CSSE 341 -- Network Security

Rose-Hulman Institute of Technology

Lab 06: ARP Cache Poisoning

Learning Objectives

At the end of this lab, you should be able to:

- Inject different ARP packets into an existing network.
- Investigate the impact of different ARP packets on a host's ARP cache.
- Conduct a *Man-In-The-Middle* (MITM) attack using ARP cache poisoning.

Name: _____

Question	Points	Score
Question 1	2	
Question 2	2	
Question 3	4	
Question 4	4	
Question 5	15	
Question 6	10	
Question 7	10	
Question 8	4	
Question 9	4	
Question 10	10	
Question 11	2	
Question 12	8	
Question 13	10	
Question 14	5	
Question 15	15	
Question 16	5	
Question 17	5	
Question 18	0	
Total:	115	

1 Step 1: Understanding the ARP cache

Question 1. (2 points) How many requests did `hostA` send to `hostB`?

Question 2. (2 points) What are the content of the caches on both `hostA` and `hostB`?

Question 3. (4 points) Based on your observation, what did `hostB` do when it received the ARP request from `hostA`?

Question 4. (4 points) Based on your observations, assuming ARP caches are empty, what can a malicious host do to poison the ARP table of a host on the network?

2 Step 2: Packet parameters

Question 5. (15 points) After inspecting the contents of the packet in an exchange of ARP requests and replies between `hostA` and `hostB`. Fill out the following table with the content of the Ethernet and ARP headers in each packet type. Assume that `hostA` sends the request and `hostB` replies.

Field	ARP Request	ARP Reply
Ethernet Header		
Destination MAC		
Source MAC		
EtherType		
ARP Header		
Hardware Type		
Protocol Type		
Hardware Address Length		
Protocol Address Length		
Operation		
Sender Hardware Address (SHA)		
Sender Protocol Address (SPA)		
Target Hardware Address (THA)		
Target Protocol Address (TPA)		

3 Step 3: Forging requests

Question 6. (10 points) Describe the experiment that you would like to setup to evaluate the impact of forged ARP requests. Your experiment must be able to address the following requirements:

- Analyze the behavior of `hostA`'s ARP cache in each of the aforementioned scenarios.
- Use appropriate packet captures to show the impact of ARP requests forged from the attacker to `hostA`.
- Analyze if and when the attack might be successful, and what happens if `hostB` starts communicating with `hostA` suddenly.

Question 7. (10 points) Based on your observations, describe the behavior of `hostA` when it receives an unsolicited ARP request. Specifically, mention what happens depending on the content of the ARP cache (the three scenarios we mention).

Question 8. (4 points) Based on your observations, suggest a way to thwart ARP cache poisoning attacks that use ARP requests.

Question 9. (4 points) If `hostB` decides to start sending ARP requests while you are conducting your attack, what do you anticipate would happen?

You don't have to test this out, just use your judgment as to what you think can happen.

4 Step 4: Forging replies

Question 10. (10 points) Based on your observations, describe the behavior of `hostA` when it receives an unsolicited ARP reply. Specifically, mention what happens depending on the content of the ARP cache (the three scenarios we mention).

Question 11. (2 points) Based on your observations, suggest a way to thwart ARP cache poisoning attacks that use ARP replies.

Question 12. (8 points) When the attack using ARP replies fails, can you suggest a way to remedy that? In other words, we'd still like to use ARP replies, but we need to force `hostA` to take those seriously.

Hint: You might need to send packets on another layer.

Hint: This relates to the incomplete mapping behavior that we've seen earlier.

Hint: You don't have to implement this, just suggest a way to make it happen.

5 Step 5: ARP gratuitous

Question 13. (10 points) Based on your observations, describe the behavior of hostA when it receives an unsolicited ARP gratuitous packet. Specifically, mention what happens depending on the content of the ARP cache (the three scenarios we mention).

Question 14. (5 points) Thinking like an attacker, which technique of the three would you prefer and why?

Question 15. (15 points) Based on all your experiments, without significant change to the ARP protocol, can we effectively thwart such attacks?

In your answer, try to hit the following points:

- What's the main weakness of ARP?
- Without a third party intervention, can we avoid this weakness?
- Can someone from the Internet conduct an ARP cache poisoning attack?

Question 16. (5 points) In your own words, please write a quick summary of what you have learned in this lab.

Question 17. (5 points) How much time did it take you to complete this lab?

Question 18. Do you have any feedback about this lab? (If you'd like to leave an anonymous feedback, feel free to detach this page and slide it under my door).