ITEC 345: Secure operations on the operating system (UNIX/Linux)

Due date: Nov.06 (Wed.) 14:00.

Warning: Please note that you are still bound by the White Hat agreement and the rules of Radford University, the State of Virginia, and the U.S government.

***You MUST work in teams of two or three.*** Submit only one solution for your entire team. **All team members must be physically working together** for all parts of each problem.[[1]](#footnote-1)

If you are looking for others to work with, post a request on the discussion boards.

**Lab to use:**

1. Login to the Deterlab and either:
   1. swap in the experiment you created as part of previous deterlab homework (or)
   2. create a new experiment with the .ns file from previous deterlab homework.
2. Use instructions from the previous deterlab homework to login to the linux machine that you swapped-in.

This document has the problems; see the accompanying document for hints on how to accomplish each task. You will also want to frequently consult the man page for the commands indicated, so that you understand what they do (and understand the output of the commands).

**Please record your answers, and insert screenshots into this word document and submit on D2L** (only one submission per team). No hardcopy is necessary, for this assignment.

|  |
| --- |
| **Name + username of all teammates:**  **Tasks and deliverables:** |
| 1. **Create new user accounts and their home directories.**     1. Create 3 new users: *Uhura, Spock and Kirk*    2. Create their home directories as /home/uhura, /home/spock and /home/kirk respectively.   Deliverable: A screenshot of the passwd (/etc/passwd) file clearly showing the entries for the new users created. |
| 1. **Create a new group and add users to that group.**    1. Create a new group ‘security’    2. Add users Uhura, Spock and Kirk to the new group.   Deliverable: Screenshot of the group (/etc/group) file clearly showing the entry for the new group. Insert the screenshot in this space (increase amount of space as appropriate): |
| 1. **Identify user id and group id’s of the users created and the group ‘security’.**   Deliverable: List the user id and group id’s in the space below. |
| 1. **Set the expiry dates on the accounts of the users you just created. Ensure that their account expire within one year after the account creation date. The 1 year period is from the day you are working on this assignment.**   Deliverable: write down the commands you used to set the expiry date on Uhura’s account here: |
| 1. **Set the expiry dates on the passwords of the users you just created to ensure that the passwords expire after approximately 6 months of the date of account creation. Ensure that the user gets a warning at least 20 days before the password is due to expire.**     Deliverable: Submit the screenshot showing Uhura’s password expiry date and warning date. Insert the screenshot here: |
| 1. **Identify the default permissions on files that are created by Spock or any of the users.**   Deliverable: enter the default permissions. Write the answer here: |
| 1. **Change the default permission such that when a user creates a file only that user has read, write and execute permissions. All other users will have no permissions.**   Deliverable: Take a screenshot of the /etc/login.defs file showing the new value of UMASK and insert it here: |
| 1. **Check for all programs running on the system.**   Deliverable: Screen shot of the processes (not all the processes maybe visible – that’s fine). Insert screenshot here: |
| 1. **Identify the processes that are using most of the memory and cpu speed.**   Deliverable: screenshot of at least the first 5 processes. Insert the screenshot here: |
| 1. **Check for all the services that are running on the system**   Deliverable: Screen shot of the services. Insert the screenshot here: |
| 1. **Switch on the service “whoopsie”.**   Deliverable: command used to switch on the service (text-only). ~~Insert the screenshot here~~: |
| 1. **~~Identify all the programs that were installed on your system~~**~~.~~   ~~Deliverable: screenshot of~~ *~~some~~* ~~of the programs installed on your system. Insert the screenshot here:~~ (Skip this step) |
| 1. **Remove the program** chkconfig   Deliverable~~: nothing to deliver~~. Command used to un-install chkconfig. |
| 1. **Ensure that spock can only execute the /sbin/ifup program as root. Ensure that uhura can excute the useradd program and nothing else.**   Deliverable: Screenshot of the /etc/sudoers file with the changes you made. Insert the screenshot here: |

1. Should you want to add a third team member after having already completed problems, you’ll have to *re*-complete those steps with them (presumably letting them ‘drive’ the keyboard). (This often takes less time than you’d think.) [↑](#footnote-ref-1)