Ok so this is quiet basic stuff... and I know that you are already aware of many things.

But I would still like to give you an introduction to Virus and Antivirus here: -

- **VIRUS** stands for Vital Information Resources Under Seize
- It is a malicious program or script which disrupts the functioning of our computer by messing with the Softwares
- They may harm the computer, crash the processes, steal all the information in the hard disk of the computer, reduce hard-disk space, slow down the running down of computers and so on.

- **ANTIVIRUS** is a software used to detect these viruses and null their effect by deleting them or blocking them from functioning.
- Its job is to prevent, scan, detect and delete viruses from a computer.
- Popular Antiviruses include Norton, McAfee, Avast, Avira, Bitdefender and so on.

As you can guess, our payloads that we use while hacking also often get detected by antiviruses and then to continue our attack, we need to find a way for bypassing the antivirus. This process is called **Antivirus Evasion.**

We apply antivirus evasion techniques to create an **undetectable payload** that does not get detected and removed by Antiviruses. But evading antivirus is a topic for another lecture. Right now, let's understand how exactly Antiviruses detect the harmful files, so that we can find a loophole in it's working and accordingly bypass the antivirus solution.

HOW ANTIVIRUS WORKS?
Antiviruses generally work in either of the two ways: -

Signature Based Detection - Signature based antivirus would scan a file, program or application in suspect, and compare its signature (think of it as a hash or checksum) to a list of known malicious file's signatures in the antivirus's database. If it finds that the file is identical or similar to a piece of known malware in the database, that code is considered malicious software (malware) and is quarantined or removed.

Behavior-Based Detection - Behavior-based AV watches processes for

Behavior Based Detection - Behavior-based AV watches processes for telltale signs of malware, which it compares to a list of known malicious behaviors.

While Signature Based Antiviruses are good for old / known malicious items, They are **pretty easy to bypass** in many scenarios because if we create a unique kind of malware that doesn't have a record yet in the database of the antivirus, we would be able to bypass it.

Whereas in Behavior Based Detection, it's a little too hard to bypass it since it doesn't care about a database of signatures. Instead, it will **check the behavior** of that file being something abnormal or unusual. However, sometimes, we may still be able to easily bypass them if we can, for example, combine our malicious file with a usually-working file to make it look less suspicious.

That's it for now. In the next video, I will show you a practical demonstration of bypassing antiviruses.

~ Avinash Yadav