Global Scientific Review
A Peer Reviewed, Open Access, International Journal
www.scienticreview.com
Volume 10, December 2022 ISSN (E): 2795-4951

Analyzing Methodology of Increasing Students' Competence Using Pentesting Platforms on The Subject of Information Security

Ibragimov U.M.
PhD, department of department of "Information-communication systems of controlling technological processes" Bukhara engineering-technological institute, Bukhara city, Uzbekistan.
Ahadov A.M.
Assistant, department of department of "Information-communication systems of controlling technological processes" Bukhara engineering-technological institute, Bukhara city, Uzbekistan.

Annotation. The scientific research illustrates that using penetration testing for teaching students Information Security Science and it has analyzed of measuring the vulnerability to data compromises provides the scientific background and analytic techniques to understand and measure the risk associated with information security threats. Penetration tester usually begins by gathering as much information about the target as possible. Then he identifies the possible vulnerabilities in the system by scanning.

Key words: Computation, penetration testing, multiple phases, test case, methodology.

Introduction. The discussion about ethical hacking is controversial in high schools as the composite statement expresses two opposing meanings: a hacker who aims to circumvent restrictions while an ethical attribute should confront them. A penetration test aims to exploit existing vulnerabilities to determine their nature and impact. The goal is to simulate an attack on a system or network to evaluate the risk of the environment. Any selected penetration-testing framework proves by itself that hacking and ethics are independent concepts that require context and purpose. Therefore, a pen-test starts by defining clear objectives and scope seeking for agreement to avoid adverse effects on the confidentiality, integrity and availability of the information that we intend to protect.

Materials and methods. An intentionally abstract methodology is preferred over a specific framework in this work since it is more flexible to design the model of challenges. After which he launches an attack. Post-attack he analyses each vulnerability and the risk involved. Finally, a detailed report is submitted to higher authorities summarizing the results of the penetration test. Penetration testing can be broken down into multiple phases; this will vary depending on the organization and the type of penetration test. The first phase is planning. Here, the attacker gathers as much information about the target as possible. The data can be IP addresses, domain details, mail servers, network topology [1]. In this phase, he also defines the scope and goals of a test, including the systems to be addressed and the testing methods to be

Volume 10, December 2022 ISSN (E): 2795-4951

used. An expert penetration tester will spend most of the time in this phase, this will help with further phases of the attack.

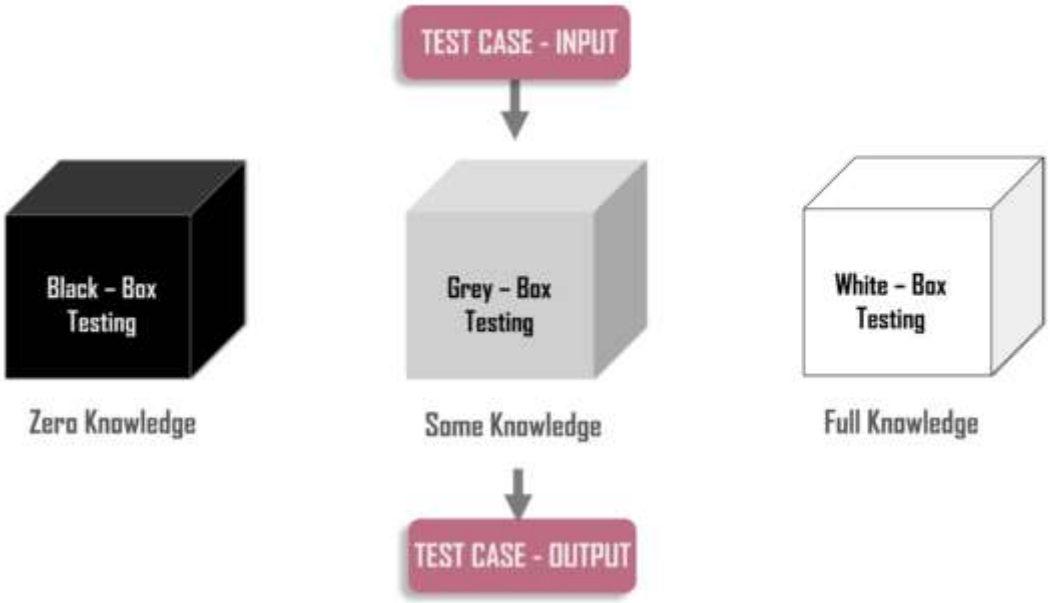

Figure 1. Penetration testing types based on knowledge of the target

Penetration testing types based on the position of tester:

- If the penetration test is conducted from outside the network, it is referred to as external penetration testing
- Suppose, the attacker is present inside the network, simulation of this scenario is referred to as internal penetration testing
- The organization's IT team and the Penetration Testing team working together usually perform targeted testing
- In a blind penetration test, the penetration tester is provided with no prior information except the organization name
- In a double-blind test, at max, only one or two people within the organization might be aware that a test is being conducted

Global Scientific Review
A Peer Reviewed, Open Access, International Journal
www.scienticreview.com
Volume 10, December 2022 ISSN (E): 2795-4951

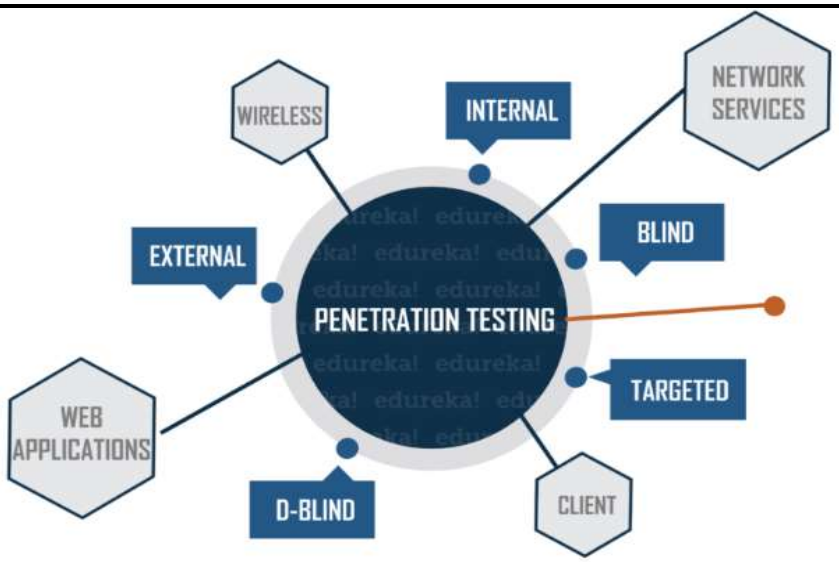

Figure 2. Structure of penetration testing

The penetration testing process is abbreviated as pen-test, an also referred by many names, such as, ethical hacking, red teaming and vulnerability testing [3]. While a methodology introduces a set of processes following a predetermined sequence, the framework is useful to guide a penetration testing under a specific structure and techniques. Consequently, the methodology adapted to this work considers a set of four stages as follows. Reconnaissance and Discovery: Searching for any available information on the target avoiding intrusive methods. Enumeration and Vulnerability Analysis: Intrusive data gathering. Mapping of known vulnerabilities.

Execution and Appropriation: Attempt to gain temporary or permanent users and privileged access based on an attack plan and access strategy. Document Findings: Document the security state of the environment. It provides the test results by means of empirical evidences and remediation [3].

A constructivist learning method, designed as chained experiences that are gradually revealed to the students, drives the challenges. The study materials in the form of theoretical formal knowledge and hands-on lessons scaffold the challenges. Throughout the experimentation of the hands-on lessons, a student reasons about a security problem and some plausible solutions. A challenge states a concise tip and hint without instructions, keeping some level of ambiguity to induce collaborative constructions among students. Therefore, the teaching and learning process for penetration testing is impossible when it lacks a realistic environment to practice in, much more when such a scenario is not legal. In addition, the teaching and learning can be diluted if a system is broken by mimicking a fun attack without any reasoning about the conditions causing such behavior that a student can also contribute to improve [4]. Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property. The subject includes four types of information technology security you should consider or improve upon Network Security, Cloud Security, Application Security, Internet of Things Security.

At the core of information security is information assurance, the act of maintaining the confidentiality, integrity, and availability (CIA) of information, ensuring that information is not compromised in any way when critical issues arise. These issues

include but are not limited to natural disasters, computer/server malfunction, and physical theft. While paper-based business operations are still prevalent, requiring their own set of information security practices, enterprise digital initiatives are increasingly being emphasized, with information assurance now typically being dealt with by information technology (IT) security specialists [5].

Information security, often shortened to InfoSec, is the practice, policies and principles to protect digital data and other kinds of information. InfoSec responsibilities include establishing a set of business processes that will protect information assets, regardless of how that information is formatted or whether it is in transit, is being processed or is at rest in storage. We can divide all the cryptography algorithms (ciphers) into two groups: symmetric key cryptography algorithms and asymmetric cryptography algorithms [2]. Figure shows the taxonomy.

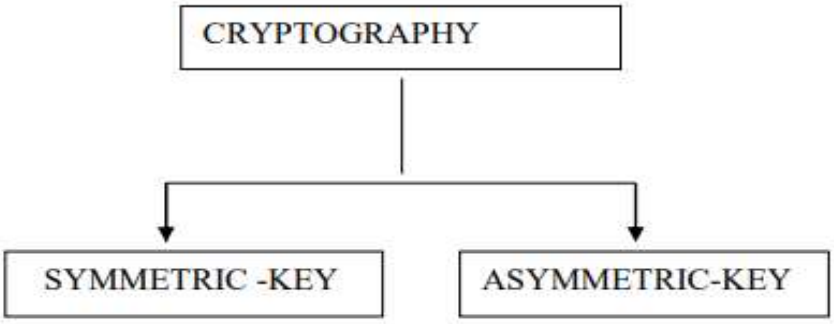

Figure 3. Categories of Cryptography

In symmetric-key cryptography, both parties use the same key. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The receiver keeps the private key.

Conclusion. The purpose is to identify the vulnerabilities that may exist in operating systems, services and applications due to flaws, improper configurations or risky end-user behavior by simulating a break-in. At present, the penetration testing methodologies are diverse as the testing is frequently tailored by the pen-tester according to the conditions of the environment.

References

1. Security in Computing – (3rd Edition) Charles P.Pfleeger, Shari Lawrence Pfleeger. PHI.
2. Cryptography and Network Security – by A. Kahate – TMH.
3. P. Herzog, The Open Source Security Testing Methodology Manual: OSSTMM 3.Institute for Security and Open Methodologies, ISECOM, 2010. Accessed on: Feb. 11,2019.
4. K. Orrey, M. Byrne, A. Doraiswamy, L. Lawson, and N. Ouchn. Penetration Test Framework (PTF) v0.59, 2014. Accessed on: Feb. 11, 2019
5. PTES Group, Penetration Testing Execution Standard, 2009. Accessed on: Feb. 11, 2019.