CSSE 490 -- Network Security

Rose-Hulman Institute of Technology

Lab 2: ARP Cache Poisoning

Learning Objectives

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

- Use `libpcap` to capture and manipulate packets on the wire.
- Compare performance between different implementations of exploits.
- Conduct a MITM attack on two hosts to act as a router.
- Explore `IPv4` routing and `TCP` set up.

Name: ______________________________

Question	Points	Score
Question 1	25	
Question 2	35	
Question 3	10	
Question 4	35	
Question 5	20	
Question 6	35	
Question 7	15	
Total:	175	

1 Implementing `ping`

Question 1. The questions below refer to the steps involved in implementing `ping`.

(a) (10 points) After completing step 2, was your `ping` successful? If not, then why?

Hint: Grab a packet capture while running your experiment and examine the headers using `Wireshark`.

(b) (15 points) The problem above is caused by a field in the `ICMP` header. What is the use of that field?

Hint: You can use a search engine, you do not have to guess.

2 Phase one: Understanding the ARP cache

Question 2. By examining the content of the ARP caches on hostA and hostB, and looking at the packet capture, answer the following questions:

(a) (5 points) How many ARP requests were sent from hostA to hostB?

(b) (5 points) What are the content of the caches on both hostA and hostB?

(c) (10 points) Based on your observations, what did hostB do when it received the ARP request from hostA?

(d) (10 points) Describe in a few sentences the steps taken by hostB when it receives a request from hostA for its MAC address.

(e) (5 points) Based on your observations, assuming ARP caches are empty, what can a malicious host do to poison the ARP cache of a host on the network?

3 Phase two: Forging replies

Question 3. (10 points) Describe the experiment that you would setup to evaluate the impact of forged ARP replies. Your experiment must be able to address the following requirements:

- Use appropriate packet captures to show the impact of ARP replies forged from the attacker to hostA.
- Show the impact of the forged replies on the ARP cache under different scenarios.
- Analyze if and when the attack might be successful, and what happens if hostB starts communicating with hostA all of sudden.

Question 4. Based on your observations from your experiment, answer the following questions.

(a) (5 points) Describe the behavior of hostA when it receives an unsolicited ARP reply. Specifically, mention what happens depending on the content of the ARP cache.

(b) (5 points) When would such an attack be successful?

(c) (10 points) Based on this experiment, suggest a way to thwart `ARP` cache poisoning attacks that use `ARP` replies.

(d) (15 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.

4 Phase three: Forging requests

Question 5. This section refers to the cache poisoning attack using ARP requests.

(a) (5 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.

(b) (5 points) When would such an attack be successful?

(c) (10 points) If **hostB** decides to start sending ARP requests while you are conducting your attack, what do you anticipate would happen?

You do not have to test this out, just use your judgment as to what you think can happen.

5 Phase four: ARP gratuitous

Question 6. This section refers to the cache poisoning attack using ARP gratuitous packets.

(a) (5 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.

(b) (5 points) When would such an attack be successful?

(c) (10 points) Thinking like an attacker, which technique of the three would you prefer? Make sure to argue for your answer.

(d) (15 points) Based on all your experiments, without significant change to the ARP protocol, can such attacks be thwarted? In your answer, try to hit the following points:

- What is the main weakness of ARP?
- Without a third party intervention, can this weakness be avoided?
- Can someone from the Internet conduct an ARP cache poisoning attack?

6 The exploit

Question 7. The questions below refer to the first step of writing the exploit, namely exploring `netcat`.

(a) (5 points) Grab a `TCP` packet and open its corresponding `IPv4` header. What is the value of the protocol number in the `IPv4` header? Record this value in your notes.

(b) (5 points) Which `TCP` packet contain the words that you have typed during the `netcat` experiment?

(c) (5 points) For those packet containing the data, open their `TCP` header. What is the value of the **flags** field? Which flags are set? Record those flags.

If you made any assumptions about the state of the network when writing your exploit, please state them here.

7 Wrap-up

In your own words, please write a quick summary of what you have learned in this lab.

How much time did it take you to complete this lab?

This page is intentionally left blank . . .

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).