Cybersecurity Essentials v1.0

Instructor Lab Manual

Lab - Cybersecurity Jobs Hunt (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Explore the career opportunities for cybersecurity professionals.

Explore the career requirements for cybersecurity professionals.

Part 1: Exploring Cybersecurity Jobs

Part 2: Cybersecurity Job Requirements

Background / Scenario

The cyber world is full of dangers and threats to individuals, organizations, and countries. These perils have resulted in a major demand for individuals with the knowledge, skills, credentials, and ethics to protect our people and systems. In this lab, you will explore the types of jobs available, job titles, job requirements, and credentials required by the cybersecurity industry. The Internet is full of job search websites that can provide you with information about careers in cybersecurity. Many of these websites are job search sites called job aggregators. This means that they collect job postings from many other sites and organizations. In part one, you will explore three of the world's most popular job aggregator websites. In part two, you will discover the requirements of cybersecurity jobs.

URL: http://burning-glass.com/infographic-geography-cybersecurity-jobs-2015/

Required Resources

- PC or mobile device with Internet access

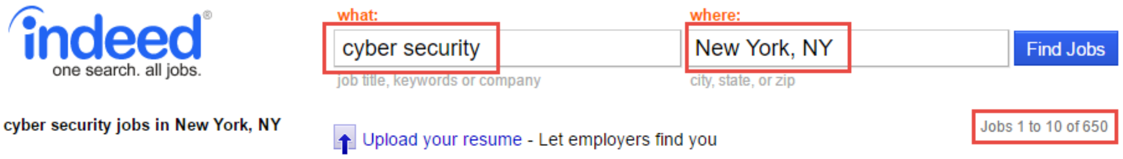
Part 1: Exploring Cybersecurity Jobs

Indeed is one of the world's largest job aggregators. Indeed helps millions of job seekers and employers find the right fit. The Indeed website posts a wide assortment of jobs from entry-level to top executives. Indeed also posts part-time jobs and internship opportunities.

Step 1: Explore Cybersecurity Job Postings:

a. Open a browser and view the following video: "How to search for jobs with Indeed.com" (https://youtu.be/9gqsnA2Lk-0)

b. Click here or got to http://www.indeed.com/ to perform a job search. Start by looking for all jobs in New York City, USA. Use the phrase **cyber security** for the first search. Record the number of job found.



what: cyber security

where: New York, NY

cyber security jobs in New York, NY

Jobs 1 to 10 of 650

indeed
one search. all jobs.
job title, keywords or company
city, state, or zip
Find Jobs
Upload your resume - Let employers find you

The number of jobs will be listed at the top right hand corner and will vary for every search.

c. Do the same search but use the phrase **information security**. Record the number of jobs found. Did you find more or less job postings? Why?

____

The number of jobs will be listed at the top right hand corner and will vary for every search. Different phrases will match to different job titles listed in the Indeed database. It is good practice to try different titles. Information security is a more common job title for individuals that work in the cybersecurity profession.

d. Repeat these steps using the phrase **network security** for the third search. Record the number of jobs found. Did you find more or less job postings? Why?

____

____

Different phrases will match to different job titles listed in the Indeed database. Network security is a subset of information security, therefore you should find less jobs. The point is that your search criteria can make a big difference in your results.

Step 2: Explore Cybersecurity Salaries.

a. Repeat the first job search by looking for all jobs in New York City, USA. Use the phrase **cyber securit**y. Pick three jobs that interest you. Record the experience required and salaries offered.

____

____

Answers will vary. Have students compare the salary levels versus experience level. In most cases, a direct correlation exists.

____

____

b. The Indeed website also advertises internships and part-time jobs. Use the **advanced job search** option to find all **IT Security** internship opportunities in New York City. How many did you find? List a few of the titles.

____

____

The answers will vary, but the student should find at least three job listings. Discuss the value of paid and unpaid internships.

c. Use the **advanced job search** option to find all **IT Security,** part-time opportunities in New York City. How many did you find? List a few of the titles.

____

____

The answers will vary but the student should find at least three part-time job listings. Discuss the value of part-time jobs.

Part 2: Cybersecurity Job Requirements

The cybersecurity field requires individuals with a high level of skill and knowledge. Many organizations require both academic and industry credentials to demonstrate the attainment of this knowledge and skill. Two very popular job search websites are CareerBuilder.com and USAJobs.gov. The websites list hundreds of cybersecurity related jobs.

Step 1: Explore Careerbuilder.

a. Open a browser and view the following video: CareerBuilder: Twenty Years, One Solution. (https://youtu.be/FVXCnqKVFKs)

b. Click here or go to http://www.careerbuilder.com to perform a job search at CareerBuilder.com. Start by looking for all jobs in San Francisco, California, USA. Use the phrase **network security** for the first search. Record the number of jobs found.

____

____

The number of jobs can be found on the second line with the **job search title** at the end of the sentence in parenthesis.

c. Select two jobs that list a salary. What is the salary range listed?

____

____

The answers will vary.

Have the students share their findings. Discuss the difference between starting salaries and a salary for an experienced cyber security professional.

d. Open the two jobs you used in the previous step. What credentials were required (academic degrees and certificates)? Did the organization require industry certifications? Please list the academic and industry credentials required.

____

____

Answers will vary.

Have the students share their findings. Discuss the different types of degrees and industry certifications.

Step 2: Explore USA Government Jobs.

a. The federal government has been the target of many high profile cyberattacks. As a result, many federal agencies need cybersecurity professionals. Click here or go to https://youtu.be/f3vRr3Lq-zI to view a video about USAjobs.gov. Click here or go to https://www.usajobs.gov to visit the USAJOBS website. Search **Information Security** as the Job Title. How many jobs did you find?

____

____

Answers can be found just below the “Keyword” search box.

b. Scroll through the first page of job listings. Count the number of federal agencies listings jobs on the first page.

____

____

Search the first page. The answers are located under Department and Agency.

c. List three of the salaries posted on the first page.

____

____

Search the first page. Have the students share their findings. Discuss the difference between the different federal agencies.

Lab - Explore Social Engineering Techniques (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Part 1: Explore Social Engineering Techniques

Part 2: Create a Cybersecurity Awareness Poster

Introduction

Cybersecurity is critical because it involves protecting unauthorized access to sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property (IP), and sensitive systems. Social engineering is a broad range of malicious activities accomplished by psychologically manipulating people into performing actions or divulging confidential information. In this lab, you will explore social engineering techniques, sometimes called human hacking, which is a broad category for different types of attacks.

Required Resources

- PC or mobile device with internet access

Background / Scenario

Recent research reveals the most common types of cyberattacks are becoming more sophisticated, and the attack targets are growing. The purpose of an attack is to steal information, disable systems or critical services, disrupt systems, activities, and operations. Some attacks are designed to destroy information or information systems, maliciously control a computing environment or its infrastructure, or destroy the integrity of data and/or information systems. One of the most effective ways an attacker can gain access to an organization’s network is through simple deception. In the cybersecurity world this is call social engineering.

Social Engineering Attacks

Social engineering attacks are very effective because people want to trust other people and social engineering attacks are not the kind of attack that the average user guards against; users are concerned with botnets, identity theft or ransomware. These are big external threats, so they do not think to question what seems to be a legitimate-looking message.

Baiting

Baiting relies on the curiosity or greed of the victim. What distinguishes baiting from other types of social engineering is the promise of an item or good that hackers use to entice victims. Baiters may offer users free music or movie downloads if the users surrender their login credentials to a certain site. Baiting attacks are not restricted to online schemes. Attackers can exploit human curiosity with physical media like USB drives.

Shoulder Surfing

Shoulder surfing is literally looking over someone's shoulder to get information. Shoulder surfing is an effective way to get information in crowded places because it is relatively easy to stand next to someone and watch as they fill out a form or enter a PIN number at an ATM machine. Shoulder surfing can also be done long distance with the aid of modern cell phones, binoculars, or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. There are even screen shields that make shoulder surfing much more difficult.

Pretexting

Pretexting is using deception to create a scenario to convince victims to divulge information they should not divulge. Pretexting is often used against organizations that retain client data, such as financial data, credit card numbers, utilities account numbers, and other sensitive information. Pretexters often request information from individuals in an organization by impersonating a supervisor, helpdesk clerk, or client, usually by phone, email, or text.

Phishing, spear phishing, and whaling attacks

In phishing attacks, the attackers try to obtain personal information or data, like username, password, and credit card details, by disguising themselves as trustworthy entities. Phishing is mainly conducted through emails and phone calls. Spear phishing is more targeted version of the phishing, in which an attacker chooses specific individuals or enterprises and then customizes their phishing attack to their victims to make it less conspicuous. Whaling is when the specific target is a high-profile employee such as a CEO or CFO.

Scareware and ransomware

Ransomware attacks involve injecting malware that encrypts a victim’s critical data. The cyber criminals request a ransom to be paid to decrypt the data. However, even if a ransom is paid, there is no guarantee the cyber criminals will decrypt the information. Ransomware is one of the fastest growing types of cyberattack and has affected thousands of financial organizations, government agencies, healthcare facilities, even schools and our education systems.

Scareware takes advantage of a user’s fear by coaxing them into installing fake antivirus software.

Tailgating

Tailgating tricks the victim into helping the attacker gain unauthorized access into the organization’s physical facilities. The attacker seeks entry into a restricted area where access is controlled by software-based electronic devices or human guards. Tailgating can also involve the attacker following an employee closely to pass through a locked door before the door locks behind the employee.

Dumpster diving

In the world of social engineering, dumpster diving is a technique used to retrieve discarded information thrown in the trash to carry out an attack on a person or organization. Dumpster diving is not limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes, it can also involve electronic information left on desktops, or stored on USB drives.

Instructions

Part 1: Explore Social Engineering Techniques

Step 1: Explore Baiting, Shoulder Surfing, and Pretexting.

The National Support Center for Systems Security and Information Assurance (CSSIA) hosts a **Social Engineering Interactive** activity. The current link to the site is https://www.cssia.org/social_engineering/. However, if the link changes, try searching for "CSSIA Social Engineering Interactive".

Click **Next** in the interactive activity, and then use the content to answer the following questions.

a. What is baiting? Did you click on the USB drive? What happened to the victim’s system?

Baiting is using a false promise to gain a victim’s interest to lure them into a trap that steals their personal information or infects their systems with malware. Yes – the system is compromised by malware.

b. What is Shoulder Surfing? What device was used to perform the shoulder surfing? What information was gained?

Shoulder surfing is looking over someone's shoulder while they are using a computer and visually capturing logins or passwords or other sensitive information. A Cell Phone. Login and Password information

c. What is Pretexting? What type of information did the cybercriminal request? Would you fall victim?

Pretexting is when an attacker establishes trust with their victim by impersonating persons who have right-to-know authority and asking questions that appear to be required to confirm the victim's identity, but through which they gather important personal data. Information requested name, work role, ???

Step 2: Explore Phishing/Spear Phishing and Whaling

Phishing is designed to get victims to click on links to malicious websites, open attachments that contain malware, or reveal sensitive information. Use the interactive activity to explore different phishing techniques.

a. In this phishing example, what is the ploy the attacker uses to trick the victim to visit the trap website? What is the trap website used to do?

The phishing scheme sends a fake notice that the victim has recently attempted to withdraw funds from their account while in another country: $174.99. The scheme is designed to steal the victim credentials including username and password.

b. What is the difference between phishing and spear phishing or whaling?

Spear phishing is more targeted version of the phishing, in which an attacker chooses specific individuals or enterprises and then customizes their phishing attack to their victims to make it less conspicuous. Whaling is when the specific target is a high-profile employee such as a CEO or CFO.

Step 3: Explore Scareware and Ransomware

Scareware is when victims are deceived into thinking that their system is infected with malware and receive false alarms prompting them to install software that is not needed or is itself malware. Ransomware is a type of malware that threatens to publish the victim's data or encrypts the victim's data preventing access or the ability to use the data. Victims are prevented from accessing their system or personal files until they make a ransom payment to regain access.

a. What data does the attacker claim to have in this example? Would you fall for this deception?

> Facebook Login

> Credit Card Details

> Email Account Login

No, now that you know what scareware is, you know better than to call an unknown number or share your account information.

b. What is the attacker requesting the victim do to get the data back?

Please call the attacker within the next 5 minutes to prevent your computer from being disabled.

Call: 44-8000-903-274

c. What is tailgating?

Tailgating is when an attacker who lacks the proper authorization follows a victim with authorized credentials through a door or other secure building access point into a restricted area.

d. Give three ways to prevent social engineering attacks?

Think before you act - Never share personal information over the phone, email, or on unsecure websites. Do not click on links, download files, or open email attachments from unknown senders.

Stay aware of your surroundings – Be skeptical of links to web forms that request personal information, even if the email appears to come from a legitimate source. Never click on or enter sensitive information into a pop-up.

Keep your accounts and devices safe - Use antivirus software, and spam filters, and update and patch your devices regularly.

Part 2: Create a Cybersecurity Awareness Poster

a. Use Powerpoint to create a poster that will make others aware of the different social engineering techniques used to gain unauthorized access to an organization or the organization’s data.

Pick from: Baiting, Shoulder Surfing, Pretexting, Phishing, Scareware, Ransomware, Tailgating or Dumpster Diving.

b. The poster should depict the techniques used and how users can avoid one of these social engineering attacks. Also include directions on where the poster should be placed within the organization.

Dear Customer,
VERIFY ACCOUNT
Would you take the bait?

Lab - Exploring the World of Cybersecurity Professionals (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Explore the security features used by organizations like Google and Cisco to keep your data safe.

Part 1: Protecting Your Data

Part 2: Improving your Google Account Security

Background / Scenario

This chapter introduces the student to the cyber world. This cyber world is full of data domains that handle unimaginable amounts of personal and organizational information. As cybersecurity professionals, it is important to understand the types of cybersecurity safeguards an organization must implement in order to protect the data they store, manage, and protect. In this lab, you will explore one of the world's largest data handling organizations, Google. You will watch two videos and then answer a series of questions. Each video presents a different aspect of cybersecurity defense at Google. Upon completion, you will have a better understanding of the security measures and services that organizations like Google take in order to protect information and information systems.

Videos:

How Google Protects Your Data

Security Key

Required Resources

- PC or mobile device with Internet access

Part 1: Protecting Your Data

As one of the world's largest personal data repositories, Google stores massive amounts of data. Google accounts for close to 50% of all internet search activity. To make things even more complicated, Google owns and operates YouTube, the Android operating system, and many other major sources of data collection. In this activity, you will watch a short video and try to identify several of the measures the cybersecurity professionals at Google take to protect your data.

Step 1: Open a browser and view the following video: How Google Protects Your Data

a. How does Google ensure that the servers they install in their datacenters are not infected with malware by the equipment manufacturers?

____

____

The engineers and cyber professionals purchase, test, and build each server in-house and install their own operating system on each one.

b. How does Google protect against physical access to the servers located in the Google datacenters?

____

____

Access to a Google datacenter is tightly controlled. Only authorized personal are allowed to enter. The security staff works 24 hours a day, seven days a week. The centers are guarded by security personnel and 24-hour video monitoring. All personnel must check in at the reception area. The team at Google does not allow outside visitors at its datacenter facilities.

c. How does Google protect customer data on a server system?

____

____

All data on Google systems are encrypted and stored in multiple locations. Google also uses data randomizing to make it more difficult to locate data. All hard drives are monitored and tested regularly. If a drive indicates signs of potential failure, it is swapped out before it fails. All retired drives are physically destroyed.

Step 2: Identify data vulnerabilities.

a. As you can see by the video, data in the Google datacenters are well protected, however, when using Google, not all your data is located in the Google datacenter. Where else can you find your data when using the Google search engine?

____

____

Data still resides at your local machine (computer, laptop, tablet or smart phone). This data must also be protected.

b. Can you take steps to protect data when using the Google search engine? What are a few measures you can use to protect your data?

____

____

Use strong passwords and/or a two-step login. You can also clear your browser history or cookies frequently. You can require device authentication to access your account.

Part 2: Improving your Google Account Security

The greatest threat when using web-based services like Google is protecting your personal account information (username and password). To make things worse, these accounts are commonly shared and used to authenticate you to other web-based services, like Facebook, Amazon, or LinkedIn. You have several options to improve the handling of your Google login credentials. These measures include creating a two-step verification or an access code with your username and password. Google also supports the use of security keys. In this activity, you will watch a short video and try to identify measures that can be taken to protect your credentials when using web-based accounts.

Step 1: Open a browser and view the following video: The Key to Working Smarter, Faster, and Safer

a. What is two-step verification? How can it protect your Google account?

____

____

Two-step verification is an enhancement to normal Google account login. Users can create a special ID number that is provided during login.

b. What is a security key and what does it do? Can you use the security key on multiple systems?

____

____

A security key log is registered to your Google account, not a particular computer. You can use your Security Key on any computer with Google Chrome.

c. Click here for common questions about the Security Key. If you set up your account to use a security key, can you still get in without having the physical key?

____

____

Yes. If you are asked for a Security Key and do not have it available, you will always have the option to use a verification code. Simply click the link at the bottom of the screen that says **use verification code instead**.

Step 2: Protect Gmail Account Access.

a. The use of a Gmail account has become extremely popular. Google now has over 1 billion active Gmail accounts. One of the convenient features of Gmail accounts is the ability to grant access to other users. This share access feature creates a shared email account. Hackers can use this feature to access your Gmail account. To check your account, log in to your Gmail account, and click the gear icon in the top right corner (settings). When the settings screen opens, a menu bar is displayed under the Settings screen title. (General – Labels – Inbox – Accounts and Import – Filters and Blocked Addresses …)

b. Click the **Accounts and Import** menu item. Check the **Grant access to your account** option. Delete any unauthorized shared users of your account.

Step 3: Check Your Gmail Account Activity.

a. Gmail users can also check the account activity in order to make sure no other users have accessed their personal Gmail account. This feature can identify who has accessed the account and from what locations. Use the **Last account activity** option to determine if someone else has accessed your account. To access the **Last account activity** follow these steps:

1) Login to your Gmail account.

2) Select **Last account activity:** found at the bottom of the page. It will display the last time the unauthorized user accessed the account and from where.

3) Just below this message is a detail hyperlink. Click the detail hyperlink.

b. View the account activity. If you find an unauthorized user, you can disconnect the unauthorized user by clicking the button at the top left **Sign out all other web sessions**. Now change your password to keep the unauthorized user from accessing the account.

Lab – The Cybersecurity Cube Scatter Quizlet (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Identify the three dimensions of the Cybersecurity Cube and the elements of each dimension.

Required Resources

- PC or mobile device with Internet access

Background / Scenario

The Cybersecurity Cube, also called the McCumber Cube, was developed by John McCumber in 1992. It is a framework or model used to establish and evaluate information and information systems security. The framework relies on the cybersecurity professional to identify information assets with a focus on the core principles of cybersecurity; confidentiality, integrity, and availability. The model is based on three dimensions, each having three elements.

Dimension One: **Cybersecurity Principles CIA**

- **Confidentiality:** assurance that sensitive information is not intentionally or accidentally disclosed to unauthorized individuals
- **Integrity:** assurance that information is not intentionally or accidentally modified in such a way as to call into question its trustworthiness or reliability
- **Availability:** ensuring that authorized individuals have both timely and reliable access to information and information systems

Dimension Two: **Information (data) States**

- **Storage:** data at rest (stored in memory, on a drive, or USB flash drive)
- **Transmission:** transferring data between systems
- **Processing:** performing operations on data like modification, backup, corrections

Dimension Three: **Security Countermeasures or Safeguards**

- **Policy and practices:** administrative controls, such as information security policies, procedures, guidelines, and management directives
- **Human factors:** ensuring that the users of information systems are aware of their roles and responsibilities. Requires awareness and education programs.
- **Technology:** software- and hardware-based solutions designed to protect information systems, like anti-virus, firewalls, and IDS/IPS systems.

Quizlet Review

Click on the Quizlet website and review the Cybersecurity Essentials - Cybersecurity Cube. You do not need to create an account on the site.

a. Review the list of terms and definitions.

b. Select the Flashcards icon. Test your knowledge by going through all ten flashcards.

c. Click the Scatter option in the menu. When prompted, click to start the game.

d. Drag each term to its definition.

Lab – Install a Virtual Machine on a Personal Computer (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Part 1: Prepare a Computer for Virtualization

Part 2: Import a Virtual Machine into VirtualBox Inventory

Background / Scenario

Computing power and resources have increased tremendously over the last 10 years. A benefit of having multicore processors and large amounts of RAM is the ability to use virtualization. With virtualization, one or more virtual computers can operate inside a single physical computer. Virtual computers that run within physical computers are called virtual machines. Virtual machines are often called guests, and physical computers are often called hosts. Anyone with a modern computer and operating system can run virtual machines.

A virtual machine image file has been created for you to install on your computer. In this lab, you will download and import this image file using a desktop virtualization application, such as VirtualBox.

Required Resources

- Computer with a minimum of 2 GB of RAM and 8 GB of free disk space
- High speed Internet access to download Oracle VirtualBox and the virtual machine image file

Note: The image file is about 2.5 GB, and can grow up to 5 GB after the virtual machine is in operation. While you can delete the image file after the virtual machine is imported, the 8 GB free disk space requirement is for users who decide to keep the image file.

Note: To install and run 64bit virtual machines on a host physical computer, the computer needs to be a 64bit system and have hardware virtualization technology enabled in BIOS. If you are unable to install the virtual machine image you may need to reboot your computer and enter setup mode in BIOS to enable hardware virtualization technology under advanced system settings.

Part 1: Prepare a Host Computer for Virtualization

In Part 1, you will download and install desktop virtualization software, and also download an image file that can be used to complete labs throughout the course. For this lab, the virtual machine is running Linux.

Step 1: Download and install VirtualBox

VMware Workstation Player and Oracle VirtualBox are two virtualization programs that you can download and install to support the image file. In this lab, you will use VirtualBox.

a. Navigate to http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html.

b. Choose and download the appropriate installation file based on your operating system.

c. When you have downloaded the VirtualBox installation file, run the installer and accept the default installation settings.

Step 2: Download the Virtual Machine image file

The image file was created in accordance with the Open Virtualization Format (OVF). OVF is an open standard for packaging and distributing virtual appliances. An OVF package has several files placed into one directory. This directory is then distributed as an OVA package. This package contains all of the OVF files necessary for the deployment of the virtual machine. The virtual machine used in this lab was exported in accordance with the OVF standard.

Click here to download the virtual machine image file.

Note: This file is 2.5 GB in size, and it may take over an hour to download, depending on the speed of your Internet connection.

Part 2: Import the Virtual Machine into the VirtualBox Inventory

In Part 2, you will import the virtual machine image into VirtualBox and start the virtual machine.

Step 1: Import the virtual machine file into VirtualBox

a. Open **VirtualBox**. Click **File > Import Appliance...** to import the virtual machine image.

b. A new window will appear. Specify the location of the .OVA file.

c. The appliance settings appear. Check the **Reinitialize the MAC address of all network cards** box at bottom of the window. Leave all other settings as default. Click **Import**.

d. When the import process is complete, you will see the new Virtual Machine added to the VirtualBox inventory in the left panel. The virtual machine is now ready to use.

Step 2: Start the virtual machine and log in

a. In the inventory shown on the left, select the virtual machine you wish to use.

b. Click the **Start** button. It is the green arrow located at the top portion of the VirtualBox application window. A new window will appear, and the virtual machine boot process will start.

   Note: If the virtual machine fails to start, either disable the USB Controller by going into the virtual machine's settings and unchecking the USB controller setting under USB or go to the VirtualBox download webpage and download and install the Oracle VM VirtualBox Extension Pack.

c. When the boot process is complete, the virtual machine will ask for a username and password. Use the following credentials to log into the virtual machine:

   Username: cisco

   Password: password

   You will be presented with a desktop environment: there is a launcher bar at the bottom, icons on the desktop, and an application menu at the top.

Note: The window running the virtual machine is a completely different computer than your host. Functions such as copy and paste will not work between the two without special software tools installed. Notice the keyboard and mouse focus. When you click inside the virtual machine window, your mouse and keyboard will operate the guest operating system. Your host operating system will no longer detect keystrokes or mouse movements. Press the right **CTRL** key to return keyboard and mouse focus to the host operating system.

Step 3: Familiarize yourself with the Virtual Machine

Use the Ubuntu_CyberEss virtual machine you just installed to complete the labs that require Ubuntu in this course. Familiarize yourself with the icons in the list below:

The launcher icons are on the left (from top to bottom):

- Search Tool
- File manager application
- Firefox Web Browser

- LibreOffice Writer, LibreOffice Calc, LibreOffice Impress
- Ubuntu Software Center
- Amazon
- System Settings
- Terminal
- Trash

a. Open the terminal application. Type the command **ip address** at the prompt to determine the IP address of your virtual machine.

What are the IP addresses assigned to your virtual machine?

____

Answer will vary. The loopback interface is assigned 127.0.0.1/8, and the Ethernet interface is assigned an IP address in the 10.0.2.15/24 network.

b. Locate and launch the web browser application. Can you navigate to your favorite search engine? _____ Yes

c. Press the right ctrl key to release the cursor from the virtual machine. Now go to the menu at the top of the virtual machine window and choose **File** > **Close** to close the virtual machine. What options are available?

____

____

Save the machine state, Send the shutdown signal and power off the machine

d. Click the **Save the machine state** radio button and click **OK**. The next time you start the virtual machine, you will be able to resume working in the operating system in its current state.

Reflection

What are the advantages and disadvantages of using a virtual machine?

____

____

____

____

With a virtual machine, you are able to test new applications or operating systems without affecting your host machine. You are also able to save the current machine state when you close virtual machine. If you have any issues, you have the option to revert the virtual machine to a previously saved state. On the other hand, a virtual machine requires hardware resources from the host machine, such as hard drive space, RAM, and processing power.

Lab – Authentication, Authorization, and Accounting (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

- Given a scenario, select the appropriate authentication, authorization, or access control
- Install and configure security controls when performing account management, based on best practices

Part 1: Adding Groups, Users, and Passwords on a Linux System

Part 2: Verify Users, Groups, and Passwords

Part 3: Using Symbolic Permissions

Part 4: Absolute Permissions

Background / Scenario

You will be conducting host security practices using the Linux command line by performing the following tasks:

- Adding Groups, Users, and Passwords
- Verifying Groups, Users, and Passwords
- Setting Symbolic Permissions
- Setting Absolute Permissions

Required Resources

- PC with Ubuntu 16.0.4 LTS installed in a virtual machine - you can use the VM from labs completed in chapter 2.

Part 1: Adding Groups, Users, and Passwords on a Linux System

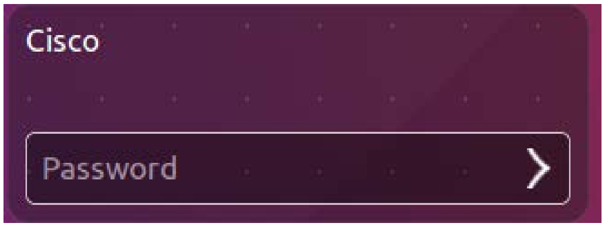
In this part, you will add users, groups, and passwords to the local host machine.

Step 1: Open a terminal window in Ubuntu.

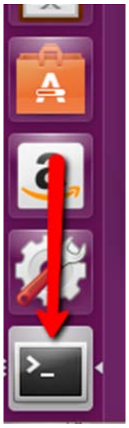
a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**

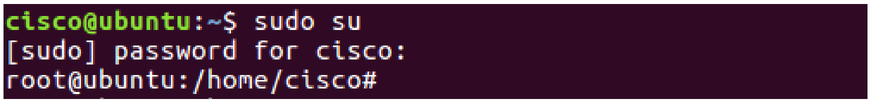


b. Click on the **terminal** icon to open a terminal.



Step 2: Escalate privileges to the root level by entering the sudo su command. Enter the password password when prompted.

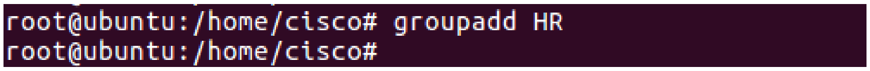
```
cisco@ubuntu:~$ sudo su
```



```
cisco@ubuntu:~$ sudo su
[sudo] password for cisco:
root@ubuntu:/home/cisco#
```

Step 3: Add a new group named HR by entering the command groupadd HR.

```
root@ubuntu:/home/cisco# groupadd HR
```

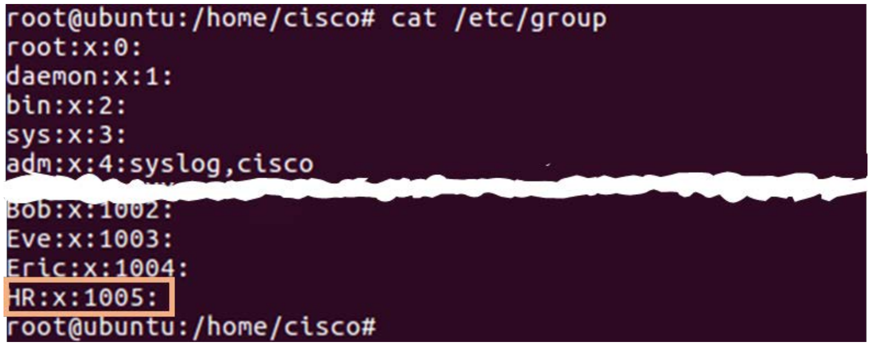


```
root@ubuntu:/home/cisco# groupadd HR
root@ubuntu:/home/cisco#
```

Part 2: Verify Users, Groups, and Passwords

Step 1: Verify the new group has been added to the group file list by entering cat /etc/group.

```
root@ubuntu:/home/cisco# cat /etc/group
```



```
root@ubuntu:/home/cisco# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,cisco
Bob:x:1002:
Eve:x:1003:
Eric:x:1004:
HR:x:1005:
root@ubuntu:/home/cisco#
```

The new group HR will be added to the bottom of the /etc/group file with a group ID of 1005.

Step 2: Add a new user named jenny.

```
root@ubuntu:/home/cisco# adduser jenny
```

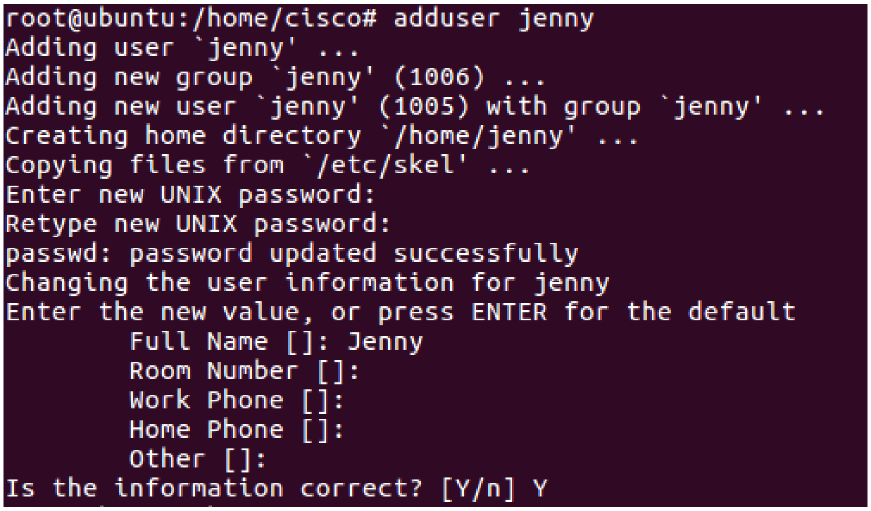
a. When prompted for a new password, type **lasocial**. Press **Enter**.

b. When prompted again, type **lasocial**. Press **Enter**.

c. When prompted for a full name, type **Jenny**. Press **Enter**.

d. For the rest of the configurations, press **Enter** until when asked is the information correct.

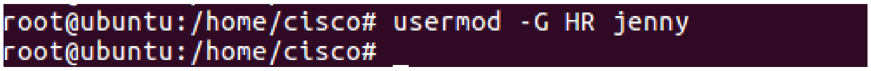
e. Type **Y** for yes and press **Enter**.



```
root@ubuntu:/home/cisco# adduser jenny
Adding user `jenny' ...
Adding new group `jenny' (1006) ...
Adding new user `jenny' (1005) with group `jenny' ...
Creating home directory `/home/jenny' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for jenny
Enter the new value, or press ENTER for the default
        Full Name []: Jenny
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

Step 3: Place the user jenny in the HR group.

```
root@ubuntu:/home/cisco# usermod –G HR jenny
```



```
root@ubuntu:/home/cisco# usermod -G HR jenny
root@ubuntu:/home/cisco# _
```

Step 4: Add another new user named joe.

```
root@ubuntu:/home/cisco# adduser joe
```

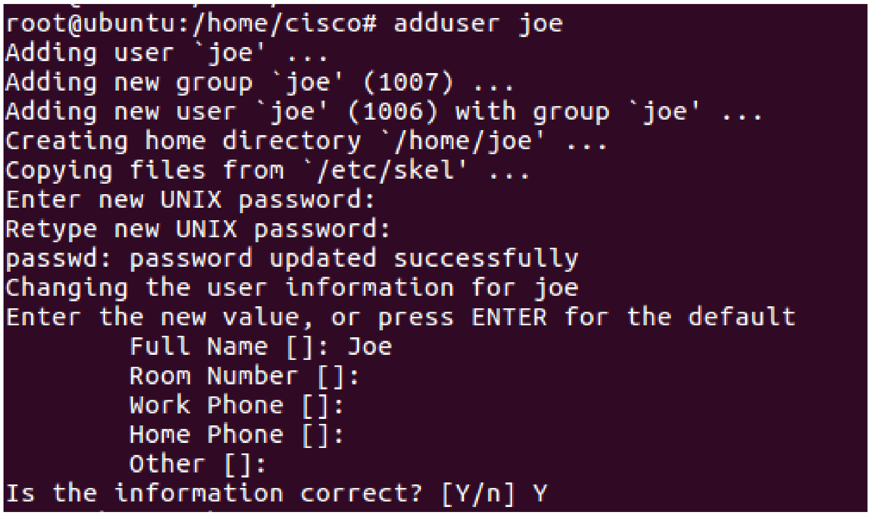
a. When prompted for a new password, type **tooth**. Press **Enter**.

b. When prompted again, type **tooth**. Press **Enter**.

c. When prompted for a full name, type **Joe**. Press **Enter**.

d. For the rest of the configurations, press **Enter** until when asked is the information correct.

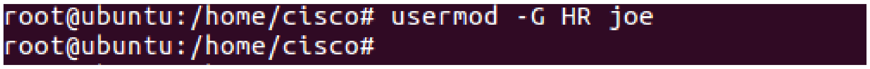
e. Type **Y** for yes and press **Enter**.



```
root@ubuntu:/home/cisco# adduser joe
Adding user `joe' ...
Adding new group `joe' (1007) ...
Adding new user `joe' (1006) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for joe
Enter the new value, or press ENTER for the default
        Full Name []: Joe
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

f. Place the user joe in the HR group.

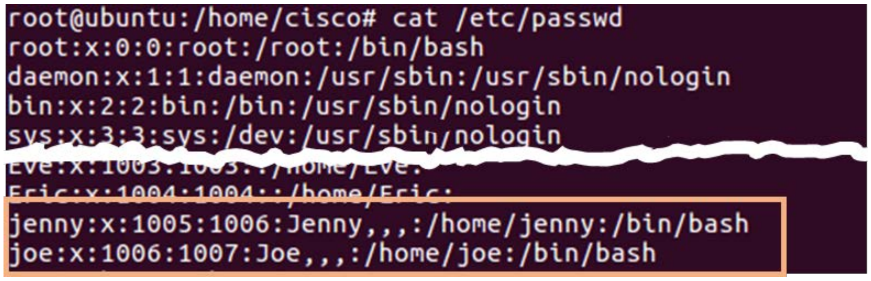
```
root@ubuntu:/home/cisco# usermod –G HR joe
```



```
root@ubuntu:/home/cisco# usermod -G HR joe
root@ubuntu:/home/cisco#
```

Step 5: Verify the newly created users in the passwd file.

```
root@ubuntu:/home/cisco# cat /etc/passwd
```



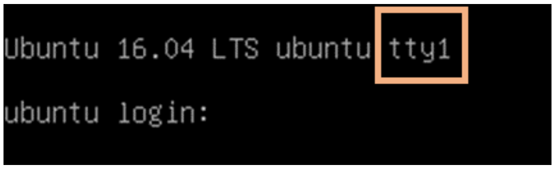
```
root@ubuntu:/home/cisco# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
Eve:x:1003:1003::/home/Eve:
Eric:x:1004:1004::/home/Eric:
jenny:x:1005:1006:Jenny,,,:/home/jenny:/bin/bash
joe:x:1006:1007:Joe,,,:/home/joe:/bin/bash
```

Step 6: View the created users in the shadow file.

```
root@ubuntu:/home/cisco# cat /etc/shadow
```

Part 3: Using Symbolic Permissions

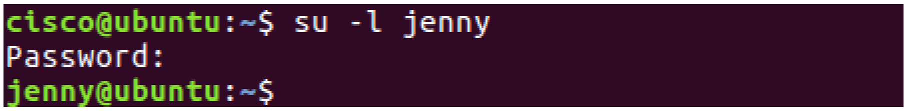
Step 1: While on the Ubuntu system, press and hold the keys CTRL+ALT+F1 until the screen changes to the tty1 Terminal.



```
Ubuntu 16.04 LTS ubuntu tty1

ubuntu login:
```

Note: If you are unable to use tty1 terminal, return to graphical user interface (GUI) of the host by using **CTRL+ALT+F7** and open a terminal window in the GUI Ubuntu OS. At the prompt, enter **su –l jenny** at the prompt and enter the password **lasocial**. Proceed to Step 4.

```
cisco@ubuntu:~$ su –l jenny
```



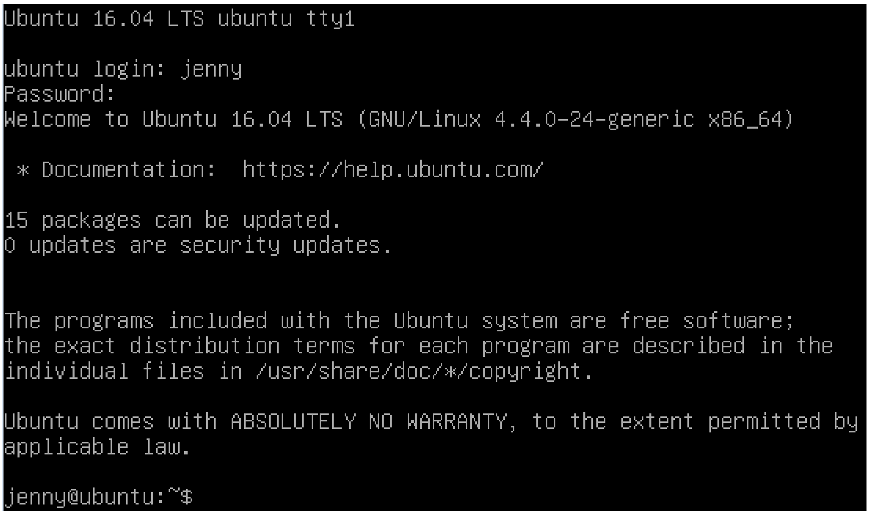
```
cisco@ubuntu:~$ su -l jenny
Password:
jenny@ubuntu:~$
```

Note: If CTRL+ALT+F7 did not work, try CTRL+ALT+F8.

Step 2: Once on the Terminal login screen, type jenny and press Enter.

Step 3: When prompted for the password, type lasocial and press Enter.

Step 4: After a successful login, you will see the *jenny@ubuntu:~$* prompt.

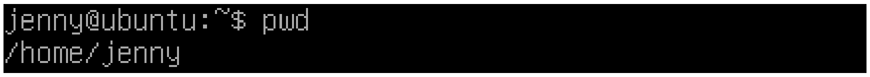


```
Ubuntu 16.04 LTS ubuntu tty1

ubuntu login: jenny
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

15 packages can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jenny@ubuntu:~$
```

Since we are not logged in as the *root* (superuser), we are presented with the dollar sign instead of the # if we were to be logged in as the user root.

Step 5: View your present directory.

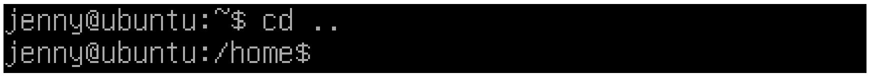
```
jenny@ubuntu:~$ pwd
```



```
jenny@ubuntu:~$ pwd
/home/jenny
```

Step 6: Go back one directory level to the /home directory.

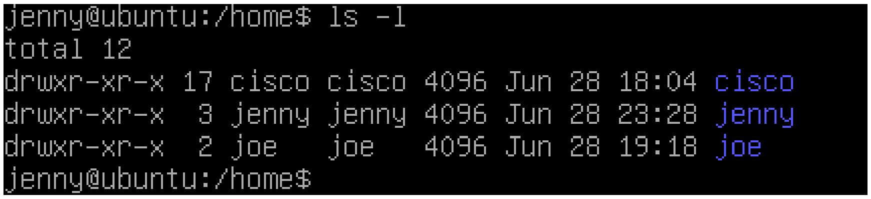
```
jenny@ubuntu:~$ cd ..
```



```
jenny@ubuntu:~$ cd ..
jenny@ubuntu:/home$
```

Step 7: List all directories and their permissions.

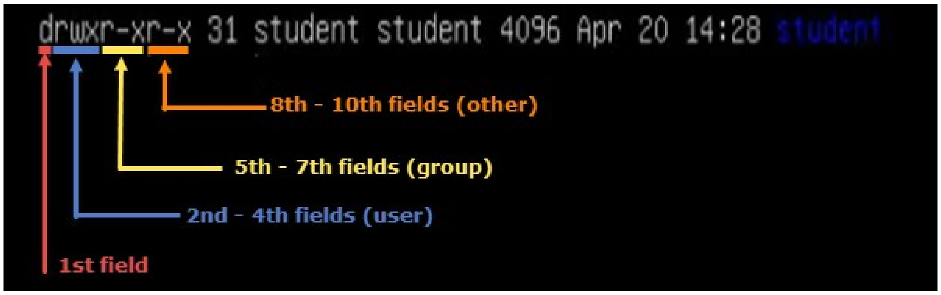
```
jenny@ubuntu:/home$ ls -l
```



```
jenny@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:28 jenny
drwxr-xr-x  2 joe   joe   4096 Jun 28 19:18 joe
jenny@ubuntu:/home$
```

The Linux operating system has a total of 10 letters or dashes in the permissions fields:

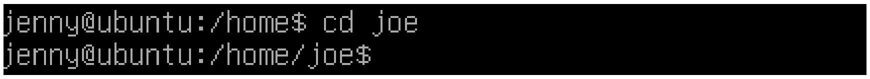
- The first field is a dash for a file an a d for a directory
- The 2nd through 4th fields are for the user
- The 5th through 7th fields are for the group
- The 8th through 10th fields are for others (accounts other than those in the group)



```
drwxr-xr-x 31 student student 4096 Apr 20 14:28 student
```

Step 8: Enter Joe's folder as Jenny by typing the command cd joe.

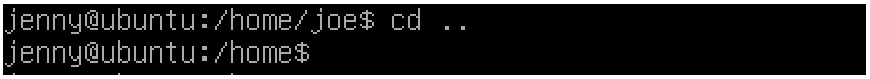
```
jenny@ubuntu:/home$ cd joe
```



```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$
```

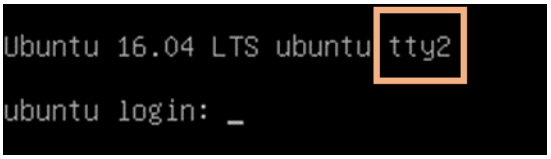
Notice that we are able to go into *Joe's home folder*.

```
jenny@ubuntu:/home/joe$ cd ..
```



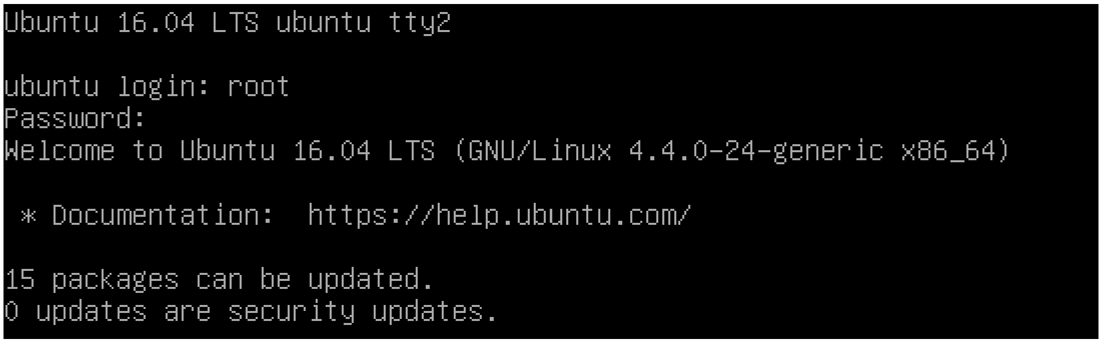
```
jenny@ubuntu:/home/joe$ cd ..
jenny@ubuntu:/home$
```

Step 9: Press and hold CTRL+ALT+F2 to switch to another Terminal session (tty2).



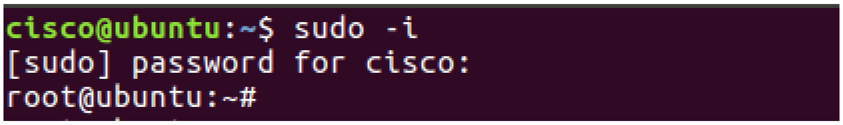
```
Ubuntu 16.04 LTS ubuntu tty2

ubuntu login: _
```

Step 10: Login as the user root with the password secretpassword.



```
Ubuntu 16.04 LTS ubuntu tty2

ubuntu login: root
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

15 packages can be updated.
0 updates are security updates.
```

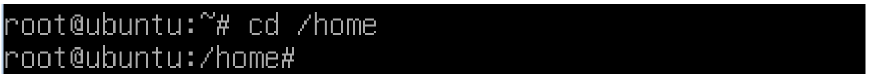
Note: If you are unable to use tty2 terminal, return to graphical user interface (GUI) of the host by using **CTRL+ALT+F7** and open a terminal window in the GUI Ubuntu OS. At the prompt, enter **sudo -i** at the prompt and enter the password **password**.



```
cisco@ubuntu:~$ sudo -i
[sudo] password for cisco:
root@ubuntu:~#
```

Step 11: Change to the /home directory.

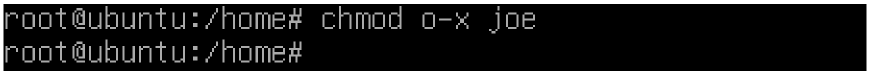
```
root@ubuntu:~# cd /home
```



```
root@ubuntu:~# cd /home
root@ubuntu:/home#
```

Step 12: Change the “other” permission on joe’s folder by making it non-executable.

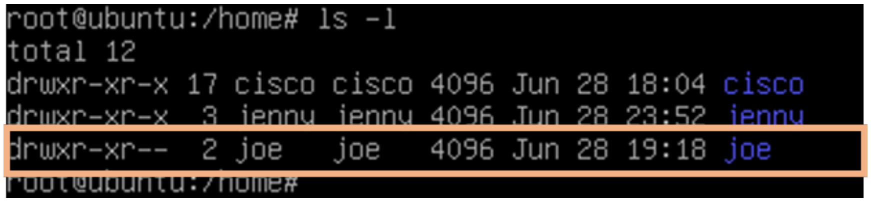
```
root@ubuntu:/home# chmod o-x joe
```



```
root@ubuntu:/home# chmod o-x joe
root@ubuntu:/home#
```

Step 13: List the directories once more with their respective permissions.

```
root@ubuntu:/home# ls -l
```



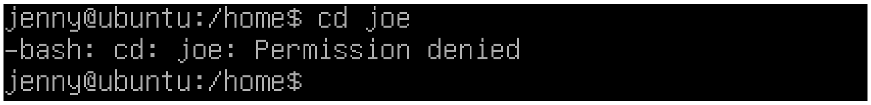
```
root@ubuntu:/home# ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwxr-xr--  2 joe   joe   4096 Jun 28 19:18 joe
root@ubuntu:/home#
```

Notice now that there are two dashes in the “others” field for joe’s folder.

Step 14: Press and hold CTRL+ALT+F1 to switch back to the other Terminal session (tty1). Make sure you are viewing the following command prompt: jenny@ubuntu:/home$.

Step 15: Attempt to go into Joe's folder once more.

```
jenny@ubuntu:/home$ cd joe
```



```
jenny@ubuntu:/home$ cd joe
-bash: cd: joe: Permission denied
jenny@ubuntu:/home$
```

Notice that we do not have the permissions to do so.

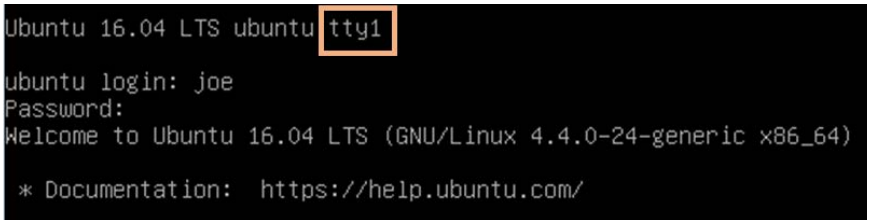
The chart below shows examples of other ways the **chmod** command can be used:

chmod command	Results
chmod u+rwx	Adds read, write, and execute permissions for the user
chmod u+rw	Adds read and write permission for the user
chmod o+r	Adds read permission for others
chmod g-rwx	Removes read, write, and execute permissions for the group

Step 16: Type exit followed by pressing Enter to logout of the Terminal session.

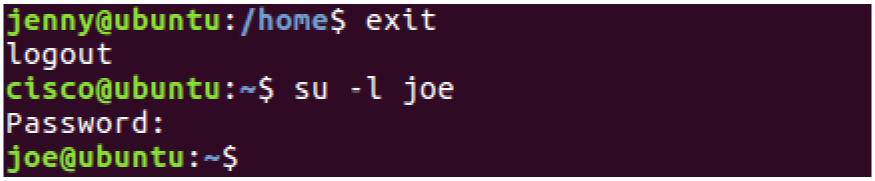
Part 4: Absolute Permissions

Step 1: Login as the user joe with the password tooth while on tty1.



```
Ubuntu 16.04 LTS ubuntu tty1

ubuntu login: joe
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
```

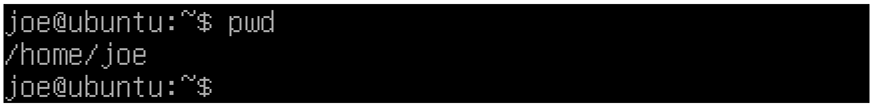
Note: If you are unable to use tty1 terminal, return to graphical user interface (GUI) of the host by using **CTRL+ALT+F7** and open a terminal window in the GUI Ubuntu OS. At the prompt, enter **sudo –l joe** at the prompt and enter the password **tooth**.



```
jenny@ubuntu:/home$ exit
logout
cisco@ubuntu:~$ su -l joe
Password:
joe@ubuntu:~$
```

Step 2: Print your current working directory.

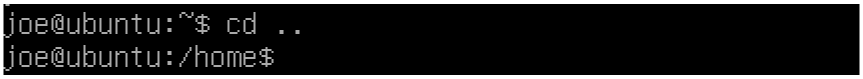
```
joe@ubuntu:~$ pwd
```



```
joe@ubuntu:~$ pwd
/home/joe
joe@ubuntu:~$
```

Step 3: Go back one directory level to the /home directory.

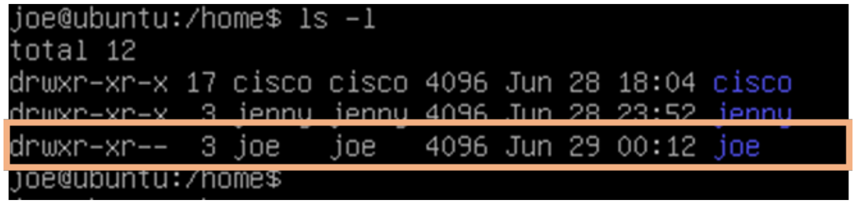
```
joe@ubuntu:~$ cd ..
```



```
joe@ubuntu:~$ cd ..
joe@ubuntu:/home$
```

Step 4: List all directories and their permissions in the current working directory.

```
joe@ubuntu:/home~$ ls -l
```



```
joe@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwxr-xr--  3 joe   joe   4096 Jun 29 00:12 joe
joe@ubuntu:/home$
```

Notice that Joe’s folder is set so that “others” are not able to access the folder.

The other way of assigning permissions besides using symbolic permissions is the use of absolute permissions. Absolute permissions use a three digit octal number to represent the permissions for owner, group and other.

The table below outlines each absolute value and its corresponding permissions:

Number	Permissions
7	Read, Write, and Execute
6	Read and Write
5	Read and Execute
4	Read
3	Write and Execute
2	Write
1	Execute
0	None

By typing the command **chmod 764 *examplefile***, the examplefile will be assigned the follow permissions:

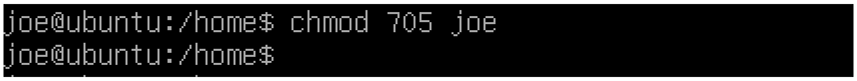
- The user will get read, write and execute permissions
- The group will get read and write permissions
- Others will get read access

Breakdown of how 764 represents these permissions:

Digit	Binary Equivalent	Permission
7 (user)	111	1-Read 1-Write 1-Execute
6 (group)	110	1-Read 1-Write 0-No Execute
4 (others)	100	1-Read 0-No Write 0-No Execute

Step 5: Modify the "others" field for Joe's folder so that others will be able read and execute but not write while still maintaining the "user" field to read, write, and execute.

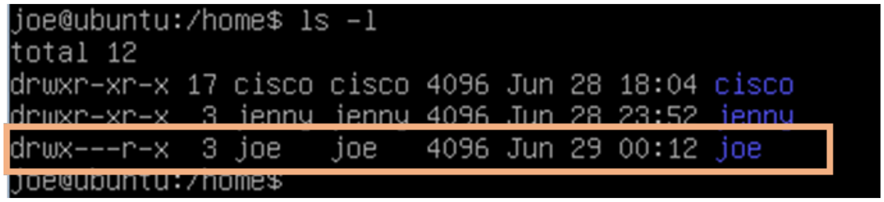
```
joe@ubuntu:/home$ chmod 705 joe
```



```
joe@ubuntu:/home$ chmod 705 joe
joe@ubuntu:/home$
```

Step 6: List the file permissions of the current directory to see that the absolute changes were made.

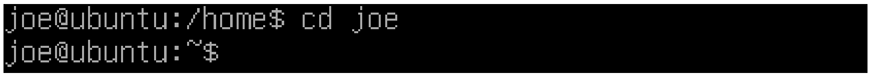
```
joe@ubuntu:/home$ ls -l
```



```
joe@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwx---r-x  3 joe   joe   4096 Jun 29 00:12 joe
joe@ubuntu:/home$
```

Step 7: Change to the */home/joe* directory.

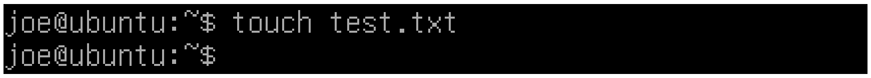
```
joe@ubuntu:/home$ cd joe
```



```
joe@ubuntu:/home$ cd joe
joe@ubuntu:~$
```

Step 8: Create a simple text file named test.txt using *touch*.

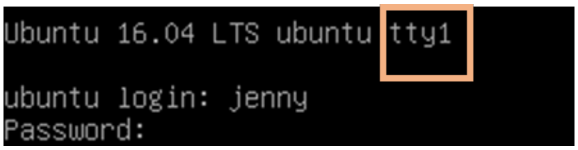
```
joe@ubuntu:~$ touch test.txt
```



```
joe@ubuntu:~$ touch test.txt
joe@ubuntu:~$
```

a. Type **exit** followed by pressing **Enter** to log out of Joe's session.

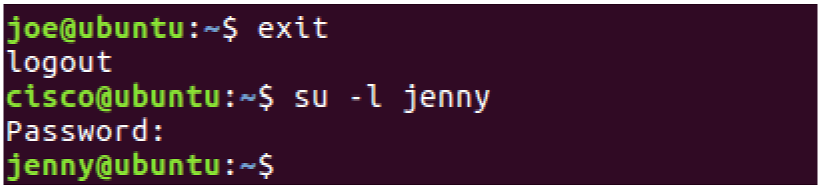
b. While on the tty1 Terminal, log back in as **jenny** and enter the password **lasocial**. Press **Enter**.



```
Ubuntu 16.04 LTS ubuntu tty1

ubuntu login: jenny
Password:
```

Note: If you are unable to use tty1 terminal, return to graphical user interface (GUI) of the host by using **CTRL+ALT+F7** and open a terminal window in the GUI Ubuntu OS. At the prompt, enter **su –l jenny** at the prompt and enter the password **lasocial**.

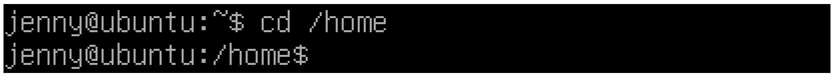
```
cisco@ubuntu:~$ su –l jenny
```



```
joe@ubuntu:~$ exit
logout
cisco@ubuntu:~$ su -l jenny
Password:
jenny@ubuntu:~$
```

Step 9: Change to the /home directory.

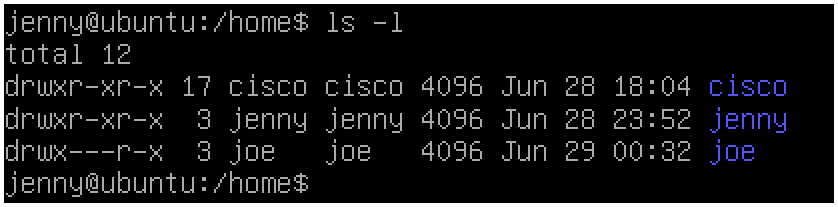
```
jenny@ubuntu:~$ cd /home
```



```
jenny@ubuntu:~$ cd /home
jenny@ubuntu:/home$
```

Step 10: List all directories with their respective permissions.

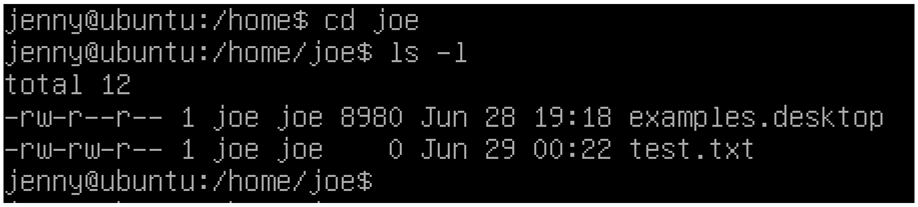
```
jenny@ubuntu:/home$ ls -l
```



```
jenny@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwx---r-x  3 joe   joe   4096 Jun 29 00:32 joe
jenny@ubuntu:/home$
```

Step 11: Change to the /home/joe directory and list the content of the directory.

```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$ ls -l
```

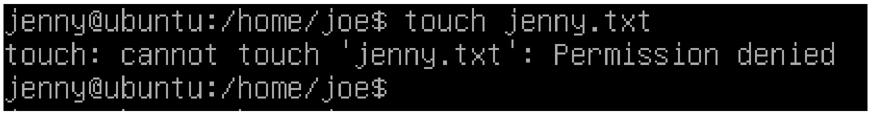


```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$ ls -l
total 12
-rw-r--r-- 1 joe joe 8980 Jun 28 19:18 examples.desktop
-rw-rw-r-- 1 joe joe    0 Jun 29 00:22 test.txt
jenny@ubuntu:/home/joe$
```

Notice that we are able to enter Joe’s folder and read the files within the directory. We are able to see the *test.txt* file.

Step 12: Attempt to create a file.

```
jenny@ubuntu:/home/joe$ touch jenny.txt
```



```
jenny@ubuntu:/home/joe$ touch jenny.txt
touch: cannot touch 'jenny.txt': Permission denied
jenny@ubuntu:/home/joe$
```

Notice we do not have permission to create the file.

Step 13: Close all remaining windows.

Lab – Detecting Threats and Vulnerabilities (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Use Nmap, a port scanner and network mapping tool to detect threats and vulnerabilities on a system.

Background / Scenario

Network Mapper, or Nmap, is an open source utility used for network discovery and security auditing. Administrators also use Nmap for monitoring hosts or managing service upgrade schedules. Nmap determines what hosts are available on a network, what services are running, what operating systems are running, and what packet filters or firewalls are running.

Required Resources

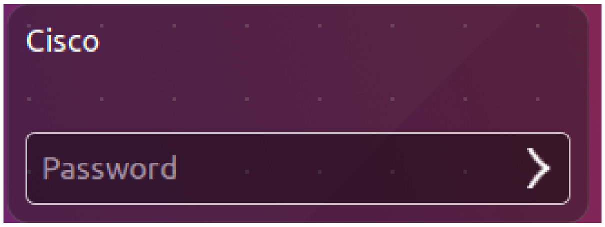
- PC with Ubuntu 16.0.4 LTS installed in a virtual machine - you can use the VM from labs completed in chapter 2.

Step 1: Open a terminal window in Ubuntu.

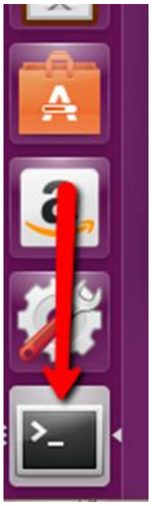
a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**



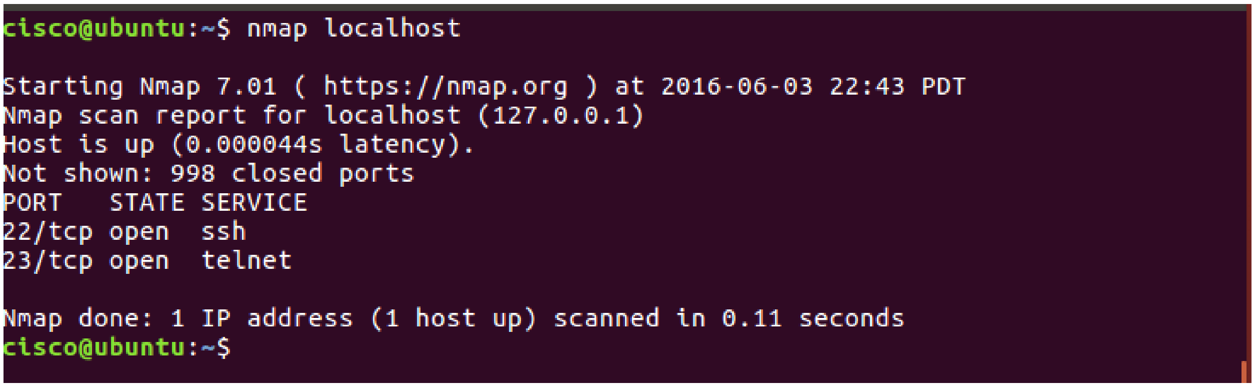
b. Click on the **terminal** icon to open a terminal.



Step 2: Run Nmap.

At the command prompt, enter the following command to run a basic scan against this Ubuntu system:

```
cisco@ubuntu:~$ nmap localhost
```



```
cisco@ubuntu:~$ nmap localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:43 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
cisco@ubuntu:~$
```

The results are a scan of the first 1024 TCP ports.

What TCP ports are open?

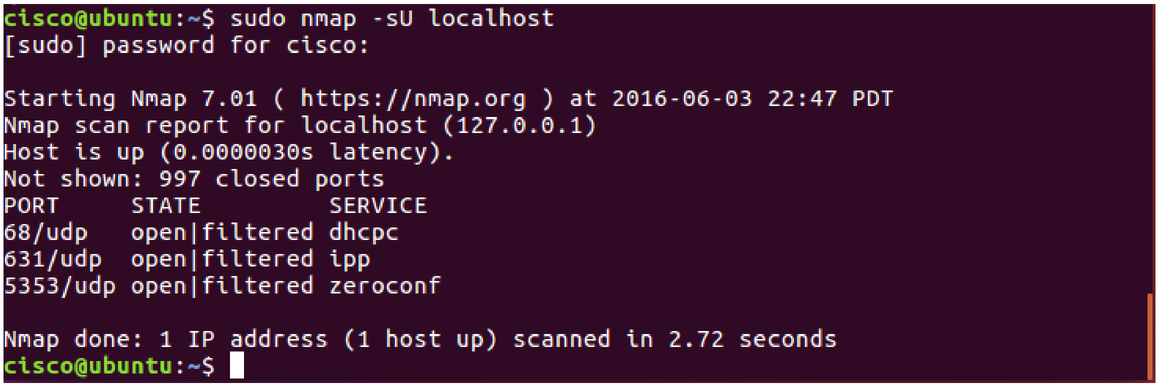
____

Ports 22, 23, and 631

Step 3: Use administrative privileges with Nmap.

a. Type the following command in the terminal to scan the computer's UDP ports (remember, Ubuntu is case sensitive) and enter the password **password** when prompted:

```
cisco@ubuntu:~$ sudo nmap –sU localhost
```



```
cisco@ubuntu:~$ sudo nmap -sU localhost
[sudo] password for cisco:

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:47 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
cisco@ubuntu:~$
```

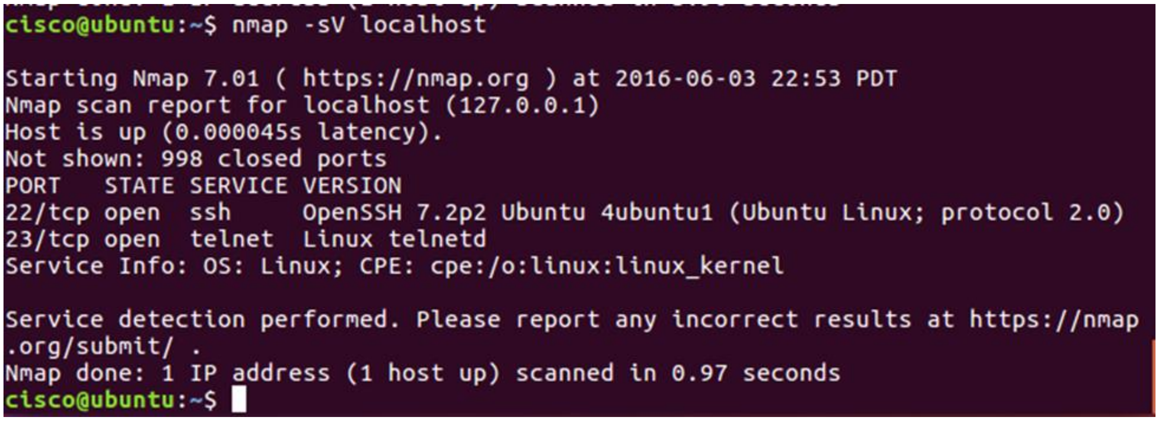
What UDP ports are open?

____

Ports 68, 631, and 5353

b. Type the following command in the terminal:

```
cisco@ubuntu:~$ nmap –sV localhost
```



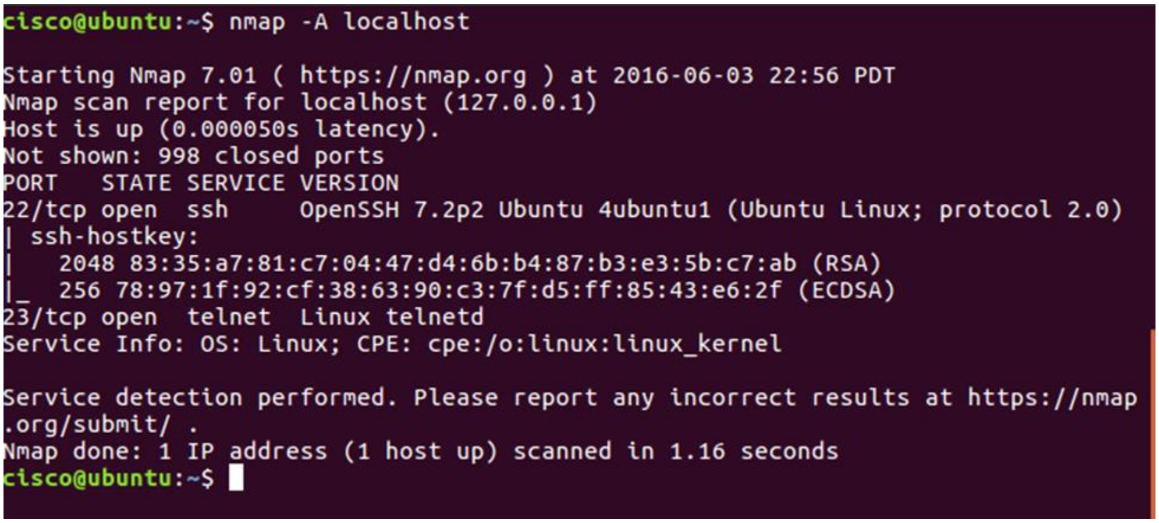
```
cisco@ubuntu:~$ nmap -sV localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:53 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
cisco@ubuntu:~$ 
```

Using the **–sV** switch with the **nmap** command performs a version detection which you can use to research vulnerabilities.

Step 4: Capture SSH keys.

Type the following command in the terminal to initiate a script scan:

```
cisco@ubuntu:~$ nmap –A localhost
```



```
cisco@ubuntu:~$ nmap -A localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:56 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000050s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 83:35:a7:81:c7:04:47:d4:6b:b4:87:b3:e3:5b:c7:ab (RSA)
|_  256 78:97:1f:92:cf:38:63:90:c3:7f:d5:ff:85:43:e6:2f (ECDSA)
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
cisco@ubuntu:~$ 
```

You captured the SSH keys for the host system. The command runs a set of scripts built into Nmap to test specific vulnerabilities.

References

Nmap: https://nmap.org/

Lab – Using Steganography (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Use steganography to hide a document within a JPEG file.

Background / Scenario

Steghide is an open source steganography program that hides data in various types of files such as audio and image files. You are going to hide a data file within an image file.

Required Resources

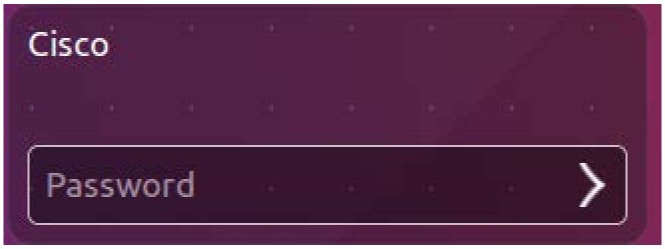
- PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine

Step 1: Open a terminal window in Ubuntu.

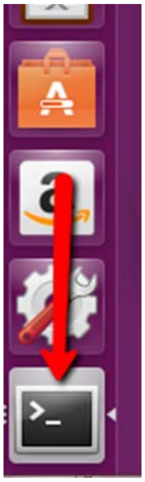
a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**



b. Click on the terminal icon to open a terminal.



Step 2: Run Steghide.

a. At the command prompt, enter the following command to change to the **Downloads** directory:

```
cisco@ubuntu:~$ cd Downloads/
```

b. Enter **libreoffice secret.odt &** at the prompt.

```
cisco@ubuntu:~/Downloads$ libreoffice secret.odt &
```

What is the message in the **secret.odt**?

____

The secret document

c. Close the **secret.odt** file when done.

d. Enter **gimp keyboard.jpg &** at the prompt to view the image file

```
cisco@ubuntu:~/Downloads$ gimp keyboard.jpg &
```

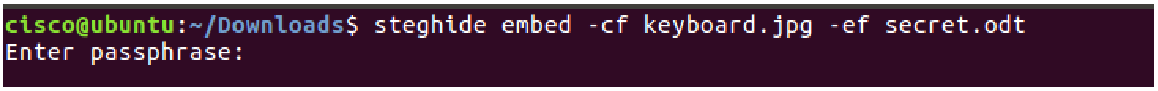
e. Close the **keyboard.jpg** file when done.

f. At the command prompt, enter the following command :

```
cisco@ubuntu:~/Downloads$ steghide embed -cf keyboard.jpg -ef secret.odt
```

This command takes the jpeg file called “keyboard.jpg” and uses it as a carrier to embed the document, **secret.odt**, into it.

g. When prompted for a passphrase, use **Cisco**. Re-enter the passphrase when prompted.



```
cisco@ubuntu:~/Downloads$ steghide embed -cf keyboard.jpg -ef secret.odt
Enter passphrase:
```

h. You have embedded the document, **secret.odt**, into the image file, keyboard.jpg.

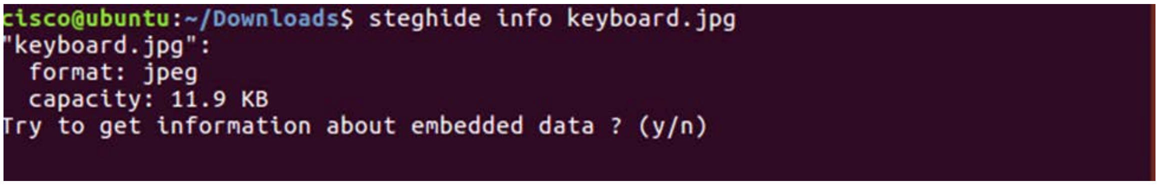
i. Open the files, **secret.odt** and **keyboard.jpg**. Did these files change? ______________________________

No. The files did not change.

Step 3: Verify the hidden file.

a. Type the following command in terminal.

```
cisco@ubuntu:~/Downloads$ steghide info keyboard.jpg
```

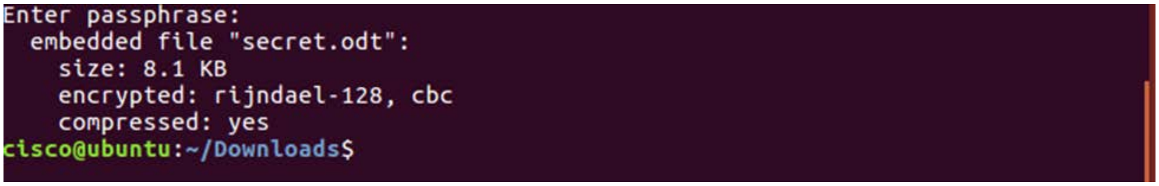


```
cisco@ubuntu:~/Downloads$ steghide info keyboard.jpg
"keyboard.jpg":
  format: jpeg
  capacity: 11.9 KB
Try to get information about embedded data ? (y/n)
```

b. Type **y** at the prompt. (Do not press **Enter**).

c. Enter the passphrase **Cisco** and press **Enter**.

d. The results below shows that the file, secret.odt, is encrypted and compressed.

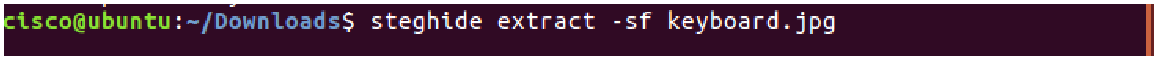


```
Enter passphrase:
  embedded file "secret.odt":
    size: 8.1 KB
    encrypted: rijndael-128, cbc
    compressed: yes
cisco@ubuntu:~/Downloads$
```

Step 4: Extract the hidden file.

a. Type the following command in terminal.

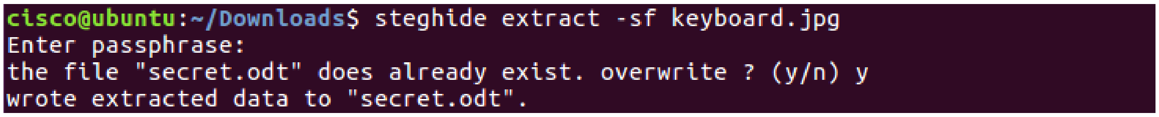
```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
```



```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
```

b. Enter the passphrase, **Cisco**, and press **Enter**.

c. Enter **y** when prompted to overwrite the existing **secret.odt** file with the new extracted **secret.odt** file.



```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
Enter passphrase:
the file "secret.odt" does already exist. overwrite ? (y/n) y
wrote extracted data to "secret.odt".
```

d. You have extracted the file. Open the extracted **secret.odt** file with LibreOffice.

Could you open the file? Is the secret message the same as before?

____

The file can be opened and the message is the same as before.

References

Steghide: http://steghide.sourceforge.net/

Lab – Password Cracking (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Use a password cracking tool to recover a user's password.

Background / Scenario

There are four user accounts, Alice, Bob, Eve, and Eric, on a Linux system. You will recover these passwords using John the Ripper, an open source password cracking tool.

Required Resources

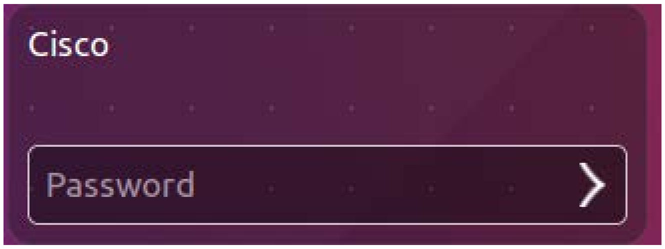
- PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine.

Step 1: Open a terminal window in Ubuntu.

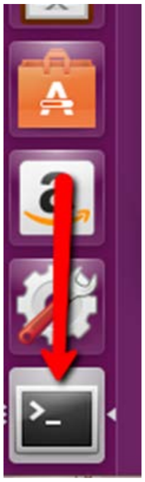
a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**



b. Click on the terminal icon to open terminal.



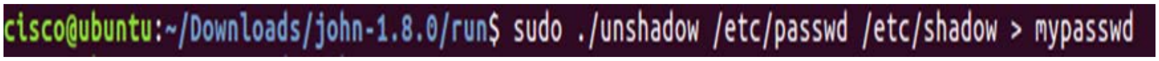
Step 2: Run John the Ripper.

a. At the command prompt, enter the following command to change to the directory where John the Ripper is located:

```
cisco@ubuntu:~$ cd ~/Downloads/john-1.8.0/run
```

b. At the command prompt, enter the following command :

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd
/etc/shadow > mypasswd
```



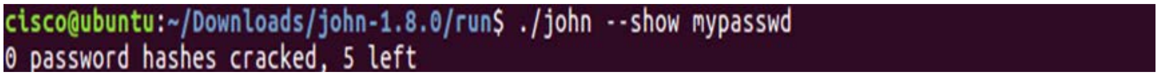
```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd /etc/shadow > mypasswd
```

This command will combine the /etc/passwd file where user accounts are stored, with the /etc/shadow file where user passwords are stored, into a new file called “mypasswd”.

Step 3: Recover Passwords.

a. Type the following command in terminal:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
```

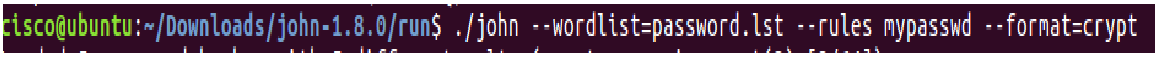


```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
0 password hashes cracked, 5 left
```

As shown above, there are no cracked passwords at this point.

b. At the command prompt, enter the following command:

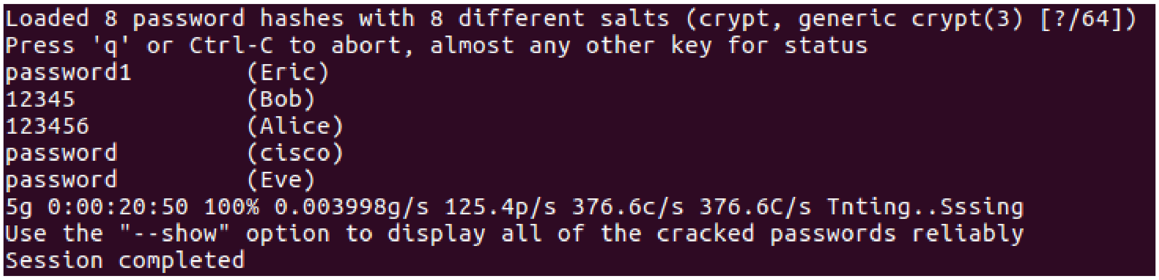
```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --wordlist=password.lst --
rules mypasswd --format=crypt
```



```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --wordlist=password.lst --rules mypasswd --format=crypt
```

The program, John the Ripper, uses a predefined dictionary called **password.lst** with a standard set of predefined “rules” for handling the dictionary and retrieves all password hashes of both md5crypt and crypt type.

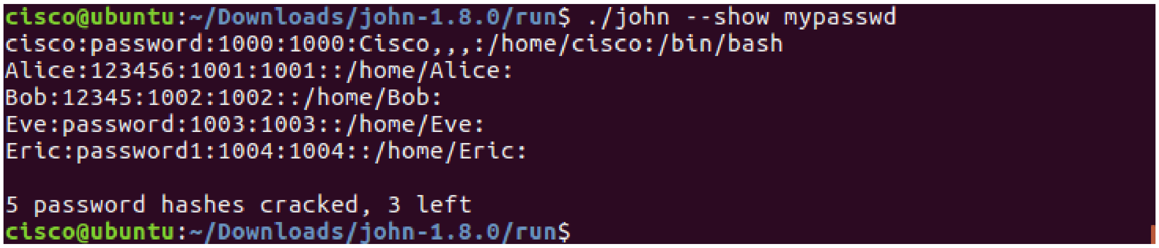
The results below display the passwords for each account.



```
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
password1        (Eric)
12345            (Bob)
123456           (Alice)
password         (cisco)
password         (Eve)
5g 0:00:20:50 100% 0.003998g/s 125.4p/s 376.6c/s 376.6C/s Tnting..Sssing
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

c. At the command prompt, enter the following command:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
```



```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
cisco:password:1000:1000:Cisco,,,:/home/cisco:/bin/bash
Alice:123456:1001:1001::/home/Alice:
Bob:12345:1002:1002::/home/Bob:
Eve:password:1003:1003::/home/Eve:
Eric:password1:1004:1004::/home/Eric:

5 password hashes cracked, 3 left
cisco@ubuntu:~/Downloads/john-1.8.0/run$
```

How many passwords were cracked?

____

Five (5)—the four user accounts plus the Cisco account.

References

John the Ripper: http://www.openwall.com/john/

Lab – Using Digital Signatures (Instructor Version)

Instructor Note: Have students pair up for this lab.

Objectives

Understand the concepts behind digital signature.

Part 1: Demonstrate the use of digital signatures.

Part 2: Demonstrate the verification of a digital signature.

Background / Scenario

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital message. A digital signature is the equivalent of a handwritten signature. Digital signatures can actually be far more secure. The purpose of a digital signature is to prevent the tampering and impersonation in digital communications. In many countries, including the United States, digital signatures have the same legal significance as traditional forms of signed documents. The United States Government now publishes electronic versions of budgets, laws, and congressional bills with digital signatures.

Required Resources

- PC or mobile device with Internet access

Part 1: Using Digital Signatures

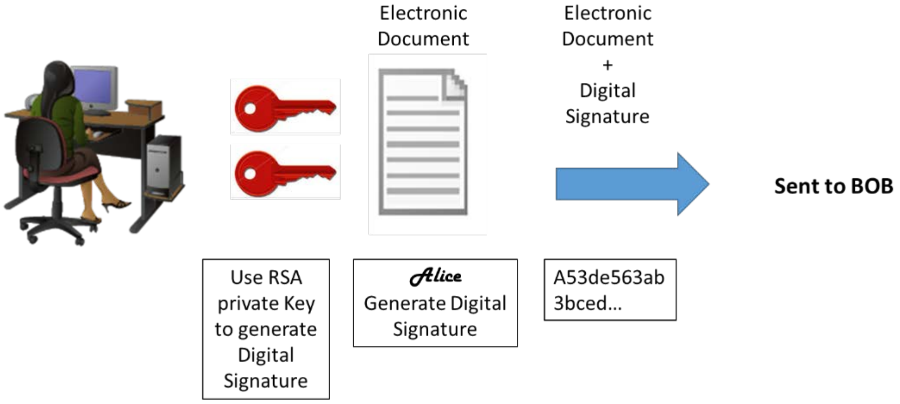
In this part, you will use a website to verify a document signature between Alice and Bob. Alice and Bob share a pair of private and public RSA keys. Each of them uses their private key to sign a legal document. They then send the documents to each other. Both Alice and Bob can verify each other's signature with the public key. They must also agree on a shared public exponent for calculation.

Table 1 - RSA Public and Private Keys

Public RSA Key	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Private RSA Key	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
Public Exponent	10001

Step 1: Sign the Document.

Alice signs a legal document and send it to Bob using the RSA public and private keys shown in the table above. Now Bob will have to verify Alice’s digital signature in order to trust the authenticity of the electronic document.


Electronic Document
Electronic Document + Digital Signature
Sent to BOB
Use RSA private Key to generate Digital Signature
Alice
Generate Digital Signature
A53de563ab 3bced...

Step 2: Verify Digital Signature.

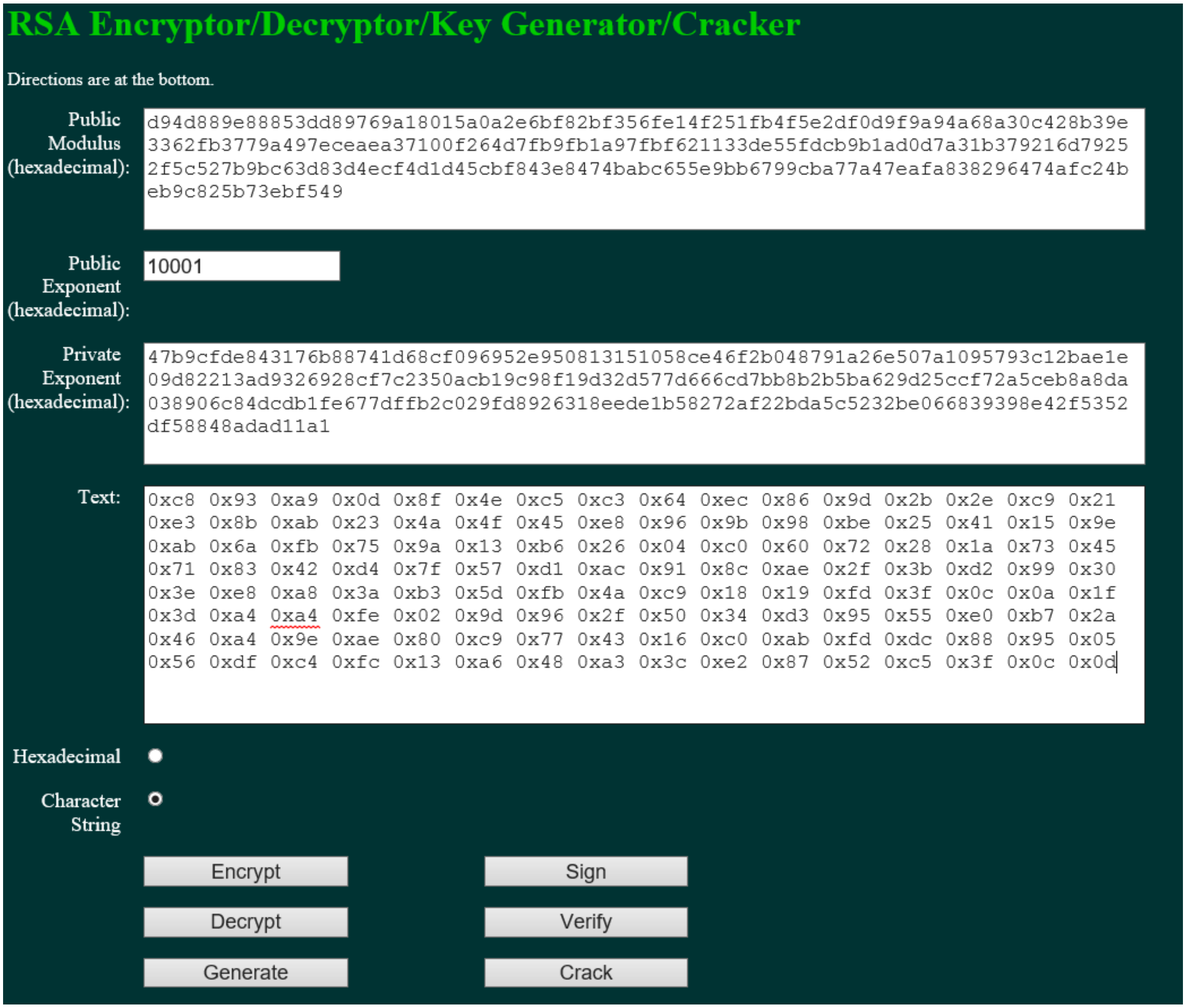
Bob receives the document with a digital signature shown in the table below.

Table 2 - Alice's Digital Signature

Alice’s Digital Signature
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21 0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e 0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45 0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30 0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f 0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a 0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05 0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d

Click here to use the online RSA tool to verify the authenticity of Alice’s digital signature.

Table 3 - Online Digital Signature Tool



RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

Public Modulus (hexadecimal):

```
d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e
3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d7925
2f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24b
eb9c825b73ebf549
```

Public Exponent (hexadecimal): 10001

Private Exponent (hexadecimal):

```
47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e
09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da
038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352
df58848adad11a1
```

Text:

```
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21
0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e
0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45
0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30
0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f
0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a
0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05
0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d
```

○ Hexadecimal

● Character String

a. Copy and paste the **public** and **private** keys from Table 1 above into the **Public Modulus** and **Private Exponent** boxes on the website as shown in the picture above.

b. Make sure the Public Exponent is 10001.

c. Paste Alice's digital signature from Table 2 in the box labeled text on the website as shown above.

d. Now BOB can verify the digital signature by clicking the **Verify** button near the bottom center of the website. Whose signature is identified?

____

Alice's name should be displayed.

Step 3: Generate a Response Signature.

Bob receives and verifies Alice's electronic document and digital signature. Now Bob creates an electronic document and generates his own digital signature using the private RSA Key in Table 1 (Note: Bob's name is in all capital letters).

Table 4 - BOB Digital Signature

BOB’s Digital Signature
0x6c 0x99 0xd6 0xa8 0x42 0x53 0xee 0xb5 0x2d 0x7f 0x0b 0x27 0x17 0xf1 0x1b 0x62 0x92 0x7f 0x92 0x6d 0x42 0xbd 0xc6 0xd5 0x3e 0x5c 0xe9 0xb5 0xd2 0x96 0xad 0x22 0x5d 0x18 0x64 0xf3 0x89 0x52 0x08 0x62 0xe2 0xa2 0x91 0x47 0x94 0xe8 0x75 0xce 0x02 0xf8 0xe9 0xf8 0x49 0x72 0x20 0x12 0xe2 0xac 0x99 0x25 0x9a 0x27 0xe0 0x99 0x38 0x54 0x54 0x93 0x06 0x97 0x71 0x69 0xb1 0xb6 0x24 0xed 0x1c 0x89 0x62 0x3d 0xd2 0xdf 0xda 0x7a 0x0b 0xd3 0x36 0x37 0xa3 0xcb 0x32 0xbb 0x1d 0x5e 0x13 0xbc 0xca 0x78 0x3e 0xe6 0xfc 0x5a 0x81 0x66 0x4e 0xa0 0x66 0xce 0xb3 0x1b 0x93 0x32 0x2c 0x91 0x4c 0x58 0xbf 0xff 0xd8 0x97 0x2f 0xa8 0x57 0xd7 0x49 0x93 0xb1 0x62

Bob sends the electronic document and digital signature to Alice.

Step 4: Verify Digital Signature.

a. Copy and paste the **public** and **private** keys from Table 1 above into the **Public Modulus** and **Private Exponent** boxes on the website as shown in the picture above.

b. Make sure the Public Exponent is 10001.

c. Paste Bob’s digital signature from Table 4 in the box labeled text on the website as shown above.

d. Now Alice can verify the digital signature by clicking the **Verify** button near the bottom center of the website. Whose signature is identified?

____

Bob’s name should be displayed.

Part 2: Create Your Own Digital Signature

Now that you see how digital signatures work, you can create your own digital signature.

Step 1: Generate a New Pair of RSA Keys.

Go to the website tool and generate a new set of RSA public and private keys.

a. Delete the contents of the boxes labeled **Public Modulus**, **Private Modulus** and **Text**. Just use your mouse to highlight the text and press the delete key on your keyboard.

b. Make sure the “Public Exponent” box has **10001**.

c. Generate a new set of RSA keys by clicking the **Generate** button near the bottom right of the website.

d. Copy the new keys in Table 5.

Table 5 - New RSA Keys

Public Key	A string of 256 hexadecimal characters will be displayed for both the public and private keys. The keys will be different from one another.
Private key	A string of 256 hexadecimal characters will be displayed for both the public and private keys. The keys will be different from one another.

e. Now type in your full name into the box labeled **Text** and click **Sign**.

Table 6 - Personal Digital Signature

Personal Digital Signature	A string of characters with this format will be displayed. 0x23 0x90 …….

Part 3: Exchange and Verify Digital Signatures

Now you can use this digital signature.

Step 1: Exchange your new public and private keys in Table-5 with your lab partner.

a. Record your lab partner's public and private RSA keys from their Table-5.

b. Record both keys in the table below.

Table 7- Lab Partners RSA Keys

Public key	A string of 256 hexadecimal characters will be displayed for both the public and private keys. The keys will be different from one another.
Private key	A string of 256 hexadecimal characters will be displayed for both the public and private keys. The keys will be different from one another.

c. Now exchange their digital signature from their Table-6. Record the digital signature in the table below.

Lab Partner's Digital Signature	A string of characters with this format will be displayed. 0x23 0x90 …….

Step 2: Verify Lab Partners Digital Signature

a. To verify your lab partner's digital signature, paste his or her public and private keys in the appropriate boxes labeled **Public and Private modulus** on the website.

b. Now paste the digital signature in the box labeled **Text**.

c. Now verify his or her digital signature by clicking the button labeled verify.

d. What shows up in the Text box?

____

Answers will vary.

Lab - Use Wireshark to Compare Telnet and SSH Traffic (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

- Use Wireshark to capture web browser traffic.
- Use Wireshark to capture Telnet traffic.
- Use Wireshark to capture SSH traffic.

Background / Scenario

Wireshark is a network protocol analyzer that lets you see what's happening on your network at a microscopic level. You can capture packets and store them for offline analysis. Wireshark includes many tools for deep inspection of hundreds of network protocols. In this lab, you will use Wireshark to capture and inspect web traffic, Telnet traffic, and SSH traffic.

Required Resources

PC with the **CSE-LABVM** installed in VirtualBox.

Instructions

Step 1: Open a terminal window in the CSE-LABVM.

a. Launch the **CSE-LABVM**.

b. Double-click the **Terminal** icon to open a terminal.

Step 2: Explore the Wireshark protocol analyzer.

a. To capture traffic on your VM, you need to run Wireshark in promiscuous mode, which requires running with escalated privileges using **sudo**. Enter the **sudo wireshark** command, and then enter **password** for the password. The Wireshark graphical user interface (GUI) will open up.

```
cisco@labvm:~$ sudo wireshark
[sudo] password for cisco: password
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

b. Under the listing of interfaces, select **any**, and then click **Capture** > **Start** from the menus. Alternatively, you can click the shark fin icon. Wireshark will begin capturing packets.

c. If you already have Firefox open, you may see traffic captured in the Wireshark interface. If Firefox is not open, go ahead and open it now. In Wireshark, you should now see captured TCP traffic in the top third of the window.

d. In Firefox, enter www.cisco.com to visit the Cisco website. After the website loads, you can close Firefox.

e. Return to Wireshark and click **Capture** > **Stop** from the menus. Alternatively, you can click the red square button next to the shark fin.

f. In Wireshark, you will see the filter field and three key panes or work areas:

- The **Apply a display filter** field is directly below the toolbar.

- The **Packet List** pane includes the following columns for each captured packet:
  - **No** - the number of the packet (in numerical order).
  - **Time** - the timestamp of the packet
  - **Source** - the source IP address of the packet
  - **Destination** - the destination IP address of the packet
  - **Protocol** - the protocol of the packet
  - **Length** - the number of bytes captured for this packet
  - **Info** - additional information about the packet’s content
- The **Packet Details** pane shows the protocols and protocol fields of the selected packet. Notice that the fields can be expanded or collapsed by clicking the arrow next to the field.
- The **Packet Bytes** pane shows the byte details of the selected packet. As you select parts of the packet in the Packet Details pane, the corresponding bytes will be highlighted in the Packet Bytes pane. The left side shows the hexadecimal representation of the bytes, and the right side shows the ASCII representation.

Step 3: Capture and analyze unencrypted Telnet traffic.

a. Start a new capture. In the **Unsaved packets…** dialog box, click **Continue without Saving**. This will clear out the packets from your last capture and start a new capture.

b. Double-click the **Terminal** icon to open a new terminal window.

c. You can simulate a remote login to your VM by entering the **telnet localhost** command, and then logging in as **cisco** with **password** as the password.

```
cisco@labvm:~$ telnet localhost
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 20.04.2 LTS
labvm login: cisco
Password: password
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-67-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.

Last login: Thu Mar 18 21:47:23 UTC 2021 on tty2
cisco@labvm:~$
```

d. Enter the **exit** command to end the Telnet session:

```
cisco@labvm:~$ exit
logout
Connection closed by foreign host.
cisco@labvm:~$
```

e. Return to Wireshark and stop the capture.

f. In the **Apply a display filter** field, type **telnet** and press **Enter** to filter for only Telnet packets.

g. On the toolbar, click the magnifying glass icon to **Find a packet**. Additional search features are now shown below the **Apply a display filter** field.

h. Click the arrows next to **Display filter** and change it to **String**. Then click the arrows next to Packet list and change it to **Packet details**.

i. To find the packet requesting login information, type **labvm login:** in the field next to **String**, and then press **Enter** or click **Find**. Wireshark will highlight the packet that contains the "labvm login:" text string.

j. In the **Packet Details** pane, click the arrow next to **Telnet** to expand its content. You should see that **labvm login:** is the data for this packet. The data for the packet is also shown in **Packet Bytes** pane. You can tell that the text was sent unencrypted because you can read it.

k. In the **Packet List** pane, click the highlighted packet with **labvm login** as the data to select it.

l. To find the username and password, use your down arrow on the keyboard to select the next packet. In the **Packet Details** pane, you should see the value for **Data** under **Telnet** is the first letter you typed in the field for "labvm login:" prompt, which was **c** for **cisco**. If you click the down arrow again, you will see the next packet's data is also **c**. This is because the packet is listed twice: one time for source sending to destination and again for destination receiving the packet. Because the source and destination are the same interface (loopback 127.0.0.1), the packet is listed twice by Wireshark.

m. Continue to press the down arrow key until you reach the last packet with a data value of **o** for the username **cisco**.

n. Continue to click the down arrow until you will see **Password:** in the **Data** field. Continue pressing the down arrow to read the data of the next eight packets which reveal, one letter at a time, that **password** is the password for user **cisco**.

o. If you continue to press the down arrow through the rest of the captured packets, you will see all the text sent and received during the Telnet session, including your **exit** command and the **logout** message.

Step 4: Capture and analyze encrypted SSH traffic.

a. Start a new capture. In the **Unsaved packets…** dialog box, click **Continue without Saving**. This will clear out the packets from your last capture and start a new capture.

b. Return to your open terminal window or start a new terminal session.

c. To simulate an SSH login, enter the command **ssh localhost**. If this is your first time to use the command, the system warns you about the authenticity of localhost and asks you if you want to continue. Enter **yes**, and then **password** as the password to log in.

```
cisco@labvm:~$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:lEvtfM55v9O8L88uvZ4Em/UL4ARo8jWGE1hV8mVnDhQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
cisco@localhost's password: password
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-67-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
```

```
0 of these updates are security updates.

Last login: Thu Mar 25 14:01:58 2021 from localhost
cisco@labvm:~$
```

d. Enter the **exit** command to end the SSH session.

e. Return to Wireshark and stop the capture. If you left **telnet** as the search term in the **Apply a display filter** field, no packets will be listed. Change the search term from **telnet** to **ssh**. All the packets from your SSH session should now be shown in the **Packet List** pane.

f. In the **Packet Details** pane, expand the **SSH Protocol** fields to view the content. In the **Packet List** pane, click the first packet, and then use the down arrow to view a variety of the SSH packets. Notice that the **Data** for the **SSH Protocol** field shows that all the data is encrypted.

Lab – Hardening a Linux System (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Demonstrate the use of a security auditing tool to harden a Linux system.

Background / Scenario

Auditing a system for potential misconfigurations or unprotected services is an important aspect of system hardening. Lynis is an open source security auditing tool with an automated set of scripts developed to test a Linux system.

Required Resources

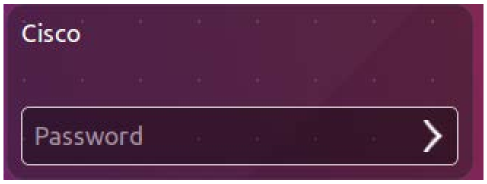
- PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine.

Step 1: Open a terminal window in Ubuntu.

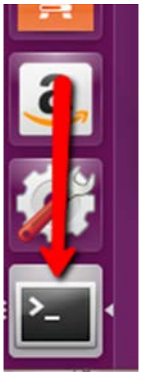
a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**



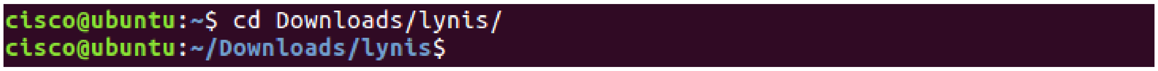
b. Click the terminal icon to open a terminal window.



Step 2: The Lynis Tool

a. At the command prompt, enter the following command to change to the lynis directory:

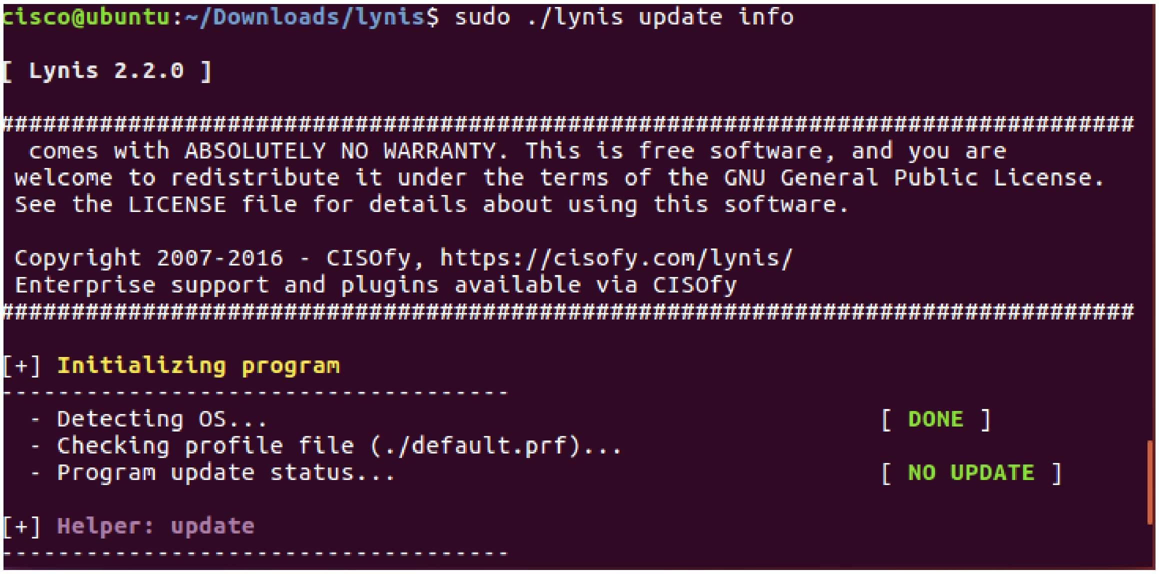
```
cisco@ubuntu:~$ cd Downloads/lynis/
```



```
cisco@ubuntu:~$ cd Downloads/lynis/
cisco@ubuntu:~/Downloads/lynis$
```

b. At the command prompt, enter the following command and enter the password **password** when prompted:

```
cisco@ubuntu:~/Dowloads/lynis$ sudo ./lynis update info
```



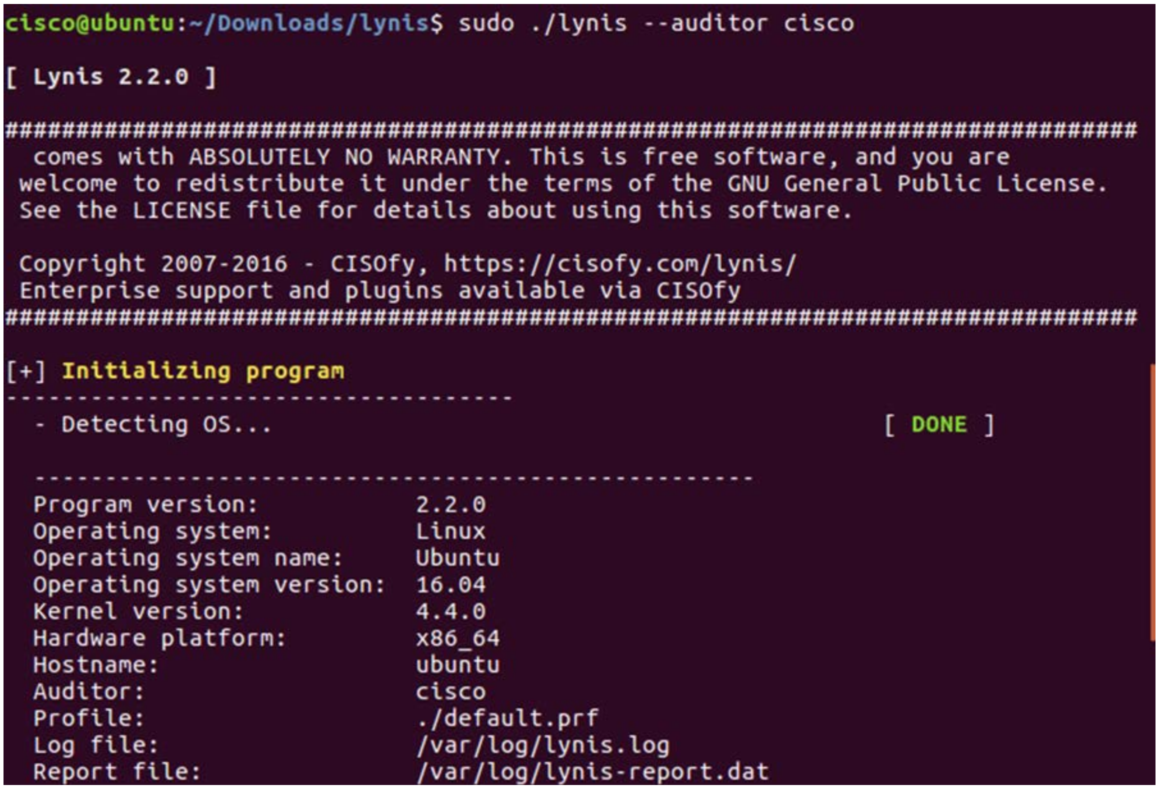
```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis update info

[ Lynis 2.2.0 ]

################################################################################
  comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
 welcome to redistribute it under the terms of the GNU General Public License.
 See the LICENSE file for details about using this software.

 Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
 Enterprise support and plugins available via CISOfy
################################################################################

[+] Initializing program
------------------------------------
  - Detecting OS...                                          [ DONE ]
  - Checking profile file (./default.prf)...
  - Program update status...                                 [ NO UPDATE ]

[+] Helper: update
------------------------------------
```

This command verifies that this is the latest version and updates for the tool at the time of writing of this lab.

Step 3: Run the Tool

a. Type the following command in terminal and press **Enter**:

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```

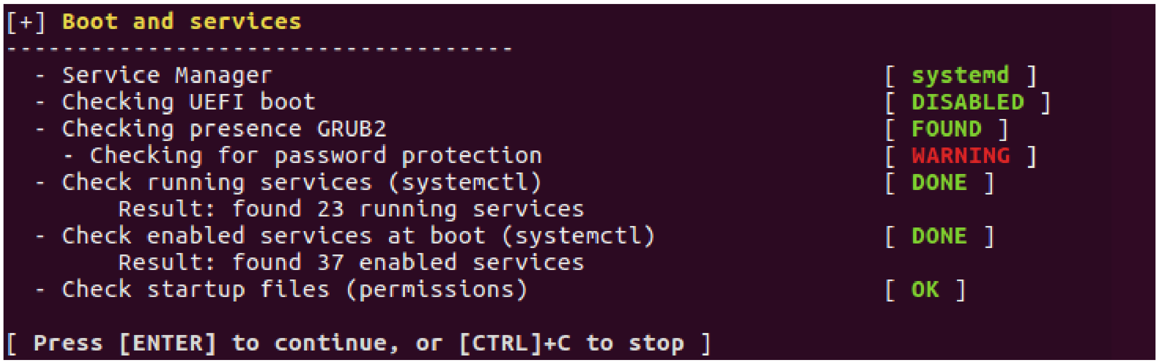


```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco

[ Lynis 2.2.0 ]

################################################################################
  comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
 welcome to redistribute it under the terms of the GNU General Public License.
 See the LICENSE file for details about using this software.

 Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
 Enterprise support and plugins available via CISOfy
################################################################################

[+] Initializing program
------------------------------------
  - Detecting OS...                                          [ DONE ]

  ---------------------------------------------------
  Program version:           2.2.0
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  16.04
  Kernel version:            4.4.0
  Hardware platform:         x86_64
  Hostname:                  ubuntu
  Auditor:                   cisco
  Profile:                   ./default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
```

As displayed above, the tool will begin auditing using the user **cisco** as the auditor.

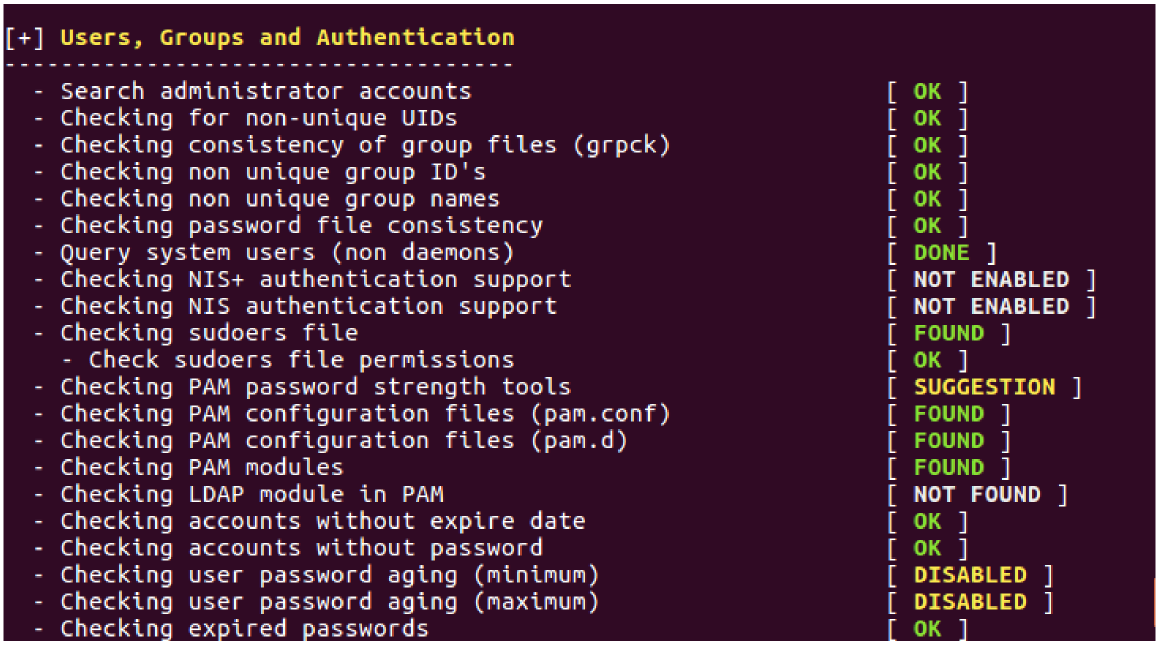
Notice: You will receive **warnings**.

b. To continue with each stage of the audit press **Enter**. You will receive warnings as shown below.



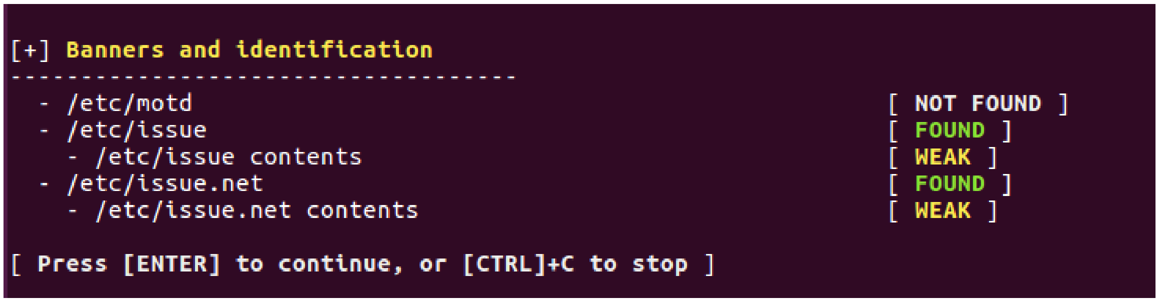
```
[+] Boot and services
------------------------------------
  - Service Manager                                          [ systemd ]
  - Checking UEFI boot                                       [ DISABLED ]
  - Checking presence GRUB2                                  [ FOUND ]
    - Checking for password protection                       [ WARNING ]
  - Check running services (systemctl)                       [ DONE ]
        Result: found 23 running services
  - Check enabled services at boot (systemctl)               [ DONE ]
        Result: found 37 enabled services
  - Check startup files (permissions)                        [ OK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

c. You will receive suggestions, as shown below.



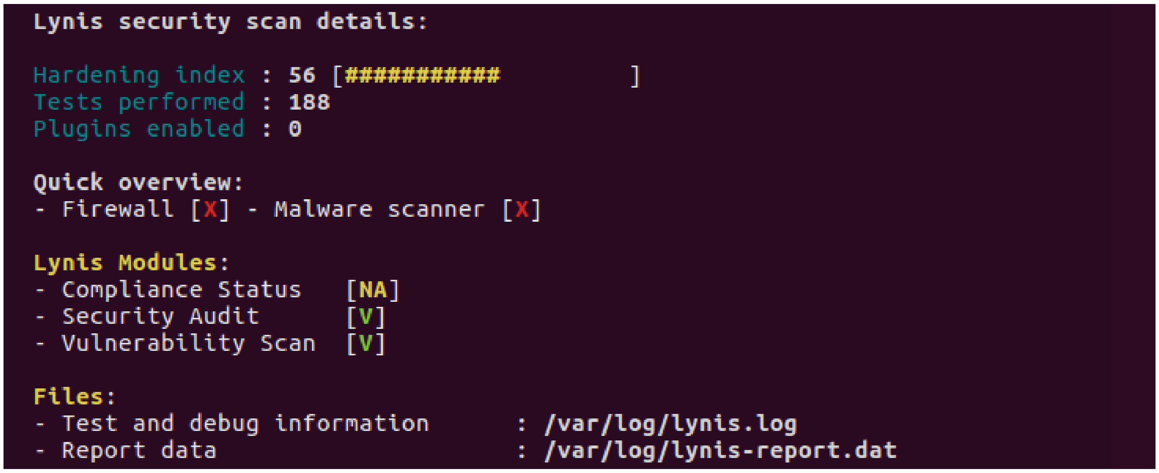
```
[+] Users, Groups and Authentication
------------------------------------
  - Search administrator accounts                             [ OK ]
  - Checking for non-unique UIDs                              [ OK ]
  - Checking consistency of group files (grpck)               [ OK ]
  - Checking non unique group ID's                            [ OK ]
  - Checking non unique group names                           [ OK ]
  - Checking password file consistency                        [ OK ]
  - Query system users (non daemons)                          [ DONE ]
  - Checking NIS+ authentication support                      [ NOT ENABLED ]
  - Checking NIS authentication support                       [ NOT ENABLED ]
  - Checking sudoers file                                     [ FOUND ]
    - Check sudoers file permissions                          [ OK ]
  - Checking PAM password strength tools                      [ SUGGESTION ]
  - Checking PAM configuration files (pam.conf)               [ FOUND ]
  - Checking PAM configuration files (pam.d)                  [ FOUND ]
  - Checking PAM modules                                      [ FOUND ]
  - Checking LDAP module in PAM                               [ NOT FOUND ]
  - Checking accounts without expire date                     [ OK ]
  - Checking accounts without password                        [ OK ]
  - Checking user password aging (minimum)                    [ DISABLED ]
  - Checking user password aging (maximum)                    [ DISABLED ]
  - Checking expired passwords                                [ OK ]
```

d. You will receive a notification for any configuration that is weak as shown below:



```
[+] Banners and identification
------------------------------------
  - /etc/motd                                                 [ NOT FOUND ]
  - /etc/issue                                                [ FOUND ]
    - /etc/issue contents                                     [ WEAK ]
  - /etc/issue.net                                            [ FOUND ]
    - /etc/issue.net contents                                 [ WEAK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

e. You will receive detailed security enhancement suggestions as well as a final summary which provides the location where you can find the log file.



```
  Lynis security scan details:

  Hardening index : 56 [###########         ]
  Tests performed : 188
  Plugins enabled : 0

  Quick overview:
  - Firewall [X] - Malware scanner [X]

  Lynis Modules:
  - Compliance Status   [NA]
  - Security Audit      [V]
  - Vulnerability Scan  [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat
```

Step 4: Review Results

a. Scroll up to the results section after the tool is finished running.

How many Warnings did you receive? ____________________________ Answers will vary. There was 1 warning in this example.

How many Suggestions did you receive? __________________________ Answers will vary. There were 33 suggestions in this example.

b. Scroll through the suggestions and select one. You will research a suggestion that you can implement to address the issue.

Which suggestion are you addressing?

____

____

Answers will vary.

What is your suggested solution?

____

____

Answers will vary.

References

Lynis: https://cisofy.com/lynis/