ENPM685 – Midterm - Due Monday March 28th @11:59pm

Version 3.0 – February 18th 2022

You have been hired to conduct a penetration test and security assessment for a fictitious company, ENPM685 Pictures, Inc. The goal of this penetration test and security assessment is to show the executive of ENPM685 Pictures, Inc. that their security posture needs to be improved.

Background

ENPM685 Pictures, Inc. is a small movie production studio that specializes in low budget "mockbusters" that are spoofs of larger budget films produced by larger studios. They have been successful by extreme cost cutting wherever possible, which shows in their IT infrastructure and hiring practices. For example, to not have to deal with employee benefits the company only has 1 employee, the CEO Bob Dobbs. Everyone else is hired as a contractor. Due to a recent issue with a rogue contractor stealing several ideas for upcoming films and an aggressive growth plan the CEO is moving towards hiring actual employees and developing the infrastructure (IT and otherwise) that supports ENPM685 Picture, Inc's production efforts.

As part of this expansion, I as a consultant to the CEO has recommended bringing in an IT security firm to assess the current state of ENPM685 Pictures, Inc's IT security through a penetration test and recommendations for improvement of the current environment. You are that IT security firm hired to perform this assessment.

Build a Replica of the Server

ENPM685 Pictures, Inc's IT operations are small -- a single server that hosts the firm's website, primary file server, as well as other resources. You can build your own copy of this server by doing the following steps:

Note: These were also written for VMWare Fusion for macOS, the VM creation process for VMWare Workstation/Windows should be similar. If you are using a different virtualization tool follow the steps you used to create the primary Ubuntu VM we use in class.

1. Download the ISO file for the type of architecture your laptop is running on.

    - x86 64bit systems - https://old-releases.ubuntu.com/releases/20.04/ubuntu-20.04-live-server-amd64.iso

    - M1-powered MacBooks/ARM-based systems - https://old-releases.ubuntu.com/releases/20.04/ubuntu-20.04-live-server-arm64.iso

2.In VMWare create a new VM by going to the **File** menu and clicking **New…**
3. Drag the Ubuntu 20.04 LTS ISO file to the "**Install from disc or image**" portion of the screen.

4. Click **Continue**
5. When you see the Easy Install screen unselect it. (It doesn't work properly.)
6. Make a boot firmware selection, I used "**Legacy BIOS**"
7. Click **Continue**
8. Click **Customize Settings**
9. Give the VM a name, I will use "**ENPM685 Midterm**"
10. Select the memory size, I will use **2048 MB** (2GB) for my VM. (If you have a system with 8GB of RAM you can lower this to 1GB.)
11. Click the large Play button in the VM window to start up the VM and begin the install.
12. Most of the questions should be straightforward. Some recommendations on settings:

- When you get to the "**Guided storage configuration**" screen select "**Use an entire disk**"
- I used the following for my user information under "**Profile setup**" **Please use the same user/password.**
    - Name: **ENPM685**
    - Server name: **enpm685**
    - Username: **enpm685**
    - Password: **password**
- For the SSH Setup screen, check the box next to "Install OpenSSH server"

13. Monitor the install which will install fairly quickly. When you see "**downloading and installing security updates**" select "**Cancel update and reboot**".

You will most likely see the VM spin for a while with "**cancelling update**" and a spinning bar. Let the VM do its job and it will reboot when it is finished.

Now that you have the base VM we need to configure it. You can do this by downloading and running a script to configure the system to meet our needs.

14. Type the following command to download the install script to your VM: **wget --no-check-certificate https://terpconnect.umd.edu/~kts/enpm685/midterm/install.sh**

15. Make the script executable with **chmod +x install.sh**

16. Run the script with **sudo ./install.sh**

Once the script has finished you will see a message that says "**ENPM685 Midterm VM Configuration Complete!**" Once you see that message you can now begin to complete the assignment.

The Assignment and Requirements

- Conduct a penetration test of ENPM685 Pictures, Inc's server and report your findings.
- There are 6 "flags" spread out across the server. By finding these you can demonstrate to the CEO the need to make security improvements. A top grade can only be attained by finding all 6 flags.
    - What is a flag? It will be a short phrase or other interesting information you discover during your penetration test. For example, if the flag is a file (named "**flagX_is_inside**" it will be the contents of the file, not just the file name/location. They are clearly marked, you will know them when you see them.

The Rules of Engagement

- Use any tools you feel are appropriate to properly test ENPM685 Pictures, Inc's computers for security vulnerabilities.
- Asking other people to assist you with this project is **NOT PERMITTED**. However, if you are stuck you **may ask the professor for a hint**. You are given **ONE** hint that will not affect your grade. If that hint is not enough that "hint" will be valid until you are able to find one of the flags. You may ask for (and be provided) more hints for additional flags if needed but extra hints will affect your grade. Technical questions about building the virtual machine for this assignment do not count towards your hint count.
- **Please direct all questions for help with this midterm to the professor. Do not contact the TA for help with the midterm.**
- Once you have built the virtual machine for this midterm you may **NOT** use the user account used to build the virtual machine for any part of your attack on the virtual machine.
- You may **NOT** analyze or reserve any part of the install script or the files it may download for building the virtual machine.
- Booting the VM into a single user/recovery mode is **NOT PERMITTED**.
- Changing a password of any kind is **NOT PERMITTED**.
- Brute forcing the CEO's email account is **NOT PERMITTED**.
- Phishing the CEO's email account is in scope however sending the CEO any kind of malware/exploit kit is **NOT PERMITTED**.
- The CEO checks his email account at least once a day but usually twice a day, once around lunch time and once in the evening. He is not the most technically savvy so a basic well-crafted phishing attempt will most likely work.

The Report

Once you have finished your security assessment you need to write up your findings and how you discovered the flags you did. What should be in your report:

- What flags you found (to receive a top grade you'll need to find all 6)
- How you discovered those flags

There is no minimum or maximum length for this assignment. I have many of these to grade so please don't make your final longer than it needs to be, please keep it to the point, and try to keep me entertained please. ☺

Due Monday March 28th @11:59pm

Review the syllabus for information on the class late policy. **Don't wait until the last minute to get started on this final project!**

Once you have completed this assignment you can delete the VM you created for this midterm, we will not be using it again.