Computer Security and Networks: Exercise 2

Deadline: 2 March 4pm

1 Access Control

For this exercise you need to explore the other home directories on the VM and find out more about what is going on at the company, in particular you need to find two tokens, get the shadow file and then crack some passwords to find two more tokens. The VM contains a number of access control vulnerabilities and you need to find and exploit these to access files that are protected.

1. Look in the directories `/home/carolmiller` , `/home/charlegarcia` `/home/jakkinkade` and `/home/nikadler`, somewhere in there are two files that contain tokens; these files are protected by the access control system. Search the home directories for these files and find access control flaws that allow you to read the files. Submit the two tokens you find to the token submission website.

   [3 marks each]

2. By exploiting mistakes in the access control settings of the VM, find a way to read the `/etc/shadow` password hash file.

   Once you have the shadow file, install a password cracker and try to crack the passwords for the staff accounts `aarushsanders` and `alayahpritchard`. You may use any password cracker you like – "John the Ripper" is probably easiest, but "Hashcat" will probably give you the best results. (N.B. you will need the "jumbo" version of john the ripper if you want to crack SHA hashes). You will find that getting a good wordlist and rule set is much more important than the speed of the computer you run the cracker on. A version of john the ripper which is compiled for the virtual machine is available in from the canvas page containing all assignments. Please make sure you download the correct version for your virtual machine. The file `JohnTheRipper_arm64.tgz` is for the M1 Macs with ARM architecture, and the file `JohnTheRipper_x86_64.tgz` is for everyone else. The canvas page for the assignments also contains a link to a suitable wordlist.

   The staff accounts `aarushsanders` and `alayahpritchard` each contain a token. Cracking the passwords to these accounts will allow you to log in as these users and read the tokens. Find these tokens and submit them to the token submission page.

   [6 marks]