English version

KNOW THE MAIN CYBER TECHNIQUES AMONG ASSESSMENTS AND TESTS

DIFFERENCES AND POINTS OF ATTENTION BETWEEN VULNERABILITY ASSESSMENT AND PENETRATION TEST

ALESSANDRO SCARAFILE

« IT security is like a promise:

if you care, you will find a way, otherwise you will find an excuse. »

Alessandro Scarafile

VP Cyber Security & Operations
Syneto

SOMMARIO

INTRODUCTION

People often speak about penetration testing, but really the enquirer wants a vulnerability assessment. And conversely, many people ask for a vulnerability assessment, when what they really need is a penetration test.

Often, it's a miscommunication problem, since many people use the two terms interchangeably, as the two look very similar from afar. However, up close it's a very different story.

Essentially, the vulnerability assessment is an automated scan used to identify vulnerabilities, while a penetration test aims to exploit those vulnerabilities to get a deeper understanding of the holes in your defenses.

1. WHAT IS A VULNERABILITY ASSESSMENT?

A vulnerability assessment is a **scan**. It uses automated tools to check your systems for known vulnerabilities. Imagine a burglar looking for and identifying a back entrance to your building, but not entering. The results of the scan will show how an application, website or other system is vulnerable, but it doesn't provide details on what would happen if the vulnerability was exploited.

Many organizations undertake vulnerability assessments to "tick a box", usually for compliance. However, there are limits to a vulnerability assessment, because it can't explain the impact, the ability to pivot on one vulnerability and use another to compromise a system. There is also the possibility of false/true positive/negatives, so it's important to verify automated results with multiple tools or manual methods.

2. WHAT IS A PENETRATION TEST?

Penetration testing is a method of identifying and **testing** vulnerabilities or gaps in IT security, that could be exploited in external or internal infrastructure, leaving your business at greater risk.

A penetration test usually begins with an automated vulnerability scan, but goes into far more depth. In our burglar scenario, this time they are checking for a back entrance and then actually entering the building (don't worry, they have permissions!).

This testing format — what many people might consider "**hacking**" — is a systematic examination of a network or system undertaken by qualified, experienced security experts who have been given permission to exploit the vulnerabilities and misconfigurations they find to determine potential impact.

The experts will work to a defined test methodology to enter the network through the identified gaps (hence the term, 'penetration'), using their knowledge, Open Source information, and a range of tools. Once gaps have been identified and tested in your systems and networks, they provide expert advice for strengthening your defenses.

3. VULNERABILITY ASSESSMENT VS. PENETRATION TEST

Let's try to better understand what is included in each service, through this handy comparison of a vulnerability assessment and a generic penetration test (each test will depend upon the system being examined).

Image 1: Categories of Activities

Description	VA	PT
Scoping call	✓	✓
Documenting of requirements and scope	✓	✓
Passive information gathering		✓
Active information gathering	✓	✓
Automated vulnerability scan	✓	✓
Exploit analysis		✓
Vulnerability confirmation		✓
Misconfiguration examination		✓
Vulnerability/misconfiguration exploitation		✓
Application/infrastructure exploit pivoting		✓
System restoration to pre-test state: removal of test files, software and account		✓
Vulnerability report (system generated)	✓	
Exploit reporting		✓
Detailed summary on overall security posture		✓
Customized remediation advice		✓

Image 2: **Table of Activities**

As you can see, a penetration test is significantly more in-depth than a vulnerability assessment. While a penetration test generally includes an initial automated vulnerability scan, it's the manual exploitation of those vulnerabilities that requires a wide range of skills and time.

4. WHICH IS RIGHT FOR YOUR ORGANIZATION?

4.1 VULNERABILITY ASSESSMENT

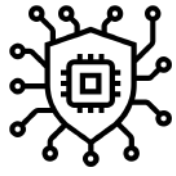
Think of a vulnerability assessment as a one-size-fits-all high-level automated scan that picks up the most common vulnerabilities. It's cheaper and quicker because it isn't resource intensive and could be considered as a health check (like running a virus scan on a laptop, but across a whole network).

While a vulnerability assessment is often conducted as a mandatory exercise as part of complying with regulatory requirements, such as ISO 27001, it is strongly recommended that vulnerability assessments are conducted regularly; on all new devices before deployment and again throughout the year (like a fire drill).

4.2 PENETRATION TEST

A penetration test is the difference between "ticking a box" and being confident you have looked at your vulnerabilities from every angle. The testing is undertaken by humans who understand the nuances of how businesses work. Unlike automated scanning software, they can ask questions when something doesn't seem quite right (which is important for ongoing business operations).

Much like carrying out an annual service on a car, regular penetration testing is recommended for all businesses, to ensure ongoing mitigation of risk; however, it is even more important if you're introducing new technologies in the workplace, moving to the cloud, outsourcing IT, have experienced a breach in the past, or aren't confident you know how mature your security is.



5. WHAT ARE YOU TESTING?

Whichever you choose truly does depend on the asset being tested; if the asset is low value (i.e. compromise wouldn't have a devasting effect on operations or reputation), then a vulnerability assessment is probably adequate.

However, if the asset is high value (i.e. a breach or failure could cause operational disruption and revenue loss or reputational damage), then it becomes a prime target for threat actors who invest time into finding more ingenious ways to compromise and gain access.

6. THE RESULTS

Both options will provide you with a detailed report explaining the findings, the criticality of the vulnerabilities, and present remediation advice. However, the vulnerability assessment report will not cover impact or exploit information, as this can only be gleaned by exploiting the vulnerabilities manually.

It's important to remember that new vulnerabilities are discovered regularly, so whether you've decided that a vulnerability assessment or a penetration test is the best choice for your organization's needs, it should be repeated **regularly**.

CONCLUSIONS

Cybersecurity is important because it encompasses everything that pertains to **protecting** our personal information, intellectual property, data, and industry information systems from theft and damage attempted by criminals and adversaries.

Because of the massive increase in hacks and hacking attempts, cybersecurity has become an unavoidable topic of discussion in the past several years. Events that occur in the cybersecurity industry can and often do have global consequences and the possibility of **catastrophic** results.

If an organization has no information security professionals, it can employ external contractors — there are numerous IT companies today specializing in security auditing, vulnerability assessments and penetration tests that offer comprehensive information security plans.