Security First Principles

Principle Minimization – Assessment

Scan for open ports

Take screenshot of currently open ports in server VM using nmap scan prior to applying iptables.

The screenshot should show all open ports including port 80.

Close unwanted ports

Use iptables to close all open ports except port 80. capture output of command 'iptables -L'. Run the nmap scan again and capture screenshot.

The screenshot should show the iptables rules that are used to close the ports.

Demonstrate lack of minimization yields vulnerability exploits

The program main.bin has a vulnerability that allows it execute privileged commands by current user. Exploit the vulnerability and execute the command 'ls /root'.

The screenshot should show the output of 'ls /root' command and it should list the contents of /root correctly.

Demonstrate how minimization improves security

Modify the program main.bin such that it uses the higher privilege only when required and reqlinquishes right after. With that demonstrate the privileged command execution vulnerability can not be exploited any more.

The screenshot should show the server returning permission error when the client tries to executed privileged command. The program main.bin should reflect the use of privilege only when required.