IT security professionals are the unsung heroes of each organization. I know, I used to be one. When I ran Security at Orbitz, it was absolutely critical that my team and I stayed on top of threats, attacks and potential exploits. And we had to ensure that our execution was flawless, every day, despite the fact that the influx of new data and threats was never ending. Any slip up could put the company at risk of a breach.

While in the trenches, we developed a series of best practices for working with vulnerability scanners such as Qualys, Nessus, Rapid7 and the rest. I found that following these practices dramatically improved our company’s security posture, and helped all of us sleep a lot better at night.
HERE’S WHAT WE LEARNED:

1. CVSS is great. But it’s only part of the picture.

CVSS is table stakes these days when examining vulnerability scan results, but you need to be careful not to place too much reliance on CVSS when prioritizing your remediation tasks. CVSS has the ability to add temporal data in the effort to account for changing threats; however, temporal scores can only lower and not raise the actual score. So if you look at CVSS and only focus on the 8's, 9's and 10's, you may be missing the actual dangers.

Let me give you a hot button, commonly referenced example: the Heartbleed vulnerability exposed the majority of web servers running over SSL on the Internet and allowed for the leaking of data (including the very encryption keys that protected them). But how did CVSS rate Heartbleed? It scored at only a five.

Why did CVSS misread Heartbleed so badly? The scoring system doesn’t allow for a high score on a vulnerability whose impact is “information leakage,” even though in this case the information being leaked could have been—and was—highly sensitive. You have to take into account an ever-shifting threat landscape and model, asset priorities, and mitigating controls in order to take a holistic approach to prioritized remediation.

2. Authenticated scans are your friend.

One of the common complaints of vulnerability scan results is false positives. While not foolproof, running authenticated scans can go a long way to removing false positives and has the added benefit in many cases of providing a CPE fingerprint.

If you’re not familiar with the acronym, CPE stands for Common Platform Enumeration. The CPE fingerprint is a machine-readable representation of what is running on a particular asset down to the exact version. This will give you the ability to track assets, and it can serve as a poor man’s asset management system. One quick security benefit of knowing what your assets are running is knowing when new vulnerabilities come out and what assets they affect without running a scan. You can find more about CPE here: https://cpe.mitre.org

Of course, authenticated scans apply to your web application scans as well. Authenticated web application scans allow for detection of vulnerabilities to the protected areas of your application, which is likely where the valuables are stored and processed. I’m still surprised to see many organizations scanning their publicly facing web applications, but not setting up authenticated scans.

One note here: authenticated scans will produce a greater volume of results. This means, of course, that you must be mindful and test these scans on non-production systems prior to rolling out.
3. Remember the OSI stack has 7 layers.

As mentioned above, you can’t forget about your applications. I see an amazing number of organizations that are far along in their network vulnerability scanning programs, yet they aren’t doing anything with their applications. Scanning your applications is a key component of a good vulnerability management program. Two areas that are continuously problematic each year in the Verizon DBIR are misconfiguration and application security.

While scanning your applications, it’s worth noting that doing so only represents the basic blocking and tackling when it comes to a mature application security program. Needless to say, as your program matures, your program is likely to include threat modeling, static analysis, penetration testing, code reviews, etc. You cannot ignore layer 7, which has become one of the most common targets for attacks and breaches.

4. Don’t dump-and-run, make it consumable.

You know what I’m talking about when I talk about the infamous dump-and-run. “Here’s your 300-page PDF with a laundry list of every vulnerability known to man!”

From what I’ve seen, being the recipient of a dump-and-run is handled by systems administrators, developers, network engineers and other remediators exactly the same way: by filing it in the trash. The least effective way of getting critical issues fixed in your environment is the oversized PDF dump.

You need to make scan results consumable and actionable for those responsible for remediation. SysAdmins don’t want a laundry list of vulnerabilities listed out by their CVE identifier; they need an actionable list of what needs to get done, such as deploying a specific patch or updating to a specific group of assets with their relevant identifiers.

As Gene Kim so eloquently stated, “The rate at which information security and compliance introduce work into IT organizations totally outstrips IT organizations ability to complete, whether it’s patching vulnerabilities or implementing controls to fulfill compliance objectives. The status quo almost seems to assume that IT operations exist only to deploy patches and implement controls, instead of completing the projects that the business actually needs.”

Or to put it another way...don’t be that guy.
5. You can actually prioritize, rather than just analyze.

Typically, security teams spend tons of time putting together Excel spreadsheets and swimming through countless rows of data. Doing so will get the job done, eventually...kind of. But the problem is, as soon as you manage to rise to the top of your current data ocean, another wave will hit you. You can’t prioritize what to fix if you can’t even keep up with the inbound volume of data regarding potential threats, breaches and attacks.

What you need is a way to immediately prioritize the data in front of you. This is a case where tools—rather than elbow grease—may be of help. Platforms exist that can sit on top of your scan data and help you identify weaknesses in your infrastructure in the context of real-time threat data (i.e. what’s actually occurring in the world right now, and which may affect you).

This kind of platform solution—a GPS for your scan data—can be an immense time savings, and help guide your efforts in a much more efficient way than simply sorting by CVSS scores, each and every day.

Now let’s take a look at some common “gotchas” of vulnerability scanning.

Common Gotcha #1: DHCP

DHCP is commonly used in organizations to manage IP addresses on various assets. It’s very popular in desktop environments and allows for flexible management of networks. However, DHCP introduces complications when managing vulnerability scan results.

By default, vulnerability scanners often report results by IP address. But what if the next time you scan your network all your assets have changed their IP address? It turns into a mess, and it becomes impossible to track remediation.

It’s best to segment scans against DHCP assets and use a different identifier for these such as hostname, NETBIOS or other identifier. You’ll need a flexible system to manage the scan results to ensure that you’re able to track remediation accurately without adding additional complications.
Common Gotcha #2: Load Balancers

Load balancers are wonderful, except when you’re scanning for vulnerabilities on the other side of them. Similar to the asset issues with DHCP, you’ll need to make sure you have access to the DHCP configuration so you can track which IP address and port numbers are responding with the reported vulnerability. Without this critical information, you’ll be left with a virtual IP address as an asset identifier (and a whole lot of guesswork).

So those are my tips, tricks and secrets. I hope they help you build a stellar security and vulnerability management program at your own organization!

About Ed Bellis & Kenna Security

Ed Bellis is the Cofounder of Kenna, a SaaS platform that correlates external Internet breach data, exploit data and zero-day threat intelligence with internal vulnerability scan data so organizations can focus on fixing the most critical vulnerabilities. Kenna processes over a billion vulnerabilities a day against Internet breach data for its users.

Ed formerly served as the CISO of Orbitz, where he built and led the information security program and personnel for over six years. Ed has over 20 years of experience in information security and technology and is a frequent speaker and contributor to the information security community.

For more vulnerability management best practices:
visit www.kennasecurity.com