ENPM809Q – Final

Version 1.9 – Dec 14th 2021

Virtual Machines (VMs) – There are 4 of them

Drive link: https://drive.google.com/drive/folders/1G0O-iE1A4VImURNn5LTicv7cmb8dHrFc

OVAs of the Final machines are available from the class Google Drive share in the "Final" folder. You should import the OVAs into your VMWare Workstation or Fusion install. If you receive and error message that the import failed click **Retry** to "relax the OVF specification and virtual hardware compliance checks"

Some of these VMs will tell you the IP address they are running on. The others you will need to use your network enumeration skills to determine what IP addresses they are using and what they are running. You will not be given any user name or password to begin this final.

Some of these VMs are large in size and for that I apologize, I tried to keep them as small as possible but Windows likes to use up disk space. They are all set to use a minimal amount of RAM (512MB-1GB each) and 1 virtual CPU each. Some of those VMs will run a little slow. You do not need to run all the VMs at the same time but I would recommend running the Windows VMs all at the same time. If you need disk space you can delete any of the other VMs we have used for the class so far minus your Kali VM which will be helpful in solving this final. These VMs are all using DHCP which will work for this final but in real life at least one of the systems would be using a static IP. You are welcome to modify that host to use a static IP and/or modify the etc/hosts file for the other systems to point to the IP address that system is using.

Background and the Assignment

The Masked DJ is a worldwide phenomenon. They have quickly taken the world by storm rising to the top of the world most popular DJ lists replacing well known DJs like Carl Cox, Fatboy Slim, Diplo, and Tiesto. Playing to sellout crowds all over the world nightly The Masked DJ has gained their following by hiding behind a mask and getting club goers to return to focusing on the music.

The Masked DJ is planning to have an "unmasked" party at the start of 2022 where they will play for the first time without the mask with all proceeds from the event and associated silent auction going to charity. There is a great concern that a leak of who The Masked DJ is before the event could lead to people not showing up and the charity event being a disaster.

You and your group have been hired as a pen testing firm to see if you can break into The Masked DJ's IT environment and discover photos of who The Masked DJ is. These photos are stored on a development version of The Masked DJ's website and show The Masked DJ when

they were much younger. You are also to make recommendations on how The Masked DJ's IT team should lockdown and improve their overall IT security.

The Masked DJ has a small office team who perform the office needs for The Masked DJ.

- A booking manager who books events and travel for The Masked DJ
- An IT manager who runs the IT infrastructure
- A webmaster (currently on leave) who set up the initial IT environment and runs The Masked DJ's website. They have grant plans for a new version of the site to be launched just after the "unmasked" party.

You have been assigned to a group of 3. Your group is to select a Group Name and then work together to solve this final and discover who the Masked DJ is and write up a professional looking report document how you moved through the environment to solve this final as well as recommendations for The Masked DJ to secure their IT environment.

This final will test your ability to enumerate, exploit, pivot, use password attacks, and use post exploitation tools to solve it. If you get stuck review the course material, exercises, and readings from both course textbooks. **YOU CAN DO IT!**

The Rules of Engagement

- Asking other people outside of your group to assist you with this final **is not permitted**. You are allowed to ask the TAs and the professor for assistance around technical questions around importing, running, or connecting to the Virtual Machines.
- Booting any of the VMs into a single user/recovery mode for any reason **is not permitted**.
- Using any forensics tools on the VM disk images **is not permitted**.
- Other than the forensics tool exclusion any other tool you feel is appropriate to solve this final is in scope and you may use them.
- **If you get stuck each group is permitted to ask the professor for 1 (one) hint to help the group. Use it wisely.**

Helpful MD5 Checksums

There are 6 files that will help you solve this final. To help you verify you have found them the MD5 checksums of these files are below. These files are all in the same location.

```
ec920f6a63f80bdaed233844dee35602
941150d01339cac745327d0d4549a0c3
dfed11803eac1bf990940cc1a500a202
dde8e712353d62de269f62b11bab847f
b5cf9353ae742b19983b269fdb5f841f
2cdf05cbc8d6a465e7361d3fa4bdf80e
```

The Report

Once your group has discovered who The Masked DJ is and verified you have found all 6 files you need to write your report. You should begin your report by listing your Group Name, all members of the group (along with UID). This report should be concise, accurate, free of typos, and include 2 main sections:

- Executive Summary
- Technical Report

The Executive Summary is a high-level overview of what you found along with your overall recommendations. This is also where you should share who The Masked DJ is.

The Technical Report goes into more detail on the step by step of our attack narrative/walk through along with more details on your recommendations on how The Masked DJ should improve their IT security posture.

If your group does not find the photos/solve who The Masked DJ and the deadline is approaching you should focus your report on what you did discover and your recommendations for improving The Masked DJ's IT security posture.

One member of the group will submit the final on behalf of all of you.

Due Friday December 17th @ 11:59pm!

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