OBJECTIVE

In this assignment you will practice inspecting an implementation of a UDP server for security vulnerabilities.

DESCRIPTION

Attached is a buggy and vulnerable implementation of a TFTP server (netascii mode, and error messages are not implemented). Assume that this server runs as root on a server in the current working directory /tftpdir. Clients should be able to download any file from this directory, but no others on the server machine.

Detailed instructions:

- Download the file tftpserver_vulnerable.c from Sakai and understand this implementation (it's also a solution for the previous homework)

- Inspect the code and identify at least two different vulnerabilities. Create a file vulnerabilities.txt that contains a description of each vulnerability. For each vulnerability provide

 + the line number(s) of the problematic code

 + the type of vulnerability (e.g., confidentiality -- multiple types are possible)

 + a one paragraph description or brief example of how this vulnerability could be exploited

- Fix these vulnerabilities in the implementation. Try to make only minimal changes to the source code and mark each change with comments (// ***) in the source code. The corrected version should be contained in the file tftpserver_patched.c

- Upload the two files vulnerabilities.txt and tftpserver_patched.c to the module.

Grading: You will receive partial credit for each vulnerability identified and for each correct fix. At least two vulnerabilities and fixes are needed for full score.

- Download the file tftpserver_vulnerable.pdf from Sakai and understand this implementation (it's also a solution for the previous homework)
- Inspect the code and identify at least two different vulnerabilities. Create a file vulnerabilities.txt that contains a description of each vulnerability. For each vulnerability provide
 + the line number(s) of the problematic code
 + the type of vulnerability (e.g., confidentiality -- multiple types are possible)
 + a one paragraph description or brief example of how this vulnerability could be exploited
- Fix these vulnerabilities in the implementation. Try to make only minimal changes to the source code and mark each change with comments (// ***) in the source code. The corrected version should be contained in the file tftpserver_patched.c
- Upload the two files vulnerabilities.txt and tftpserver_patched.c to the module.