Operational Security Definitions:

**Vulnerability**: the absence of a safeguard. A weakness in a system. For example, having weak **passwords** is a vulnerability.

**Threat**: Any potential danger in regards to vulnerability. There is the potential that if someone compromises my passwords, they will gain access to my system**.**

**Threat agent**: The attacker, malicious code, software utility, etc that actually carries out the attack. L0phtcrack is a password cracking utility that could carry out a brute force attack and discover my password. It would be the threat agent.

**Risk**: The likelihood that a treat agent will attack a vulnerability. I’ve just been notified that a particular IP address has been doing port scans and O/S fingerprinting. There is a strong risk that there will be an attempt to compromise my network.

**Exposure**: Very similar to a vulnerability, but refers to the instance of being exposed to losses from a threat agent. As in, if I have no password policy on my network, I am exposed to the possibility of having passwords cracked and systems accessed in an unauthorized manner.

#### Controls (technical or non technical means to lessen probability or impact of a risk event

##### Safeguards—preventative and deterrent (proactive)

##### Countermeasure detective and corrective (reactive)

There is a strong **risk** that a **vulnerability** on my system will **expose** me to a threat that a **threat agent** will exploit, unless I provide a **safeguard.**