Important Terms

TERMS

- **Vulnerability:** A design, coding, or logic flaw affecting the target system. The exploitation of a vulnerability can result in disclosing confidential information or allowing the attacker to execute code on the target system
- **Exploit:** A piece of code that uses a vulnerability present on the target system to perform a malicious operation

TERMS

- **Payloads:** Payloads are codes that will run on the target system. Exploits will leverage a vulnerability on the target system, but to achieve the desired result, we will need a payload. Examples could be; getting a shell, loading a malware or backdoor to the target system, running a command, or launching calc.exe as a proof of concept to add to the penetration test report. Starting the calculator on the target system remotely by launching the calc.exe application is a benign way to show that we can run commands on the target

- **Exploitation:** Establishing access to a system/machine/resource by bypassing security restrictions. For a Pen Tester exploitation is gaining access to a machine to run commands on it. We are interested in the piece of code that makes a target machine do something on behalf of an attacker against vulnerabilities

- **Encoders:** Encoders encode the exploit and payload in the hope that a signature-based antivirus solution may miss them. Signature-based antivirus and security solutions have a database of known threats. They detect threats by comparing suspicious files to this database and raise an alert if there is a match. Thus encoders can have a limited success rate as antivirus solutions can perform additional checks.

- **Evasion:** While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, “evasion” modules will try that, with more or less success

THANKS