# Day 1

### How Antivirus Works

Antivirus software scans a file, program, or an application and compares a specific set of code with information stored in its database. If it finds code that is identical or similar to a piece of known malware in the database, that code is considered malware and is quarantined or removed.

### How does a traditional antivirus identify a virus?

All the executable programs that pass through the system go through an antivirus scan. They then undergo a comparison test with the blacklisted signatures. If they appear to be the same as a blacklisted one, then they are considered to be a malware file. The other program files are then processed through Defense+ HIPS (Host Intrusion Prevention System) – this permits only the known files while the unknown files that look suspicious are moved into a restricted virtual environment. The identified good files are documented in the Whitelist, while the suspicious files will be quarantined in the Sandboxed environment.

### Features of Antivirus Software

- Background Scanning - Antivirus software helps to scan all the applications, files and programs that are opened from the backend. This process is called an on-access scanning. This ensures real-time protection, giving complete computer protection from threats and other malware attacks.
- Complete System Scans - Full system scans are by and large not really vital when you have an on-access scanning system in hand. Full system scans become indispensable when an antivirus software is installed for the first time or if the antivirus software is not updated with new virus definitions recently. This is done to ensure that there are no malware infections hiding behind the

codes on the system. Full framework checks are additionally valuable when you repair your contaminated PC.

- Virus Definitions - Antivirus software functions based on the virus definitions to recognize if the file/program is genuine or malware intended. That is the main reason to archive on the new virus definitions. The virus definitions stashes the signatures of any viruses that has been categorized as infectious in the wild. In the event that the antivirus software checks any application or file and that it finds the document infected by a malware that looks similar to the malware in the malware definition, then that file or program is stopped from executing and then it is moved into the quarantine. The antivirus software then processes the malware and later sends it to the lab for analysis on the traits and the purpose behind the malware creation.

**How traditional antivirus works?**

- Signature-based detection - This is most basic in any traditional antivirus programming that checks each .EXE document and approves it with the known infections of the database and different sorts of malware. Or, on the other hand, it checks if the obscure executable document malfunctions, which denotes signs of infections.

  Documents, programs and applications are generally scanned for viruses when they are being used. Once an executable program is downloaded, it is instantly scanned to check if it is infected with a malware. Antivirus programming can likewise be utilized without on-access scanning techniques. However, it is prudent to constantly deploy on-access scanning method as it becomes a challenge to eliminate any viruses once they infect the system.
- Heuristic-based detection – The heuristic-based detection generally works better in combination with signature-based detection. Both Hueristic and signature-based detection, when combined, make the antivirus more effective. The Heuristic-based detection has been most used in all the antivirus software.

This causes the antivirus programming to recognize new or a variation of an adjusted rendition of malware, even without the most recent infection definitions. Antivirus programs utilize heuristics, by running vulnerable files or applications containing suspicious code , inside an isolated runtime virtual condition. This shields the vulnerable code from contaminating this normal working environment.

- Behavioural-based recognition
- Sandbox detection
- Data mining techniques

Behavioral-based recognition - This type of recognition is utilized as a part of Intrusion Detection component. This is more biased in recognizing the attributes and traits of the malware during the process of execution. This method functions well to identify malware only when there is malicious performance of the applications.

Sandbox recognition - It works destined to that of behavioral-based identification strategy. It executes any applications in the virtual condition to track the type of activities it performs. Confirming the activities of the application/program when signed in, the antivirus programming can distinguish if the program is malevolent or not.

Data mining strategies - This is one of the most recent patterns in recognizing a malware. With an arrangement of the traits of a program, Data mining finds if the file or an application is a malware.

## How 3rd gen Antivirus works?

3rd gen Antivirus offers 360° security against online dangers by consolidating a capable antivirus, an enterprise packet filtering firewall, and host intrusion prevention system called HIPS.

3rd gen Antivirus enables you to perform web-based banking and shopping without t delicate data like charge card numbers and passwords being followed or stolen. The3rd gen Antivirus have 'Virtual Desktop' allows you to open applications and sites that you are uncertain of in a safe domain disengaged from whatever is left of your computer.

**What is Firewall?**

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic.

**How Does a Firewall Work**

As mentioned previously, firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer’s entry point which only allows trusted sources, or IP addresses, to enter your network.

A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rules.

These rules are based on several aspects indicated by the packet data, like their source, destination, content, and so on. They block traffic coming from suspicious sources to prevent cyberattacks.

For example, the image depicted below shows how a firewall allows good traffic to pass to the user’s private network.

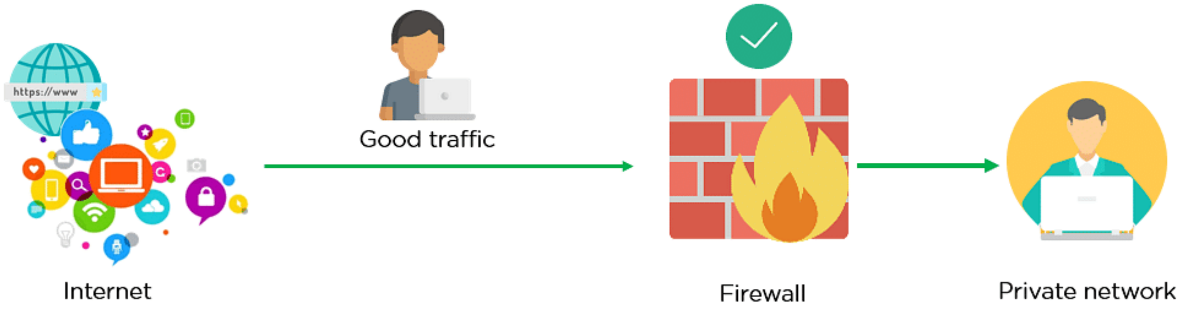


Fig: Firewall allowing Good Traffic

However, in the example below, the firewall blocks malicious traffic from entering the private network, thereby protecting the user's network from being susceptible to a cyberattack.

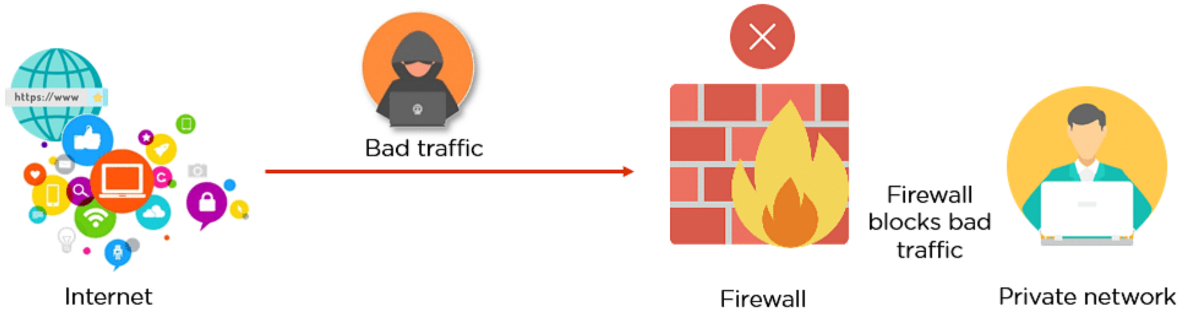


Fig: Firewall blocking Bad Traffic

This way, a firewall carries out quick assessments to detect malware and other suspicious activities.

There are different types of firewalls to read data packets at different network levels. Now, you will move on to the next section of this tutorial and understand the different types of firewalls.

**Types of Firewalls**

Five types of firewall include the following:

- packet filtering firewall
- circuit-level gateway
- application-level gateway (aka proxy firewall)
- stateful inspection firewall
- next-generation firewall (NGFW)

**Packet filtering firewall**

Packet filtering firewalls operate inline at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets; rather they compare each packet received to a set of established criteria, such as the allowed IP addresses, packet type, port number and other aspects of the packet protocol headers. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped -- that is, they are not forwarded and, thus, cease to exist.

**Circuit-level gateway**

Using another relatively quick way to identify malicious content, circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered trusted. They don't inspect the packets themselves, however.

### Application-level gateway

This kind of device -- technically a proxy and sometimes referred to as a proxy firewall -- functions as the only entry point to and exit point from the network. Application-level gateways filter packets not only according to the service for which they are intended -- as specified by the destination port -- but also by other characteristics, such as the HTTP request string.

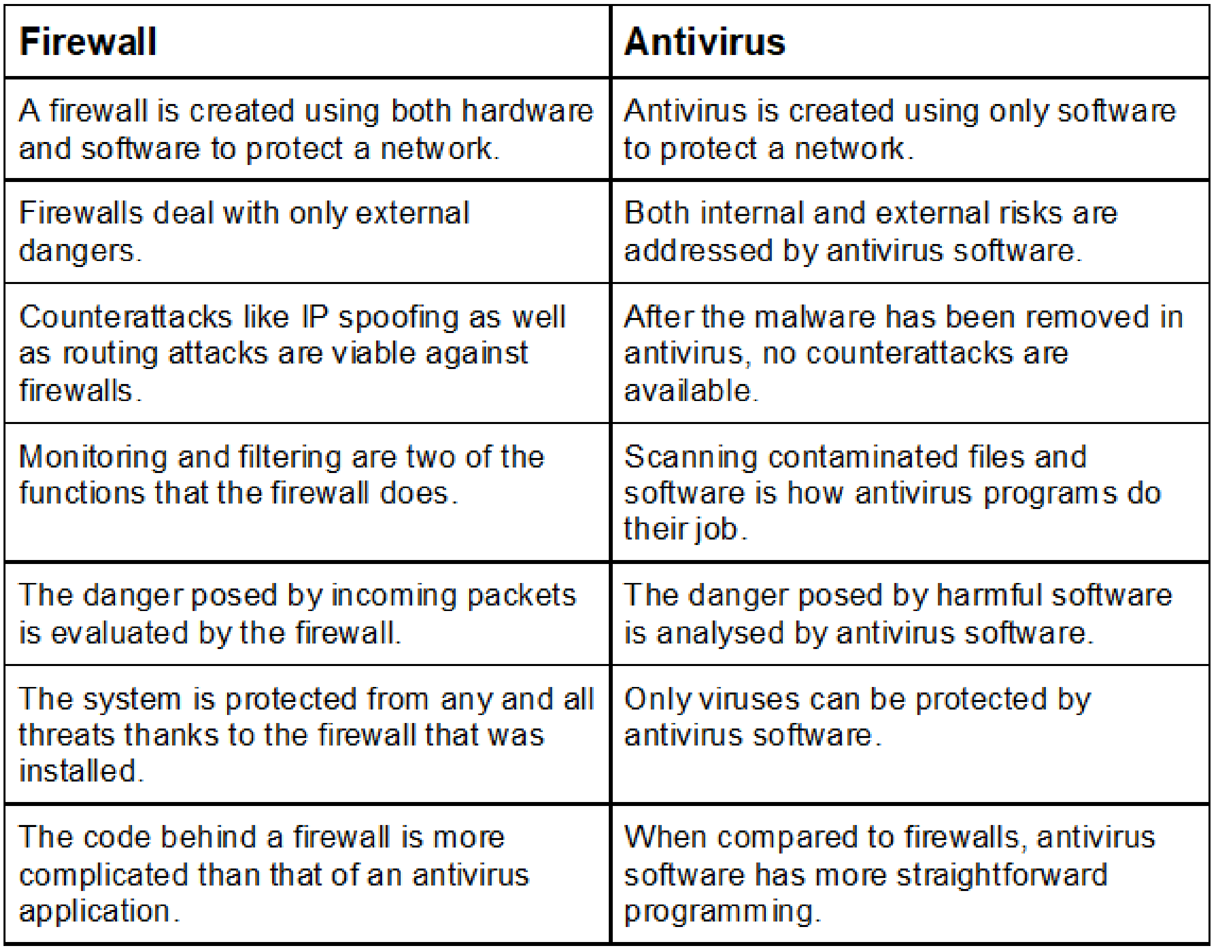
### Stateful inspection firewall

State-aware devices not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.

### Next-generation firewall

A typical NGFW combines packet inspection with stateful inspection and also includes some variety of deep packet inspection (DPI), as well as other network security systems, such as an IDS/IPS, malware filtering and antivirus.

## Difference between Firewall and Antivirus



| Firewall | Antivirus |
|---|---|
| A firewall is created using both hardware and software to protect a network. | Antivirus is created using only software to protect a network. |
| Firewalls deal with only external dangers. | Both internal and external risks are addressed by antivirus software. |
| Counterattacks like IP spoofing as well as routing attacks are viable against firewalls. | After the malware has been removed in antivirus, no counterattacks are available. |
| Monitoring and filtering are two of the functions that the firewall does. | Scanning contaminated files and software is how antivirus programs do their job. |
| The danger posed by incoming packets is evaluated by the firewall. | The danger posed by harmful software is analysed by antivirus software. |
| The system is protected from any and all threats thanks to the firewall that was installed. | Only viruses can be protected by antivirus software. |
| The code behind a firewall is more complicated than that of an antivirus application. | When compared to firewalls, antivirus software has more straightforward programming. |

# Day 3

**What Is an Exploit?**

- An exploit is a program, or piece of code, designed to find and take advantage of a security flaw or vulnerability in an application or computer system.
- An exploit is a segment of code or a program that maliciously takes advantage of vulnerabilities in software or hardware to infiltrate and initiate an attack.
- An exploit is a code that takes advantage of a software vulnerability or security flaw. It is written either by security researchers/hackers as a proof-of-concept.

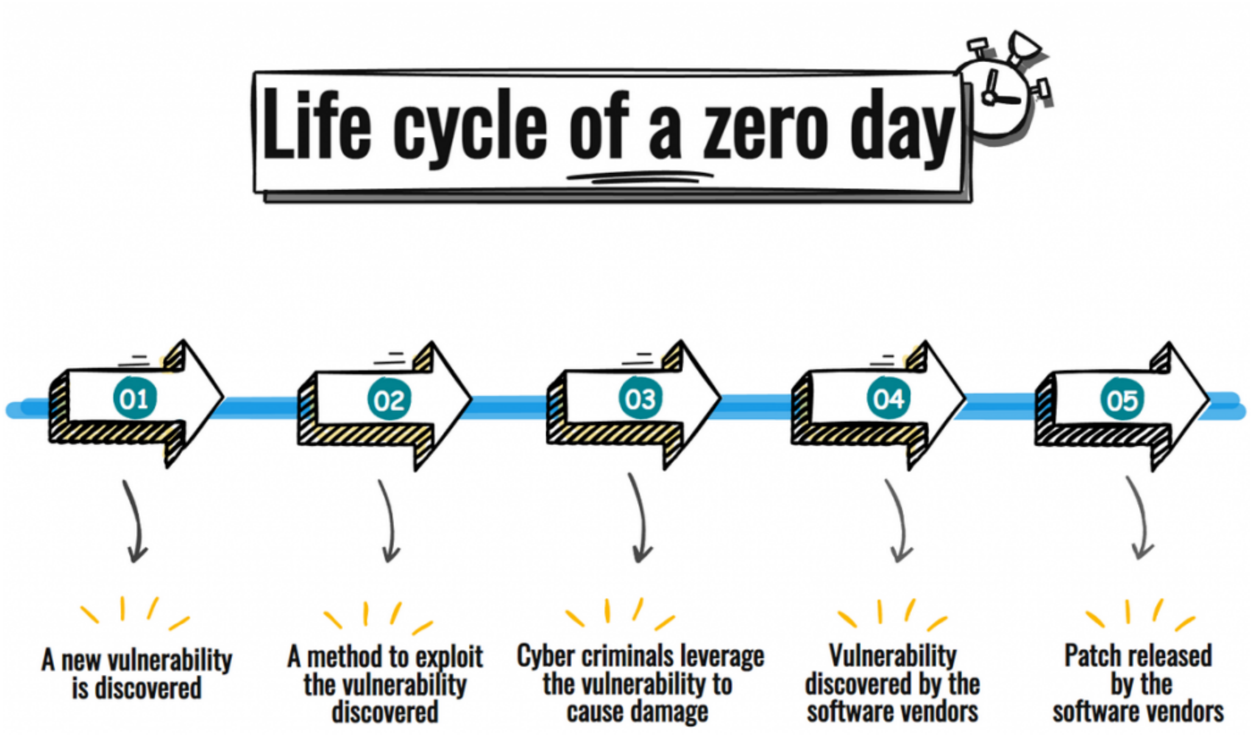
**What is a Zero-day Exploit?**

- An exploit which is not known before expect the hacker or that security researchers/hackers.
- A zero-day attack is a cyberattack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of.
- A zero-day (0day) exploit is a cyber-attack targeting a software vulnerability which is unknown to the software vendor or to antivirus vendors.
- The term "zero-day" (or 0-day) is used for a software exploit or hack referring to the fact that the developer or creator of the at-risk program has only just become aware of it - so they literally have zero days to fix it.
- The term “zero day” refers to a vulnerability that exists in the wild without the software manufacturer's knowledge, leaving them open to attack.

**Typical properties of a zero-day exploit**

- A flaw or vulnerability in a computer software.
- Vulnerability was previously unknown to the software vendor.
- There is no immediate fix available for the vulnerability.
- The vulnerability is open to be exploited by the hackers.

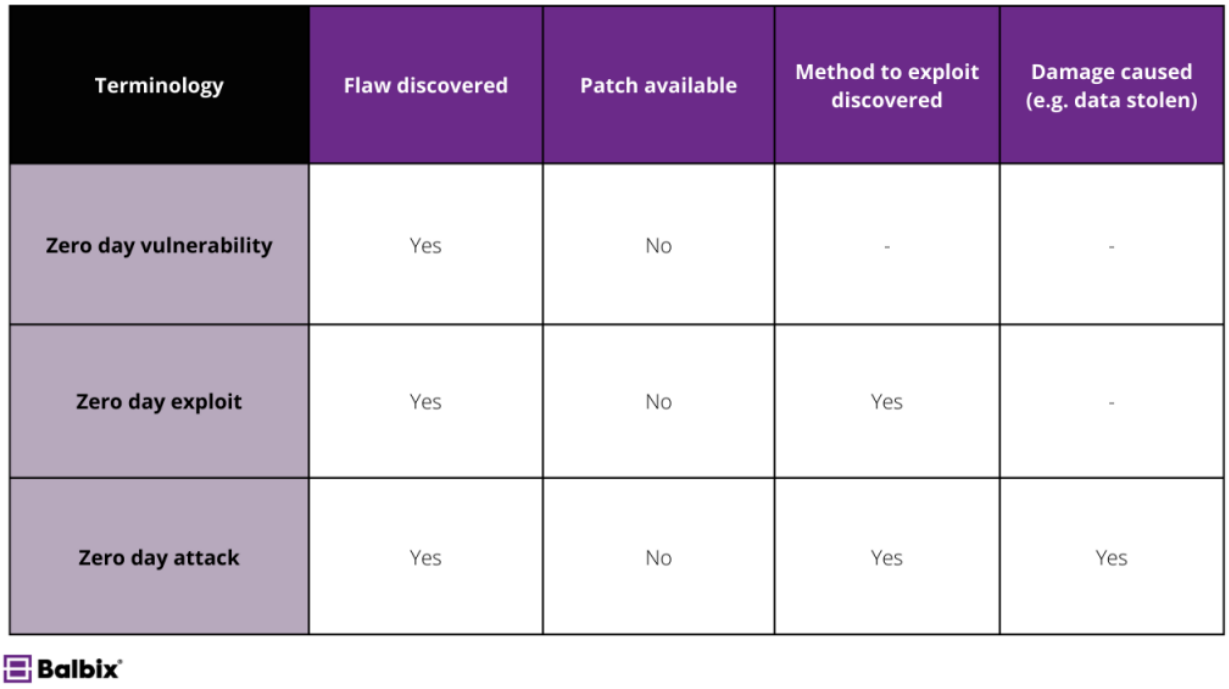
Zero-day exploit example


Life cycle of a zero day
01
02
03
04
05
A new vulnerability is discovered
A method to exploit the vulnerability discovered
Cyber criminals leverage the vulnerability to cause damage
Vulnerability discovered by the software vendors
Patch released by the software vendors

## What is the difference between a zero-day vulnerability, a zero-day exploit and a zero-day attack?

The terms- zero-day vulnerability, zero-day exploit and a zero-day attack are often used interchangeably but they are not the same.

- A Zero-day vulnerability is simply a flaw that is discovered before the software vendor knows about it. There is no fix available for it.
- A zero-day exploit indicates that the method to exploit the zero-day vulnerability has been discovered.
- A zero-day attack leverages zero-day vulnerability to cause damage e.g. steal the data, bring down the systems.



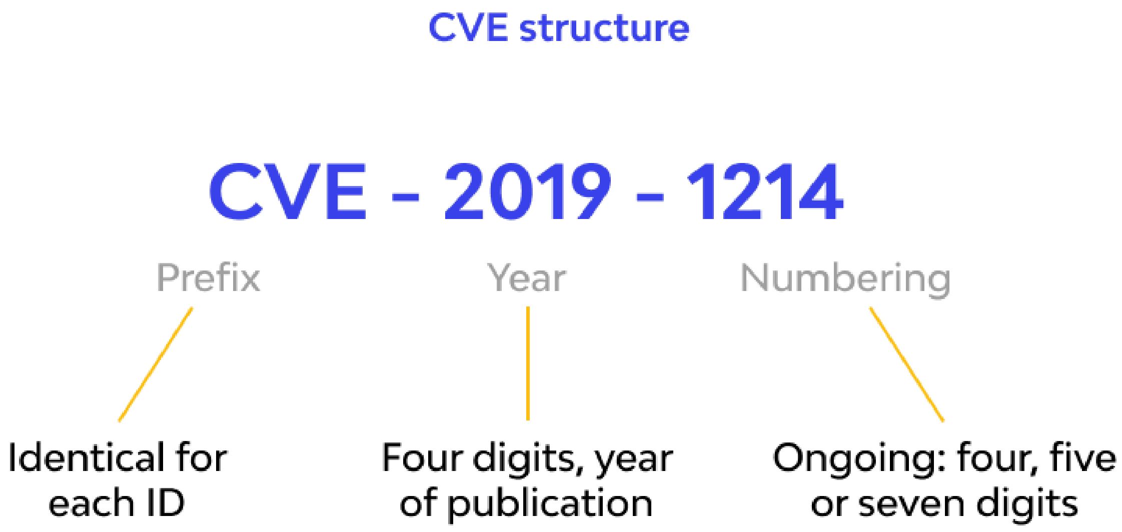
| Terminology | Flaw discovered | Patch available | Method to exploit discovered | Damage caused (e.g. data stolen) |
|---|---|---|---|---|
| Zero day vulnerability | Yes | No | - | - |
| Zero day exploit | Yes | No | Yes | - |
| Zero day attack | Yes | No | Yes | Yes |

□

**What is a CVE?**

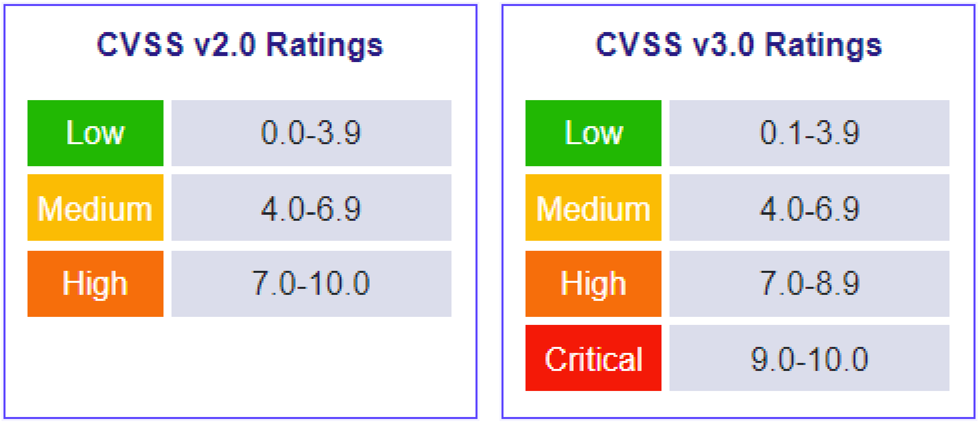
- CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number. Security advisories issued by vendors and researchers almost always mention at least one CVE ID.
- The mission of the CVE® Program is to identify, define, and catalog publicly disclosed security vulnerabilities.
- The CVE program is overseen by the MITRE corporation with funding from the Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security.
- CVE entries are brief. They don’t include technical data, or information about risks, impacts, and fixes. Those details appear in other databases, including the U.S. National Vulnerability Database (NVD), the CERT/CC Vulnerability Notes Database, and various lists maintained by vendors and other organizations.

CVE ID Example:



### What is a CVSS?

- A CVSS score of 0.1 to 3.9 earns a severity rating of Low; from 4.0 to 6.9 gets a medium rating; **7.0 to 8.9** is rated High; and 9.0 to 10 is Critical.
- The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.



CVSS v2.0 Ratings

| | |
|---|---|
| Low | 0.0-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-10.0 |

CVSS v3.0 Ratings

| | |
|---|---|
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-8.9 |
| Critical | 9.0-10.0 |

### Differences between CVSS and CVE

CVSS is the overall score assigned to a vulnerability. CVE is simply a list of all publicly disclosed vulnerabilities that includes the CVE ID, a description, dates, and comments. The CVSS score is not reported in the CVE listing – you must use the NVD to find assigned CVSS scores.

## Vulnerability Assessment and Penetration Testing

- Vulnerability Assessment and Penetration Testing (VAPT) are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a more complete vulnerability analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus.
- Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot. Vulnerability scanners alert companies to the preexisting flaws in their code and where they are located. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application. Penetration tests find exploitable flaws and measure the severity of each. A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system. Together, penetration testing and vulnerability assessment tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws.

## Vulnerability Assessment Report

- A vulnerability assessment report is a document that records all the vulnerabilities found in your systems during a vulnerability scan. The report provides you with a list of the vulnerabilities indexed by severity along with suggestions for fixing the vulnerabilities.
- The vulnerability assessment report is basically the result of the vulnerability scan, and it is what helps you understand the security posture of your organization, and build a strategy for vulnerability management. Let us learn more about its importance.

**Components of a Vulnerability Assessment Report**

A vulnerability scan report is usually divided into 3 parts. An executive summary, the details of the vulnerabilities, and the details of the scan. Let us understand the significance of each segment.

- The executive summary: As the name would suggest, the executive summary is meant to create a high-level understanding of the vulnerability situation of an organization. This part talks about the vulnerabilities, their CVSS scores, the impact they could have on the business, and how much risk they pose to the system they're in.
- The details of vulnerabilities: This is the part where each of the detected vulnerabilities is explained with technical details along with suggestions for fixing them. This is the most important part of the vulnerability report from a developer's perspective because this part allows them to plan the remediation.
- Details of the scan: Vulnerability assessments involve hundreds of test cases. All these tests have to be documented in the report. This part tells you what tests were conducted, their categories, whether they were manually done or automated. All this information is very important in terms of validating a vulnerability scan.

Sample VAPT Report

https://www.getastra.com/blog/wp-content/uploads/2021/06/Astra-Security-Sample-VAPT-Report.pdf