CS393 - Network Security - Lab Assignment 3
Remote Exploits
DUE: March 12

Summary:
In the previous lab, you gathered knowledge about the network and services running on the machines network using a powerful scanning tool. In this lab you will learn how an adversary could take control of a server by taking advantage of vulnerabilities in the services running on the server and how one can actually break in to these machines and get a root shell.

Pre-Lab:
- Read the following CERT advisory http://www.cert.org/advisories/CA-2000-13.html
- Download all the .c files from my poly.

Lab Work:
Part A
Having read the CERT advisory, you should realize that most of the hosts you discovered in the previous lab had ftp service running in them. Telnet to any of them and check what OS is installed. If the version, of the OS you see in the opening telnet screen, is mentioned in the CERT advisory then there is very real possibility that a vulnerable ftp service is running on it. So for this part compile the any or all of the .c files and try to use it against one of the hosts you discovered in the previous lab. If you are successful you will have a root shell from the other host. **You must produce the screen shot and tcpdump (remove data unrelated to ftp session) of the successful exploit that gives you a root shell.**

FAQ:
- How do I know whether I have the root shell?
  Wait for few minutes after you run the exploit and type “ls” you will see the listing of root directory from the host you hacked into.
- Where do I compile and run the exploit code?
  You should compile and run the code from Xserver.sisl.poly.edu
- How do I upload the code to Xserver?
  Use sftp to upload the code
- I get a lot of compiler errors when I compile a particular code?
  Well that particular code is not well written or not meant to be compiled in the platform you are compiling. So don’t use that code and move on to the next one
- Do all of the .c code files supplied work successfully?
  May be … may be not. This is something you have to find out
Part B
Answer the following questions:
1) Explain why and how the exploit code you used in Part A works.
2) What does this code do to the ftp service running in the remote machine to spit out a root shell?
3) Is exploit sending a code or some sort of binary code to the remote machine? If yes what is it sending and in what form is it sending (i.e is it C code, machine code, perl script, shell script, or just garbage)? (Hint: This question itself has a hint).
4) In a sense this exploit code is taking advantage of an “unintentional back door” in ftp service- what is it?
5) Can this exploit code work on all hardware platforms using the same OS and ftp version. Explain why or why not?

Part C
As you would notice that the shell you get after you run the exploit code is not really friendly and dies if you try to run a editor or even a more command. Find a way to create a user and make that user have root privileges. Report how you did it.

Part D
Identify another service running that has similar problem (i.e. “unintentional back door”) in the host you used for part A and try to find and exploits for it in the web.

Place were you can find reports on bugs and exploits:
- http://www.securityfocus.com
- http://www.cert.org
- http://www.linuxsecurity.com
- http://www.google.com/search?hl=en&q=linux+redhat+6.2+exploits

Report what exploit you have identified, how did you find it, and list the exploits you used. Again attach the screenchots and tcpdump outputs.

Estimated time to finish this lab:
Based on the amount of time it took for us to create this lab, we estimate that it will take at least 5 hours for you to finish this lab.

What to Hand in:
- Your reports for Part A, B, C and D.