Evaluation of Penetration Testing and Vulnerability Assessments

Eshwar Mattadi  
M.Tech Student, Department of CSE  
CMR College of Engineering and Technology, Hyderabad

Prof. K. Vijaya Kumar  
Professor, Department of CSE  
CMR College of Engineering and Technology, Hyderabad

Abstract – In today’s present day period vital organization data is gotten to, put away, and exchanged electronically. The security of this data and the frameworks putting away this data are basic to the notoriety and success of organizations. In this manner, powerlessness appraisal of PC frameworks to get a complete assessment of the security dangers of the frameworks under scrutiny. In current period there is more intricate undertaking IT frameworks comprise of hundreds or a large number of frameworks. Every part of these frameworks is carefully arranged and coordinated into complex frameworks construction modeling. Proficient IT staffs are in charge of safely setting up and keeping up these IT infra structures are surveying, on a continuous premise, the genuine dangers displayed by framework vulnerabilities. Assaults against PC frameworks and the information contained inside of these frameworks are turning out to be progressively incessant and evermore advanced. Progressed Persistent Threats (APTs) can prompt ex filtration of information over expanded periods. Associations wishing to guarantee security of their frameworks may look towards receiving proper measures to ensure themselves against potential security breaks. One such measure is to contract the administrations of infiltration analyzers (or “pen-analyzer”) to discover vulnerabilities present in the association’s system, and give proposals with reference to how best to relieve such dangers. This paper talks about the definition and part of the cutting edge pen-analyzers, highlighting contrasts from what is by and large expected of their part in industry to what is requested by expert capabilities. The paper further distinguishes issues emerging from pen-analyzers, highlighting contrasts from what is by and large expected of their part in industry to what is requested by expert capabilities. In this paper we can examination of The paper further distinguishes issues emerging from pen-analyzers, highlighting contrasts from what is by and large expected of their part in industry to what is requested by expert capabilities. In this paper we give a review of entrance testing, talk about security vulnerabilities, and compress the outcomes and advantages of infiltration testing acknowledged by the IT administrators met.

Keywords – Penetration Testing, Pen Tester, Cyber Security, Vulnerability Assessments, Risks, Attacks.

I. INTRODUCTION

In data framework, we more than once hear that security is an adventure and not a destination. That is genuine on the grounds that when dealing with the security of system, we generally need to Endeavor and stay one stage in front of our adversaries – the crooks, grumblers, programmers, spies and villains. They take information and data without breaking any glass. Keeping information private is one center mission of system security. Rivals are continually sharpening their system and strategies every day to adventure system security and access the classified data. These adventures are assaults against: secrecy, uprightness and accessibility of system assets. Classifiedness (being sheltered from unapproved access) Confidentiality alludes to restricting data access and divulgence to approved client and keeping access and exposure from unapproved ones. Trustworthiness (rightness and completeness of information) Integrity alludes to the validity of data assets. It guarantees that information have not been changed improperly either by purposely or accidentally censure movement. Accessibility (assets are constantly accessible to approved client) Availability alludes to the openness of the data assets. It guarantees that data must be accessible to approved client when they got t

1. Internal: This testing is often performed from different network access points that include both the physical and logical segments; this provides a more detailed view of the security.

2. External: This testing has its focus on the infrastructure components, servers, and the related software of the target. It also provides a detailed analysis of the information that is available from public sources, such as the Internet. Enumeration of the network is also performed and analyzed. The filtering devices, such as firewalls and routers, are also scrutinized for their vulnerabilities. Finally, the impact and consequences are accessed. The two types of penetration have three variations, each depending on the degree of knowledge provided by the target company to the pen testing team.

3. Black Box: This testing does not provide the tester with any information and therefore is a much better testing method because crackers and script kiddies normally do not have any information that is directly obtained from the target company and need to gather their information from public sources. It simulates real-world attack scenarios. The steps of mapping the network, enumerating shares and services, and operating system fingerprinting are typical for black box testing.

4. White Box: For this, related information is provided and is done so to assess the security against specific attacks or specific targets. This is the chosen method when the company needs to get a complete audit of its security.

5. Grey Box: In this testing, some knowledge is provided to the testers but this testing puts the tester in a privileged position. This would normally be a preferred method when cost is a factor as it saves time for the pen testing team to...
uncover information that is publicly available. Also, this approach would be suitable when the organization needs to obtain knowledge of the security assessment practices. A. Methods of Penetration: We have two choices when it comes to getting penetration done. However, we will describe the details of the manual alternative for this paper because this would be the preferred method in providing a nonbiased report that might be necessary to meet legal regulations.

i) Automatic: The automatic penetration is often chosen when cost is a key factor. Due to the free software availability of many penetration tools, a company could choose to have the penetration performed by this method. Also, commercial tools that could be used have a cost associated with them; however, this tool cost could be spread out and would still be a less costly solution than manual penetration. However, the learning curve for each penetration tool is usually much higher, and the knowledge required and experience in doing such work demands the skills of an expert.

ii) Manual: Manual penetration is usually chosen to give an independent assessment of the penetration. Normally an external company that is experienced in the field and does it on a regular basis, with a good track record, is chosen.

II. VULNERABILITY ASSESSMENT

A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed include, but are not limited to information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems. Such assessments may be conducted on behalf of a range of different organizations, from small businesses up to large regional infrastructures. IT infrastructures are assessing, on an ongoing basis, the real risks presented by system vulnerabilities. The task of correctly assessing the real security risks associated with a seemingly endless stream of vulnerability and patching reports is a critical and time-consuming activity for IT staffs. However IT professionals understand that despite their best efforts, vulnerabilities may still present significant security risks for their companies.

III. PENETRATION TESTING VS. VULNERABILITY ASSESSMENT

The main focus of this paper is penetration testing but there is often some confusion between penetration testing and vulnerability assessment. The two terms are related but penetration testing has more of an emphasis on gaining as much access as possible while vulnerability testing places the emphasis on identifying areas that are vulnerable to a computer attack. An automated vulnerability scanner will often identify possible vulnerabilities based on service banners or other network responses that are not in fact what they seem. A vulnerability assessor will stop just before compromising a system, whereas a penetration tester will go as far as they can within the scope of the contract. It is important to keep in mind that you are dealing with a ‘Test.’ A penetration test is like any other test in the sense that it is a sampling of all possible systems and configurations. Unless the contractor is hired to test only a single system, they will be unable to identify and penetrate all possible systems using all possible vulnerabilities. As such, any Penetration Test is a sampling of the environment. Furthermore, most testers will go after the easiest targets first. Vulnerability Analysis is the process of identifying vulnerabilities on a network, whereas a Penetration Testing is focused on actually gaining unauthorized access to the tested systems and using that access to the network or data, as directed by the client.

1. A Vulnerability Analysis provides an overview of the flaws that exist on the system while a Penetration Testing goes on to provide an impact analysis of the flaws identifies the possible impact of the flaw on the underlying network, operating system, database etc.

2. Vulnerability Analysis is more of a passive process. In Vulnerability Analysis we use software tools that analyze both network traffic and systems to identify any exposures that increase vulnerability to attacks. Penetration Testing is an active practice wherein ethical hackers are employed to simulate an attack and test the network and systems’ resistance.

3. Vulnerability Analysis deals with potential risks, whereas Penetration Testing is actual proof of concept. Vulnerability Analysis is just a process of identifying and quantifying the security vulnerabilities in a system. Vulnerability analysis doesn’t provide validation of security Vulnerabilities. Validation can be only done by Penetration testing.

4. The scope of a Penetration Testing can vary from a Vulnerability Analysis to fully exploiting the targets to destructive testing. Penetration Testing consists of a Vulnerability Analysis, but it goes one step ahead where in you will be evaluating the security of the system by simulating an attack usually done by a Malicious Hacker.

5. For instance a Vulnerability Analysis exercise might identify absence of anti-virus software on the system or open ports as a vulnerability. Penetration Testing will determine the level to which existing vulnerabilities can be exploited and the damage that can be inflicted due to this.

6. A Vulnerability Analysis answers the question: “What are the present Vulnerabilities and how do we fix them?” A Penetration Testing simply answers the questions: “Can any External Attacker or Internal Intruder break-in and what can they attain?”

7. A Vulnerability Analysis works to improve security posture and develop a more mature, integrated security program, where as a Penetration Testing is only a snapshot
of your security program’s effectiveness. A vulnerability assessment usually includes a mapping of the network and systems connected to it, an identification of the services and versions of services running and the creation of a catalogue of the vulnerable systems.

8. A vulnerability assessment normally forms the first part of a penetration test.

9. A penetration test is the exploitation of any detected vulnerabilities, to confirm their existence, and to determine the damage that might result due to the vulnerability being exploited and the resulting impact on the organization.

10. In comparison to a penetration test a vulnerability assessment is not so intrusive and does not always require the same technical capabilities. Unfortunately it may be impossible to conduct such a thorough assessment that would guarantee that the most damaging vulnerabilities (i.e., high risk) have been identified.

11. The difference between a penetration test and a vulnerability assessment is becoming a significant issue in the penetration testing profession. There are many penetration testers that are only capable of performing vulnerability assessments and yet present themselves as penetration testers. If a company is unfamiliar with the skills and abilities required of the pen tester, and less so on the legal, social, ethical and professional issues arising from such sensitive work. A notable exception to this assertion is the work by Pierce, Jones and Warren. In their paper they provide a conceptual model and taxonomy for penetration testing and professional ethics. They describe how integrity of the professional pen tester may be achieved by “...avoiding conflicts of interest, the provision of false positives and false negatives, and finally legally binding testers to their ethical obligations in [their] contract”. This is certainly noteworthy and should be expected of an individual working with potentially sensitive information, however this appears more of a personal “ethical code of conduct” rather than something which can be enforced and assessed. Pierce et al. (Pierce, J. et al, 2007) also discuss the then provision by universities “…toward offering security testing courses”. Additionally, in 2006, McRue (McRue, A., 2006) commented on the “…first U.K. university to offer a dedicated degree course in hacking”. This has certainly shown an emerging trend in the education sector for penetration testing courses, however these tend to be degree classifications and not necessarily an industry recognized certification standard.

V. EXISTING SYSTEM

The skills and abilities required of the pen-tester, and less so on the legal, social, ethical and professional issues arising from such sensitive work. A notable exception to this assertion is the work by Pierce, Jones and Warren. In their paper they provide a conceptual model and taxonomy for penetration testing and professional ethics. They describe how integrity of the professional pen tester may be achieved by “...avoiding conflicts of interest, the provision of false positives and false negatives, and finally legally binding testers to their ethical obligations in [their] contract”. This is certainly noteworthy and should be expected of an individual working with potentially sensitive information, however this appears more of a personal “ethical code of conduct” rather than something which can be enforced and assessed.

VI. PROPOSED WORK

A risk means something is about to done or cause harm or reduces the operational utility of the system. Threats are those things which may occur independent of the system under consideration and which may pose the risk. There are two primary methods of risk analysis and one hybrid method:

- Qualitative - Improve awareness of Information Systems security problems and the posture of the system being analyzed.
- Quantitative - Identification of where security controls should be implemented and the cost envelope within which they should be implemented.
- Hybrid method - A selected combination of these two methods can be used to implement the components utilizing available information while minimizing the metrics to be collected and calculated. It is less numerically intensive (and less expensive) than an in-depth exhaustive analysis.
- Metrics: IT security metrics can be obtained at different levels within an organization. Detailed metrics, collected at the system and network level, can be aggregated and rolled up to progressively higher levels, depending on the
VII. IMPLEMENTATION

a) Council Of Registered Ethical Security Testers (CREST):

One system operating in the UK is CREST (CREST, 2010). This not-for-profit organization is governed by a memorandum of association, with about 19 member organizations at the time of writing (CREST, 2010). Its main purpose is to provide assurance of competency for organizations, and for the individuals within those organizations. CREST was created to fill a niche in the UK security testing industry, by providing assurance for Non-Government Organizations (NGOs), i.e. the private sector. This is because the existing CHECK standard is only applicable for Government organizations. Members are provided with guidance on standards, methodologies, further recommendations and a code of practice. However it should be noted that this information is not publicly available from the CREST website (CREST, 2010) at the time of writing. The scheme provides assurances of professionalism to organizations, but not to individuals. “Individuals not employed by CREST Companies can take the CREST Certification Examination to become CREST Associates, but cannot undertake CREST approved testing without working under the auspices of a CREST member company” (CREST, 2010).

b) TIGER Scheme:

The TIGER Scheme (Tiger Scheme, 2010) is focused on providing an independent method of determining the skill and ability of a penetration tester. The scheme has a number of levels from the Associate Membership to the Senior Tester qualification. The structure of the scheme involves separate management committee, operating authority and examination body. These form the strength of the TIGER Scheme; with the technical and professional standards enforced by the Examination Body being derived from the advice of a technical panel composed of independent experts. The technical panel acts on behalf of the Management Committee, to ensure the examination are relevant to the penetration test community. The University of Glam organ in the UK currently acts as the Examining Body for the TIGER Scheme.

The TIGER Scheme Senior Tester is equivalent to CHECK Team Leader. Since it is a multi-tiered system candidates without UK security clearance can still be awarded TIGER Scheme Senior Tester status but not CHECK Team Leader status, as this is confirmed through a separate process with CESG (CESG, 2010).

VIII. CONCLUSION

Regardless of the way that invasion testing is an industry saw term, there is still dubiousness in appreciation to what a passage analyzer truly does and how they give affirmation that the work they finished is fit for reason. It is key to make a capability between penetration testing and framework security evaluations. A framework security or lack of protection assessment may be significant to a degree, yet don't for the most part reflect the extent to which software engineers will go to enterprise a shortcoming. Penetration tests attempt to duplicate a "honest to goodness" attack to certain degree. The passageway analyzers will generally deal a system with vulnerabilities that they adequately abused. Software engineers and gatecrashers need to find one and just hole to abuse however enchant analyzers need to conceivably find all if not whatever number as could be normal the situation being what it is crevices that exist. This is a mind-boggling task as passageway tests are routinely done in certain time period. Finally, a passage test alone gives no adjustment in the security of a PC or framework. Move to made to address these vulnerabilities that is found as a result of driving the invasion test.

REFERENCES


