CSCE 629 Lab 1
Winter 2019
Reconnaissance / Linux / Interacting with Targets

Assigned: **Lesson 1, 3 Jan**
Due: **Lesson 7, 15 Jan, 1400**

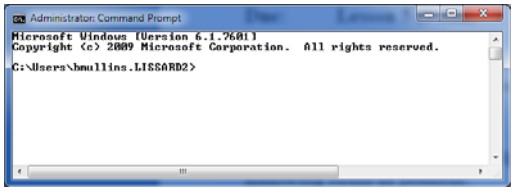
You must include these questions in your submitted solution. In other words, your submission must include the question listed followed by your solution with the answer clearly indicated (e.g., put a box or circle around the final answer).

You are not authorized to attack any machine during this lab. Do not alter the targets in any way. You will be tempted, but don't. You'll get the opportunity later. Also, turn off all of your firewalls so your tools are not blocked.

You must clearly indicate your answers. Do not simply provide a screenshot; use arrows or boxes to indicate your answer. The best response to each answer is a screenshot using arrows or boxes followed by a short narrative.

These instructions apply to all lab and project assignments.
You will document your results in the form of a report. The key word for all course reports is CONCISE! Explain your methodology for arriving at the answers. Provide succinct and logical responses. You'll be graded on your **documentation of the process** as well as the results themselves. The following should help you generate an outstanding report:

- Your target audience is the M4I IT staff. Your report should contain enough details such that the IT staff (not the brightest bunch) can replicate your results. **The IT staff prefers bullet format.**
- As you prepare your report, remember the IT staff needs to understand exactly how you were able to accomplish each task. You must take screenshots and include the command line in the image.
- The report must contain detailed instructions including tools and/or exact commands used.
- If you used a tool, include how you configured the tool.
- If you use a command line, include the exact command entered including all switches and arguments.
- You may want to also use photographs where a screenshot is not feasible; this proves you actually found the information.
- The IT staff is minimally manned and cannot afford to read about unproductive attempts to assess/penetrate their systems. Therefore, they do **not** want a listing/discussion of unproductive paths or techniques; report just what worked.
- It is your responsibility to keep the report succinct yet covering all vital information. You should NOT include 100 pages of Nessus scan results; distill the information for the IT staff.
- Ensure all text (including figures) are legible, and circle or box the area of interest.
- Cropping your screenshots typically helps draw the reader's attention to the area of interest.
- Add page numbers to each page in the lower right corner except the cover page.
- Use Times New Roman 11 point font for text. You may use smaller font for tables so they will fit on one page.
- Use portrait orientation; do not use landscape unless the diagram is best displayed in landscape.
- Do not include my figures or tables in your solution (e.g., do not include the Frank and Ernest cartoons or the network diagram in this lab). Also, you are not required to include long narratives given in the assignment.
- Print in color. You may use double-sided pages. Be sure to staple such that your work is visible.
- You must use black text on white background command shells as shown here.



Part 1 - Reconnaissance

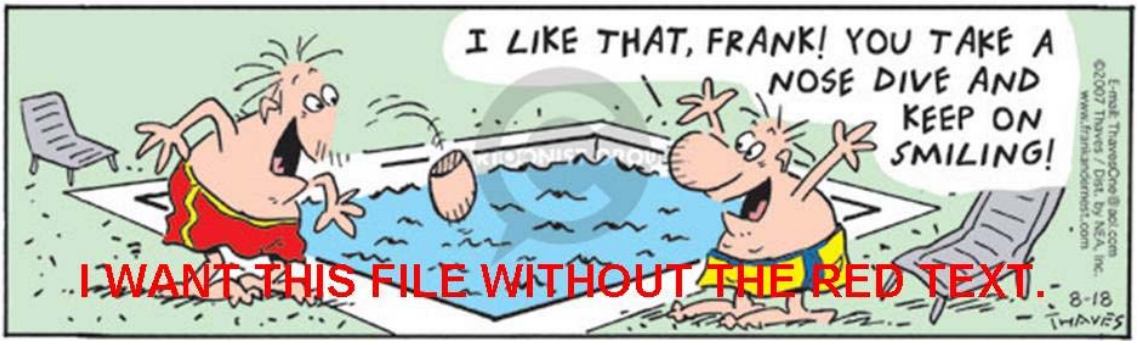
1. Provide the name, complete email address, and phone number for the web POC at USAFA on 24 Feb 2001.

2. List the social security numbers for Kevin Mitnick. Explain how you learned this information.

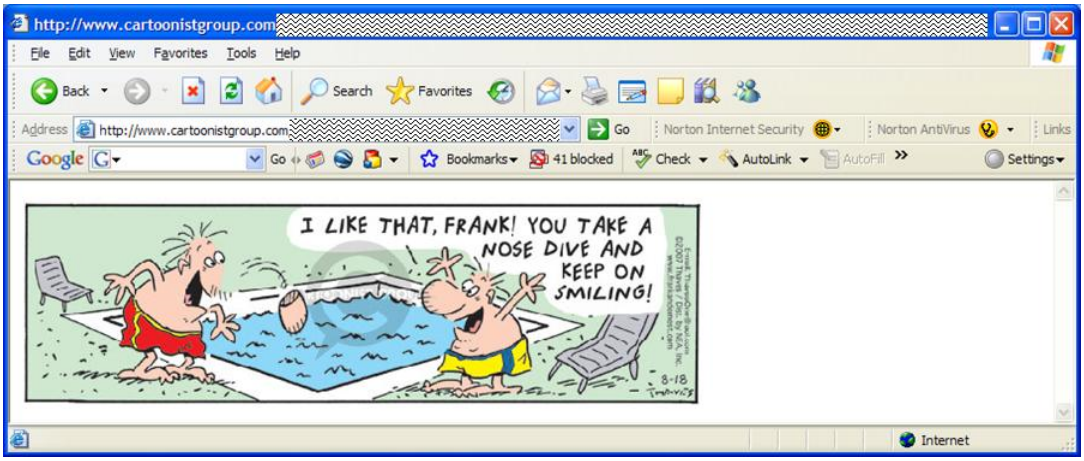
3. On the author's (Ed Skoudis) website, what is the title of the third puzzle in the author's "Math Puzzles" list? I am not referring to his "Hacker Challenges" list.

4. Give the complete URLs for three distinct sites that link to www.ci.beavercreek.oh.us. These sites must not include any from the beavercreek.oh.us domain.

5. I like the Frank and Ernest cartoon. I <u>really</u> like the following .JPG image (without the annoying red text of course):



Retrieve a copy of the file from http://www.cartoonistgroup.com/store/add.php?iid=18317. You must submit a screenshot of your browser clearly showing the file's URL and the cartoon as shown below, except your screenshot will contain the full URL. The only object in the browser window is the cartoon. Explain how you obtained your file. You must download from the www.cartoonistgroup.com site.



6. Provide an image of the front and back of Ed Skoudis' house. What full postal address, email address, and contact phone number would you use to tell him his sprinklers were left on all night?

7. Watch the following found in the Resources directory:
   a. History of hacking video (also at https://www.youtube.com/watch?v=Y47m1cOyKjA)
   b. Recon video: "Watch hackers break into the US power grid.mp4"
   c. Slideshow "Killing with Keyboards"
   d. Short clip at http://www.aclu.org/pizza/images/screen.swf

Indicate in the answer section of this question that you actually watched all videos and presentations.

Part 2 - Working with Linux and gcc

8. You will practice working with c programs in Linux for this problem.

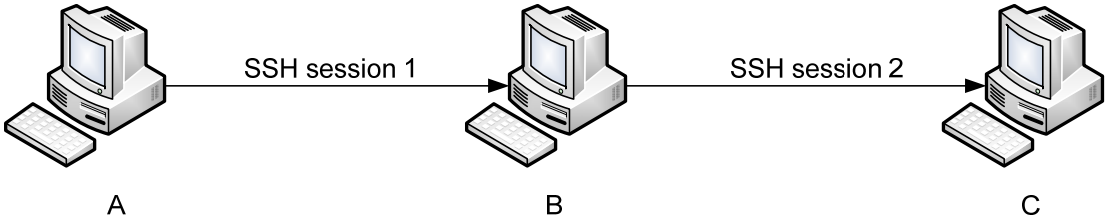
   a. In Linux (e.g., Kali), compile and run the following program called **`Caesardecrypt.c`**; this file is in the Lab1 directory. Hint: look up the **`gcc`** command.
   b. Provide a screenshot showing the successful compilation.
   c. Provide another screenshot showing the execution after you enter the following string as input: **`FBEHUDWWDFNLVFRRO`**.
   d. Finally, what was the original unencrypted message?

```
#include <stdio.h>

int main(void)
{
   char messageClear[BUFSIZ];
   char messageCrypt[BUFSIZ];
   int shift, i;

   printf("\nThis program decrypts a capital string using all 25 key values of
the Caesar Cipher. \n\n");
   printf("Enter Ceasar encrypted string in all capital letters: ");
   fgets(messageCrypt, BUFSIZ, stdin);
   fflush(stdin);

   printf("\nEncrypted Message:%s ", messageCrypt);

   for (shift=0; shift<26; shift++)
   {
      i=0;
      while (messageCrypt[i])
      {
        messageClear[i] = messageCrypt[i] - shift;
      if (messageClear[i] < 'A')
         messageClear[i] = messageClear[i] + 26;
         i++;
      }
      messageClear[i-1] = '\0';

      printf("Message after %d shifts: %s\n", shift, messageClear);
   }
}
```

Part 3 - Interacting with Targets

You must be on the CDN network to connect to the targets.

Part 3 requires you to connect to targets using various protocols. The targets are listed as B and C in the figure below; you are running Windows on machine A. The IP addresses are 10.1.0.63 (B) and 10.1.0.198 (C).



9. Working with SSH.
   a. What transport protocol and port is the SSH server using?
   b. Establish SSH session 1 from A to B using username of **`user`** and password of **`Password!123`**.
      1. I suggest the tool called Putty (putty.exe at http://www.chiark.greenend.org.uk/~sgtatham/putty/) as your SSH client. Putty will issue a warning asking if you trust the target; select "yes" to accept the target's certificate. Putty will open a command window allowing you to execute commands on the target.
      2. Once connected, display the name of the target as well as the operating system type and version number of the computer you are accessing; provide a screenshot of this window.
      3. Display the active TCP connections on B. Highlight your connection to the target?
      4. Find a picture of a horse. How did you find the horse picture? Take note of the file's location; you will download this file later. Hint: to suppress error messages like "Permission denied", you can redirect error messages (i.e., 2) to the null device by including the following after your command: **`2>/dev/null`**

   c. Within the same Putty window, ensure you can reach C from B using ping. Now type **`ssh user`**`@<<C's IP>>` to establish SSH session 2 from B to C where **`user`** is the username. Use **`Password!123`** for the password.
      1. Accept C's certificate. Once connected, display the name and operating system version of the computer you are accessing.
      2. Find a file on C that has a filename with the format **`flag?.*`** where ? is a number and * could be any extension. Hint: files with ".lnk" extensions are only links. Remember to start your search from the \ directory. Take note of the file's location; you will download this file later.

   d. Now type **`exit`** at the command prompt while logged into C to tear down SSH session 2. You should see your Linux command prompt return meaning you are now interacting with B. Once again, type **`exit`** to tear down SSH session 1; this will close the Putty window.

10. Using FTP, transfer the horse picture to your machine. You must use the native (command line) Windows FTP command. Provide a screenshot of the FTP window showing your successful FTP session including file download. What transport protocol and port is the FTP server using? Are you using active or passive FTP? How can you tell? What port numbers are the client and server using? What is the name of the horse? Filtered Wireshark screenshots are required.

11. Using SCP or WinSCP (http://winscp.net/eng/download.php), transfer the flag file to your machine. If SCP does not connect to the target, try SFTP. Provide a screenshot of the [Win]SCP window showing successful file download and another screenshot of the image contained in the flag file. Describe exactly how you learned the contents of the flag file and displayed the image; screenshots are a must as you describe your process.

12. Now upload an interesting photograph of yourself to machine C in the "**`Documents and Settings/user/My Documents`**" folder. Ensure your file name starts with your last name (e.g., Smith.jpg) and your face is clearly visible.

13. Using Remote Desktop Protocol (RDP), connect to the machine called RDP# where # is your team number. Provide screenshots of the windows/commands used. What transport protocol and port is the RDP server using? Provide a

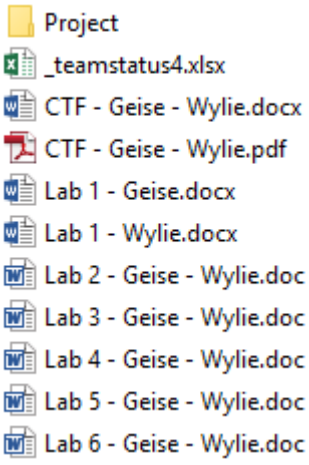
Wireshark screenshot of your computer using the protocol and port listed; filter your Wireshark capture to only include frames involved. What is the secret message found on the target (filename contains "secret")?

CDN Team Folder

As you complete assignments during this course, you will need to place a copy of the files listed below in a folder called Mullins in your team folder (e.g., public\CSCE 629\Cady-Harris\Mullins\). Use the naming convention shown to the right.

- Reports for labs. Be sure to include both Lab 1 reports
- CTF report in both Word and PDF format
- Folder for the Project files

Do not create subfolders for the labs. Your directory structure should resemble the figure at the right.



General Observations

These questions must also be answered and count towards your score.

How long did it take you to complete Part 1 of the lab?

How long did it take you to complete Part 2 of the lab?

How long did it take you to complete Part 3 of the lab?

Was it an appropriate length lab?

What corrections and or improvements do you suggest for this lab? Please be very specific, and if you add new material, provide the exact wording and instructions you would give to future students in the new lab handout. You may cross out and edit the text of the lab on previous pages to make minor corrections/suggestions.