Lab 11 - Final Project Week 1

You have been working part-time for a local company doing web dev this semester. It isn't the big bucks, but it keeps the bills paid and gives you a little free money for cookies and milk.

Each week after lab you head to work. Most days you have a conversation about the lab topic with your manager, usually asking him about the same kinds of security issues you've just worked with in lab. The week after doing remediation you asked him about the patch schedule for the web servers in all three areas: development, QA testing, and production. His casual response was, "Well, we only worry about updating the system when we buy new hardware. It is so inconvenient to test the applications when new patches are applied." You figure that if the web servers are behind in patches so are the workstations and desktops.

You also asked him about permissions on files and plaintext protocols. Ironically, his response was similar. "I'm a web developer. I don't need to worry about those things."

Needless to say, you have walked away shaking your head. One day you happen to be in a meeting with the CIO and the topic of conducting a penetration test and internal audit comes up. None of the full-time staff offered any suggestions on how that could occur, so you decided to speak up. You explain that you think a penetration test should be done of the network, the servers, and applications that are running. You don't verbalize this part, but you think to yourself, "Well, it's about time!" Since you want to work in cyber security in the long-term and you think you could perform the penetration test for the company you offer to do it.

The CIO is unsure whether you can perform the penetration test successfully, but she asks you to conduct a **non-destructive penetration test** on a small subset of the IP space. Specifically, she asks you to work on the range of X.X.X.150-159. Since you work there you know this IP range uses a /24 netmask. She also has agreed to the following rules:

1. To let you exploit the machines since you are pentesting, but not to do anything malicious to them.
2. You also can move laterally through the machines and look at any files you find, including cracking passwords.
3. She did not give you permission to establish persistence.
4. She won't give you console access or usernames and passwords. You have to find all ways into the machines and any holes on your own.
5. You will, however, have full access to the local network's Security Onion at https://onion.homework.231.com/squert, credentials: **viewer/cpre231**.
6. You will have access to exactly one account from the getgo - your account
    a. Username: Eve, Password: h@ckerz

You decide to go back to the labs you did this semester to help guide your penetration test. You realize that many of the machines in the network could be just like the ones you tested in lab. You don't do any passive information gathering to start. You decide to start with host discovery and move on from there. You will do some passive discovery after you figure out what machines and OSes you are working with.

You created the tables below to try to organize your thoughts before you have to write your report for the CIO.

Host Discovery

Host	Open Ports	Services	OS guess
X.X.X.150			
etc.			

Information leakage
After completing the table above, you decide you may want to look to see if there is any information being leaked on any of the servers or workstations. This could happen before, during, and after any of the other steps.

Host	What I tried	What I found	How I could use it
X.X.X.150			
etc.			

Sniffing the traffic
You saw that there are some cleartext protocols running when you did host discovery, so you decided to sniff the traffic. You created the following table to record what you found

Source IP	Source Port	Destination IP	Destination Port	Useful cleartext captured/recorded
X.X.X.150				
etc.				

Vulnerability discovery

You decided to pull out the big guns and scan for vulnerabilities. Below you need to record the ones that are a realistic threat to your network security.

Host	Vulnerability	Why it is a threat
X.X.X.150		
etc.		

Exploiting the vulnerabilities

You were given the go ahead to exploit the systems, but **NOT TO DO DAMAGE**. Remember, you are hoping that if you do a good job you can get future work as a pentester and/or cyber security professional for the company. More money == more cookies!

Host	Exploit	Countermeasure to suggest to the CIO
X.X.X.150		
etc.		

In week 2 the CIO will be hiring you to secure the network. You will be given more details about what services have to stay running and what services can be removed at that time. **You need to be careful if you decide to move forward before the week 2 instructions are published.** Also, in week 2 you will receive console access to help with your remediation efforts.

NOTE:

1.You may not count disabled firewalls nor double-count misconfigured/rouge user accounts as vulnerabilities! You are encouraged to find and document issues with user accounts, but you're paid enough cookies to warrant a thorough investigation of the entire machine.

2. If you use a vulnerability scanner, remember, they can return both false-negatives and false-positives. You must verify that the vulnerability is present on a machine, even if Nessus says the machine is vulnerable. For example, if Nessus reports that a service is out-of-date and

is vulnerable to a specific CVE, you need to test the service in question for the vulnerability mentioned in the CVE.

Turnin

Please complete the tables found in the lab description above. Your lab report is **REQUIRED** to use the above tables/formats, or points will be taken away.