ARP ATTACK TREE THREAT MODELING

Group Project

Attack Tree Steps:

1. Identify Asset
2. Identify Threats
3. Understand Threats- this requires an understanding of which systems are threatened.
4. Categorize Threats
5. Rate Threats
6. Identify mitigation strategies (countermeasures, controls)

Task:

1. The class will be given the amount of time to complete the group exercise.
2. Each individual will create their own document to submit as their work, even as they work collaboratively for ideas.
3. Each individual will submit their own work as an assignment.
4. Each individual will document their work, and then submit a visualization of their attack tree.

Informational Statement:

Topic: ARP Attack Tree Threat Modeling

Category: ARP Spoofing – Address Resolution Protocol spoofing/poisoning

ARP spoofing allows attackers the ability to insert themselves into network communications.

**Ideas**

**1.**

**TASK:**

METHOD 1:

Use the gitlab (https://jackson\_t.gitlab.io/walter-planner/) to map out an example Attack Tree Threat Model for ARP Spoofing/Poisoning.

METHOD 2:

Use <https://attacktree.online/> to map out the example Attack Tree Threat Model for ARP Spoofing/Poisoning.

METHOD 3:

Use <https://app.diagrams.net/> to map out the example Attack Tree Threat Model for ARP Spoofing/Poisoning.

Information Gathering:

1. Step 1: Identify the Assets
   1. Select a possible Asset that could be affected by the attack type (ARP spoofing).
2. Step 2: Identify the Threats
   1. List the two common threats/attacks that an attacker can launch on the victim.
3. Step 3: Understand the Threats
   1. List how these threats may be performed on the chosen asset.
   2. List the potential impacts of these threats.
4. Step 4: Categorize the Threats
   1. consider how hard or easy the threat is to execute for a hacker
5. Step 5: Rate Threats
   1. Rate the risk level of the threats
6. Step 6: Identify mitigation strategies
   1. How can these threats be mitigated? Listing multiple possible mitigations is allowed and encouraged.

Gitlab Work:

1. Layout the above-answered information into the visualization.

a. There needs to be a MINIMUM of

1. Layer 1: 1 Asset
2. Layer 2: 2 Capabilities (the identified 2 common attacks)
3. Layer 3: 4 Threats with connections to the 2 common attack types
4. Layer 4: 2 Impacts with connected mitigations (1 mitigation each is all that is necessary for the visualization.)

**ANSWERS:**

Information Gathering:

1. List the possible asset
2. List the two common threats/attacks that an attacker can launch on the victim of an Arp spoof.
   1. <Replace with the answer>
   2. <Replace with the answer>
3. List the possible threats from the 2 attacks
   1. <Replace with the answer>
      1. <list estimated ease of execution, Easy/Medium/Hard>
      2. <list estimated risk level to the security of the organization 1-10, 1 being an annoyance, 10 being a major breach of security>
   2. <Replace with the answer>
      1. <list estimated ease of execution, Easy/Medium/Hard>
      2. <list estimated risk level to the security of the organization 1-10, 1 being an annoyance, 10 being a major breach of security>
   3. <Replace with the answer>
      1. <list estimated ease of execution, Easy/Medium/Hard>
      2. <list estimated risk level to the security of the organization 1-10, 1 being an annoyance, 10 being a major breach of security>
   4. <Replace with the answer>
      1. <list estimated ease of execution, Easy/Medium/Hard>
      2. <list estimated risk level to the security of the organization 1-10, 1 being an annoyance, 10 being a major breach of security>
4. List possible impacts of the threats
   1. <Replace with possible impact>
      1. <list possible mitigations> ii. <list possible mitigations>
   2. <Replace with possible impact>
      1. <list possible mitigations> ii. <list possible mitigations>
   3. <Replace with possible impact>
      1. <list possible mitigations> ii. <list possible mitigations>

Paste a Screenshot of your completed gitlab below:

Copy your full gitlab script(left side of the gitlab) (CTRL+A),(CTRL+C), Paste it into a notepad .txt file.

Upload this txt document to the LMS as well so that the script can be reviewed.

Tips with this gitlab

* Use the provided example as a helpful template.
* Indentation errors are caused if lines are not aligned properly, ensure you’re copying a full portion of the code rather than just the text.
* Tag Errors can occur if a tag does not match the complete lists defined at the bottom of the script.
* Tagging: Ensure the tags all show the appropriate color to properly display
* Organization: Organize your Threats top to bottom, followed by their associated threats top to bottom to help with the organization of the tree.

PLACE VISUALIZATION HERE: