Breaking Down What Vulnerability Scanning & Penetration Testing Are

Introduction

Given the transformation that the world has been through, with both the pandemic and what is happening in the Ukraine, businesses are now on their highest guard to protect their digital assets against any looming threats. Because of this, many vendors are now offering different kinds of services, especially when it comes to Vulnerability Scanning and Penetration Testing.

However, there is a great of confusion between the two of them, as they are used interchangeably with another. But in reality, they are actually quite different methodologies, which will be further explored in this article.

Vulnerability Assessments

This type of test runs automated scans across the major components that reside in both your IT and Network Infrastructures. These primarily include the servers, and other workstations and wireless devices. These assessments primarily look for known vulnerabilities that exist, without any human intervention involved.

The scans can run as short as a few minutes to as long as a few hours. After the probing has been completed, a report is usually generated for the client, and from there, it is up to them to decide how to proceed with any specific actions to remediate the issues.

This test is also known as a "Passive" kind of test in the sense that it only detects those weaknesses that are highly visible and can be exploited very easily by a Cyberattacker. This just serves as a tipping point of what other vulnerabilities could be lurking. In a sense, the Vulnerability Scan van be viewed as merely conducting an EKG as to what is going on in terms risk exposure.

One of the primary advantages of this kind of assessment is the cost. It is very affordable, even to the SMB which makes it a very attractive option. The downside is that if there are any recommendations that are provided in the report, it will not be specific to your business, rather, it will just be general in nature, based upon previous threat profiles. Because of its low cost, a Vulnerability Scan can be run on a continual cycle, at different timing intervals.

Further, the vulnerabilities that have been discovered are not exploited to see what the root cause of them are, or to see if there are other vulnerabilities that could lie underneath.

Penetration Testing

This can be viewed as the "Angiogram" in the detection of the vulnerabilities, weaknesses and gaps that reside in your IT/Network Infrastructures. A huge deep dive is done, with many kinds of tests being conducted. They won't last for just a matter of a few hours, rather, they go on for long and extended periods of time.

Second, there is not much automation that is involved when conducting a Penetration Test. It is primarily a manual based process, which takes the work of many skilled professionals, with years of experience. These people are also known as "Ethical Hackers" because they are taking the mindset of Cyberattacker and using every tactic in the book in order to break down your walls of defense.

With this effort, these individuals are not only looking for the known vulnerabilities, but they are also looking for the ***unknown ones*** as well, such as covert backdoors that could have been left behind in source code development. In other words, heavy active scanning is involved, unlike the Vulnerability Assessments.

Third Penetration Testing is not just done on digital assets. It can also be used to unearth any gaps or weaknesses that are found within the Physical Infrastructure of a business as well. For example, a team can be specifically assigned to see how easy it is replicate an ID badge and use that fool the security guard at the main point of entry.

Fourth, Penetration Testing can also be used to ascertain the level of vulnerability the employees have to a Social Engineering Attack. In this regard, a specialized team can be called upon to make Robocalls to the Finance and Accounting departments to see if they can be tricked into making payments on fake invoices. Or the calls could involve reaching out to the administrative assistants of the C-Suite and luring them into wire large sums of money to a phony, offshore account.

Fifth, Penetration Testing can be used in both the internal and external environments of a business.

Typically, there are at least two teams involved (perhaps even three) when conducting these kinds of tests, which are as follows:

- The Red Team: These are the Ethical Hackers that are trying to break into your systems as previously described;

- The Blue Team: These are the Ethical Hackers that work internally with your IT Security Team, to see how well they react to and fend off the attacks that are being launched towards them by the Red Team;

- The Purple Team: This may or may not be used, depending upon the security requirements of the client. This team is a combination of the Red and Blue ones and provide an unbiased feedback to both teams as to how they have done during the course of the exercise.

At the end, the client is given an exhaustive report of the findings from the Penetration Test, as well as suggestions of actions that can be taken to remediate the problem. Although the biggest advantage of this kind of exercise is the deep level of thoroughness that is involved, the downside is that they can be quite expensive. As a result, Penetration Tests are typically only carried out perhaps once, or at most, twice a year.

Conclusions

The following matrix summarizes some of the key differences between a Vulnerability Scan and a Penetration Test:

Vulnerability Assessment	*Penetration Test*
Tests are passive	Tests are active
Tests are automated, no human intervention	Tests are primarily manual, lots of human intervention
Tests are short in time frame	Tests are much longer in time frame
Reports are provided to the client, but not specifically for actions that can remediate issues	Reports are provided to the client, and are specific to actions that remediate specific issues
Scans can be run on a continual cycle	Scanning is done only at a point in time intervals due to their exhaustive nature
Tests are primarily done on digital assets	Tests are done on both physical and digital assets
Only known vulnerabilities are discovered	Both known and unknown vulnerabilities are discovered
Costs are affordable	Costs can be quite expensive
Only general tests are done	All kinds of tests are done, depending upon the requirements of the client

The question which often get asked: “What kind of test should I get”? It all comes down to cost. Typically, the smaller businesses can only afford the Vulnerability Scan, whereas the medium sized business can afford the Penetration Test. But truthfully, each and every business should know all of the vulnerabilities that lurk in their systems, especially the unknown ones, as this is what the Cyberattacker will primarily go after.

A security breach can cost easily 10X more than any of these tests just described. Therefore, the CISO and his or her IT Security team need to remain constantly proactive; thus making the Penetration Test the top choice to go with in the end.