H/R: Class Materials And I googled stuff I couldn't find in the presentations

303 - HW2

William Stelley

① Identifying vulnerabilities and potential vulnerabilities and then putting in the counter measures so they are not exploited.

Attacker Approach: Focus on goals of attacker -> what from your network do they want

Architecture Perspective: what is on your network -> how are they vulnerable.

Asset Approach: what is the valuable parts of your network -> how hard is it to get to

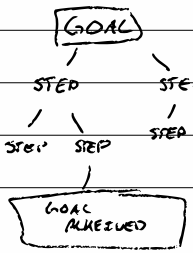
② IOC: Attack already happened

IOA: Attack is in progress

The statement is false b/c IOA is still in progress so it can potentially be stopped. -> IOC your system has already been compromised.

③ Attack Tree is the different ways that an attack could be accomplished mapped out.

↳ the root node is the goal, and the leafs are how it can be carried out.



(4) Threat Intelligence: knowing the different ways that an attacker could potentially attack your system.

Very important so you can secure your system. Important for building things like attack trees. How can you know what to defend against when you don't know the possible attacks.