Tutorial 2
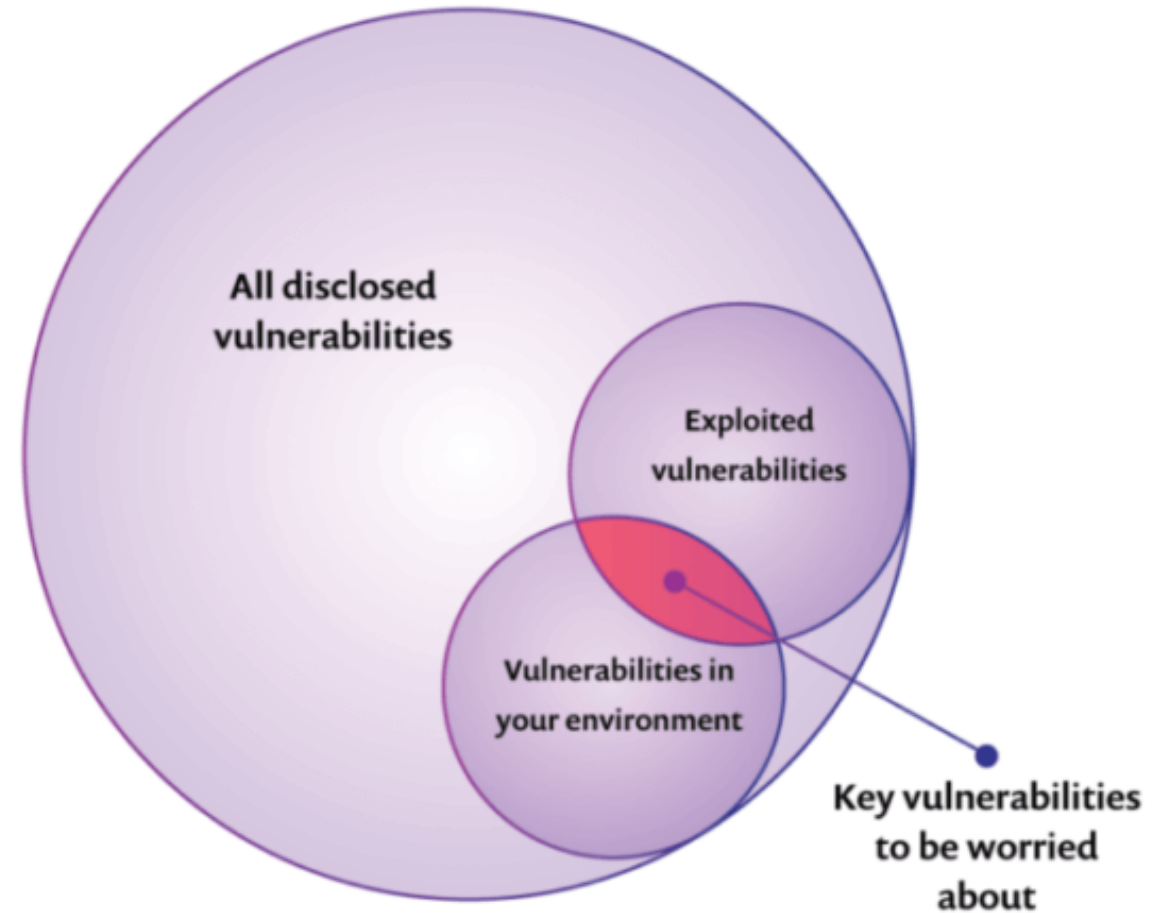
Understanding the effect of cyberattacks part 2

Basics

❖ What is the difference between the following terms:

➤ Weakness VS Vulnerability?

✓A weakness is an error (problem), typically in the software code or system hardware, that might lead to a vulnerability.

✓ A Vulnerability is a Weakness that can be exploited by threat actor.

➤Lemma: Each vulnerability is a weakness but not each weakness is a vulnerability (proof it by using an example from real-life)

✓Attacker targets to access a PC remotely using Windows XP administrator account weakness point (no password is assigned for this account), while the PC is not connected to the internet.

Basics

➢ Vulnerability VS Threat?

✓The threat is the exploitation of a security vulnerability to damage or destroy an asset.

➢Threat VS Risk?

✓Risk is the potential for loss, damage or destruction of an asset.

✓Risk= F(threat, impact, Likelihood)

✓Risk= F(severity, criticality, impact, likelihood)

All disclosed vulnerabilities

Exploited vulnerabilities

Vulnerabilities in your environment

Key vulnerabilities to be worried about

RISK ANALYSIS — LOW, MEDIUM, HIGH, VERY HIGH, EXTREME

Basics

- According to these definitions, some databases are published as follows:

•CWE: Common Weakness Enumeration

[CWE - CWE List Version 4.6 (mitre.org)](#)

•CVE: Common Vulnerabilities and Exposures

[Industrial Control Systems | CISA](#)

- CVSS: Common Vulnerability Scoring System

[Common Vulnerability Scoring System Version 3.1 Calculator (first.org)](#)

- CAPEC: Common Attack Pattern Enumeration and classification.

[CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™) (mitre.org)](#)

[Matrix | MITRE ATT&CK®](#)

Cybersecurity exercises
(Imagine that you are an attacker)

1. ICSA-20-252-07
2. ICSA-20-266-02
3. ICSA-20-252-03
4. ICSA-19-283-01
5. ICSA-21-257-21
6. ICSA-22-286-04

➢ Advisories that content some vulnerabilities

➢ What is the risk evaluation of these vulnerabilities?

➢ What is the CVSS score of these vulnerabilities?

➢ Which attack techniques can be used to exploit these vulnerabilities?

➢ How can you mitigate these vulnerabilities? (as you are a cybersecurity engineer)