ANYBODY HOME?

Vulnerability Scans vs. Penetration Tests

A RESOURCE FROM SKOUT CYBERSECURITY

SKOUT
CYBERSECURITY

One of our readers recently asked: “My company recently underwent a Vulnerability Scan, but our counsel says we need to have a Penetration Test done. Aren’t they the same thing?”

Vulnerability scans and penetration tests are definitely two different things. To put this in simple terms, one is a professional checking each door and window to make sure they have locks, the other is someone purposely trying to break in to see if the locks are working.

WHAT IS A VULNERABILITY SCAN/ASSESSMENT?

Vulnerability scanning, (AKA a vulnerability assessment and a few other names) is the process of looking at each server, application, and networking platform to see if there are any known security weaknesses – also called vulnerabilities – present on those systems. This often includes looking at desktops, laptops and mobile devices. Vulnerabilities can be unpatched software, misconfigured networking options (like open ports), insecure platforms (such as older software that has no more security patches from the manufacturer), and other potential areas that make up attack surfaces. While vulnerability scans do find these problems, they’re looking for potential problems, not useable attack openings. That’s a key difference between a vulnerability scan and a penetration test, so let’s look a bit deeper at the concept.

Just because a vulnerability exists, does not mean it can be exploited. Exploits are methods by which an attacker can use a vulnerability to gain access to something they’re not supposed to be able to see or manipulate. One great example in the recent past is the security hole in Windows XP that allowed NotPetya to propagate across the internet. The security flaw was a vulnerability, but until someone created the exploit (NotPetya, in this case), it was just a potential vector for attack, not an actual exploitable hole in security.

Vulnerability scans also point out many issues that are not directly exploitable. Open networking ports on a server are only an issue if that server talks directly to the outside world – otherwise the firewall and other security tools would keep an attacker from getting to that open port in the first place. This is why most vulnerability scans provided by third-party companies also rate the potential danger of the vulnerabilities they find. You need to know which vulnerabilities need to be addressed first because they are directly exploitable in your current environment.

Finally, vulnerability scans are typically not very “heavy” on your systems. By that, I mean that a vulnerability scan can typically be done during normal business while the systems are in use; because it doesn't disrupt normal operations. While some forms of scanning can use a lot of memory and other system resources, most are designed to be run while users are active on the systems to make everyone's lives easier.

WHAT IS PENETRATION TESTING?

Penetration testing (often shortened to "pen testing") is a different discipline completely, and takes a totally different approach to security. While a vulnerability scan will find all the potential security holes in your environment, a penetration test seeks to actually use one or more of those holes to breach your organization – in the same way an attacker would. While they use the same methods as attackers do in order to gain access to your systems, pen testers are bound by very strict contract language and can be prohibited from touching certain systems, taking systems offline, or destroying data if you include those restrictions in their contracts. This means that a pen tester will be performing a very real attack, but may be doing so while playing by rules you both have agreed on.

Pen testers also contractually promise not to share any data they acquire or the results of the test itself except with those organizations you explicitly allow. For example, most pen testing contracts prohibit the testing firm from releasing test results to your customers or regulators without your express permission. That's a good thing, since they will most likely find a way in, and you want the ability to remediate (close the hole) before anyone else finds out about it.

That being said, it's important to say again that **a pen test is an attack against your system.** While they may be bound by contract language, they will try every trick at their disposal and within the terms of the agreement to defeat your security protocols. Pen testers are very good at what they do, and even with rock-solid security there is a high likelihood that they'll still get in.

So why would you expose yourself to a purposeful attack? The idea is that a security system is only as good as its weakest link, and finding the weakest link takes testing – that's what the pen tester will do. Finding the weak links means you can begin to remediate and strengthen the weak spot in your security, making everyone safer overall.

The other major difference with pen testing is that **the tester will generally stop once they achieve their goal.** Unlike the vulnerability scan, once a pen tester gains access to the data or system they're trying to reach, they don't usually continue to find other ways they could have reached that goal. So relying on the pen test alone isn't giving you the entire security overview throughout your organization; just helping you find the weakest link that allowed the tester to get in.

Pen testing can be exceptionally heavy on your systems. Testers will try to perform Denial of Service attacks, attempt to push the boundaries of software, and even purposely trigger reboots of servers. The goal is to force a system to give them access they shouldn't have, and that often requires making quite an impact on the applications and platforms themselves. Because of this, pen testing isn't done frequently - generally once or twice a year is normal. While it can be disruptive, it's also critical to perform these tests, so do not let the potential for temporary business disruptions stop you from doing your testing.

HAVING A LOCK VS. CHECKING THE LOCK

Going back to our starting analogy, a vulnerability scan is having a professional locksmith make sure that you have operational locks on every door, window, and other point of entry in your house. They can make sure that those locks are not known to have easy-to-defeat features, and can advise you on how to secure any unsecured entry-points as well. They'll also do this review for all points of entry, not stop with the first issue they find, so you can be aware of all potential problems.

Pen testers are going to make sure all the locks and other security devices are being used, and used correctly, by trying to break into the house. Sure, they're promising not to break your furniture or steal your valuables, but the only way to make sure the locks are really working is for someone to try to get in when they're in use. They'll also – generally – stop once they break in, so they won't keep going and try to find other ways to gain entry once they've successfully gotten into the house.

It's not uncommon, therefore, to see auditors or regulatory agencies require both regular vulnerability scans and pen testing within an organization. **That agency or auditor wants to know both that you are keeping ahead of known issues and that you are properly defending against those issues with your security protocols and policies.** For the former, you use vulnerability scans. For the latter, penetration testing. Having both done on a regular basis (vulnerability scans about once every three or four months, pen testing once or twice a year) will keep your organization secure; and keep any surprises from sneaking up on you.