RELEASE DATE:	CONTACT:
February 18, 2021	Mike Sullivan
	Sr. Security Architect
RELEASE METHOD:	Enterprise IT Security
Social Media and Website	info@eits.com

How Penetration Testing Changed Over a Decade

High-profile security breaches created a cybersecurity boom and an increased demand for penetration testing, but with it came challenges. The boom arguably started in 2010 with the publicity of Stuxnet that compromised Siemens and the Iran nuclear program, moving into 2011 with Lulzsec's high-profile, embarrassing-yet-simple compromises of household names such as the Central Intelligence Agency, Sony, Minecraft, News Corp, and AT&T. With it the term "Advanced Persistent Threat" became a buzzword in the public-sector security industry, and corporate security budgets were increased to respond to the new focus. What once was an activity for large, mature corporations and government organizations was now being requested by smaller and less mature customers with the hope that they would not be part of the next embarrassing headline.

In the first two parts of this series (Network Pen Testing - EITS), I outlined the reasons for conducting pen tests and described common weaknesses that I continue to see but may not have ever been reported on your previous tests. This final installment expands on the reasons these vulnerabilities may have been omitted from previous pen test reports and provides an additional dimension: rising demand as a catalyst for decreased standards and pseudo-offerings.

Vulnerability Scans Undercut Pen Tests

As the demand for penetration testing increased, the supply of trained, qualified testers evaporated, resulting in the creation of subpar service offerings. The most common of these became the use of an automated vulnerability scanning tool to generate hundred- or thousand-page reports full of un-validated findings. The size of the report was touted to represent the amount of effort involved, which was quite the opposite. Organizations that were already ill-prepared for a cyberattack were buried under pages of false positives that discouraged them from performing remediation for the few actionable findings.

Over the years the final product of these types of tests has been polished to appear more realistic, but the work performed to generate them remains the same. A key indicator to identify these counterfeit products is the lack of screenshots accompanying findings and the absence of post-exploitation evidence. Showing the result of compromise cannot be proven where no exploitation occurred.

One potential reason that you have not seen the old vulnerabilities from Part II (Pen Test Article 2 Pen Test Findings) exploited in your environment may be that you procured a vulnerability scan disguised as a pen test.

Vulnerability scans consist of automated checks searching for the existence of static information like version numbers or specific strings in a configuration. The existence of this information implies that a vulnerability exists, but it is not proof alone. Automated scans also do not have the ability to identify the impact of chaining vulnerabilities together to achieve a specific goal.

Vulnerability scanning has its place in your security program, specifically in your Vulnerability Management program. However, not all vulnerabilities are exploitable and penetration testing is supposed to dive deeper into what can be proven, to allow you to prioritize your remediation activities.

The resulting output of one of these types of tests may include findings for some of the vulnerabilities discussed in Part II. However, they are likely to be reported as Medium or Low severity – the default of the scanner – and are either overlooked or remain under the threshold of remediation for most organizations.

Shorter Timeframes Limit Accuracy and Narrow Focus

Other reasons you may not have seen these findings before stems from the same restriction of supply vs. demand. With a limited number of qualified resources to perform testing comes shorter timeframes and a more limited scope of investigation.

The One-week Standard

High demand for testing and low supply of testers, now coupled with the invasion of low-level effort vulnerability scans, resulted in a race to the bottom for the length of an engagement. Unfortunately, once the dust settled, the industry appeared to settle on one week for the total duration of a pen test. While this allows for a significant number of penetration tests to be completed each year in a metrics-driven business world, corners must be cut. Not all devices can be tested, not all attack paths can be explored, and testers may not be able to spend more than 15 minutes on an anomaly that may have been discovered. In an effort to standardize testing methodology for the tight timeframe, many methods are left on the cutting room floor.

One size does not fit all so work with your vendor to ensure that all use cases that you need tested will be performed. If you do not have use cases in mind, ask your tester how they handle running out of time on an engagement. My preference on time-boxed tests is closer to 4 weeks to simulate low and slow attacks, which are hard to detect. This also allows for just as much time to focus on post-exploitation activities, which are arguably more valuable than knowing the point-in-time vulnerability that a real-world attacker can take advantage of to access and siphon off your sensitive information.

One Path of Attack

This compressed timeline creates another problem: testers find themselves focusing on a single attack path, though you may have an environment containing multiple compromise vectors. They work through their process of exploitation, elevation and pivoting to achieve their goal but have only explored one path. The documentation is great, and the recommendations make it possible to fix and validate, but your next pen test results in complete compromise all over again via a different method. This and many more methods existed during the first test but were not explored because of time constraints.

As the customer, your remediation process has been dragged out over multiple years, during which you may have suffered from a false sense of security and believed that all the holes had been identified and plugged. Customers and vendors should be reasonable when setting timeframe expectations during the

scoping portion of their tests. While time directly affects cost, you must remember that you get what you pay for. Would you like to have?

- A test that exploited one weakness which results in privilege escalation but relies on you to imagine the impact to the business?

- OR -

- A test that exploits multiple weaknesses which results in access to sensitive information and explains the thought process used to get there, as well as the proof of what information was accessed?

New Talent in the Field Presents New Challenges

While the cybersecurity industry has responded to the lack of qualified staff and attempted to remedy this portion of the equation, we have also introduced another problem: the next generation does not have the same prior knowledge to pull from as experienced security staff. Many of these new penetration testers were not in the IT field or even the job market when these vulnerabilities were discovered and discussed at length. Pen-testing skills are built on top of fundamental administration experience. Knowing how to abuse existing functionality in a system requires knowledge of how that system is being used. This knowledge comes from painful experience during the implementation and maintenance of that system.

The reinforcements have been taught the latest techniques to take advantage of the newest vulnerabilities because of the ever-increasing pace that they are discovered, but they are missing the old attack methodologies that still exist due to lack of experience. So, the new breed of tester may be adept at identifying and exploiting modern-day problems while not even realizing that the attack surface is even larger. This highlights the need for differing sources to perform your regularly scheduled penetration tests.

Even among well-seasoned penetration testers, everyone has their own unique skillsets, backgrounds, and capabilities. A tester with a networking background will attack an organization in a completely different way from one with a background in web design. Both tests may end successfully and provide customers valuable information on how to secure their environment, but the tests will in no way be equal. Therefore, it is important to have multiple vendors perform your scheduled testing so that you have a variety of methodologies and skillsets focusing on your environment.

How to Get the Best Penetration Test Results

The cybersecurity boom that came on the heels of highly publicized attacks caused some adverse effects for the IT security world. Keep these industry trends and shortfalls in mind when securing your next pen test:

Ensure you are not settling for a vulnerability scan disguised as a penetration test. A vulnerability scan is not a penetration test. Vulnerability scanning is a legitimate piece of your security program, but customers should expect them to cost much less due to their entirely automated nature. Do not be afraid to ask for a sample report or come right out and ask if the offering is just a vulnerability scan. If the vendor does not provide proof of the exploitation in the report, then you did not get a penetration test.

Give the testers enough time to do a good job. Plan ahead, don't wait until a month before your requirement date to procure a pen test. If the vendor proposes a one-week timeline, ask them why. Is it due to availability or cost? Ask them what they do after gaining elevated access to an environment. Do they stop there, or do they start over, looking for other attack paths?

Change up your vendors. Having the same team look at your environment year after year slowly becomes no different than you looking at your own environment. Different skillsets and approaches give a fresh perspective and will identify problems that have been overlooked. This does not mean that vendor A is better or worse than vendor B. It is just applying the same principle as asking for a second opinion from another physician.

If your team does not conduct penetration testing, develop a plan to systematically challenge your defenses, preferably with help from third-party professionals who can guide you through the process. Even if your organization performs routine testing, time frames can be highly compressed, so not all testers will look for older problems. Remediating these vulnerabilities in advance and knowing what you are paying for will allow you to avoid findings or devote time to more problematic ones.

This three-part series described why pen testing is performed, offered ways to begin remediating vulnerabilities and explained some industry shortfalls to consider before an external tester begins trying to exploit your environment. If you missed either of the first two parts, please visit our website (Network Pen Testing - EITS) to read more. Make time to harden your environment and prevent findings on your next pen test.

The experts at EITS focus on helping industry professionals develop robust security practices. Please share with any peers and partner organizations you think may benefit from this – sharing information improves everyone's security posture.