Gregory Ododa

ITIS 3110L-L01

System Auditing

Lab 08

03-27-2017

# Introduction

Lab 8’s purpose was to explore a VM using commands to assess the security state of the machine.

# Overview

## Goals

This lab is more open-ended than the previous labs. It is designed to give you a chance to experiment with the commands presented to you in the previous lecture. Some of the questions may require using commands and knowledge from previous labs as well.

## Deliverables

* Lab report that includes
  + The steps you took to audit the system including discussing why you think it might be important to know this information.
  + The results from the steps you took and what the results might indicate.
  + Anything else you found that you think is suspicious.
  + For each item, consider the who, what, when, where, why and how and address each one of those when appropriate. Remember – Auditing is the process of deep inspection for discovering hard-to-see flaws that might exist. Detail is important.

# Auditing

## Downloading the VM

Navigate to http://lab302-web.hades.lab/ (172.16.1.250) in the lab using a web browser. In the 3110 *morningcatch* directory download the file *morningcatch.zip* from the link and save it to /scratch on your host workstation. Note The .zip file is compressed.

## Running the VM

Decompress the zip file. The VM is VMWare based and will need to be imported into VirtualBox

To set up the VM:

1. Start VirtualBox
   1. Open VirtualBox and create a new virtual machine
      1. Click *New* and enter a name, e.g. MorningCatch
      2. Ensure *Type:* is Linux and Version is Linux 2.4 (64 bit)
      3. Click *Next* and set *Memory Size* to 1024 or 2048 MB
      4. Click *Next* and select *Use Existing virtual hard disk drive*
      5. Click on the little green arrow box and find your VM you downloaded and unzipped
      6. In the directory find and select the *Mint.vmdk* file and Click *Open*
      7. Click *Create*
      8. Click the *Settings* button.
      9. Click *Storage*
      10. Click *SATA Controller*
      11. Ensure *Mint.vmdk* is there
      12. Click *OK* to save the setting.
      13. Click the green *Start* icon to open the VMDK file and boot the virtual machine.
   2. It will take several minutes for VirtualBox to check the new VM, be patient
   3. The VM should start. There may be some minor warnings about mouse and monitor settings.

The system has Windows and Linux Desktops. To access the Linux Desktop logon to the Boyd account.

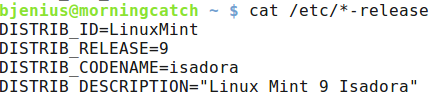
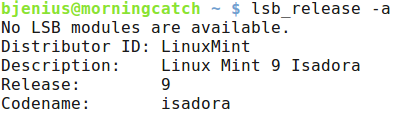
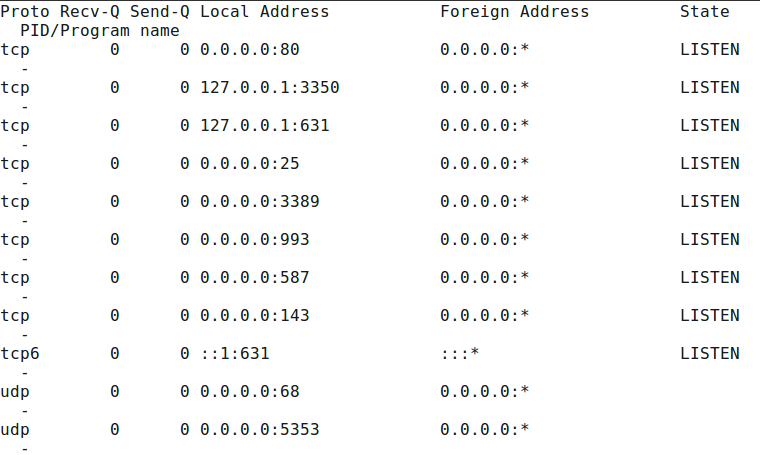
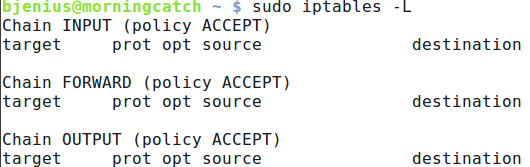
Username: boyd

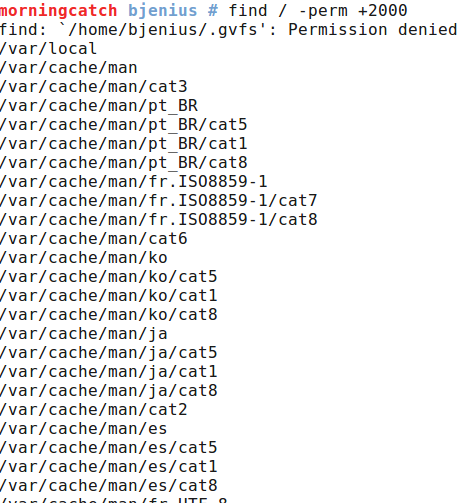
Password: password

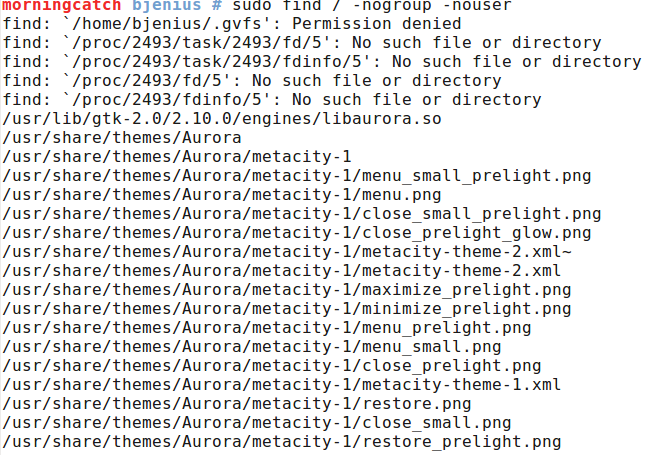
## When you are finished

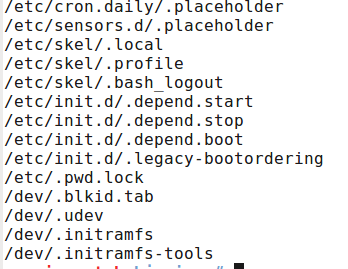
You may want to delete the virtual machine when you are finished with the lab. The computers have limited space available in /scratch and most of it is used this late in the semester. You may save the VM to a USB device if you wish, but it is about 12GB in size.

# Questions your lab report should answer

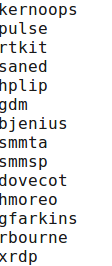
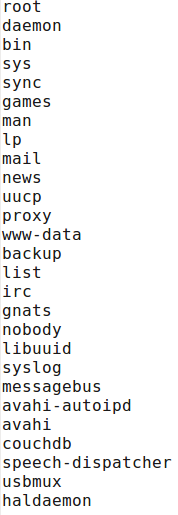
* Is this Linux distribution Debian based or Red Hat based? Describe where you looked and how you discovered your answer.
  + **A:** **I searched the internet for how to find out the distribution and used $ cat /etc/\*-release to determine that it is a Linux distribution.** 
* What is the exact distribution and version? Describe where you looked and how you discovered your answer.
  + We have not covered how to determine this, but a Google search for “Linux get distribution and version” will show you some cool stuff.
  + **A:** **Using $ lsb\_release -a I found out that the machine is Linux Mint 9 Isadora.** 
* Is this version of this distribution still supported? Find information on why this might be important and discuss security issues with running unsupported distributions.
  + This is something you will need to ask Google
  + **A: No it is not still supported. There are several risks such as new holes in the system are no longer being monitored thus there may not be a solution, this can result in loss of private information.**
* What services are running on the machine? Why is it important to know the services that are running on a machine?
  + Give the installed versions of three of the services
  + **A: Apache2(2.2.14), cups, pulseaudio(0.9.21). It is important to know which services are running to keep track of the system status and monitor things like cpuspeed.**
* What network ports are open and what is listening to them? Why is it important to know what ports are open? How might this step provide evidence of unauthorized use?
  + **A: It is important to know which ports were not opened by the system admin because that could mean that an unauthorized user has access to the network.** 
* What run level does the system boot into? Why is it important to know what run level the system boots into?
  + **A: level 2. It is important to know the run level because it defines what system services are operating.**
* Is iptables running on this system? If so, what rule set? Discuss what these rules indicate and how this could affect system security?
  + **A: There are no rules set. This means the system is vulnerable to attack.**
* What SUID and SGID files exist on the system? List a few of these and explain why is it important to know these files exist? How does that relate to system security?
  + The find on this machine does not support the –perm /6000 format. Use the obsolete –perm +6000 instead.
  + **A: It show file locations of important system settings. This information should be private because these programs grant special privileges to the user who is executing them, it is necessary to ensure that insecure programs are not installed to prevent hackers from entering through possibly open back doors. Below is the output.**

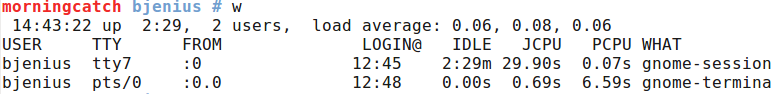


* Are there any files on the system that do not have an owner or group? List a few of these and explain why this might be important information.
  + **A: This might be important because it shows the files that are allowed by all.** 
* What hidden files exist on the system? Again, list only a few of these and discuss about how an attacker might use hidden files while compromising a system.
  + The patterns you want to search for are ‘.??\*‘ and ‘.[^.]’.
  + The quotes around the patterns are important
  + **A: An attacker can use hidden passwords, hidden file names, or easy-to-discover bugs to break in. Below is the output.**



* Does this system use an external authentication source? Why would it be important to know if the system is using an external authentication source?
  + How to do this was only hinted at in lecture. Try asking Google but do not spend too much time trying to figure it out.
  + **A: No it is not external. It is important to know the type of authentication that your system is using in order to defend from known possible attacks.**
* What local users are on the system? Do any users look suspicious? Discuss why these look suspicious.
  + **A: I used cut -d: -f1 /etc/passwd to find the users. nobody and man are suspicious users because they don’t have a relevant/specific name like the others. Below are the users.**



* What users have logged into the machine recently? From where? Why is it important to check this frequently? What are a couple indications if you check and find that nobody has logged on recently (especially if this a heavily used machine)?
  + **A: If there is nobody in the recent log that could mean that the log was cleared, most likely by a unauthorized user trying to hide its activity. Below are the users.**

# Appendix

* Morning Catch
  + <http://blog.cobaltstrike.com/2014/08/06/introducing-morning-catch-a-phishing-paradise/>
* Running VMWare on VirtualBox
  + <https://blogs.oracle.com/thaniwa/entry/en_how_to_use_vmware>
  + <http://smallbusiness.chron.com/open-vmdk-virtualbox-28847.html>
  + <http://smallbusiness.chron.com/can-virtualbox-read-vmware-machines-33435.html>

# Conclusion

Lab 8 was interesting because it allowed us to explore and find our own answers to the questions. Researching the many different problems that can occur if the proper security checks aren’t regularly monitored. For the most part the lab went smoothly but with so much information out there I had to try several different commands to find the proper output for some of the questions but I learned more that way.