**CSC 436 Lab 11** – 30 points

This assignment is to be performed in the IA Lab. To access this, navigate to <https://ialab.dsu.edu/> and enter the Learn environment.

Refer to the walkthrough video for additional details.

**Instructions**

1. Open Kali Linux 2020-3: **kali / kali**. An older version of Kali is there as well - you are free to user either: **root/toor**

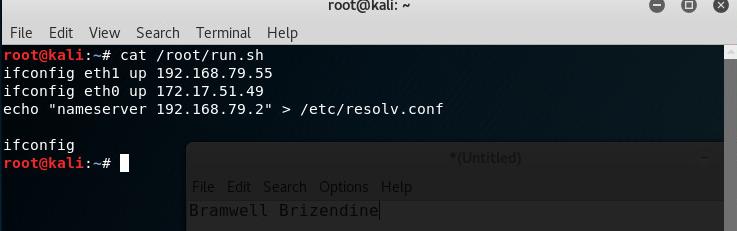
2. We must first run the **run.sh** contained on the Desktop (or at /root/run.sh on the old Kali). Navigate to that folder and enter **sudo ./run.sh**. Some network settings can get lost being cloned and copied out, so this will help ensure the IP address is correct for us. If you run into network issues, e.g. network connectivity disappears, run this script again and make sure it retains the ip address.

3. You are given the URL **www.candy.lane**. This address is only valid within this lab; it does not work outside the lab, as .lane and some other domains used are not valid domains. Use **www.candy.lane** to find a target. Once you have found this target, use the ip address and begin your fun. We got this. Think of what kinds of commands can allow us to gain DNS information.

4. For Kali 2020-3, you may use Nessus if you like. The username and password is **kali/kali**. It can take 5-10 minutes to load. If you wish to use Kali-2017, that also has an install of OpenVas. The password for OpenVas is in **/root/pass** should you need it.

**Getting Started:** How will you find the ip address? Think back to our earlier phases. *Hint:* You will not want to use the www.candy.lane URL in some of our tools, such as Nmap. (There is no http.) Stick to the ip address once you figure it out. How can we turn [www.candy.lane](http://www.candy.lane) into a useful URL? Again, once you get the IP address, start to use that ip address, not the domain.

Preface: You must provide screenshoots of each of the following. **Number your responses. Unnumbered labs will receive a 0.** I hate to be this “strict,” but this is a 400-level course, so putting your name on the assignment and numbering responses should be second nature. For Part I. you can simply go I.A., I.B., or one overarching I and A, B, C, etc. below it. **Make sure your name is visible in the background for all screenshots (see below image). I will check the logs to ensure each student logs in.**

Notice also how the screenshot is not the entire desktop. Screenshots that are unreadable or include vast amounts of other material will not be accepted.

**Provide screenshots in response to all of the below questions/asks, while adhering to the guidelines above:**

*\*\*If it is not obvious, provide any necessary commentary. The burden of proof is on the student.*

*\*\*Unless otherwise specified, only provide ONE screenshot for each of the following.*

**Part 1: Candy.lane Adventures** *13 points*

A. Show how you found the ip address for www.candy.lane.

B. Show your use of nmap to identify open ports on candy.lane.

C. Show your use of Nessus/OpenVas/nmap to identify vulnerabilities on candy.lane. You are required to run a vulnerability scan and provide the screenshot, but you may use other methods as well to find vulnerabilities. Please describe and include up to two additional screenshots if this applies.

D. Show your use of Metasploit to compromise candy.lane. What is the exploit? What are the options? You may include two or three screenshots here.

E. Obtain a meterpreter shell on candy.lane. You may upgrade if need be. Refer to our lecture content on upgrading meterpreter and alternate ways of doing so.

F. Navigate and find the confidential secret.

G. Use five meterpreter commands. You may use two or three screenshots here if necessary.

H. Upload Netcat to your target. Execute Netcat on the target and use it to download a file. Show that the file downloaded successfully.

I. Obtain passwords for users. Your method of doing this will vary, and it is at your discretion is to how you perform this.

**Part 2: Candy.lane Redux** *12 points*

Preface: There is another target owned by the same business. Can you find it? There are a couple ways. First, you could use some of the techniques in our earlier phases to find the location. You also might find information in the candy.lane machine. *Hint:* Try looking in My Documents.

A. How did you find the ip address for the new target?

B. Show your use of nmap to identify open ports for this target.

C. Show your use of Nessus/OpenVas/nmap to identify vulnerabilities on the target. You are required to run a vulnerability scan and provide the screenshot, but you may use other methods as well to find vulnerabilities. Please describe and include up to two additional screenshots if this applies.

D. Show your use of Metasploit to compromise the target. In this case, you may open up the machine if you wish to and interact with it. (Hint: You may need a password to do this.) That way you can make use of client side attacks. For instance, you might give the user a link to click on, and you could simulate that yourself. If you find a password that works, you might also attempt to pass the hash. How you compromise this is up to you. You may certainly use multiple screenshots here.

E. Obtain a meterpreter shell. Partial credit for other shells is available.

F. Use five meterpreter commands. You may use two or three screenshots here if necessary.

H. Obtain passwords for users.

**Part 3: Questions** *5 points*

\*\*\*Screenshots are not acceptable for these questions. Provide typed responses.

A. List all the domains you found. You should find at least two.

B. List all the IP addresses you found. Provide identifying information, e.g. ports open. Can you identify any services or software (versions)? Expect reduced credit if specific software and specific versions are not identified.

C. Where does the DNS come from? What do you know about it?

**Bonus** *Point Varies based on quality*

1. What is the Candy Lane bank routing number? (This is not on one of the above two targets.) Notes: You do not need to use Metasploit here, although you could attempt it. Show how you found it. Use sufficient screenshots and commentary to describe your process.

**Deliverable**

* Turn in a PDF/DOC/DOCX that has requested responses. Screenshots must be cropped appropriately and readable to be accepted. Please respond to all questions, numbering the responses that you provide.
* **Your name must be visible in screenshots, as shown in example on page 1.**