**Digital Forensics**

**Assignment 1 – Ethical Hacking via Armitage**

**10 points**

# Instructions

**Please read the instructions carefully. Those students who fail to follow the instructions may get a zero score for this assignment.**

1. This is a group assignment. Each group can have 3 or 4 students. Every student must submit the same group report to Blackboard. Otherwise, students missing the submission will get a zero for this assignment.
2. Answer each question following the original question. Do NOT delete the original question.
3. Answers to all questions must be put into **ONE** document.
4. Students must put answers following each question in this assignment. The instructor will not grade a report with only answers in it and the student gets zero for such an assignment. An assignment report must include original questions.
5. Students MUST submit the finished assignment in pdf format to Blackboard. The doc must be submitted as ONE standalone file and cannot be tarred or zipped into a container unless explicitly instructed not to do so.
6. All required files or docs must be submitted in one submission. Note: Blackboard allows unlimited number of submissions of one assignment by students and the instructor counts only the last one.
7. Refer to [Print screen](http://en.wikipedia.org/wiki/Print_screen) on how to take a screenshot.
8. Underlined blue text points to a web link. Ctrl + Click to follow link.

# Lab ENVIRONMENT

**1. PERSONAL COMPUTERS**

If you plan to use your personal computer for the labs, please use [this link](https://www.cs.uml.edu/~xinwenfu/VMs/) to download  [Kali-CR-25G.ova](https://www.cs.uml.edu/~xinwenfu/VMs/Kali-CR-25G.ova) and  [Windows10-CR-60G.ova](https://www.cs.uml.edu/~xinwenfu/VMs/Windows10-CR-60G.ova). At least 100GB free disk space is needed. Please do NOT download at last minute since downloading takes a long time.

Here are the steps to start (Click the links embedded in the blue and unlined text to watch videos):

1. Install VirtualBox on [Windows 10](https://www.youtube.com/watch?v=8mns5yqMfZk) or [Mac OS X](https://www.youtube.com/watch?v=lEvM-No4eQo).
   1. You may need to download VirtualBox at home since the University blocks the downloading.
   2. Mac M1/M2 computers cannot use the two VMs since they do not support VirtualBox.
2. [Import .ova](https://youtu.be/us5N0X75v-o) file into VirtualBox.
3. If a student feels the VM is slow, please watch [How to Speed up your VMs in VirtualBox!](https://www.youtube.com/watch?v=2z7icd0vm0M) For Windows and [How to improve Linux performance in a VirtualBox VM](https://www.youtube.com/watch?v=tbF8jNjD_IE).
4. If there are errors when trying to use the two VMs, students may try to install VirtualBox Extension Pack. Please watch YouTube videos such as [Install VirtualBox 6.1 in Windows 10 | With Extension Pack](https://www.youtube.com/watch?v=HC5obz0YPuc). Students shall always use the newest version of VirtualBox.

**Note**: Please create *NatNetwork* first within VirtualBox before using the Nat Network. Under Windows, this can be done within VirtualBox: *File*->*Tools*->*Network Manager*.

**2. CYBER RANGE**

Room 445 of Wannalancitt Building at 600 Suffolk St, Lowell, MA 01854

**CREDENTIALS**

**VMs**

Windows 10 VM Credentials

* User: Malware Analysis
* Password: Malware

[Kali's Default Credentials](https://www.kali.org/docs/introduction/default-credentials/)

* User: kali
* Password: kali
* sudo password: kali

**Cyber Range PCs**

User name: student

Password: CyberSecurity

# Questions

Read the tutorial [Penetration Testing](https://github.com/xinwenfu/GenCyber/tree/main/FieldTrips/V2) at <https://github.com/xinwenfu/GenCyber/tree/main/FieldTrips/V2>. **Note:**

* The tutorial is only a reference and students have to adapt the tutorial to the current lab environment.
* Watch the related class recordings to see how to use the two VMs, vchat and Armitage.

1. Please include a screenshot of two vchat clients on the Kali VM chatting via the vchat server running on the Windows VM. (2 points)
2. Please include a screenshot of the compromised Windows VM. (3 points)
3. Please include a screenshot of using Meterpreter shell to capture the screenshot of the Windows VM. (3 points)
4. Did you see any suspicious behavior on the Windows VM when it is hacked? (2 points)

**References**

1. [Chapter 6](https://www.virtualbox.org/manual/ch06.html). Virtual Networking, Accessed on Feb. 16, 2020

1. [VirtualBox for a Kali Guest](https://www.kali.org/docs/virtualization/install-virtualbox-kali-guest/), Accessed on Feb. 19, 2020
2. VirtualBox Network Settings: [Complete Guide](https://www.nakivo.com/blog/virtualbox-network-setting-guide/), July 16, 2019