Security First Principles

Principle MINIMIZATION

LAB: SECURE NETWORK APPLICATIONS USING MINIMIZATION PRINCIPLE

Lab Description: This lab provides hands on experience for you to understand the importance of minimization principle for application and network security. In this lab, you will build an environment with two virtual machines - one for running the server application and the other to scan the server application's network.

You will identify the open ports and use iptables to close unwanted ports. Next you will analyze the server application code to identify a privilege escalation vulnerability and print sensitive information. Finally you will use the minimization principle to modify the server application's privileges such that the privilege escalation vulnerability can not be exploited any further.

Lab Environment: This lab requires you to set up two virtual machines and connect them to a host only network where they can ping each other. Let's call one VM the server VM, and the other attacker VM. On the attacker VM, install nmap utility. Also make sure the command nc exists. Refer to the enclosed network diagram for environment setup.

Once the above setup is done, copy the provided server application to server VM and compile using the command 'make all'. It will prompt for sudo permission to set the uid flag for the binary. Now run the server application binary main.bin. You can use nc <server_vm_ip> 80 to connect to server. Once it's connected to server, you can enter a directory path under server VM user and server should send the response back to the client.

From here onwards, you will do lab exercises1 and 2 and Puzzler as a stretch goal.

Lab Files that are Needed: In this lab following files are provided to you.

- main.c
- Makefile

After copying these files to server VM, you can generate main.bin by running the command ‘make all’.

Lab Exercise 1

In this exercise you will identify the unwanted ports open by server VM. You will close the unwanted ports and verify it using nmap.

A. Use nmap utility in the attacker VM to scan the ports open in server VM. Take a screenshot of open ports.
B. Use iptables utility in the server VM to close the ports except port 80 used by main.bin server application
C. Run nmap again and verify only port 80 is now open. Take a screenshot.

Lab Exercise 2

In this lab you will analyze a vulnerability in the main.c program exploiting which you can execute any command with superuser privilege.

A. You can use the command ‘nc <server_vm_ip> 80’ to connect to server and pass a string. The server assumes this string is the path to a directory that current user has access to, and lists its contents.
B. The way the main.c is written making it vulnerable to inject commands that can be run in superuser mode. Execute the command ‘ls /root’ and capture a screenshot.

Puzzler

This is an optional exercise for those who are able to complete the exercise 2 and execute privileged command. Given that there is a vulnerability of insufficient parameter validation that we don’t want to fix, see how we can address the privileged command execution, by minimizing the privilege in the code. Note that minimizing privilege doesn’t mean lower the privilege, instead acquiring the privilege only when necessary and relinquishing it right after.

A. Analyze main.c and use the principle of minimization to fix the privilege escalation vulnerability we exploited in exercise 2.
B. After fixing main.c run the binary and verify that from client we can no longer exploit the privileged command execution. Take a screenshot of the same.

WHAT TO SUBMIT

Capture screenshots as instructed in each exercise and upload to D2L. For puzzler, upload the modified main.c file to D2L in addition to the requested screenshot.