PROJECT TASK 3

CONFIGURING SNORT IPS TO DETECT, MONITOR AND ALERT CYBERSECURITY ATTACKS

Alabi Kehinde Oluwasemilore

Information Systems Engineering and Management, Harrisburg University

CISSC 661: Principles of Cybersecurity & Cyberwarfare

Dr. Bruce Young

28/05/2023

Snort IPS Setup

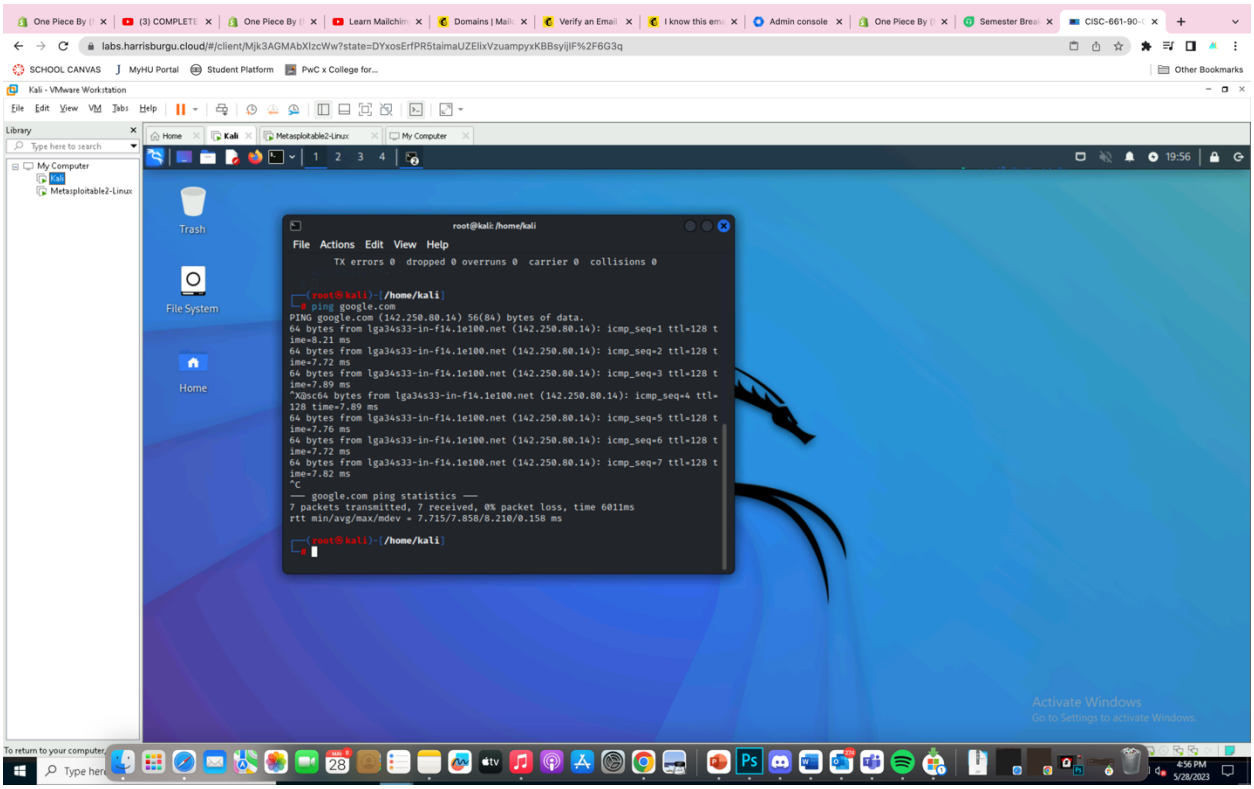
Performed a successful exploit for this project. For this project we needed Kali Linux, Metasploitable.

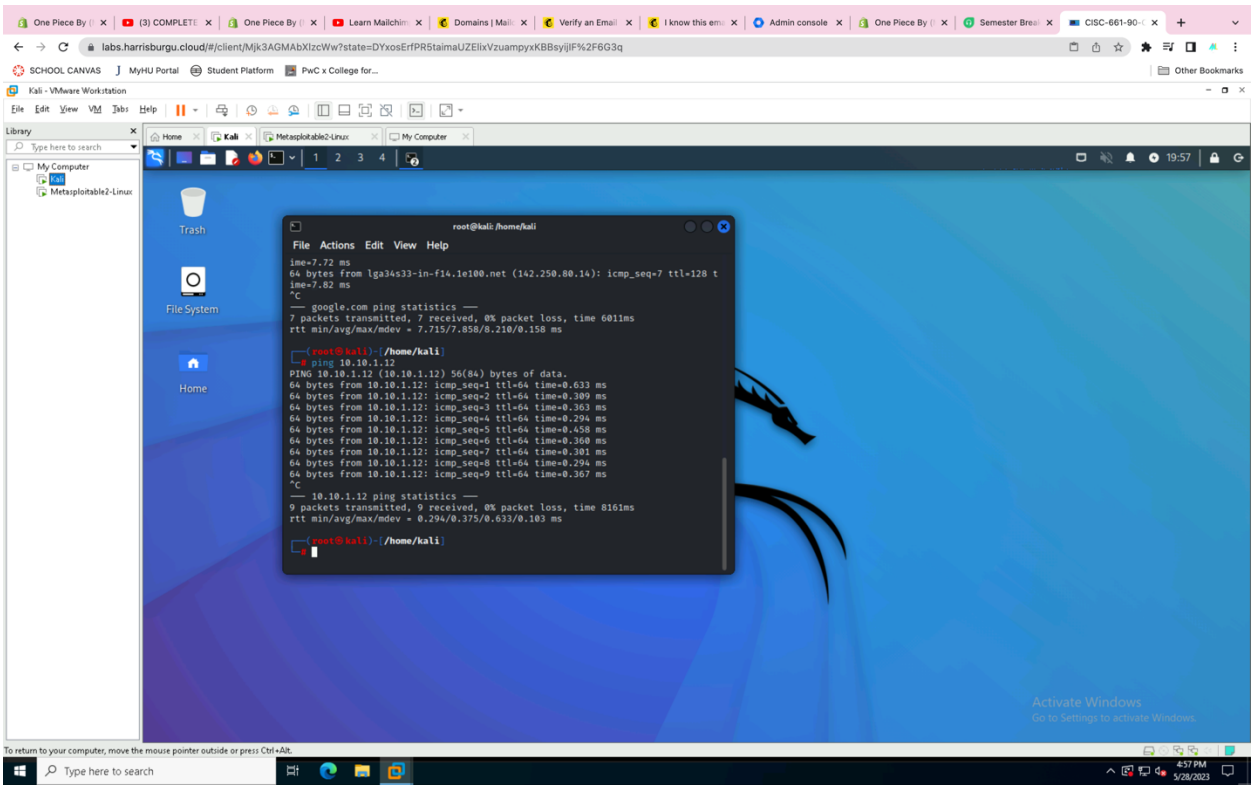
System Configuration:

- Macbook Pro 2016
- Mac OS Ventura
- 32 GB RAM
- 2.3 GHz 8-Core Intel Core i9

Step 1: Test for connection

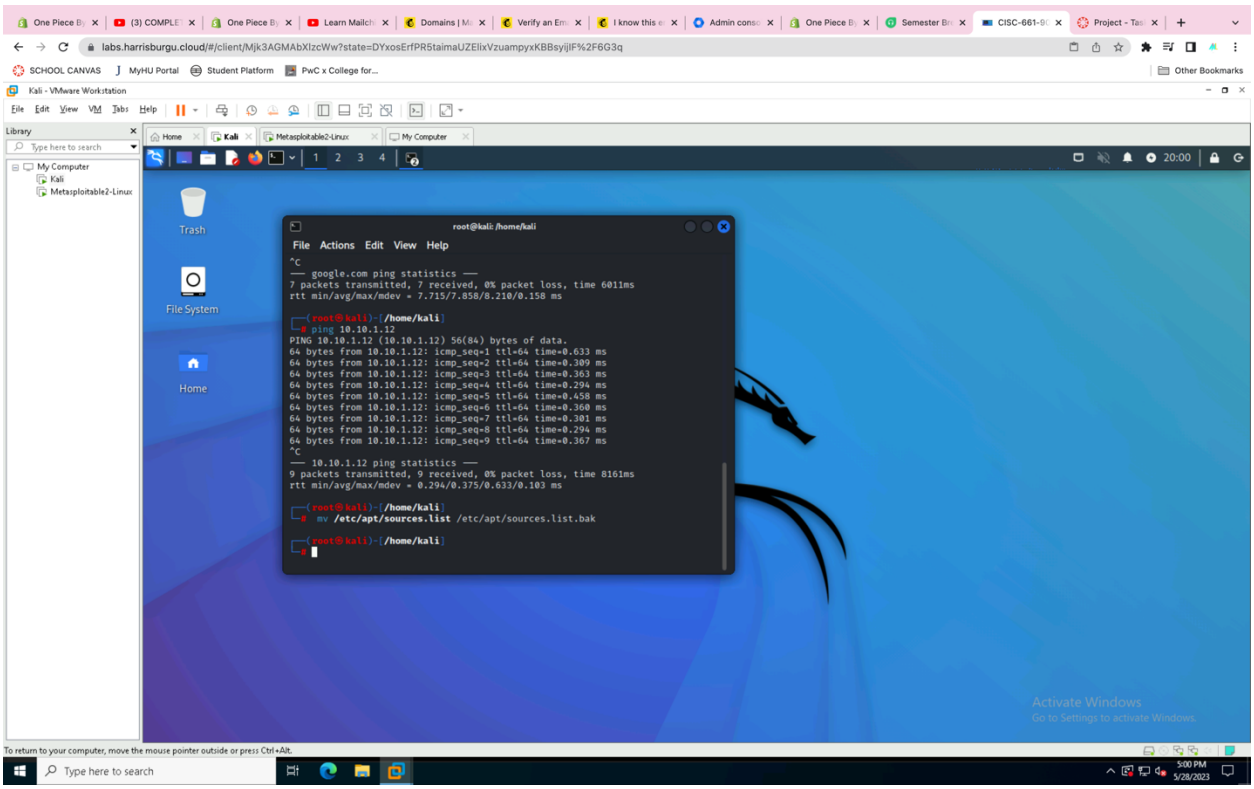
- Using Ping to test for connection.



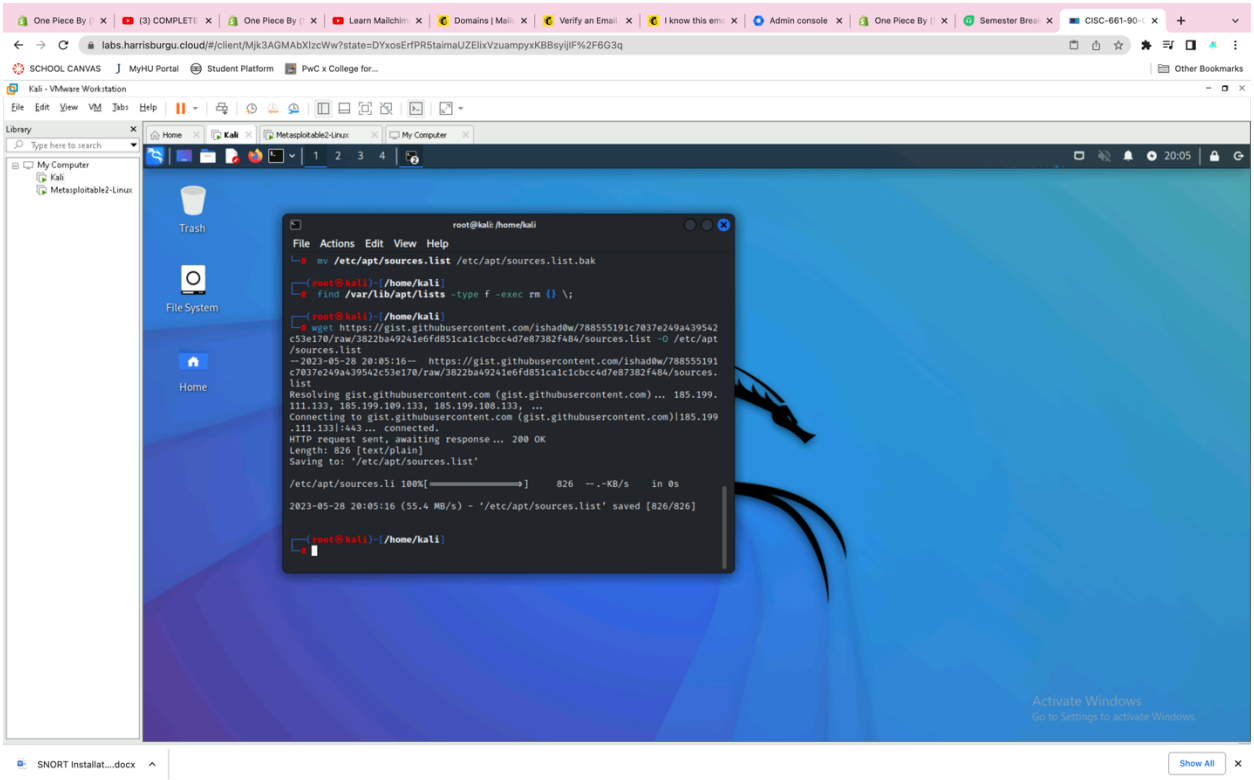


Step 2

- Move sources list by making backup copy

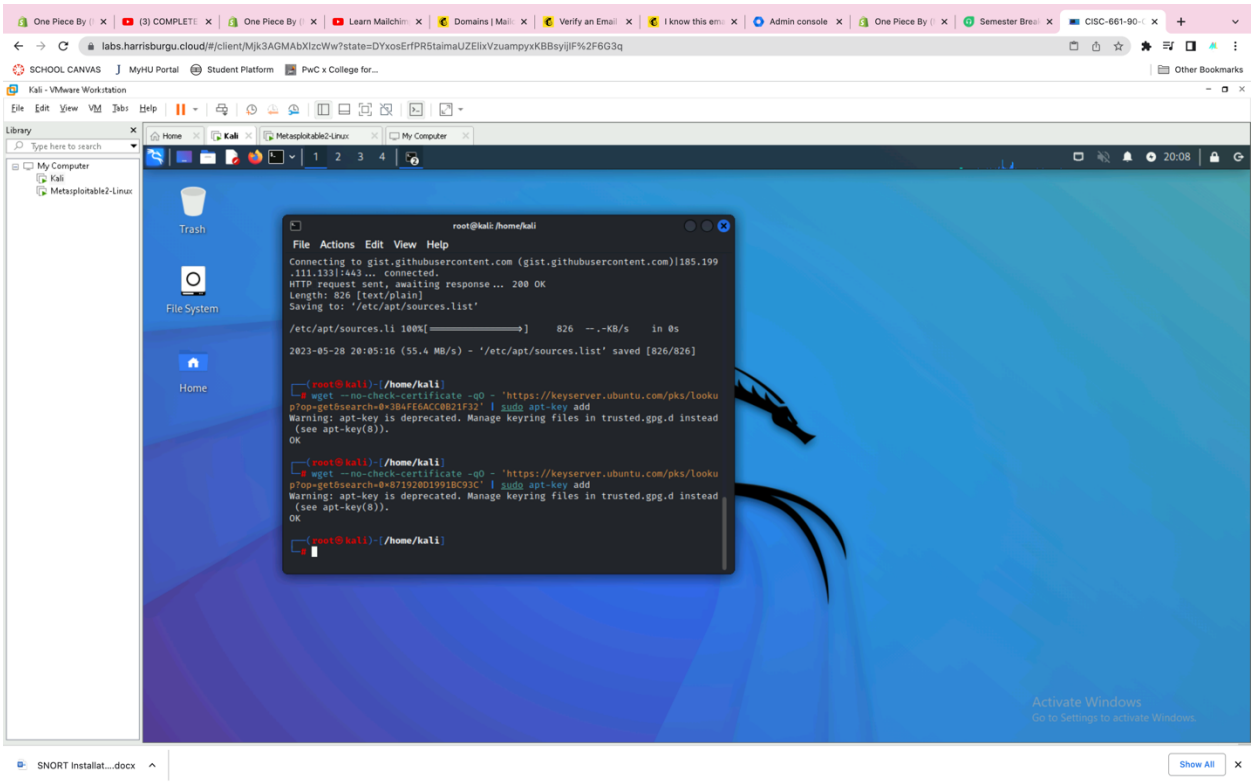


- Create certificate in place to ensure secure connection.

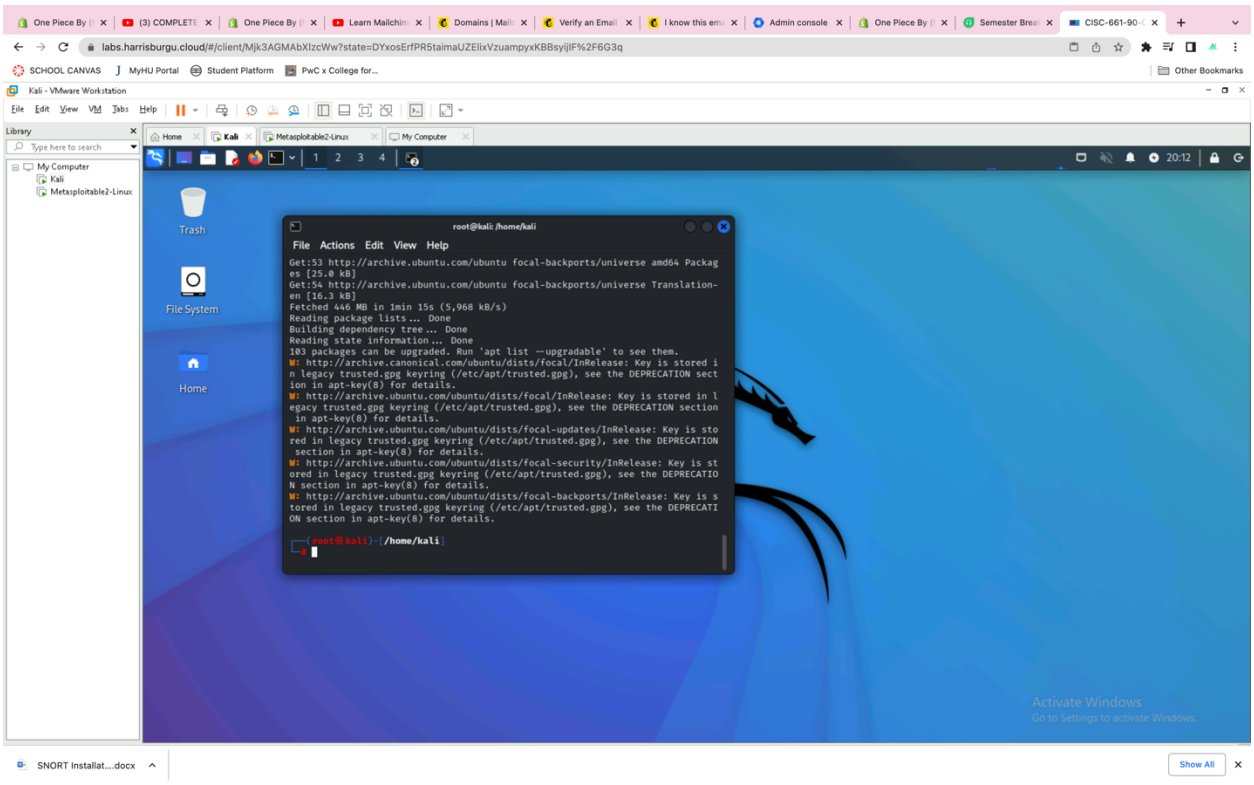


Step 3

- Perform apt update

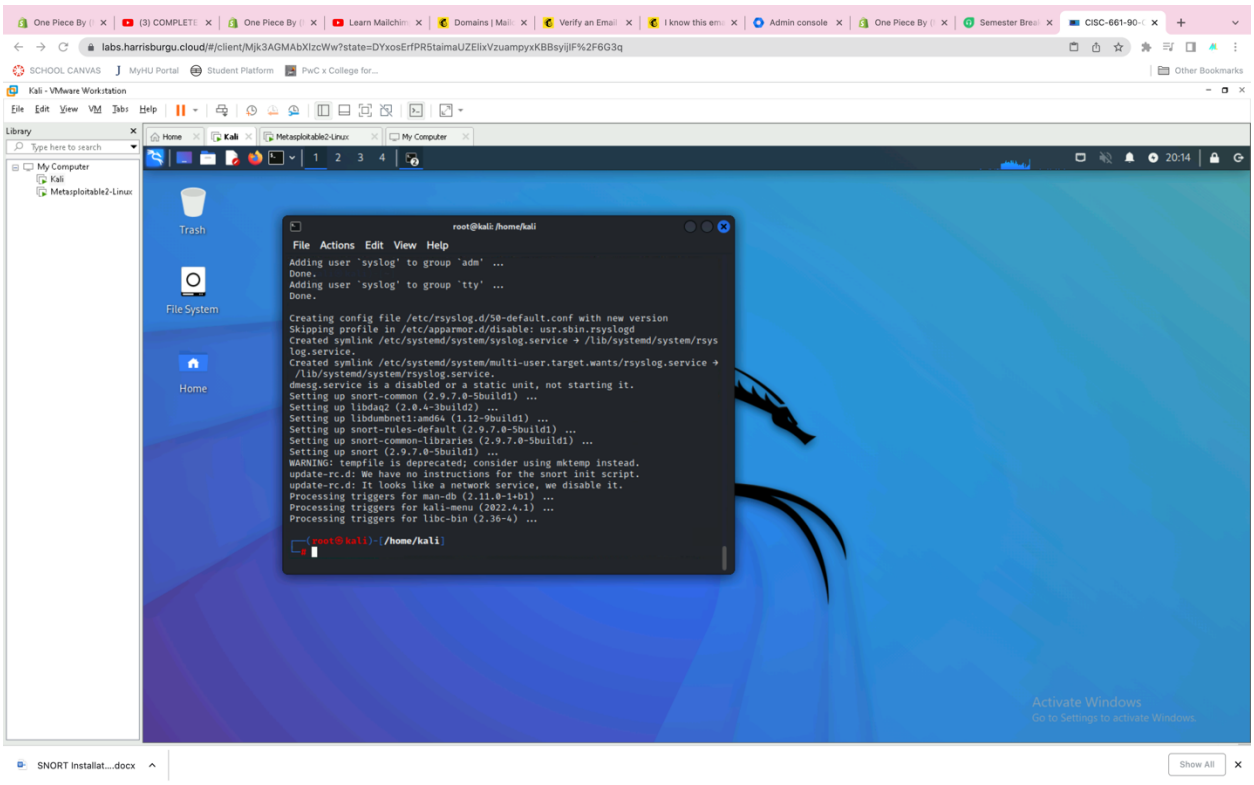


- Perform apt install snort.
- Change default network to local network

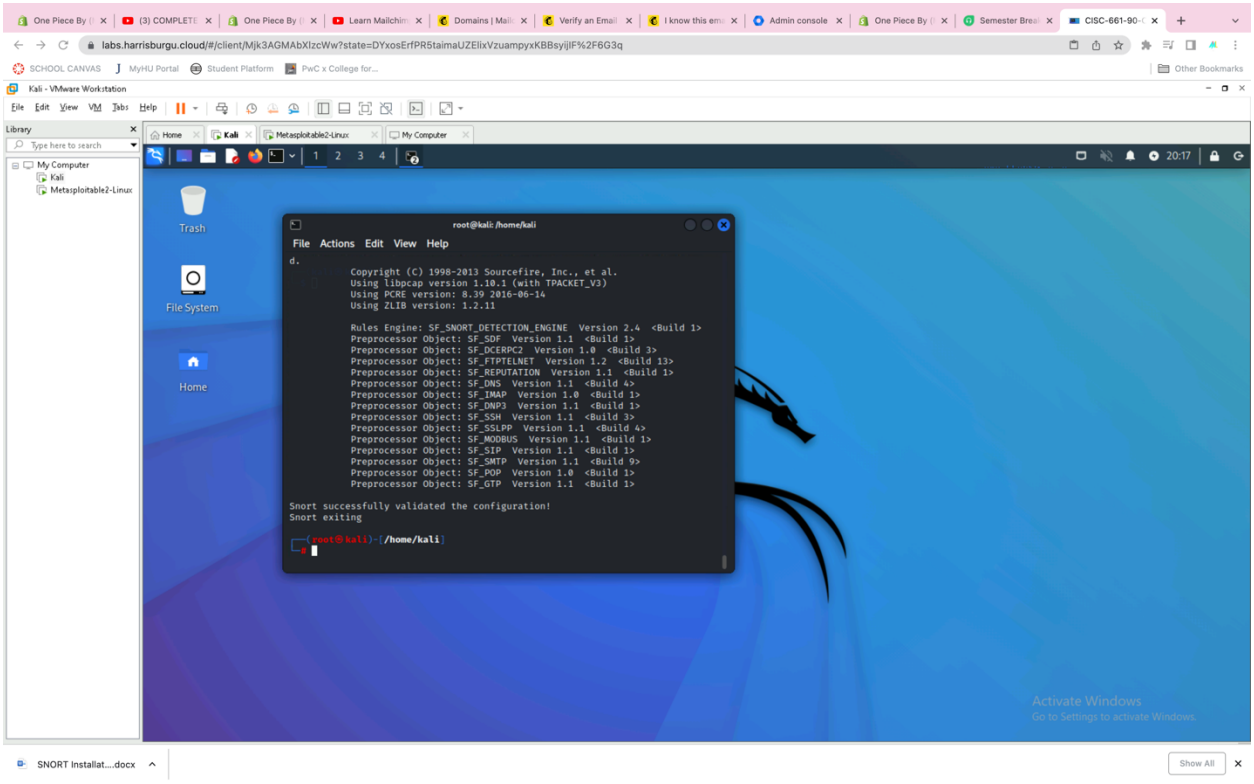


Step 4

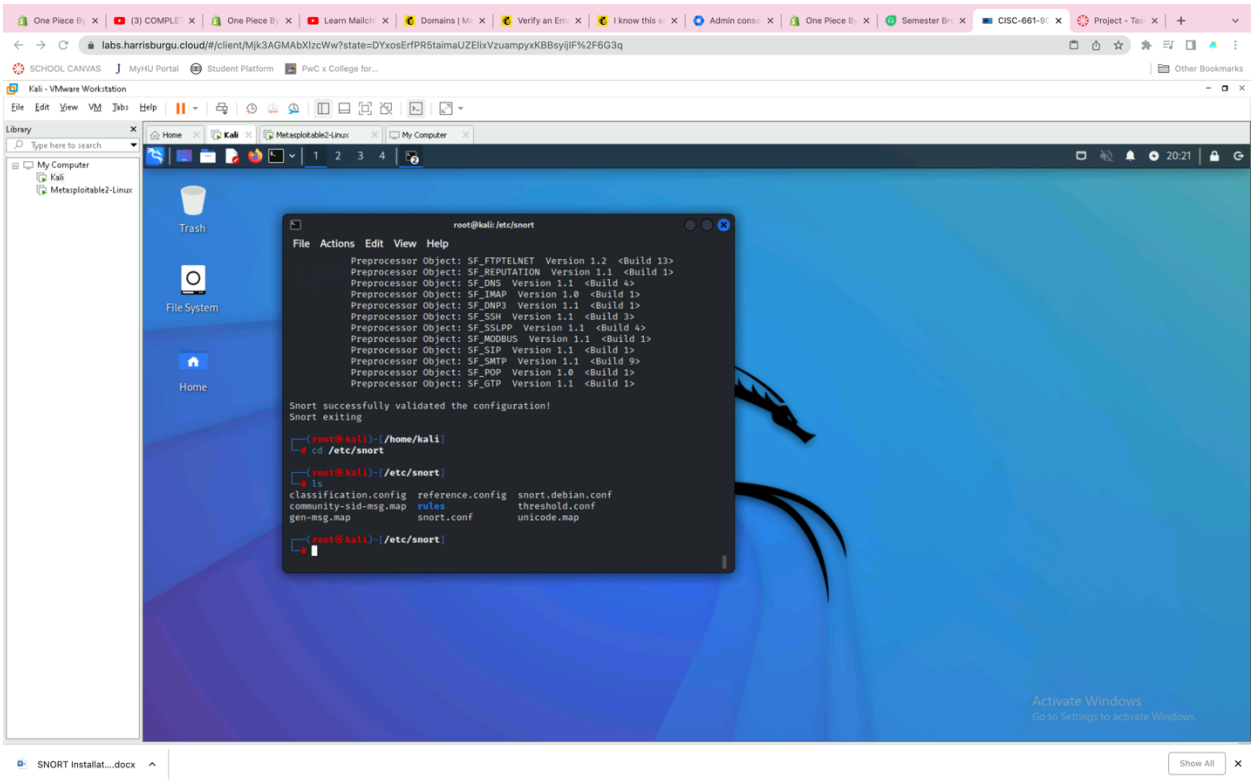
- Move sources file back to original file by overwriting.
- Test configuration



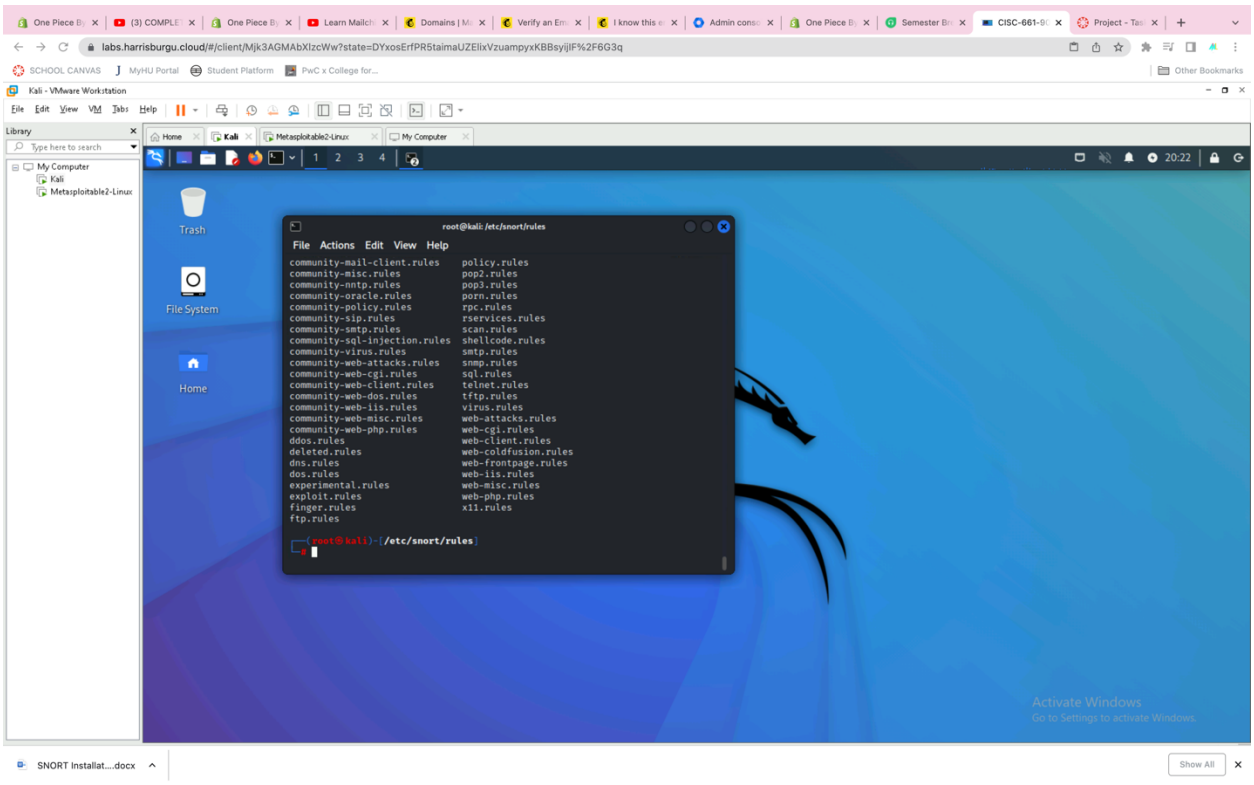
- Access directory where Snort is deployed.

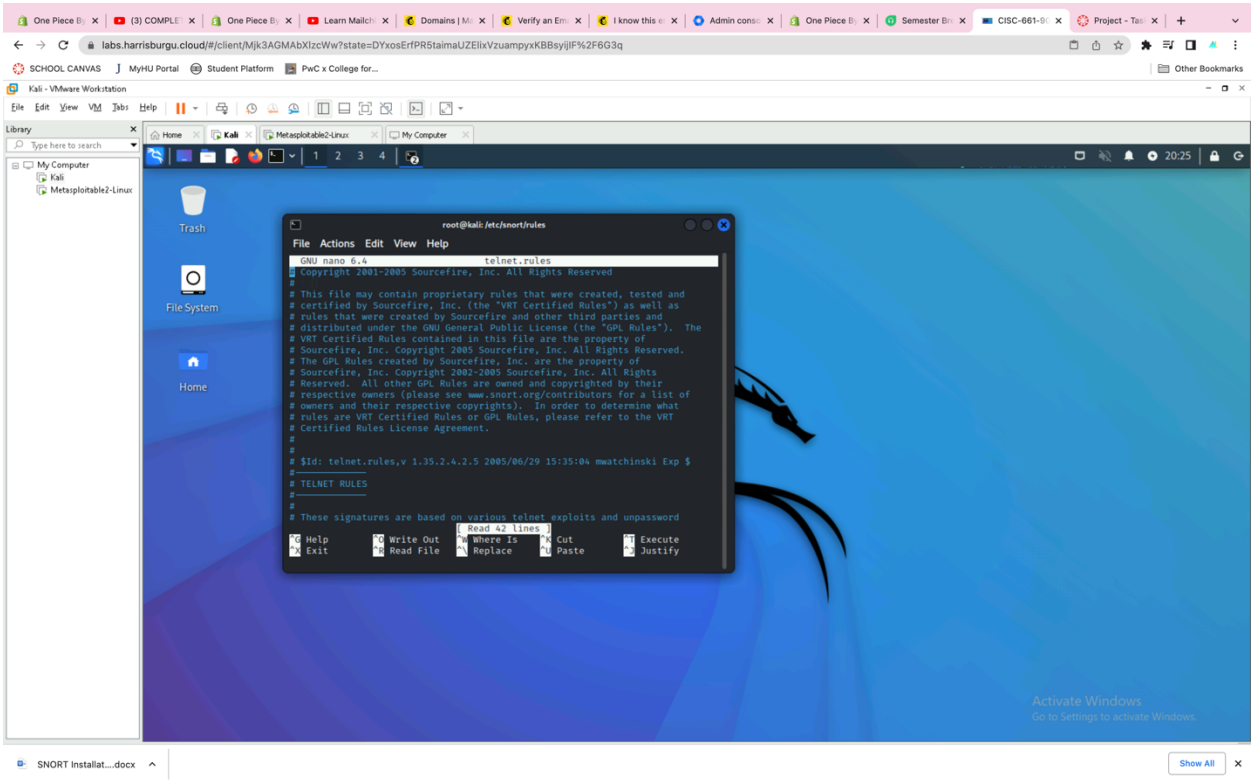


- Access rules file

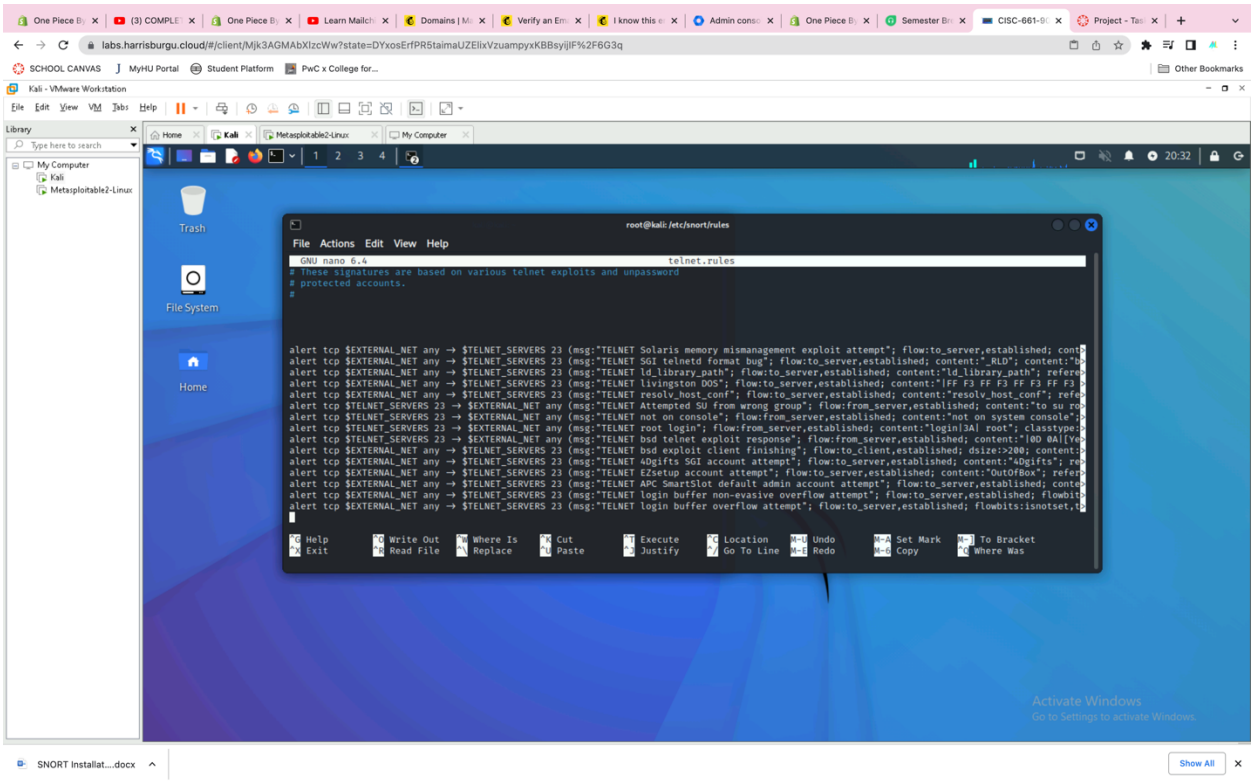


- Create syntax to detect activity using “telnet.rules”

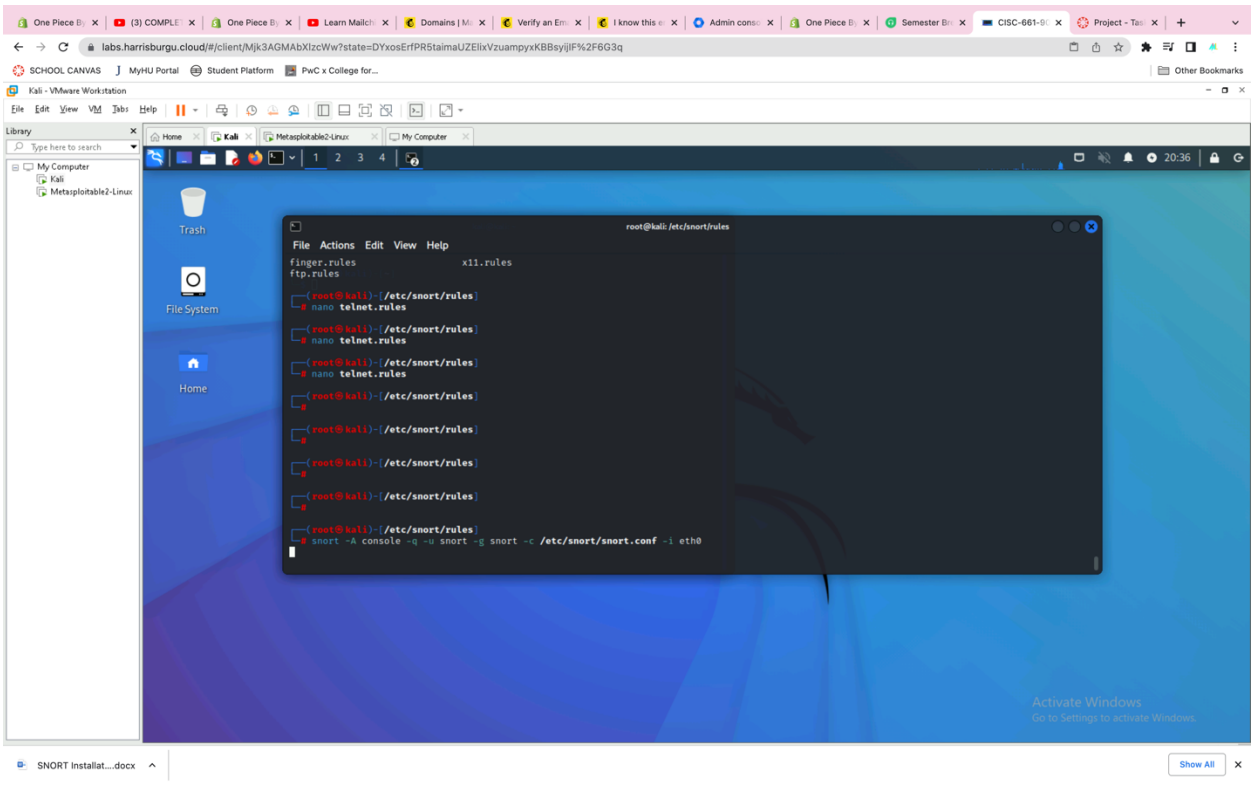

labs.harrisburgu.cloud/#/client/Mjk3AGMAbXlzcWw?state=DYxosErfPR5taimaUZElixVzuampyxKBBsyijlF%2F6G3q
Kali - VMware Workstation
root@kali: /etc/snort/rules
File Actions Edit View Help
community-mail-client.rules
community-misc.rules
community-nntp.rules
community-oracle.rules
community-policy.rules
community-sip.rules
community-smtp.rules
community-sql-injection.rules
community-virus.rules
community-web-attacks.rules
community-web-cgi.rules
community-web-client.rules
community-web-dos.rules
community-web-iis.rules
community-web-misc.rules
community-web-php.rules
ddos.rules
deleted.rules
dns.rules
dos.rules
experimental.rules
exploit.rules
finger.rules
ftp.rules
policy.rules
pop2.rules
pop3.rules
porn.rules
rpc.rules
rservices.rules
scan.rules
shellcode.rules
smtp.rules
snmp.rules
sql.rules
telnet.rules
tftp.rules
virus.rules
web-attacks.rules
web-cgi.rules
web-client.rules
web-coldfusion.rules
web-frontpage.rules
web-iis.rules
web-misc.rules
web-php.rules
x11.rules
(root㉿kali)-[/etc/snort/rules]
Trash
File System
Home
Activate Windows
SNORT Installat....docx
Show All


labs.harrisburgu.cloud/#/client/Mjk3AGMAbXlzcWw?state=DYxosErfPR5taimaUZElixVzuampyxKBBsyijlF%2F6G3q
Kali - VMware Workstation
root@kali: /etc/snort/rules
File Actions Edit View Help
GNU nano 6.4 telnet.rules
Copyright 2001-2005 Sourcefire, Inc. All Rights Reserved
#
This file may contain proprietary rules that were created, tested and
certified by Sourcefire, Inc. (the "VRT Certified Rules") as well as
rules that were created by Sourcefire and other third parties and
distributed under the GNU General Public License (the "GPL Rules"). The
VRT Certified Rules contained in this file are the property of
Sourcefire, Inc. Copyright 2005 Sourcefire, Inc. All Rights Reserved.
The GPL Rules created by Sourcefire, Inc. are the property of
Sourcefire, Inc. Copyright 2002-2005 Sourcefire, Inc. All Rights
Reserved. All other GPL Rules are owned and copyrighted by their
respective owners (please see www.snort.org/contributors for a list of
owners and their respective copyrights). In order to determine what
rules are VRT Certified Rules or GPL Rules, please refer to the VRT
Certified Rules License Agreement.
#
#
$Id: telnet.rules,v 1.35.2.4.2.5 2005/06/29 15:35:04 mwatchinski Exp $
#----------
TELNET RULES
#----------
#
These signatures are based on various telnet exploits and unpassword
[Read 42 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
Trash
File System
Home
Activate Windows
SNORT Installat....docx
Show All

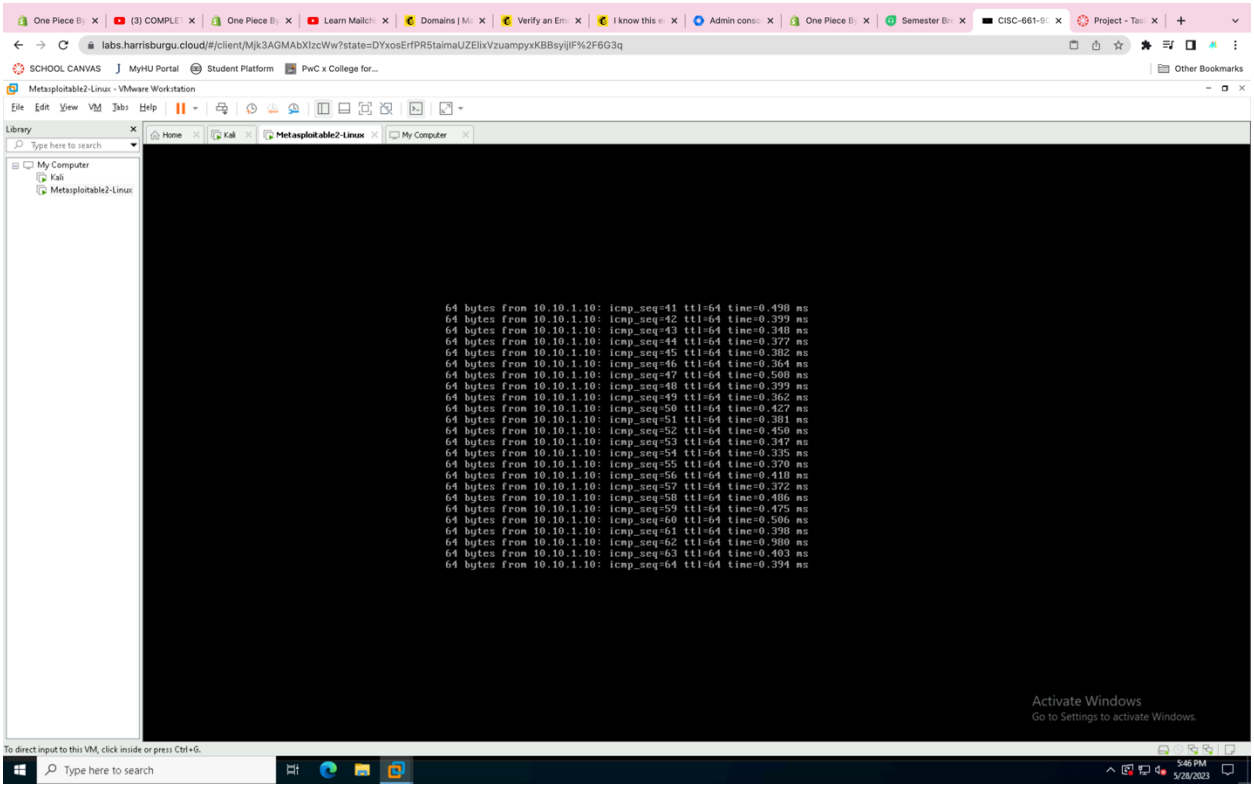
- Add command rule to alert tcp



- Start display information from detection on our screen.



- Ping 10.10.1.10 on Metasploitable



- Detection is then shown on Kali.