USC CSci530
Computer Security Systems
Lab notes Fall 2022

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
CSci530: Security Systems
Week 1 Lab Notes – August 26, 2022
Lab Introduction

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute

http://ccss.usc.edu/530
Relationship to CSci530

• Class home page
  http://ccss.usc.edu/530

• Lab Component of Class
  – 10 Labs during Semester
  – Grade based on 8 best scores
  – Labs graded Pass, High Pass, Low Pass and Fail
Lab Lecture Component

- 4:30 – 5:20 in OHE and online
  - Lab Lectures are recorded
  - Purpose is to provide you with guidance for the lab you will perform in the following week.
  - For the lab component it is acceptable to view the “lectures” asynchronously.
Hands on Lab Component

• Through 2019 we required most students to visit our instructional lab in OHE to use equipment established for the lab during one of several sessions assigned to groups of students. Some labs were performed online using the DETER Computer Security Testbed at USC-ISI.

• Clearly, in-person lab instruction was not possible in Fall of 2020 because of COVID, so last year we converted most lab exercises to VirtualBox and you can now perform those exercises using your home machines.

• Different exercises run on different Virtual machines, and we will describe the requirements and how to run the exercises in the Lab Lecture components each week.

• This week is a broad overview. There is no lab assigned for the coming week. Next weeks lab “lecture” will describe the first assigned lab on “cryptography”
Virtual Box Configuration

- Like last semester, you will use VirtualBox to configure the virtual machines used in your lab exercises.
- The instructions provide the VirtualBox commands to configure the machines you need, set up addresses and interconnections, etc.
  - A series of scripts will be provided for each exercise you will perform.
  - Some exercise on Fedora, others on Kali Linux and we will provide the VM’s that you will load and run.
M1 Macs and Other Platforms

- Unfortunately, VirtualBox does not run on the newer M1 Macs, and you might have difficulty using it on certain other older machines.
  - For students that do not have their own machines capable of running VirtualBox, it may be possible to check out a laptop for the semester from the Viterbi Engineering Computer Center.
  - This should be the approach of last resort, as I expect the may be limited in the number of loaner laptops that are available.
  - If you have access to a lab machine on which can load VirtualBox, that might be the best approach. Alternatively, if you have a friend or roommate that has a system that supports virtualbox, using their machine for the several labs that require virtualbox may also work.

More information is available here:
https://viterbiit.usc.edu/services/engineering-computing-center/ (see the tab for Long Term Loaner Laptops).

You might start the process of obtaining a loaner laptop with a message to engrhelp@usc.edu.
Lab Exercise Weekly Topics

- Cryptography/Key Management
- Authentication
- Authorization
- Application Security
- Packet Sniffing
- Firewalls
- Intrusion Detection
- ARP Spoofing
- Tunnels & VPN’s
- Filesystem Labeling

Separate Instruction Pages will be added to the CSci530 website for each week’s lab, starting with Cryptography next Friday (for you to perform before September 10th).
# Tentative Lab Schedule

<table>
<thead>
<tr>
<th>Topic</th>
<th>Lecture Date</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>8/26</td>
<td></td>
</tr>
<tr>
<td>Cryptography</td>
<td>9/2</td>
<td>9/16</td>
</tr>
<tr>
<td>Authentication</td>
<td>9/9</td>
<td>9/23</td>
</tr>
<tr>
<td>Authorization</td>
<td>9/16</td>
<td>9/30</td>
</tr>
<tr>
<td>Application Security</td>
<td>9/23</td>
<td>10/12</td>
</tr>
<tr>
<td>Packet Sniffing</td>
<td>10/7</td>
<td>10/21</td>
</tr>
<tr>
<td>Firewalls</td>
<td>10/21</td>
<td>11/4</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>10/28</td>
<td>11/11</td>
</tr>
<tr>
<td>ARP Spoofing</td>
<td>11/4</td>
<td>11/18</td>
</tr>
<tr>
<td>Tunnels &amp; VPNs</td>
<td>11/11</td>
<td>12/2</td>
</tr>
<tr>
<td>Filesystem Labeling</td>
<td>11/18</td>
<td>12/2</td>
</tr>
</tbody>
</table>
Lab Exercise Mechanics

- Like last semester, you will use VirtualBox to configure the virtual machines used in your lab exercises.
- The instructions provide the VirtualBox commands to configure the machines you need, set up addresses and interconnections, etc.
  - A series of scripts will be provided for each exercise you will perform.
  - Some exercise on Fedora, others on Kali Linux, some on CentOS and we will provide the VM’s that you will load and run.
Lab Platform

• VirtualBox
  – How do I get Virtual Box?

• Several VMs will be distributed
  – What VMs are there?
  – How do I get the VMs?
  – How do I import the VMs into VirtualBox
How do I get VirtualBox

- [www.virtualbox.org/wiki/Downloads](http://www.virtualbox.org/wiki/Downloads)
What VMs are there?

• There will be 3 or 4 of them
  – In the form of .ova files
  – Ova files are large
  – I will spit them into smaller fragments for download
  – You will combine the fragments post download
• The first of these will be posted by Monday
  – Others will follow as needed for subsequent labs

• For some labs you will run multiple instances of a Virtual Machine. Scripts and detailed instructions to do this will be provided in the instructions associated with each lab assignment.
# Which Labs use Which VMs

<table>
<thead>
<tr>
<th>Topic</th>
<th>VMs used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptography</td>
<td>May be done on laptop</td>
</tr>
<tr>
<td>Authentication</td>
<td>(tba/tbd)</td>
</tr>
<tr>
<td>Authorization</td>
<td>Fedora30-fall20</td>
</tr>
<tr>
<td>Application Security</td>
<td></td>
</tr>
<tr>
<td>Stack overflow</td>
<td>CentOS 4.3 min-gdb</td>
</tr>
<tr>
<td>Heartbleed</td>
<td>(tba/tbd)</td>
</tr>
<tr>
<td>C sign extension</td>
<td>Fedora30-fall20</td>
</tr>
<tr>
<td>Packet Sniffing</td>
<td>Fedora30-fall20</td>
</tr>
<tr>
<td>Firewalls</td>
<td>Fedora30-fall20</td>
</tr>
<tr>
<td>Intrusion Detections</td>
<td>CentOS 4.3 min-gdb</td>
</tr>
<tr>
<td>ARP Spoofing</td>
<td>Fedora30-fall20</td>
</tr>
<tr>
<td>Tunnels and VPNs</td>
<td>Fedora30-fall20</td>
</tr>
<tr>
<td>Filesystem labeling</td>
<td>(tba/tbd)</td>
</tr>
</tbody>
</table>
How do I get the VMs

• The VM’s will be made available using USC’s Google drive, and links will be distributed with the lab assignment instructions which will be posted in D2L and on the course webpage.
How do I import the VMs to VirtualBox

- Per the detailed instructions that will be provided with each lab, you will download the OVA fragments and combine them, yielding an OVA files (approx. 5 or 6GB).
- You then “import appliance” into the Virtual Box Manager.
Some Configuration Scripts

• Virtualbox includes “vboxmanage” command
  – A command line equivalent for GUI features
• We will provide short scripts that use vboxmanage to automate VM setup work for you.
  – To create VMs
  – To make settings (virtual cabling, Ips, hostnames)
  – To power the on and off
  – To destroy them
• Because your lab is to perform functions using the VM’s, not to configure the VMs.
Where to get the lab scripts

- There are 10 labs
- Each set of scripts will be in their own directory for a particular lab, obtainable through Google drive, per the instructions for the individual assignment
  - There are two sets, “.bat” for windows, and .sh (bash) for Linux/Apple. These are functionally equivalent.
  - Each set will likely have 4 to 6 scripts for different functions, e.g.:
    - Populate
    - ConstructNetwork (optional)
    - InternalSettings (optional)
    - Poweron
    - Poweroff
    - Destroy
Your tasks for Next Week

• We want you to familiarize yourself with the basic infrastructure for the labs, absent the individual instructions for the specific labs. Thus:
  – Download and install virtual box
  – By Monday we will make one appliance available for download, and you should download that appliance and provision it into VirtualBox.
  – You will download some relevant scripts for your platform (Windows, Linux or Apple).
  – We have posted instructions for the cryptography lab already, but that lab will not require the use of Virtualbox. The following Lab will be posted by the end of next week, and that lab will require the use of VirtualBox.