester and the targeted nature, a variety of methodologies can be used. For this given scenario The penetration testing execution standard (PTES) will be followed. This methodology involves the phases of the brief in the previous section. PTES aimed to provide complete, and contemporary penetration testing standard (PTES, 2014). Also, it provides both technical and business aspects of penetration testing at the same time.

**Test type**

In penetration testing, there are three types of tastings available (Chapple & Seidl, 2018). At first black box, which provides no information about the target environment/technology behind it and let the tester to perform the penetration testing. The only issue with Blackbox method is time-consuming. Since the tester has no information about the application, the tester must perform all the techniques to get started. Secondly white box, this type is more common in the software development domain where the testing team will be provided with complete information about the application which makes the work easier. Same as the software development domain, in penetration testing, the tester will be provided with detailed information about the application which helps to reduce the time consumption. And thirdly grey box where the tester will be provided with little information about the target/application.

For the given scenario here, the suitable approach would be a black-box type test. The reason behind choosing black box type is, no information about the target is given. So, this would be the appropriate test type.

**Scope**

As a part of the scope, the company has provided a brief outline of the requirements. The in-scope of the penetration test would be the machine that provided since the machine comes from the organization network, the network area of the company included in the in-scope. Out-of-scope for the given scenario including, usage of external-IP, and social engineering.

**Ethical considerations**

Ethical considerations play a vital role in penetration testing. Though there are no fixed guidelines for all the organizations, some of the standards considerations (EC-Council, 2014) are followed,

* Signing a non-disclosure agreement (between the penetration tester and the company)
* Protesting the test information/findings within the penetration tester and the company.
* Obtaining concern/permission from the employer, if the test required to use the company devices/services.
* Following the test plan approved by the concern company/employer.

These are the standard ethical considerations that apply most of the time. The additional considerations are depended between the company and the penetration tester.

**Time frame**

|  |  |
| --- | --- |
| **Timeline** | **Deliverable** |
| 12 October 2020 | Penetration Testing Plan |
| 15 –16 October 2020 | Information gathering |
| 17-18 October 2020 | Vulnerability assessment |
| 19 - 30 October 2020 | Exploitation |
| 1 November – 7 November 2020 | Post exploitation |
| 8 November – 12 November 2020 | Reporting |

**Requirements**

The requirements consist of two categories. One is hardware, and second is software. Requirements of the proposed penetration testing are followed,

**Hardware requirements**

A laptop/Desktop with,

* + 4 GB or more RAM
  + 15 or above processor
  + 50 GB (Minimum) Hard Drive space

**Software requirements**

* Windows 8.1 or above (minimum) as the host system
* VMware workstation or Virtual box (to install and run the target application)
* Kali Linux/Parrot OS/ Commando OS or similar with the default tools installed.

**References**

* Aditya, K. (2017). Manual or automated application security testing whats more effective [Blog]. Retrieved from https://blog.securityinnovation.com/manual-or-automated-application-security-testing-whats-more-effective.
* Chapple, M., & Seidl, D. (2018). CompTIA PenTest+ Study Guide (pp. 36-38). Wiley.
* Crest. What is Penetration Testing. Crest-approved.org. Retrieved from https://www.crest-approved.org/what-is-penetration-testing/index.html.
* EC-Council. (2014). Code Of Ethics | CERT. Cert.eccouncil.org. Retrieved from https://cert.eccouncil.org/code-of-ethics.html.
* PTES. (2014). The Penetration Testing Execution Standard. Pentest-standard.org. Retrieved from http://www.pentest-standard.org/index.php/Main\_Page.
* Shon Harris. Allen Harper. Chris Eagle. Jonathan Ness. (2008). Gray Hat Hacking: The Ethical Hacker's Handbook; Second Edition (pp. Chapter 4, Pen-Testing Process, 73-90). McGraw-Hill.