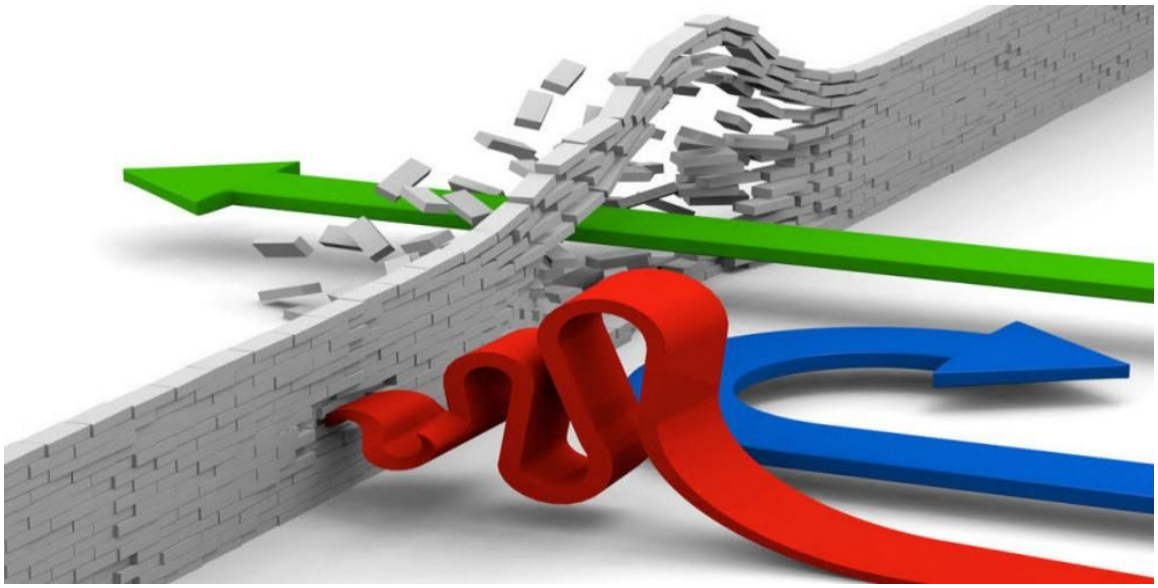
Penetration Testing



Scion Li & Yingzi Ma

Bentley University

IPM723: Information Security, Control and Ethics

Professor Proudfoot

July 25, 2018

Table of Contents

I. Introduction

Penetration Testing is the practice of simulating an authorized simulated attack on a computer system, network or web application to find vulnerabilities that an attacker could exploit. It involves gathering information about the target, finding possible entry points, and attempting to break into the system. The objective of penetration testing is for a business to find weaknesses within their system's security and to assess the overall health and security of a system. Typically, an outside security company is hired to perform the penetration testing by breaking into the company's system in the same way an attacker would and reporting their findings. They are considered white hat hackers as they attack ethically to help secure a company's digital assets, while black hat hackers will hack a company for personal or malicious gain. After the penetration testing is complete, the findings are reported back to the company to determine the best mitigation measures and patch up their systems to prevent hackers from exploiting these vulnerabilities in the future.

II. History

Penetration testing has been around for many years since the 1960's with increasing sophistication, as computer systems became more prevalent in businesses, and companies wanted to secure their data systems from cyber attacks ("The history of penetration testing"). One of the very important early pioneers of penetration testing development was James P. Anderson. In 1972, Anderson published a report called

“The Anderson Report” that outlined a list of steps that testers should follow when testing the ability for systems, networks, hardware, and software to be penetrated or compromised (“The history of penetration testing”). Anderson’s approach included identifying the vulnerability, designing an attack on it, finding the weakness in the attack itself and then determining ways to neutralize its threat. He wrote almost two hundred other reports and standards that greatly influenced the world of cybersecurity. As the different types of cyber attacks and the magnitude of successful attacks in the past increased, the methods and tools used to perform penetration tests became more sophisticated as well. However, these steps outlined in Anderson’s fundamental method are still in use today.

III. The Importance of Penetration Testing

There are several reasons why it is important for companies to conduct penetration testing. The first reason is to prevent data breaches. In the news today, we constantly hear about companies falling victim to data breaches. These breaches damage the company’s reputation and the trust their customers have in them. The damage from these data breaches, especially if the personal or financial information is stolen can cost the company millions of dollars so companies should use penetration testing to tighten up their security to defend against such attacks. Another reason why companies need penetration testing is to test their security controls such as firewalls and antimalware software. Penetration tests can make see if they are actually working

and ensure that their systems are safe against targeted attacks. If a company recently purchased a new system, it is also a good idea to run a penetration test to make sure there are no holes in their security from day one. The next reason why companies should do penetration testing is for baselining. Say a new Chief Information Security Officer joins a company, they may want to run a penetration test to see where the vulnerabilities are. This will tell the CISO where to spend their security budget money on. Last but not least, companies should run penetration tests to be compliant. To be PCI certified, it is required for companies to run regular penetration tests in order to keep up with the ever-evolving security threats today. Failure to do so could result in hefty fines.

Penetration testing is an important means to provide business visibility into aggregations of misconfigurations/vulnerabilities that could lead to an attack. It is crucial for security and risk management leaders to use penetration testing to prevent data breaches, test their security controls, ensure system security, baseline, and be compliant with PCI regulations.

IV. Types of Penetration Testing

Penetration testing has three main use cases for businesses:

- Compliance - Control audits
- Risk Reduction - Gray-box, white-box and code review
- Attacker Simulation - Black-box and red team

Within these three use cases, information security providers usually offer three major types of penetration testing including White-Box Test, Gray-Box Test, and Black-Box Test. Each of these types has different characteristics and can be utilized differently based on organizations' security objectives and priorities.

Lightweight (White-Box) testing is a broad-scope test across the internal and external environment. It is also known as clear box testing. It refers to the testing of a system with full knowledge of architecture, source code and the access to the documentation. Vulnerabilities and weaknesses in system-level security, devices, configurations, authorization, and access are evaluated in this test. This type of test requires less time for reconnaissance of the enterprise environment. The main goal of the test if to identify as many as possible vulnerabilities and weak points through a basic level of exploitation. Organizations that are in the initial state of adopting the penetration test should begin with a lightweight approach. This methodology is the least expensive and complex. Most of the testing activities can be automated. (Neiva, Gartner)

Gray-Box testing is also known as targeted testing. It is a combination of white-box and black-box testing. The tester is provided with limited information such as the scope of the environment and the software product's inner code structure. This methodology utilizes automated tools in the white-box approach and uses attack simulation against a specific target. Gray-Box testing allows for the customization of different objectives and use cases, such as industrial control systems (ICSs),

environments and new web application feature testing. The targeted testing approach can also demonstrate the degree of access that an authorized user can obtain. The potential damages of the insider attack or privileged attacks could also be evaluated. In the gray-box test approach, the limits on the scope and timeframe of testing may cause testers to overlook nontrivial vulnerabilities. So that the organization should define which area needs a penetration test and which one should be accessed by the tester. (Neiva, Gartner)

Standard Assessment, also known as black-box testing or ethical hacking, simulates a full chain of attacking activities. In opposition to white-box testing and gray-box testing, this approach does not require any prior knowledge of the internal coding structure or environment. Paul Midian, CISO at Dixons Carphone, suggests five phases of black-box testing: reconnaissance, scanning, enumeration, gaining access and privilege escalation, and access maintaining. This type of penetration test uses any possible measures to attack the target to achieve the goals. The purpose of this methodology is to simulate an attack against the target, exposing security control weaknesses and the environment's defensive posture instead of trying to identify all possible vulnerabilities and weak points. Organizations that are employing this type of testing are required to have high-security maturity in order to achieve the entire ROI of this penetration testing. In most cases, this test will examine the effectiveness of current security controls, monitoring and incident response teams' preparedness to the attack. Some suggest the major advantage of black-box testing is that it mimics the life-like

situations so that the real-life threats and vulnerabilities are discovered. Moreover, black-box testing testers usually use open source tools that are likely to be used by hackers. So the cost of penetration test is reduced because of these free tools. (Ravi, InfoSec) However, Gartner suggests that this type of penetration testing is the more expensive one among the three since it requires manual work performed by testers with special expertise and most of the works cannot be automated. One of the drawbacks of black-box testing is that testers are not able to see the entire infrastructure so that they might miss some significant vulnerabilities.

Red team is another important aspect in penetration testing. Gartner concluded that red teaming is mission-driven, objective-oriented and involves the use of a simulated, goal-directed adversary attacking a system or network. Red team may employ black-, gray- and white-box testing. (Neiva, Gartner) It challenges an organization's security control by applying more realistic exercises such as role-playing and threat investigation to identify high-priority target continuously. Gartner describes the red team as a military team with a mission.

V. Process for Penetration Testing

The process for penetration testing used today is outlined by the following four steps:

1. Information Gathering
2. Vulnerability Assessment

3. Exploitation
4. Deliverables

In the Information Gathering phase of penetration testing, the penetration tester will identify what the company assets are, what systems they use, how they are used, who the users are, and other general information on the organization, systems, and its employees. During this time, it is also important to identify what the scope of the penetration testing will be, and what areas of the company's systems will (and will not) be tested. For example, a company may choose to test their systems but not want to test the social engineering aspect of the company. Of note, the wider the scope, the more expensive the penetration testing will cost to an organization. It is important for a company to determine how much they want to spend given their budget, resources, and risk their current systems have against malicious attacks.

The next step of the penetration testing is running the vulnerability assessment. This is an automated assessment that scans the company's systems for the vulnerabilities and weak spots in the company's security. From the output of this vulnerability assessment, the company will know which areas of their security are prone to attacks and hone in on them during the next phase of the penetration testing process - the exploitation.

The exploitation phase of the process is the point at which a penetration tester will actually attempt to attack and infiltrate the target system as if he/she is a real

attacker. The testers will use their hacking tools and resources to see how much of the systems they can gain unauthorized access to, and analyze the loopholes and soft spot entry points that exist in the system's security. This can be done both manually via brute force hacking methods or with automated hacking software. Once they have completely accessed the system and identified what and how they were able to infiltrate the system, the penetration tester will record their findings and begin developing their deliverables for the company in a detailed report.

The deliverables phase of penetration testing is when the penetration tester develops and delivers a complete and thorough report that outlines all findings from their exploitation, prioritizing the most crucial findings first. Their analysis will include the steps taken to infiltrate the system, an assessment of the system's overall security, and recommended remediations for these findings. This report is presented to the company so that they can prioritize and implement the remediations that would be most important and require the most immediate fix. After the remediations have been implemented, it is important for the company to do additional testing to make sure that the implementations were successful and effective.

This penetration testing process is iterative, meaning that the process never ends. Penetration testing should be done regularly and each time the test is run, new findings will be presented and the company will continuously find new ways to improve their systems. A company is never considered safe so they much keep up with the most

recent and potential cyber threats that are still evolving today.

VI. Best Practices for Penetration Testing

The goal of penetration test is to fulfill the two main purposes, to protect people and environment against the machine and to protect the machine against people. Ultimately, penetration testing should minimize the number of weak points in the system.

To ensure the success of pentest, leaders in information security should:

- Review the organization security objectives and select the appropriate types of pentest to achieve the goals
- Compare and select the pentest vendors to balance the cost and rotation of pentesters
- Evaluate the importance of the company assets, resources and environments to prioritize pentest tasks and distribute resources and time efficiently
- Review the service-level agreement (SLA) of the vendors to make sure it covers all necessities

First, the organization should perform a Vulnerability Scanning to get a baseline of the potential weakness within its environment. After the vulnerability assessment has been completed. The organization should prioritize and rank the vulnerabilities based on the criticality and the ease to fix. Those that are the most serious and the easiest to fix

should be remediated first. After the successful completion of Vulnerability Scanning, the organization is ready to employ penetration test. Setting very clear expectations from the beginning is good practice as to make sure that everyone is on the same page and that by the end of the project, they have a clear understanding of whether their goals were met for the penetration testing.

The security and risk reduction is vital when employing the penetration test. Thus, it is important to define the restrictions and boundaries of the engagement of penetration test in order to reduce the potential risks of negative impacts from test activities. It is also beneficial to establish a governance structure for the penetration test. This will help in coordinating with the test vendor to regulate the scope of the test and the personnel who are responsible for the testing activities. Moreover, the organization should also determine if an internal team can implement the test and give temporary authorization to the employee who can perform remediation during the test period. In addition, the organization should use a scattered testing approach to identify as many weak points as possible. Last but not least, the results from the white-box approach should be utilized in order to refine the scope for the grey-box tests to distribute budget and resources more efficiently and effectively. (Neiva, Gartner)

VII. Key Challenges of Penetration Testing

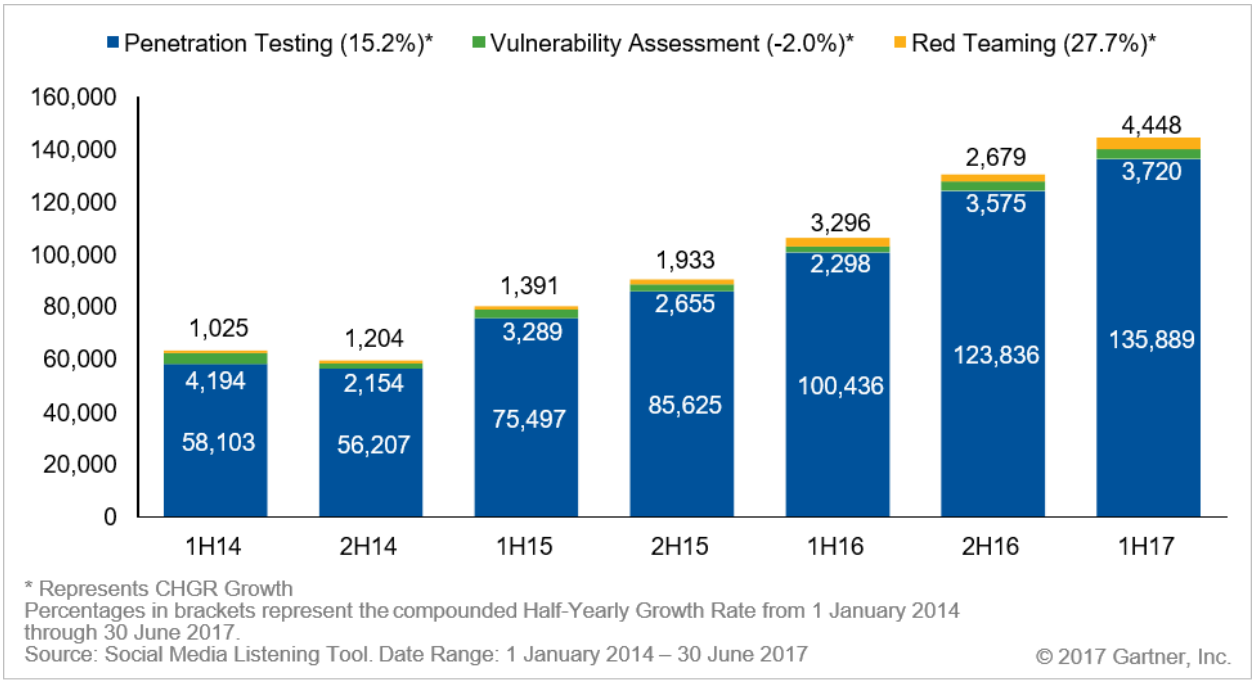
Although penetration testing is very useful and beneficial, there are many challenges that organizations will encounter if they want to employ it. Due to the lack of security awareness and training, some organizations may not fully understand the differences between a penetration test and a vulnerability assessment. This will result in a failure to meet the objectives and a mismatch of the expectations. The personnel who are responsible for the penetration tests must fully understand that the main goal of the vulnerability scanning is to determine and evaluate potential vulnerabilities in a technical perspective, whereas the penetration testing attempts to exploit the determined vulnerabilities, which may result in unauthorized malicious access, modification, interception of normal organization process and data.

Moreover, leaders in security and risk management can be confused when selecting the best option of the pentest based on their situations because there are many types of penetration test in use. The misjudgment on the type of penetration test can cause potential risks and could delay the entire project. The best way to handle it is facilitating the communication between the security teams and business stakeholders, and involving the entire mandatory roles when deciding the type of penetration testing. In addition, based on Gartner's research, leaders in security and risk management also show a limited awareness of different testing models and their relevance to specific security needs.

VIII. The Future of Penetration Testing

The future of penetration testing is strong with no signs of slowing down. In a 2017 Gartner publication, it is estimated that “By 2020, 25% of security teams will use network pentests as a core capability, up from 10% in 2017” (Neiva, Gartner). The figure below shows the number of social media mentions for Penetration Testing between 2014 to 2017 in a Gartner publication. We see that the number of mentions has increased from 58,103 in 1H14 to 135,889 in 1H2017. This is a 234% increase in only 3 years with a very clear upward trend.

Source: Gartner



Although this graph only trends from 2014 to 2017, it can be expected that the upward trend continues to rise with the number of data breaches we still hear about

today. In just the past year, we have heard of countless data breaches from even the major profitable organizations. These include household name companies such as Macy's, Whole Foods, Adidas, Facebook, Ticketfly, Delta Airlines, just to name a few. These major corporations probably have conducted penetration testing in the past given their high profile names and the amount of sensitive customer and financial data that they have. Even then, they were no exception to the major data breaches today which suggests that cyber-security has and still is a major issue today. As long as we live in the dangerous world of cybersecurity, there will be penetration testing. It is here to stay.

IX. Conclusion

Penetration testing relates to information security and control because it is a widely used practice that most companies use today for their cybersecurity. It is a crucial measure that companies use to make sure their systems are secure and to control who can gain access to the company's data and resources. It is so relevant to our world today with the amount of data we have out there and the undeniable fact that there will always be people out there looking to steal or exploit it. We will always have this ethical and cyber warfare where hackers are constantly looking to maliciously exploit company data and cybersecurity companies are using everything they have to defend companies against them.

In the future, companies will become more and more interested in penetration testing. More companies will use IoT devices for connectivity and migrate to cloud-based services for accessibility and convenience. Such a trend will make penetration testing grow in importance because information security is vital in the age of the internet. With technology becoming more and more advanced, hackers will come up with more elaborate and sophisticated ways to gain unauthorized access to business systems. Thus, penetration testing will be more important than ever and will evolve with the times. As a society, we need to be cognizant of the cyber threats that are possible and very much exist. So much of our data is already out there, and companies do have an important responsibility to keep their customers' data safe. If they are not careful and do not take control of their data security, they are exposing major threats that can lead to major financial, personal, and even political implications. That is why penetration testing is so important, and the reason why it will always be a very important security measure that all companies need to apply.

Work Cited

Das, Ravi. “The Types of Penetration Testing.” InfoSec Resources, 30 June 2016, resources.infosecinstitute.com/the-types-of-penetration-testing/.

Neiva, Claudio, et al. “Understand the Types, Scope and Objectives of Penetration Testing.” Gartner, Inc., 29 Sept. 2017, www.gartner.com/doc/3810671/understand-types-scope-objectives-penetration.

“The History of Penetration Testing.” InfoSec Resources, 20 July 2016, resources.infosecinstitute.com/the-history-of-penetration-testing/.