[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@5a7fea5bb55a4765b3202d9cfe8651a9?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

reference https://purplesec.us/internal-vs-external-vulnerability-scans/

**Internal VS External Vulnerability Scans: What’s The Main Difference?**

by [Josh Allen](https://purplesec.us/author/joshua_selvidge/)

Reviewed by [Jason Firch, MBA](https://purplesec.us/author/purplesecllc/)

In a world with ever-evolving technology comes ever-evolving threats and [performing vulnerability scans and assessments](https://purplesec.us/services/network-vulnerability-scanning/) are one of the best ways to protect the networks businesses rely on to operate.

**An internal vulnerability scan is performed typically with  access to the internal network, with the main benefit of identifying  at-risk systems while providing insight for patch management processes.  An external scan is performed outside of a network and targets specific  IP addresses to identify vulnerabilities. An external scan can also  detect open ports and protocols,**[**similar to an external penetration test**](https://purplesec.us/external-vs-internal-network-penetration-tests/)**. Both application and network scans not only detect vulnerabilities but may check for compliance against several different baselines.**

In this article, I’m going to discuss the main differences between  internal and external vulnerability assessments. By the end, you will  have a better understanding of which scan should be performed for a  given situation, and how your business can use them to protect a  network.

**Article Navigation**

* [What Is An Internal Vulnerability Scan?](https://purplesec.us/internal-vs-external-vulnerability-scans/#WhatIs)
  + [What Are The Benefits?](https://purplesec.us/internal-vs-external-vulnerability-scans/#BenefitsInternal)
  + [How Often Should Scans Be Performed?](https://purplesec.us/internal-vs-external-vulnerability-scans/#OftenInternal)
  + [Credentialed VS Non-Credentialed](https://purplesec.us/internal-vs-external-vulnerability-scans/#Cred)
* [What Is An External Vulnerability Scan?](https://purplesec.us/internal-vs-external-vulnerability-scans/#External)
  + [What Are The Benefits?](https://purplesec.us/internal-vs-external-vulnerability-scans/#BenefitsExternal)
  + [How Often Should Scans Be Performed?](https://purplesec.us/internal-vs-external-vulnerability-scans/#OftenExternal)
* [What Are The Next Steps After Performing The Scan?](https://purplesec.us/internal-vs-external-vulnerability-scans/#NextSteps)
* [Vulnerability Scans And Risk Assessments](https://purplesec.us/internal-vs-external-vulnerability-scans/#Assessments)
* [Popular Vulnerability Scanning Tools Used](https://purplesec.us/internal-vs-external-vulnerability-scans/#Tools)

[](https://purplesec.us/cyber-security-trends-2021/)

**What Is An Internal Vulnerability Scan?**

Internal vulnerability scans are performed from a location that has  access to the internal network you are scanning. These scans show  vulnerabilities at a greater depth as they can see more of the network  compared to an external scan.

Internal scans are best used when you need to verify patching has  occurred, or when you need to provide a detailed report of  vulnerabilities in the network.

**Read More**: [How To Develop & Implement A Network Security Plan](https://purplesec.us/network-security-plan/)

**What Are The Benefits Of Internal Scans?**

There are a number of benefits that come from performing internal  scans. By performing internal scans on a regular basis, you are taking a proactive approach to protect your network from known vulnerabilities.

Internal scanning can also provide insight to your patch management  process. When analyzing the data from the scan, pay close attention to  trends such as the top missing patch and top vulnerable machines.

**Common vulnerabilities to be aware of include:**

* A lack of third party patches.
* Timeliness in patching known vulnerabilities with a high-risk rating.
* Named vulnerabilities such as DROWN, EternalBlue, or Heartbleed.

**How Often Should Internal Scans Be Performed?**

[Frequency of scans largely depends on the organization and the type of business](https://purplesec.us/how-often-perform-vulnerability-scan/). For a small, locally-owned shop, it may not be feasible to run  vulnerability scans as often as a large enterprise performs them.

My recommendation is to run internal scans at least monthly,  following Microsoft’s Patch Tuesday and your company’s “patch day”. If  there are financial constraints preventing monthly scans, then consider  performing them once per quarter.

You may be wondering why I called out [Patch Tuesday](https://en.wikipedia.org/wiki/Patch_Tuesday). This is because Patch Tuesday not only informs the public of new  patches available but also informs hackers of new, most likely  unpatched, vulnerabilities.

Take WannaCry for example. [This exploit took advantage of a known Microsoft vulnerability](https://techcrunch.com/2019/05/12/wannacry-two-years-on/) which had patches available to mitigate but computers were still found  vulnerable, most likely due to poor patch management processes.

**Credentialed Vs Non-Credentialed Scans**

When thinking about internal vulnerability scans, you may wonder why  you would even consider running a non-credentialed scan. Wouldn’t  credentialed scans provide more information?

**Well, the answer is yes AND no.**

While credentialed scans provider a better and deeper understanding  of what vulnerabilities exist to an outsider attempting to exploit a  known vulnerability via a malicious download or phishing attempt, we  need to realize that not all attacks come from the outside in.

With technology becoming more readily available and easier to use for non-technical users, the risk of an insider attack has never been more  real. Non-credentialed scans simulate [what type of information an insider, without privileged access](https://purplesec.us/privilege-escalation-attacks/), can gain about the security posture of your network.

While this type of scan may not seem useful, do not dismiss it. You  may be surprised to see what a regular user can learn about the network  or what information they might have access to that they shouldn’t.

**What Is An External Vulnerability Scan?**

External vulnerability scans are performed from outside of the  network you are testing. These scans are targeted at external IP  addresses of your network. The type of information you will find useful  in these scans are not only the vulnerabilities but the list of ports  that are open to the internet.

External scans are best used when you need to verify the strength of your externally facing services.

**What Are The Benefits Of External Scans?**

External scanning, much like internal scanning, has many benefits.  Again, you are taking a proactive approach to protect your network by  performing these scans. External scans show weaknesses in your network  that could lead to a potential incident.

By looking at your network from this view, you can easily identify  what that most pressing issue is within your network. You can also  identify any services or new servers that have been set up since the  last scan and identify if they present any new threats to your  organization.

**Common vulnerabilities to be aware of include:**

* Services listening on unsecured transfer protocols.
* Servers configured with deprecated services (SSL, TLS 1.0, TLS 1.1).
* Named vulnerabilities.

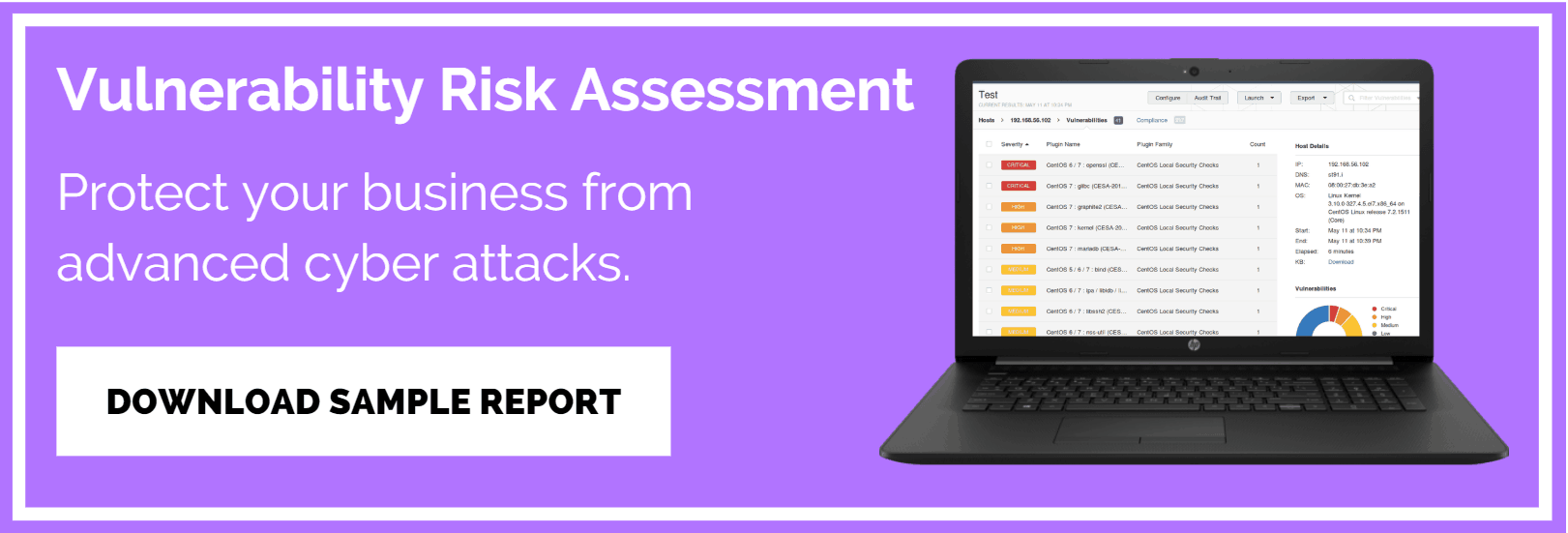
**How Often Should External Scans Be Performed?**

I recommend running external scans on a monthly basis, at a minimum. I have found that running external scans one month apart is a happy  medium between scanning too much and not enough.

While running these scans you should pay close attention to any new  IP addresses or services that appear. Ensure any anomalies you come  across have been approved by a formal process and were implemented in a  secure fashion.

**What Are The Next Steps After Performing A Vulnerability Scan?**

After performing your scans, it is important to act on them. Often  times these scans are run with no analysis performed on the backend.  Analysis should occur in a format that makes sense to the company and in a way that minimizes the possibility of overlooking a potential threat.

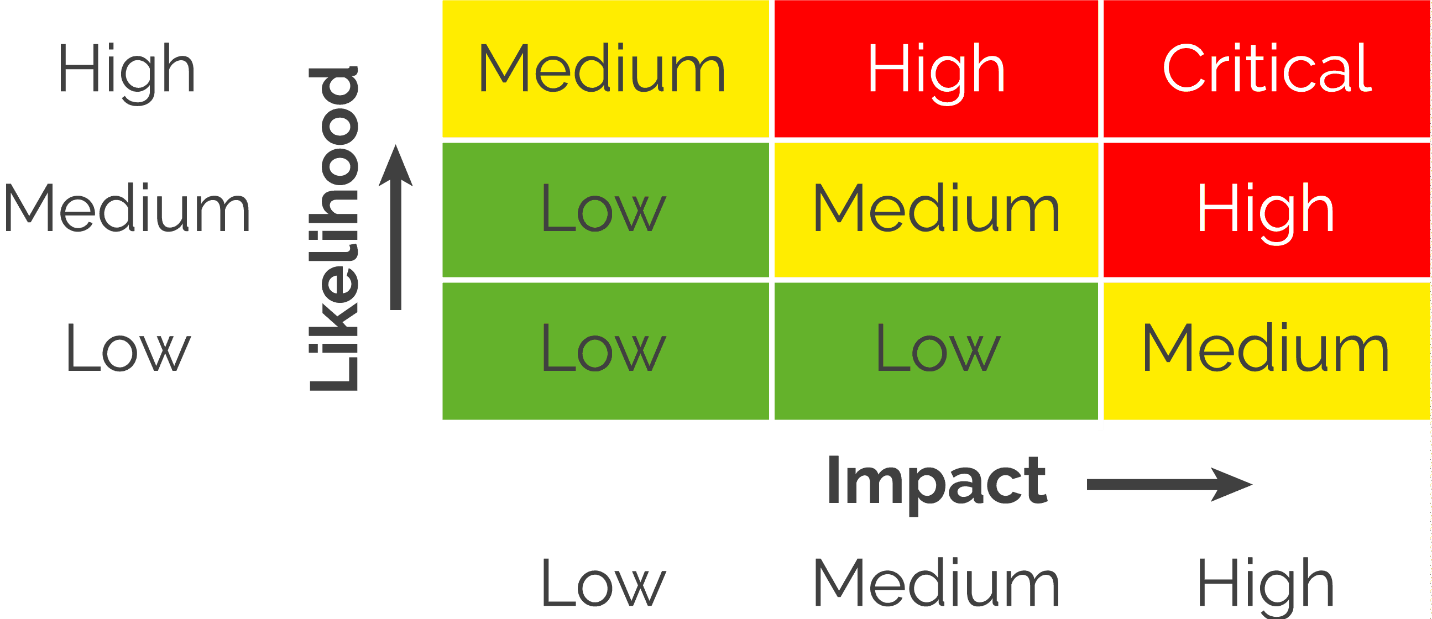
[](https://purplesec.us/resources/sample-vulnerability-assessment-report/)

I have seen analysis occur by manually reviewing the results and by  having an automated process for reporting on the top missing patches.  Either way, there should be some type of action to take away from each  scan.

The ultimate goal of vulnerability scans is to provide insight so you may improve the overall security posture for your company. Scanning  should be a step that is built into your patch management and risk  management processes. Each scan should be reviewed for concerning  patches and the remediation efforts should be discussed and approved  with IT management.

Determining what to look for in scans really depends on the company  and what their approach is to security. Do not get blindsided by the  risk ratings most tools provide though.

A **vulnerability assessment risk matrix** is often used to visually represent scan results in an easily understood and  digestible format for all stakeholders within an organization. This  includes security teams, IT staff, finance, operations, and executive  leadership.



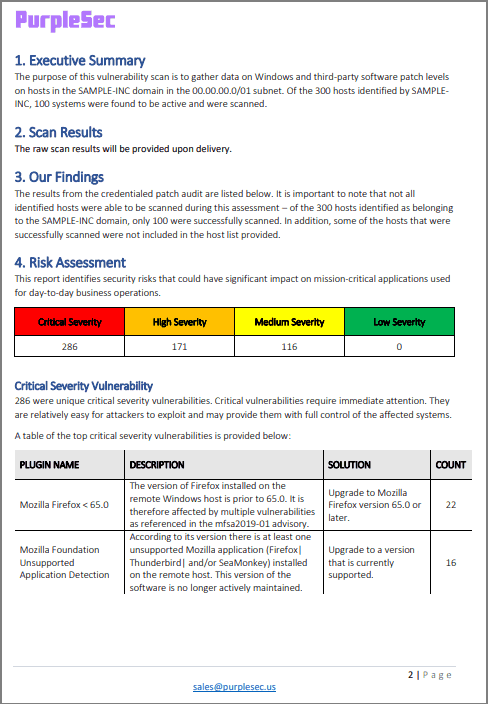
Although there may be a number of high and medium vulnerabilities,  take your time and review the low and information vulnerabilities as  well. In my experience, I have found low and informational  vulnerabilities that showed remote desktop services and unencrypted file transfer services accepting requests over the internet.

**Vulnerability Scans And Risk Assessments**

As previously mentioned, vulnerability scans are part of a risk assessment.

[Vulnerability assessments](https://purplesec.us/perform-successful-network-vulnerability-assessment/) are conducted when required by regulatory compliance, like HIPAA or  PCI, or by request from company leadership to better understand their  risk posture.

While performing a risk assessment, vulnerability scans are often one of the first things done to gain a better understanding of the network  and the company’s stance on security. By performing these types of scans you are provided an almost instant report of the security posture of  your network.

[](https://purplesec.us/wp-content/uploads/2019/03/Sample-Network-Security-Vulnerability-Assessment-Report-Purplesec.pdf)

Risk assessments, coupled with vulnerability scans, provide company’s a road map of what they should either be doing or continue doing, to  strengthen their security posture.

[](https://purplesec.us/wp-content/uploads/2021/01/Vulnerability-Patch-Management-Template-PurpleSec.pdf)

**Popular Vulnerability Scanning Tools Used**

There are a number of products that can perform vulnerability scanning including [Tenable](https://www.tenable.com/), [Qualys](https://www.qualys.com/), and [OpenVAS](http://www.openvas.org/) to name a few.

Keep in mind that commercial applications, such as Tenable and  Qualys, will be a more “out of the box” solution whereas open-source,  such as OpenVAS, will require more configuration upfront. Whichever tool you use, ensure you are configuring in a way that will best serve you  and the network you are protecting.