PCS Lab 2: ShellShock Instructions

Instructions

Read and follow the SEED lab instructions below, and answer the questions in the next page.

SEED Lab Instruction on ShellShock:
http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Software/Shellshock/Shellshock.pdf

Some useful materials for you to get familiar with the shellshock vulnerability:

- Shellshock Attack Lecture from the SEED Labs: http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Software/Shellshock or just https://youtu.be/pEpOSCgTabs
- Practical Shellshock Exploitation: https://resources.infosecinstitute.com/practical-shellshock-exploitation-part-1/
- Shellshock Vulnerability by Tudor Enache: https://www.owasp.org/images/1/1b/Shellshock_-_Tudor_Enache.pdf

You can use the same VM as the one in Lab 1.

NOTE: Be careful of the white spaces when copy-pasting commands from the PDF files. The commands need to be the exact same as the given but the copy-pasting may introduce extra spaces or change the quotation marks. You can use ctrl+shift+v to paste in terminal.

Submission

Due: March 13, 11:00 PM (EST)

Late submissions are accepted with 50% grading penalty within 24 hours of the due. Submissions that are late for more than 24 hours will NOT be accepted.

Please submit your solution in PDF or image on https://www.gradescope.com/courses/38640, using Entry Code: **95KJWX**. Please choose the right page for your answer to every question.

Questions

Question 1: Please provide the names and NetIDs of your collaborator (up to 2). If you finished the lab alone, write None.

Collaboration Policy

1. **You can optionally form study groups consisting of up to 3 people per group (including yourself).**
2. **Everybody should write individually by themselves, and submit the lab reports separately. DO NOT copy each other's lab reports, or show your lab reports to anyone other than the course staff, or read other students' lab reports.**

Question 2: Please describe a function that will test the vulnerability of the bash shell as given in "*Task 1: Experimenting with the bash function*". Try the experiment on both the vulnerable version (/bin/bash_shellshock) and the fixed version (/bin/bash) and report your observations (including screenshots).

Question 3: Please set up the CGI program as described in "*Task 2: Setting up CGI programs"*

Question 4: Please describe your findings after executing the code given in "*Task 3: Passing Data to Bash via Environment Variable*" along with necessary screenshots. Explain how the data from a remote user can get into those environment variables.

Question 5: A lot of web applications hard-code database usernames and passwords in the server's source files (such as *.php files). Please use the Shellshock attack to find the PHP source file containing the server's database username and password under /var/www/CSRF/Elgg. Please describe what you did as an attacker to find the file, the username and password of the database, and attach relevant screenshots.

Question 6: Will you be able to access the /etc/shadow file using the shellshock attack? Why or why not? Explain in brief.

Question 7: One activity the attackers typically do after compromise is to search for secret files that are readable by them. Please find which files in the /etc folder are readable through the shellshock attack. What steps did you follow to obtain the list?

Question 8: Please launch a reverse shell via the Shellshock vulnerability as described in "*Task 5: Getting a Reverse Shell via Shellshock Attack* " and explain how the reverse shell can be obtained in brief.

Question 9: Please describe and explain your observations of "*Task 6: Using the Patched Bash*", including necessary screenshots.