

Cybersecurity Notebook

Unit 3

Name:

Table of Contents

**Unit 3**

* [**3.1.1**](#3xjqpy677yrv)
* [**Linux Commands Table**](#cug4wedo24s9)
* [**3.1.2**](#n002yttni4fz)
* [**3.1.3**](#2d852427qlq2)
* [**3.1.4**](#hc1xcj7kay89)
* [**3.2.1**](#o92jbhts9sqk)
* [**3.2.2**](#8wkeuk1oq81w)
* [**3.2.3**](#b4dnoqfzqcw2)
* [**3.2.4**](#k3t6ce1vcmp0)
* [**3.2.5**](#w6u4auj48ro4)
* [**3.2.6**](#k2es246cxrmg)
* [**3.3.1**](#ewf1hi6n7u7y)
* [**3.3.2**](#qzggjr1hzy3z)
* [**3.3.3**](#ai14kn5c5084)
* [**3.3.4**](#rzpy4njljgnv)
* [**3.3.5**](#v663u9b8drnh)
* [**3.4.1**](#qgoz10u762er)

Unit 3 Cyber Case

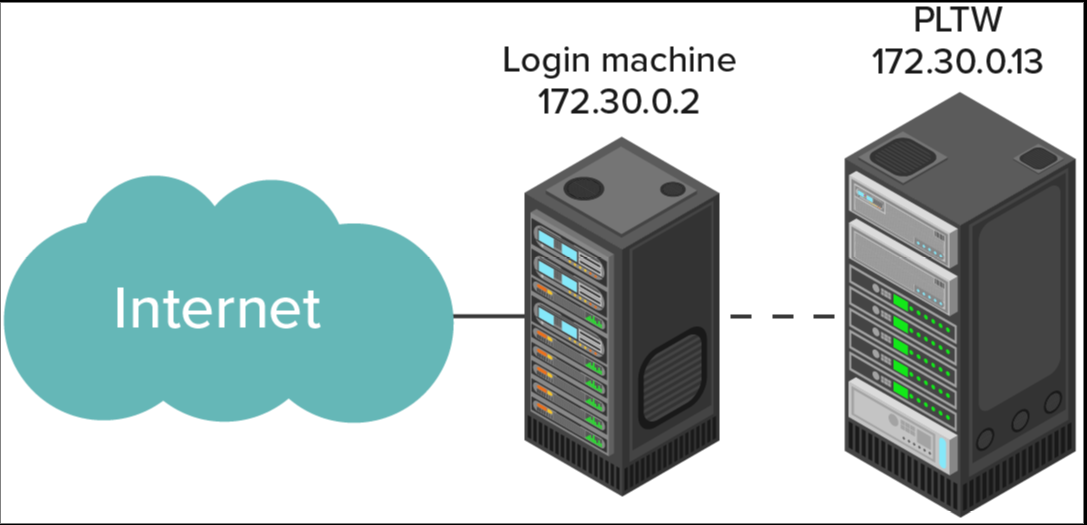
The Water Treatment Facility Breach

You have just graduated from the prestigious Malware Awareness Academy where you mastered malware detection and prevention. With your new training, you can identify common attack methods and stop criminals in their tracks. Many local companies actively recruit you. You decide to accept an offer as a Junior Security Analyst from your city’s water department, working in their state-of-the-art, fully automated facility. The facility’s treatment system filters and treats all of the city water and flushes all water lines, ensuring the water is clean and safe for consumption.

Within a few weeks of your start date, the water treatment facility is hacked. The network is running slowly and so are its water pumps that move water through the system. In fact, at times, the system is running so slowly it appears the network is “under water.” The treatment facility cannot keep up with the city's need for clean water! The town has a small reserve but at this rate, the city run out of water in three days. It’s up to you and your team to find the breach, fix the problems the breach may have caused, modify the system to prevent future attacks, and bring the water system back online.

**The activities and projects in this unit will arm you with the skills and knowledge you need to find a workable solution to the water treatment facility breach and bring the clean water back on for the city.**

**Unit 3.1.1**

****

#5 - Linux Command Table

|  |  |
| --- | --- |
| **Command** | **Description** |
| ls | Lists the contents of a directory |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

#8 Put into Command Table

#11 Put into Table

#12 Put into table

#13 Screenshot

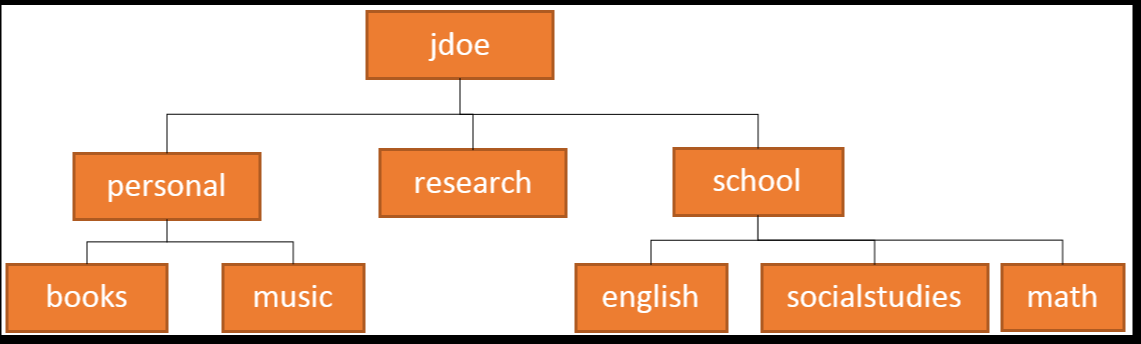
#14 Screenshot

#17 Screenshot & Add to table

#18 Screenshot

#19 Screenshot

Figure 1



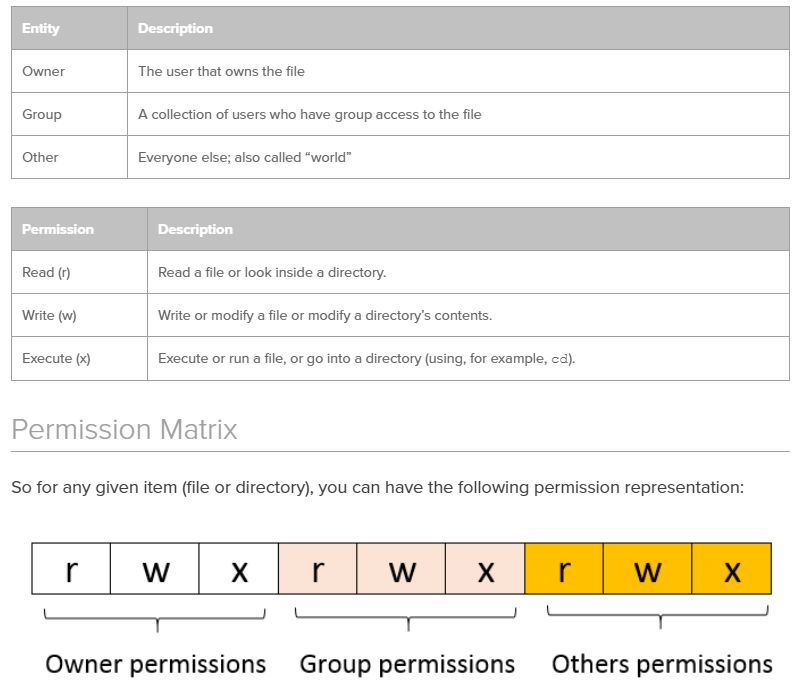
#20 Put into table

#25 Put into table & Screenshot

#30 Put into table

#37 Notebook - Put into table

**Unit 3.1.2**



#3 Put into table in 3.1.1

#4 - Complete table

|  |  |  |
| --- | --- | --- |
|  | **message.sh** | **welcome.tx** |
| Owner | Read, write, execute |  |
| Group |  |  |
| Other |  |  |

#5 Who Owns message.sh?

Group?

File size?

Date last modified?

#7 Notebook - what was the output?

#9 Put into table

THIS PORTION IS VERY DIFFERENT FROM WINDOWS -

MAKE NOTE OF FILE TYPE INFORMATION

#11 Notebook

#12 Screenshot

#13 Screenshot - Put into table

#18 Screenshot

#19 Put into table

#23 Screenshot

#24 Put into table

#25 Notebook

#26 Notebook

**Unit 3.1.3**

#3 Notebook

#4 Put into table

#6 Screenshot

#8 Screenshot of just 1 page

#12 Screenshot - Put into table

What is the PID of your -bash?

What is the PPID of your bash?

What is the command the spawned your -bash process?

#13 Put into table

#14 List the Users

#20 Put into table

#23 Put in table

#29 Put in table

#36 Put into table

#37 Screenshot of beta terminal after #38

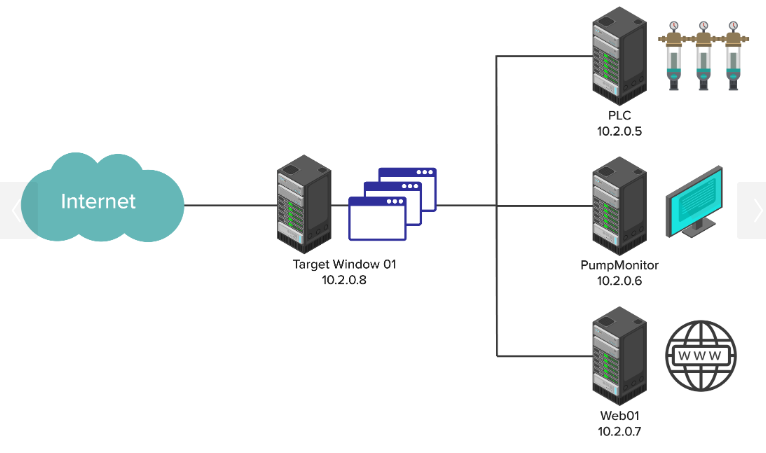
#40 Put into table

**Unit 3.1.4**

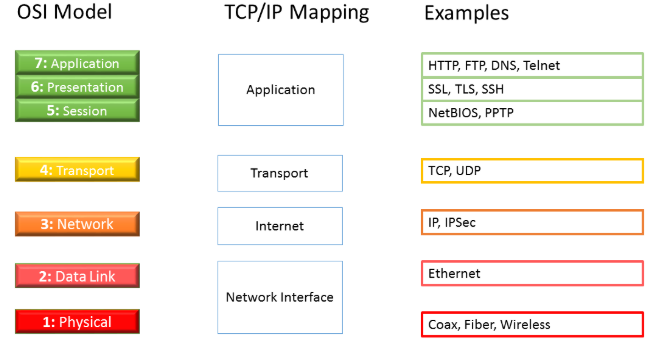
**Enter report here**

**#10 Answer three questions here.**

**Unit 3.2.1**

****

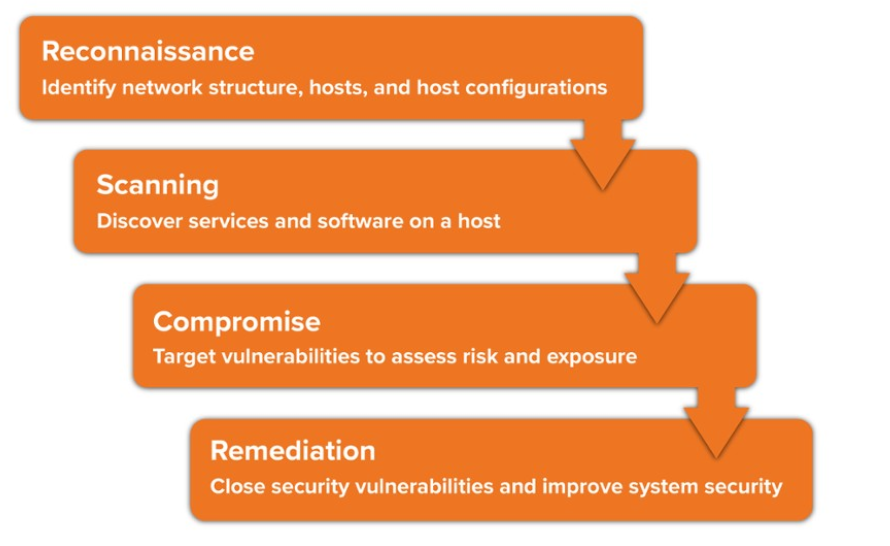
**Pay attention to the IP addresses of each.**



#1-8 Take notes in notebook

Create and share your plan. - Each person add to the notebook but can be done in groups.

**Unit 3.2.2**



Before #1 Screenshot & Notebook - Topology

Before #1 Screenshot & Notebook - OSI Model

#4 Screenshot

#16 Screenshot

#17 Notebook

#29 Screenshot

#32 Screenshot & Notebook

#41 Screenshot & Notebook

**Unit 3.2.3**

#7 Screenshot & Notebook

#8 Notebook  
#9 Screenshot

#14 Notebook

#24 Notebook

#33 Screenshot & Notebook

**Unit 3.2.4**

#11 Notebook

#12 Screenshot & Notebook

#13 Notebook

#14 Notebook

#15 Notebook

# iptables -Notebook

#27 Screenshot

#28 Notebook

#29 Notebook

**Unit 3.2.5**

# Ethical Hacking - Notebook

#9 Screenshot & Notebook

#20 Screenshot & Notebook

#22 Screenshot

#23 Screenshot

#24 Notebook

#39 Screenshot & Notebook

#41 Notebook

#44 Screenshot

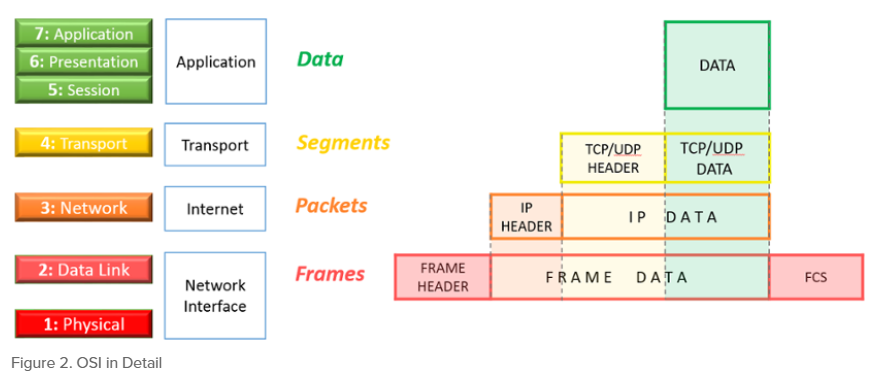
#45 Screenshot

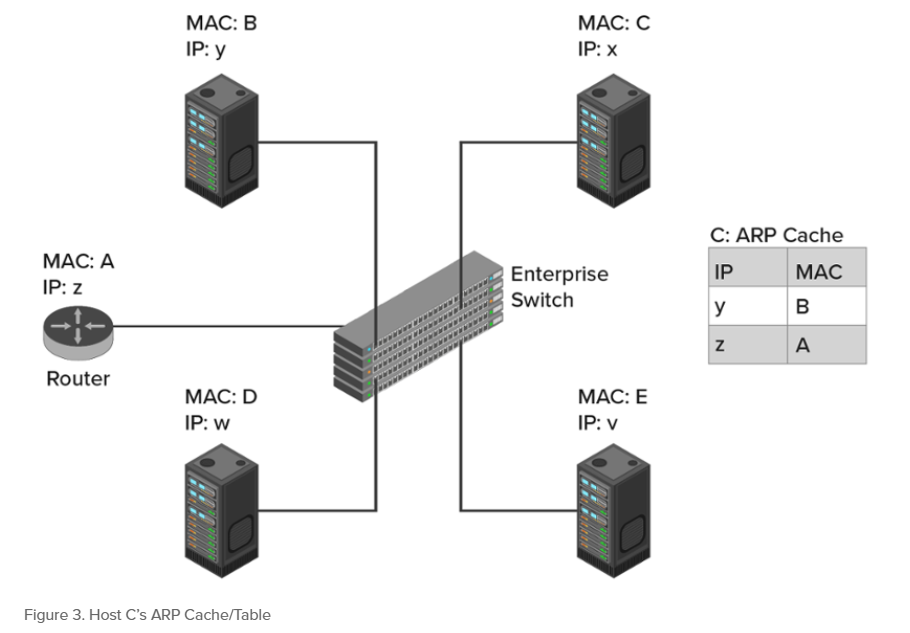
**Unit 3.2.6**

#8 Screenshot & Notebook

Incident Report - Insert Here

**Unit 3.3.1**

****

****

#4 Notebook

#5 Notebook

#6 Notebook

#12 Notebook

#14 Notebook

#15 Notebook

#17 Notebook

#27 Notebook

#29 Notebook

#30 Notebook

#33 Notebook

#34 Notebook

#37 Notebook

#40 Screenshot & Notebook

Activity Feedback - Screenshot

**Unit 3.3.2**

#3 Notebook

#6 Notebook

#14 Screenshot & Notebook

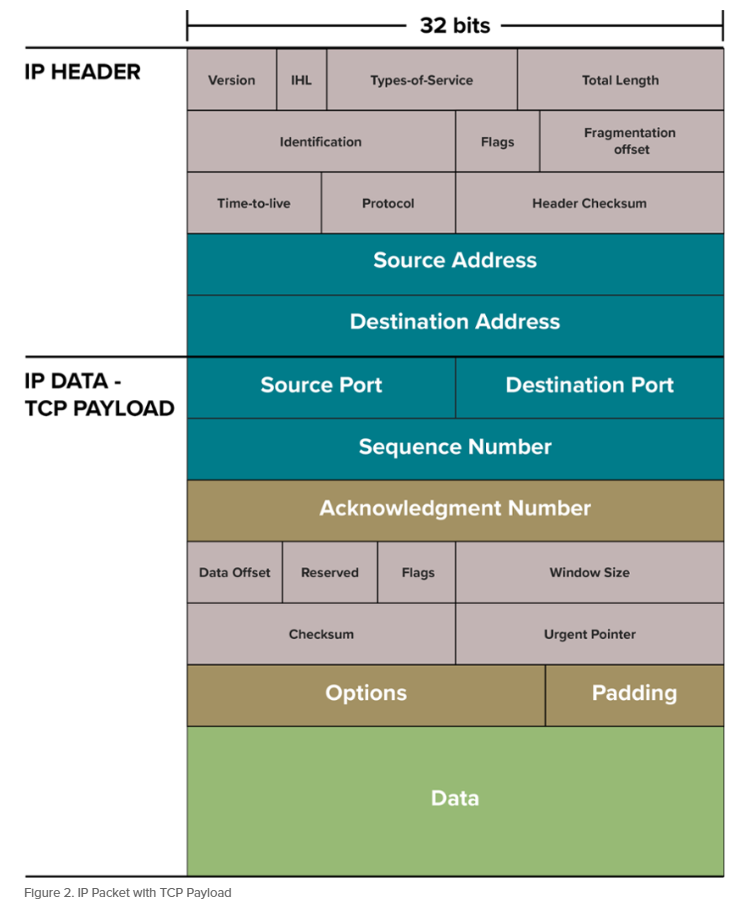
#17 Notebook

#18 Notebook

#19 Notebook

#20 - Make another note on how to set firewall to deny ICMP

**Unit 3.3.3**

****

# 4 Complete chart

#6 Screenshot of the pane to show three segments

#8 Notebook

#11 Complete the chart

#12 Complete the chart & Complete drawing requested

#14 Notebook

**Unit 3.3.4**

#5 Notebook

#6 Notebook

#13 Notebook

#31 Notebook

#33 Notebook

#34 Notebook - Both questions

**Unit 3.3.5**

#11 Notebook

Conclusion Questions - Notebook

**Unit 3.4.1**

A full and complete report based on questions.

**Activity Feedback - Screenshot**