Information Security Thought Paper
Vulnerability Assessment and Penetration Testing

Introduction

This document explains the differences between vulnerability assessments and penetration tests to help understand when each may be appropriate.

For Vulnerability Assessments Consider:

A vulnerability assessment is not a test, it is a scan which is then reviewed and analyzed by a human to understand the scan results. A vulnerability scan itself is normally automated and it attempts to passively scan and detect a response from a system which could infer a potential vulnerability but does not attempt to do anything using the suspected vulnerability. Therefore, vulnerabilities detected are not confirmed, they are only suspected through inference of response. This means there can be false positives. One benefit to conducting a vulnerability assessment on a system is that it can give you an idea of potential vulnerabilities without posing a substantial risk to the system as the suspected vulnerabilities are not being tested (e.g. there is no attempt made to use / exploit the detected vulnerabilities, which could result in unintentional harm to the system). Because a vulnerability assessment is relatively unobtrusive, there is little risk to data integrity or confidentiality. The biggest risk associated with a vulnerability assessment is a potential impact to availability due to system or network load generated by the scanner. For this reason, it is advisable to throttle scans to a level which your network and system(s) can reasonably handle.

For Penetration Tests Consider:

A penetration test takes suspected vulnerabilities which have been detected as part of a vulnerability scan and goes one step further. A penetration test attempts to exploit (use) detected vulnerabilities. This confirms or dispels the existence of the vulnerability and removes false positives. A penetration test takes longer because of this added step. Another downside to this approach is that there is a higher risk that you could inadvertently cause harm to your system(s). It is important for a penetration tester to keep a clear log of commands run and actions taken in case any issues occur. Like a vulnerability assessment, a penetration test can also potentially cause system and network load issues.

Conclusion:

- Vulnerability assessments against a production system can be OK if they are confirmed to be strictly scans and not tests.
- Vulnerability assessments against a production system should be performed carefully to ensure that unreasonable load is not introduced to the system resulting in availability issues to clients.
- Vulnerability assessments should not be run against shared network infrastructure, devices, or systems without prior permission from the unit responsible for these.
- Running penetration tests on production systems poses the potential for unintended harm without first being aware of the risks this poses.
- Penetration tests can be helpful on non-production systems with non-production data which are otherwise configured the same as a production system. In this way, the results provide useful and actionable information, but the test itself does not pose a risk to the production system(s).
- The top reason for having third parties assist with penetration tests is to provide a degree of independence. This segregation / separation of duties is important to ensure that vulnerabilities are not overlooked or dismissed, and that accountable individuals are made aware of the risks.
- Third party penetration testers should be carefully assessed and vetted prior to being hired. You should ensure they are trustworthy, qualified, and skilled. If an unskilled third party conducts a penetration test and nothing is found, you may be left with the false impression that you are secure.
- Penetration tests can be costly, and it is important to consider the value, pros and cons, based on the context of the system prior to procuring a Penetration test.
- Prior to a penetration test commencing, ensure you have agreed on the scope with the penetration testers.
    - For example, often penetration tests can involve social engineering or phishing and attempts to physically enter buildings to gain access to sensitive environments as part of a full penetration test.
    - You need to be clear with the penetration testers about what is acceptable as part of the engagement.
- When conducting a Security Threat and Risk Assessment (STRA):
    - You will consider how likely a threat is to act on a vulnerability, the potential impact, and what this might mean to your organization.
    - Generally, an STRA is a point-in-time assessment using whatever data you have readily available.
    - A vulnerability scan or penetration test does NOT need to be performed for every STRA conducted.
    - In special circumstances, if a system is critical, or highly complex, the primary risk evaluator may deem it appropriate and worthwhile to conduct a vulnerability scan or penetration test to help inform an STRA.
    - It is advisable that the primary risk evaluator of an STRA be empowered to make this decision where possible.