Take Test: Homework13

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.

Save All Answers | Save and Submit

QUESTION 1

30 points | Save Answer

Connect to Kali with RADISH and go to your M:\Tools\Password Homework Lab and copy the two files to your /usr/share/john folder. If your M: drive is not mounted in Kali already, follow the steps from this week's lecture slides 71-74. You should notice that there are three users in those files which are jwren, bthomas, and apatel. First, use the unshadow command to combine the passwdhw13 and shadowhw13 files into a file called hw13tocrack.

The current version of john the ripper has a bug so if you didn't already do this during the lecture you will need to upgrade john first by running this command:

apt-get --only-upgrade install john

Now, you will need to run john in various ways to crack all three of these passwords. Two of the passwords can be cracked using similar dictionary methods that we covered in the hand's on portion of the lecture. The third password will involve figuring out how to add the below incremental ruleset to the john configuration file at /etc/john/john.conf which performs a brute force on all numbers and letters for a six character password.

[Incremental:All6] File = $JOHN/alnum.chr MinLen = 6 MaxLen = 6 CharCount = 95

You will then run this new above ruleset by using the incremental option for your john cracking command and and specifying the ruleset as All6.

None of the attempts to crack the first two passwords should take longer than 10 minutes to crack if your john options are correct. The third password may take a little under 15 minutes. You can also hit the spacebar while john is running to see its current attempt.

Answer this question by providing uploading a document with a screenshot of each john command you used followed by the cracked password for each username.

This question is worth 30 points and you will receive 10 points for each successfully cracked password / provided command in your screenshots document.

Attach File Browse My Computer Browse Content Collection

QUESTION 2

10 points Save Answer

Check out the DMZ Scenario 2 - Isolated Forest example that was in the lecture. Answer the following questions:

1. The two domains are in the same forest (True or False).
2. The two domain controllers are individually both writable. (True or False)
3. Both domain controllers talk to each other and replicate. (True or False)
4. Both domains are managed separately. (True or False

QUESTION 3

10 points Save Answer

What is the difference between a Kerberos ticket granting ticket and a service granting ticket?

Arial 3 (12pt)

Path: p Words:0

QUESTION 4

5 points Save Answer

Which Access Control Model does Windows NTFS use?

- RBAC (Role Based)
- MAC
- DAC
- RBAC (Rule Based)

QUESTION 5

30 points Save Answer

You will upload a single document with screenshots to answer this question. First create a user in Kali named bparton and a user named tprentice. The document must contain the following:

1. Screenshot of the chage command used to set options that will generate the below output

of chage -l bparton: (Your "Last password change" will be different.)

```
root@KLY-IR105:~# chage -l bparton
Last password change                                    : Nov 15, 2015
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : Dec 01, 2016
Minimum number of days between password change          : 30
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 3
```

2. (You will perform the following as the root user.) Screenshot of all of the commands involved to: Create a file called testfile2, change the permissions (using numbers) so that the owner can read, write to the file but the group and others can only read. Then, show ls -l. Next, change the permissions again (using letters) so that the user, group, and others can all execute the file. Then, show ls -l. Lastly, set at ACL so that tprentice can also write to the file. Show the output of the getfacl command for the testfile2 file.

3. Create a new text file on the desktop of your Win 8.1 VM. Then take a screenshot of the Security Properties of the file after you give me (Shawn Davis) read permissions on it.

Attach File Browse My Computer Browse Content Collection

QUESTION 6

5 points Save Answer

What is the salt value of the following hash?

6dQmPokW.$Uad80dR1MP1jUUjo/h9EHN7H0FStKY51MdaRT/4sDPjwR.LFAceUTs4ZZySqPo4rdIp66l1BLQjoiwCQoohzF0:16754:30:99999:3:10:17136:

- 6
- dQmPokW.
- Uad80dR1MP1jUUjo/h9EHN7H0FStKY51MdaRT/4sDPjwR.LFAceUTs4ZZySqPo4rdIp66l1BLQjoiwCQoohzF0
- 16754:30:99999:3:10:17136

QUESTION 7

5 points Save Answer

A Linux user created a new directory and wants all users on the system to be able to enter the directory with the cd command. What permission type would need to be set on the directory?

- Read
- Write
- Execute
- N/A

QUESTION 8

5 points Save Answer

Which of the following Windows permissions allow deletion of a file?

- Read

- [ ] Write
- [ ] Read & Execute
- [ ] List Folder Contents
- [ ] Modify
- [ ] Full Control

Question Completion Status:

QUESTION 9

10 points Save Answer

In LM Windows password, plaintext passwords must be less than or equal to 14 characters. Why is an LM hash of a 14 character password easier to crack than an NT hash of a 14 character password?

Arial | 3 (12pt)

Path: p Words:0

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

Save All Answers | Save and Submit