IP/ICMP Attacks Lab

1 Overview

The objective of this lab is for students to gain the first-hand experience on various attacks at the IP layer. Some of the attacks may not work anymore, but it is important for students to learn the underlying attack techniques.

Lab environment. This lab has been tested on our pre-built Ubuntu 16.04 VM, which can be downloaded from the SEED website.

2 Task 1: IP Fragmentation

In this task, you need to construct an UDP packet and send it to a UDP server. You can use "`nc -lu 9090`" to start a UDP server. Instead of building one single IP packet, you need to divide the packet into 3 fragments, each containing 32 bytes of data (the first fragment contains 8 bytes of the UDP header plus 32 bytes of data). If you have done everything correctly, the server will display 96 bytes of data in total.

3 Task 2: IP Fragments with Overlapping Contents

Similar to Task 1, you also need to construct 3 fragments to send data to a UDP server. However, the first two fragments should overlap. Please use your experiment to show what will happen when the overlapping occurs. Please try the following scenarios separately:

- The end of the first fragment and the beginning of the second fragment overlap by 5 bytes.
- The second fragment is completely enclosed in the first fragment.
- The first fragment is completely enclosed in the second fragment.

4 Task 3: Sending a Super-Large Packet

As we know, the maximal size for an IP packet is 2^{16} octets. However, using the IP fragmentation, we can create an IP packet that exceeds this limit. Please construct such a packet, and send it to the UDP server. Please report your observation.

5 Task 4: DOS Attacks using Fragmentation

In this task, we are going to use Machine A to launch the Denial-of-Service attacks on Machine B. In the attack, Machine A sends a lot of incomplete IP packets to B, i.e., these packets consist of IP fragments, but some fragments are missing. All these incomplete IP packets will stay in the kernel, until they time out. Potentially, this can cause the kernel to commit a lot of kernel memory. In the past, this resulted in denial-of-service attacks on the server. Please try this attack and describe your observation.

6 Task 5: ICMP Redirect Attack

An ICMP redirect is an error message sent by a router to the sender of an IP packet. Redirects are used when a router believes a packet is being routed incorrectly, and it would like to inform the sender that it should use a different router for the subsequent packets sent to that same destination.

In our VM, there is a countermeasure against the ICMP redirect attack. Before we do this task, we need to turn it off, i.e., configure the operating system to accept ICMP redirect messages.

```
sudo sysctl net.ipv4.conf.all.accept_redirects=1
```

In this lab, you should have two VMs, the victim VM (Host A) and the attacker VM (Host M). You should also pick a destination B, which should be a host outside of your local network (e.g., an outside web server). Normally, when A sends a packet to B, the packet will go to the router provided by VirtualBox (usually it is `10.0.2.1` if you use the default IP prefix for NAT Network). Your job is to launch an ICMP redirect attack on Host A from Host M, to redirect those packets to M, where you can make changes, and then send the modified packets out. This is a form of MITM attack.

I am going to leave it to you to decide what kind of modification you want to make. Use your imagination. The grade for this task will be affected by how creative and interesting your modifications are.

7 Submission

Students need to submit a detailed lab report to describe what they have done, what they have observed, and how they interpret the results. Reports should include evidences to support the observations. Evidences include packet traces, screenshots, etc. Reports should also list the important code snippets with explanations. Simply attaching code without any explanation will not receive credits.