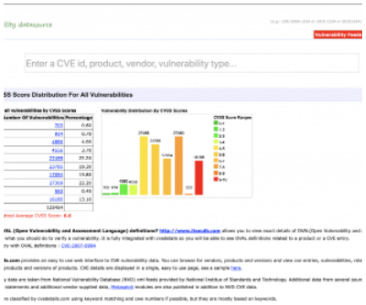
The Future of Threat Intelligence

Threat intelligence is ever-changing. One big step forward in the threat intelligence and vulnerability management world is the development of **predictive prioritization** by Tenable, the company behind the Nessus vulnerability scanners and auditing tools. Before we cover it, we need to set the scene and introduce some vulnerability management basics as it is out of scope for this course.

CVEs AND CVSS SCORES

What are CVEs?

- CVEs (common vulnerabilities and exposures) are a method of uniquely tracking publicly-reported vulnerabilities. If someone finds a vulnerability in the Windows operating system, they'll report it and apply for a CVE. If granted, a CVE value is generated based on the year and the number of the vulnerability. An example of this is CVE-2019-0708 which was a critical vulnerability in the Remote Desktop Protocol (RDP) in 2019. Using CVEs makes sharing information easier – you can simply provide someone with a CVE number, and they can lookup the ID and find all the information they need (provided it has been published). Revisiting CVE-2019-0708, you can view information about this specific vulnerability by visiting the National Vulnerability Database offered by NIST (just click the CVE number in this sentence!).
- https://CVEDetails.com is a security vulnerability database that has lots of information, and can allow us to search for specific CVEs, or even look at vulnerabilities sorted by release date.



What are CVSS scores?

- **Example CVSS rating:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H.

This is the Common Vulnerability Scoring System, used to help rank vulnerabilities based on their attributes. Whilst this may look like some confusing code, it's actually fairly simple. **Base Score: 8.8 HIGH** tells us that this vulnerability has a high severity. The idea behind these scores is that it provides value at a glance, so you can look at the score and immediately tell if this vulnerability is bad. Obviously, this is a generic score, and what may be a critical vulnerability for one company may not affect another company at all – it all depends on the products and versions you're using, the security controls you have in place, and a number of other factors, so this score value should only be taken as a

the security controls you have in place, and a number of other factors, so this score value should only be taken as a generic guideline.

VULNERABILITY CONTEXT

The issue with CVSS scores is that a vulnerability which may be rated 10.0 CRITICAL might not actually affect some organizations, as it depends on the technology that is being used. A vulnerability in Solaris systems isn't going to affect a company that uses only Windows systems.

Another issue is that whilst some vulnerabilities could be very damaging if executed correctly, hackers might not actually bother trying to exploit them due to factors such as technical complexity. If no threat actors are exploiting a critical-rated vulnerability, then there is less of a risk than a high-rated vulnerability which is actively being exploited in the wild (a term used to describe activity across the internet).

It's all about context and tracking exploitation activity to determine the prioritization rating for the organization. But the guys and girls over at Tenable have had a very clever idea.

PREDICTIVE PRIORITIZATION

Tenable claims that predictive prioritization will help "focus first on the security issues that matter most". Predictive Prioritization combined vulnerability data with threat intelligence to provide context, and generate new scores that consider which vulnerabilities are most likely to actually be exploited. The new scoring system, named Vulnerability Priority Rating, or VPR, is a dynamic value that will change based on threat intelligence updates – if a previously quiet vulnerability was suddenly seen being exploited in the wild, the VPR number would go up, so that security teams know it has a higher priority for remediation. This is the perfect case study to talk about when considering how threat intelligence will change the future of cybersecurity. By providing scores that actually reflect the genuine risk of a vulnerability being exploited, organizations can patch security issues that need to be done as a priority, instead of completing remediation work that will have immediate defensive benefit.

Want to read more about VPR? Check out Tenable's site.

Previous Topic
Mark Complete
Next Topic
Back to Lesson