Question Completion Status COURSES SERVICES COPYRIGHT STUDENT CORNER HI ALEX WANG WEI JIE . 105

CONTENT ... LAB TAKE TEST: LAB 3 ?

TAKE TEST: LAB 3

Test Information

Description	
Instructions	
Multiple Attempts	Not allowed. This test can only be taken once.
Force Completion	This test can be saved and resumed later.

QUESTION 1

1 points Saved

Can we try to run rootprog from rootdo and attempt to write something onto rootfile.txt, i.e: do you think the message "helloFromUser" can be written onto rootfile.txt?

○ Yes

● No

QUESTION 2

2 points Saved

Upon successful write, will the entire file be overwritten with the new sentence from buffer or is the content of buffer appended onto the end of the file?

○ ***The entire file be overwritten with the new sentence from buffer***

● ***The content of buffer appended onto the end of the file, original content of the file is unchanged***

QUESTION 3

2 points Saved

Can root user overwrite this userfile.txt, although it belongs to normal user and not root?

● Yes

○ No

QUESTION 4

3 points Saved

What is a symbolic link?

This question will be graded manually.

Provide a very short explanation (not more than 2-3 sentences).

Answers that are too lengthy wont be graded.

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

Paragraph Arial 3 (12pt)

Mashups

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Save All Answers Save and Submit

Question Completion Status:

a shortcut to another file. text string interpreted and followed by OS to actual path of the other file

Path: p Words:18

QUESTION 5

3 points Saved

What is the difference between symbolic link and the actual file?

This question will be manually graded.

Provide a very short explanation (not more than 2-3 sentences).

Answers that are too lengthy wont be graded.

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

Paragraph Arial 3 (12pt)

Mashups

symlink does not increase reference count of the linked file, whereas actual file does.

Path: p Words:14

QUESTION 6

1 points Saved

Can you (a normal user) delete a file like rootfile.txt belonging to the root? Note: these files are located inside the Root directory that belongs to the root.

○ Yes

● No

QUESTION 7

2 points Saved

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Save All Answers Save and Submit

Question Completion Status:

lrwxr-xr-x: l stands for symbolic link, owner can read, write and execute, users in the same group can read and execute, all other users can read and execute

○ ***lrwxr-xr-x: l stands for text file, all other users can read, write and execute, users in the same group can read and execute, owner can read and execute***

○ ***lrwxr-xr-x: l stands for directory, all other users can read, write and execute, users in the same group can read and execute, owner can read and execute***

QUESTION 8

5 points Saved

How does the script exploit.sh check if the attack is successful and stop the loop?

This question will be graded manually.

Provide a very short explanation (not more than 2-3 sentences).

Answers that are too lengthy wont be graded.

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

Paragraph Arial 3 (12pt)

Mashups

check the output of ls -l Root/rootfile.txt

if attack is successful, the size will increase (characters appended), OLDFILE differs from NEWFILE, then while loop exits

Path: p Words:27

QUESTION 9

2 points Saved

What "attack message" is injected into rootfile.txt when the attack is successful?

○ HELLO THIS IS ROOT FILE

○ Hello this is attacker!

● username1 fake_password

○ SUCCESS! The root file has been changed.

QUESTION 10

5 points Saved

Comment on your output (With regards to the task in The Attack section). Is your attack successful? If yes, how long does it take for the attack to be successful. If not, why not?

This question will be graded manually.

Provide a very short explanation (not more than 2-3 sentences).

Answers that are too lengthy wont be graded.

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

Paragraph Arial 3 (12pt)

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Save All Answers Save and Submit

Question Completion Status:

many attempts of executing. with access granted, and permission denied. ending with SUCCESS!, Exit success

yes, successful. about 1-2 seconds

Path: p Words:21

QUESTION 11

5 points Saved

If we only sleep for 1 ms instead of 1s, comment its impact to the attacker.

This question will be graded manually.
Provide a very short explanation (not more than 2-3 sentences).

Answers that are too lengthy wont be graded.

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

Paragraph Arial 3 (12pt)

Mashups

doesnt matter, still able to execute the attack, as it is automated

Path: p Words:12

QUESTION 12

5 points Saved

After fixing rootprog.c, relaunch the attack script using User/exploit.sh again and comment on

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Save All Answers Save and Submit

Question Completion Status:

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

Paragraph Arial 3 (12pt)

Mashups

different. attack cant be executed successfully, stuck in while loop, terminal output continuous, alternates between permission denied and Access granted, but always file cannot be opened.

Path: p Words:26

QUESTION 13

1 points Saved

Paste your fixed rootprog.c code to the space provided below.

This question will be graded manually

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

-- Format -- Arial 3 (12pt)

Mashups

```
/* toctou_prog.c */

#include <stdio.h>
#include <unistd.h>
#include <string.h>
#include <time.h>
#include <sys/types.h>
#define DELAY 1

int main(int argc, char *argv[])

{
   char *fileName = argv[1];
   char username[64];
   char password[64];
```

Path: div » div » span Words:227

QUESTION 14

5 points Saved

After editing the shell script, relaunch the attack script using User/exploit.sh again and comment on your output. Why do you think the output with this modification is different from the output by the original rootprog.c code?

This question will be graded manually.

Provide a very short explanation (not more than 2-3 sentences).

Answers that are too lengthy wont be graded.

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Save All Answers Save and Submit

Question Completion Status:

attack cant be executed successfully, stuck in while loop, terminal output continuous, alternates between permission denied and Access granted, but always file cannot be opened.

the new executable does not have SUID bit, running it wont change the effective ID to root. seteuid(getuid()) has no effect. permission is always the real ID so it can never fopen Root/rootlogfile.txt

Path: p » span Words:58

QUESTION 15

3 points Saved

If the SUID bit of rootprog is **not enabled**, can the attack still succeed? Provide a very short explanation (not more than 2-3 sentences).

Answers that are too lengthy wont be graded.

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

Paragraph Arial 3 (12pt)

Mashups

no. it will behave the same as rootprog_nosuid (answer to q14). because executing it as normal user does not elevate the effective ID to root

Path: p Words:26

QUESTION 16

5 points Saved

This lab talks about TOCTOU Race Condition attack. Why is the attack named as such? Who is racing with who in this case?

This question will be graded manually.

Provide a very short explanation (not more than 2-3 sentences).

Answers that are too lengthy wont be graded.

For the toolbar, press ALT+F10 (PC) or ALT+FN+F10 (Mac).

Paragraph Arial 3 (12pt)

Mashups

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Save All Answers Save and Submit

Question Completion Status:

the shared variable is userfile.txt

attacker's shell script is racing with Root/rootprog to create the symlink, pointing userfile.txt to Root/rootfile.txt, while Root/rootprog is executing access() and fopen() on userfile.txt, so it can fool fopen to open rootfile.txt with effective ID of root

Path: p Words:48

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Save All Answers Save and Submit