Professor Messer

Vulnerabilities, Threat Vectors, and Probability – CompTIA Security+ SY0-401: 2.1

The bad guys are very good at infiltrating our computer systems. In this video, you'll learn about system vulnerabilities, examples of threat vectors, and how to calculate the probability of a security risk.

<< **Previous Video:** Quantitative and Qualitative Risk Assessment

Next: Risk Avoidance >>

A vulnerability is a flaw or a weakness that's going to affect security. For example, if you have a door that has a broken lock, that's certainly going to affect the security of everything inside of that room. Or it may be something in software. Or maybe a file in a Microsoft operating system library happens to have a programming vulnerability inside of it that now means that people can get access to the operating system itself. Of course, just because a vulnerability exists doesn't mean that anybody has taken advantage of that vulnerability. For example, someone has to first know that the vulnerability exists to be able to take advantage. If nobody knows that the lock on the door is broken, then nobody will know they can easily gain access to that room.

It’s also very common in software to have vulnerabilities that might be sitting inside of operating system software for months or even years before anyone discovers that the vulnerability even exists. In that particular case, you might think that our operating systems are wide open. But of course, to be able to take advantage of the vulnerability, you first have to know about it. And that’s why we’re constantly telling you to update your operating system and make sure it’s patched, because we’re constantly discovering new vulnerabilities inside of that software.

The threat vector is the path that someone takes to be able to gain access to a device so that they can take advantage of that vulnerability. This might be your computer, it might be a mobile device, but somehow that bad guy has got to gain access to be able to take advantage of that problem. You might consider something like an email. In an email, a common threat vector might be an embedded link or an attached file, and the bad guys want you to be able to click that file so that they can then gain access to your computer.

All of these things like a web browser, wireless hotspot, or a telephone, all have threat vectors. You need to protect against fake sites or session hijacks in a browser. You need to protect against rogue access points, and you certainly need to protect against social engineering over the telephone. Some of these things have technological solutions, and others may require training of people to make sure someone doesn’t take advantage of that particular threat vector.

A USB flash drive, for instance, might have an executable inside of it that automatically runs when you plug-in that USB flash drive. That’s a very common threat vector. And even something like physical access. If someone’s able to gain access inside of your organization, they may be able to physically change data or steal data or equipment from inside your building.

There are many other ways that people can gain access, so you want to be sure you’re covering the bases against all of these particular threat vectors. Some of these are more susceptible to attack than others. It really depends on the threat vectors that apply to your organization. And you also have to consider what vulnerabilities might be there. If someone gains access to email, but you’re already removing all embedded links and you’re already removing all the attached files before they even get to the end user, then that threat vector is not available to the bad guys.

So what’s the probability that you might be affected by some of these vulnerabilities? First you have to understand what all of the potential threats might be and all the actual threats might be. So you need to have a very good understanding of the different possible vectors and understand where the different places might be inside of your environment that someone might be able to take advantage of. Really doesn’t matter what the probability is, you’re really trying to determine where those might be.

Then we have to identify just how many vulnerabilities do exist in our environment. This is a very large task. We have to look at all of the different operating systems we running, we have to understand what patch level they may be up to, we need to look at what applications may be in use, what services may be running, so that we can really understand what the potential might be for somebody to take advantage of a vulnerability.

Now we can start calculating how likely it might be that we would have an attack in our environment. There’s no exact formula for this. You really have to look at the number of operating systems and exactly what you might have out there that’s susceptible, and then understand where the threat vectors are and how someone might gain access to this. So this is going to be very different depending on the organization. But once you start examining this, you get a better idea of just how susceptible you might be to these particular threats in your environment.

Categories

Select Category

Recent Posts

Today's N10-008 Network+ Pop Quiz: More is better

Anti-Malware Tools – CompTIA A+ 220-1102 – 2.3

Malware – CompTIA A+ 220-1102 – 2.3

Authentication Methods – CompTIA A+ 220-1102 – 2.2

Wireless Encryption – CompTIA A+ 220-1102 – 2.2

Site Information

Contact Us

About Messer Studios

Privacy Policy

Terms of Service