Cyber Threats vs. Attacks

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity, Professor Dr. Joseph Kovacic

September 14, 2025

What is the difference between a cyber threat and an attack?

Risk management is key to any organization's health, safety, and success in today's modern economy, whether the organization is a company, municipality, national government branch, or non-profit organization. To manage one's risk, an organization must first understand its risk tolerance, possible threats that may seek to undermine it (i.e., internal and external), scan and assess its infrastructure for all possible vulnerabilities, and to develop a plan of action by determining the impact of a breach or an attack on them should it happen (Kim & Solomon, 2021, Chapter 3; Nelson et al., 2025).

A cyber **threat** is a potential danger or malicious event that could exploit vulnerabilities and cause significant damage to an entity and/or person(s). The threat has the potential to cause severe damage, whether it is a weather event (i.e., natural disasters like tornadoes and hurricanes) or a cyber hacker group (i.e., BlackByte) with the ability and resources to infiltrate, control, and/or leak sensitive data to the public, sometimes for profit.

A cyber **attack** is a realized expression of one's ability and power to inflict harm on others. It is an outward act and manifestation of that power in the real world and surrounding environment to thwart, confuse, steal, and/or destroy another organization and its data. Think of it like this: a hungry wolf is a threat, but the wolf breaking into the chicken coop is an attack.

How do exploits relate to vulnerabilities?

Exploits are often pieces of code or a specific method to take advantage of a vulnerability. A **vulnerability** is any weakness, flaw, or exposure in a system waiting to be exploited by a threat (i.e., software bugs, misconfigured settings, unintentionally clicking malicious URLs in a phishing email, or being slow to update or patch modern security systems). Without a vulnerability, an exploit cannot work. The vulnerability is the open window, and the exploit is the specific ladder or tool used to climb through it.

Is there an ethically acceptable reason to study and use the various attack methods described in this module?

Yes, there are ethically acceptable reasons to study and use attack methods. The primary reason is for **defensive purposes**. Known as **ethical hacking** or **penetration testing**, it involves using the same techniques as malicious hackers to identify and fix vulnerabilities in a system proactively. By understanding how an attacker thinks and operates, cybersecurity professionals can build stronger, more resilient defenses. That helps protect individuals, businesses, and critical infrastructure from real-world attacks.

References

Kim, D., & Solomon, M. G. (2021). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2022). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3