Approach cybersecurity with an attacker mindset

Cybersecurity is a continuously changing field. It's a fast-paced environment where new threats and innovative technologies can disrupt your plans at a moment's notice. As a security professional, it’s up to you to be prepared by anticipating change.

This all starts with identifying vulnerabilities. In a video, you learned about the importance of **vulnerability assessments,** the internal review process of an organization's security systems. In this reading, you will learn how you can use the findings of a vulnerability assessment proactively by analyzing them from the perspective of an attacker.

Being prepared for anything

Having a plan should things go wrong is important. But how do you figure out what to plan for? In this field, teams often conduct simulations of things that can go wrong as part of their vulnerability management strategy. One way this is done is by applying an attacker mindset to the weaknesses they discover.

Applying an attacker mindset is a lot like conducting an experiment. It's about causing problems in a controlled environment and evaluating the outcome to gain insights. Adopting an attacker mindset is a beneficial skill in security because it offers a different perspective about the challenges you're trying to solve. The insights you gain can be valuable when it's time to establish a security plan or modify an existing one.

> Un groupe de personnes se sécurisant à l'aide de différentes technologies.

Simulating threats

One method of applying an attacker mindset is using attack simulations. These activities are normally performed in one of two ways: *proactively* and *reactively*. Both approaches share a common goal, which is to make systems safer.

- *Proactive simulations* assume the role of an attacker by exploiting vulnerabilities and breaking through defenses. This is sometimes called a red team exercise.

- *Reactive simulations* assume the role of a defender responding to an attack. This is sometimes called a blue team exercise.

Each kind of simulation is a team effort that you might be involved with as an analyst.

Proactive teams tend to spend more time planning their attacks than performing them. If you find yourself engaged in one of these exercises, your team will likely deploy a range of tactics. For example, they might persuade staff into disclosing their login credentials using fictitious emails to evaluate security awareness at the company.

On the other hand, reactive teams dedicate their efforts to gathering information about the assets they're protecting. This is commonly done with the assistance of vulnerability scanning tools.

Scanning for trouble

You might recall that a **vulnerability scanner** is software that automatically compares existing common vulnerabilities and exposures against the technologies on the network. Vulnerability scanners are frequently used in the field. Security teams employ a variety of scanning techniques to uncover weaknesses in their defenses. Reactive simulations often rely on the results of a scan to weigh the risks and determine ways to remediate a problem.

For example, a team conducting a reactive simulation might perform an external vulnerability scan of their network. The entire exercise might follow the steps you learned in a video about vulnerability assessments:

- **Identification:** A vulnerable server is flagged because it's running an outdated operating system (OS).
- **Vulnerability analysis:** Research is done on the outdated OS and its vulnerabilities.
- **Risk assessment:** After doing your due diligence, the severity of each vulnerability is scored and the impact of not fixing it is evaluated.
- **Remediation**: Finally, the information that you've gathered can be used to address the issue.

During an activity like this, you'll often produce a report of your findings. These can be brought to the attention of service providers or your supervisors. Clearly communicating the results of these exercises to others is an important skill to develop as a security professional.

Finding innovative solutions

Many security controls that you've learned about were created as a reactive response to risks. That's because criminals are continually looking for ways to bypass existing defenses. Effectively applying an attacker mindset will require you to stay knowledgeable of security trends and

emerging technologies.

Pro tip: Resources like NISTs National Vulnerability Database (NVD) can help you remain current on common vulnerabilities.

Key takeaways

Vulnerability assessments are an important part of security risk planning. As an analyst, you'll likely participate in proactive and reactive simulations of these activities. Preparing yourself by researching common vulnerabilities only goes so far. It's equally important that you stay informed about new technologies to be able to think with an innovative mindset.

Revision #1
Created 2023-08-21 09:07:59 UTC by naruzkurai
Updated 2023-08-21 09:08:10 UTC by naruzkurai