

Team Exercise #1
Logging
Exercise: February 20, 2006
Report Due Date: February 27, 2006

Team: Cars

Network Instructions

(1) Add shares to

- toyota.cosc.tu
- camero.cosc.tu
- alaska.cosc.tu

that can be read by any authenticated user. In each shared directory, create a plain text file with a message of your choice.

(2) In the home directories of each user of

- cobra.cosc.tu
- sage.cosc.tu
- blade.cosc.tu

create a plain text file with a message of your choice.

Authentication Credentials

You have the following authentication credentials

<i>Machine</i>	<i>User</i>	<i>Password</i>
white.cosc.tu	colorUser02	**02userColor
colors1.cosc.tu	colorUser3	**3userColor
seattle.cosc.tu	user1	16#71d*ci
philadelphia.cosc.tu	user2	ci2!to2%i
creampuffs.cosc.tu	User3	fghj159753
nutterbutter.cosc.tu	auser	Dy%%965Rr

Exercise Instructions

You may not access machines from other teams until after the start of the exercise.

For each machine for which you have authentication credentials, do the following:

- Determine the OS
- If it is a SuSE machine, use your credentials to log in to the SSH server. Check the home directory of your user to find the message file. Record the message.
- If it is a Windows XP machine, use your credentials to access the shared directory. Locate the message file, and record the message.

For each machine for which you do not have authentication credentials, attempt to do the same thing.

While the exercise is running, you may use any and all means to prevent your activities from appearing in the logs of the target machine. Creativity in this regard is not only permitted, but encouraged.

IMPORTANT!

For each command you execute, you must complete the corresponding Command Summary Form. Failure to do so will result in a substantial grade penalty.

After the Exercise

For each machine in your network, answer the following questions:

- Who logged on to your SSH servers?
- Who accessed your shared files?
- Which teams have read your message files?

In your final report, you will give complete and concise answers to each of these questions.

The final report will be neat, organized, and well-written. It will contain:

- A copy of the Machine Information Sheet for each of your machines.
- A copy of each of your Command Summary Forms for each command executed.
- A copy of the messages for each of your machines.
- The results of your reconnaissance as described above.
- The analysis of your logs, described above.

Team Exercise #1
Logging
Exercise: February 20, 2006
Report Due Date: February 27, 2006

Team: Colors

Network Instructions

(1) Add shares to

- colors1.cosc.tu
- colors2.cosc.tu
- colors3.cosc.tu

that can be read by any authenticated user. In each shared directory, create a plain text file with a message of your choice.

(2) In the home directories of each user of

- white.cosc.tu
- purple.cosc.tu
- red.cosc.tu

create a plain text file with a message of your choice.

Authentication Credentials

You have the following authentication credentials

<i>Machine</i>	<i>User</i>	<i>Password</i>
toyota.cosc.tu	user_1	@ @!1Kstu
cobra.cosc.tu	user2	789BVTS14
newyork.cosc.tu	user1	b8*92c#dc
baltimore.cosc.tu	user3	3x76)5mi*
doublestuffed.cosc.tu	User3	/\..tgb4
bordeaux.cosc.tu	buser	#*HxP82Aa

Exercise Instructions

You may not access machines from other teams until after the start of the exercise.

For each machine for which you have authentication credentials, do the following: