Lab 13 - Final Project Part 3

Congladurations again this week! You so impressed the CIO that she has provided your name to the national trade organization of widget makers, of which the company for whom you work is a member. The trade organization is trying to ensure its members are taking every precaution in the cybersecurity area. No one wants a black eye from something as simple as unpatched systems.

Therefore, the trade organization is having the best pentesters from each of their member companies participate in a very large, very robust penetration test of each other's networks. You have proven that you were the best penetration tester that your company has, so the CIO put you up for the competition. Plus, with the extra pay you will earn from working on this project you can upgrade from milk and cookies to milk and Ghirardelli chocolate.

The rules of the penetration test are similar to the first pentest you conducted on your own network with some twists.

1. To make the test more manageable, all pentesters have been put into one of three groups: 1, 2, or 3. You will find yourself assigned to a group on the student network information sheet. Your group number is the same as your lab section number.
2. This is a **non-destructive penetration test** on a small subset of each member company's IP space. Specifically, the range of X.X.X.151-155. All companies use a class C subnet mask.
3. Using the list, you need to first select the group you have been assigned to (1, 2, or 3 based upon your lab section), find your name/netid in the list, and then target the **two IP ranges** in the list immediately **below** yours. If you have questions about which IPs in which ranges you are to be testing, please ask one of the adjudicators of the pentest (the TAs and Dr. Rursch).
4. You can exploit the machines since you are pentesting, but **cannot do anything malicious** to them. The pentesters have to respond to the incidents on their own machines, as well as fix them (continue reading for more details).
5. You also can move laterally through the machines and look at any files you find, including cracking passwords.
6. You have permission to establish persistence.
7. You may plant flags as long as they are **not destructive**. If you can, add a user as your netID so the System Administrator (other student) can verify your work and fix any issues (will require root/sudo access). If you cannot add a user, then create a file with your netid. You may direct message the System Administrator (the other student in your lab section) so he/she can make updates to their machine.
8. You will have to find usernames and passwords on your own.
9. You still have full access to the local network's Security Onion at https://onion.homework.231.com/squert, credentials: **viewer/cpre231**. If you are on a

different board (1 through 3), then you cannot sniff other companies' traffic. **However, you could work with other pentesters on that board to get that information if you want. You must note any cooperation of that kind in your report. That is the only cooperation you are able to do.**

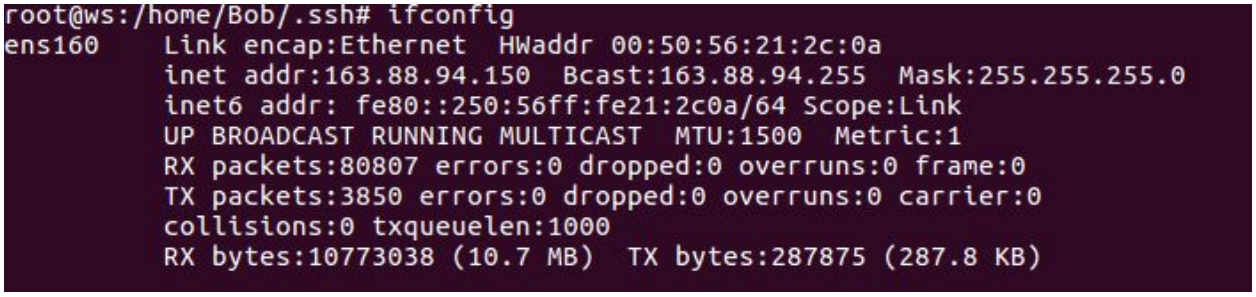
10. You can attempt to use social engineering, but you may not impersonate the Instructor or the TAs.

To prove you accessed the other company's system or information you need to complete the following table. You will also need a screenshot that corresponds to each line of the table. The screenshot must show the IP address and whatever was found or exploited.

#	Host IP	What was accessed?	How was it accessed?
1	X.X.X.150		
2	163.88.94.150	Bob's private key	ssh to ftp.lab11.231.com with key

A numbered screenshot of the IP and whatever you found/did. The number matches the number in the table above.

2a. IP



2b. Found the ssh information

```
root@ws:/home/Bob# cat note_to_self.txt
Hi Bob, it's Bob

Remember when you made that ssh key just like in a previous lab that would let y
ou log into your remote account on ftp.lab11.231.com on port 22?

Yeah,

nor do I.


root@ws:/home/Bob# cat note_to_self_ps.txt
It's in the .ssh directory.


Wow - you need to get some memory pills.
```

2c. sshed as Bob to ftp.lab11.231.com

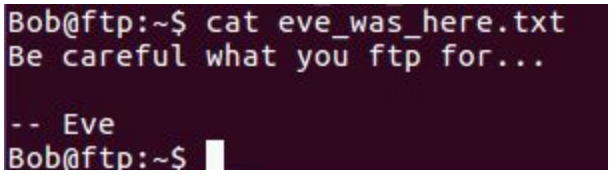
```
Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '13.04' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Apr  3 02:19:29 2018 from ws.lab11.231.com
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

Bob@ftp:~$
```

In addition to doing pentesting of 2 IP ranges that are not your own, you also need to report incidents on your own network. You will use the following table to do that. This isn't a full incident response report, but you would use it when you write your report to the national organization once your pentesting is complete.

Again, to prove how you responded to the incident and remediated it, take a screenshot and number it so it corresponds with the line in the table.

#	Host IP	What was accessed?	How it was accessed?	What was the impact of the incident?	How did you respond to the incident?
1	X.X.X.150				
2	etc				

1. Flag planted by Eve



Turnin

Please complete the pentesting table and the incident response table found in the lab description above. Each line in the table must be numbered and have a numbered corresponding screenshot to prove your claim. Your lab report is **REQUIRED** to use these tables/formats, or points will be taken away.