Approaches to vulnerability scanning

Previously, you learned about a **vulnerability assessment**, which is the internal review process of an organization's security systems. An organization performs vulnerability assessments to identify weaknesses and prevent attacks. Vulnerability scanning tools are commonly used to simulate threats by finding vulnerabilities in an attack surface. They also help security teams take proactive steps towards implementing their remediation strategy.

Vulnerability scanners are important tools that you'll likely use in the field. In this reading, you'll explore how vulnerability scanners work and the types of scans they can perform.

What is a vulnerability scanner?

A **vulnerability scanner** is software that automatically compares known vulnerabilities and exposures against the technologies on the network. In general, these tools scan systems to find misconfigurations or programming flaws.

Scanning tools are used to analyze each of the five attack surfaces that you learned about in the video about the defense in depth strategy:

1. **Perimeter layer**, like authentication systems that validate user access
2. **Network layer**, which is made up of technologies like network firewalls and others
3. **Endpoint layer**, which describes devices on a network, like laptops, desktops, or servers
4. **Application layer**, which involves the software that users interact with
5. **Data layer**, which includes any information that's stored, in transit, or in use

When a scan of any layer begins, the scanning tool compares the findings against databases of security threats. At the end of the scan, the tool flags any vulnerabilities that it finds and adds them to its reference database. Each scan adds more information to the database, helping the tool be more accurate in its analysis.

Note: Vulnerability databases are also routinely updated by the company that designed the scanning software.

Performing scans

Vulnerability scanners are meant to be non-intrusive. Meaning, they don’t break or take advantage of a system like an attacker would. Instead, they simply scan a surface and alert you to any potentially unlocked doors in your systems.

Note: While vulnerability scanners are non-intrusive, there are instances when a scan can inadvertently cause issues, like crash a system.

There are a few different ways that these tools are used to scan a surface. Each approach corresponds to the pathway a threat actor might take. Next, you can explore each type of scan to get a clearer picture of this.

External vs. internal

External and internal scans simulate an attacker's approach.

External scans test the perimeter layer outside of the internal network. They analyze outward facing systems, like websites and firewalls. These kinds of scans can uncover vulnerable things like vulnerable network ports or servers.

Internal scans start from the opposite end by examining an organization's internal systems. For example, this type of scan might analyze application software for weaknesses in how it handles user input.

Authenticated vs. unauthenticated

Authenticated and unauthenticated scans simulate whether or not a user has access to a system.

Authenticated scans might test a system by logging in with a real user account or even with an admin account. These service accounts are used to check for vulnerabilities, like broken access controls.

Unauthenticated scans simulate external threat actors that do not have access to your business resources. For example, a scan might analyze file shares within the organization that are used to house internal-only documents. Unauthenticated users should receive "access denied" results if they tried opening these files. However, a vulnerability would be identified if you were able to access a file.

Limited vs. comprehensive

Limited and comprehensive scans focus on particular devices that are accessed by internal and external users.

Limited scans analyze particular devices on a network, like searching for misconfigurations on a firewall.

Comprehensive scans analyze all devices connected to a network. This includes operating systems, user databases, and more.

Pro tip: Discovery scanning should be done prior to limited or comprehensive scans. Discovery scanning is used to get an idea of the computers, devices, and open ports that are on a network.

Key takeaways

Finding vulnerabilities requires thinking of all possibilities. Vulnerability scans vary depending on the surfaces that an organization is evaluating. Usually, seasoned security professionals lead the effort of configuring and performing these types of scans to create a profile of a company's security posture. However, analysts also play an important role in the process. The results of a vulnerability scan often lead to renewed compliance efforts, procedural changes, and system patching. Understanding the objectives of common types of vulnerability scans will help you participate in these proactive security exercises whenever possible.

Tip: To explore vulnerability scanner software commonly used in the cybersecurity industry, in your preferred browser enter search terms similar to "popular vulnerability scanner software" and/or "open source vulnerability scanner software used in cybersecurity".

Revision #1
Created 2023-08-20 08:23:41 UTC by naruzkurai
Updated 2023-08-20 08:23:54 UTC by naruzkurai