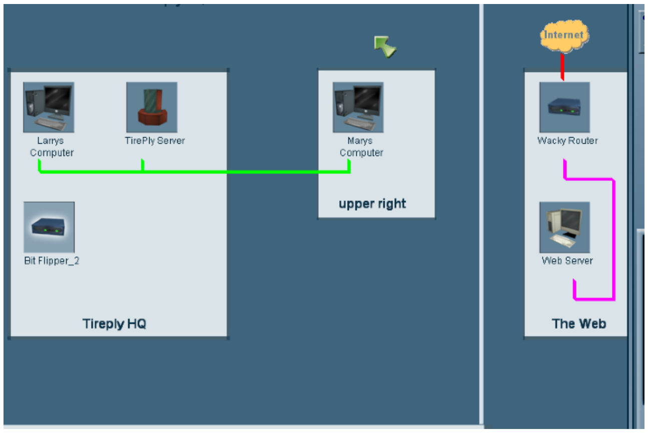
Lab 4 – ECE 1155 – Rayan Hassan – 4511021

Network security is a topic that is widely studied, as it involves every individual, company and organization in todays' world. Whenever we surf the internet, make a call or send an email, communication links are formed and requests are sent from a source to a destination. Every entity has an IP address and a port number that allows it to communicate with other entities. This communication is done through means like routers or servers. Naturally, the network is exposed to multiple threats that include interception, interruption and modification. To prevent attacks from happening, one must understand the functionalities and links present. In this lab, we will use CyberCIEGE to virtually monitor and play around with the network in a company. We will also filter packets sent between two machines and understand the concept of a firewall, which is a network security device that filters incoming and outgoing network traffic.

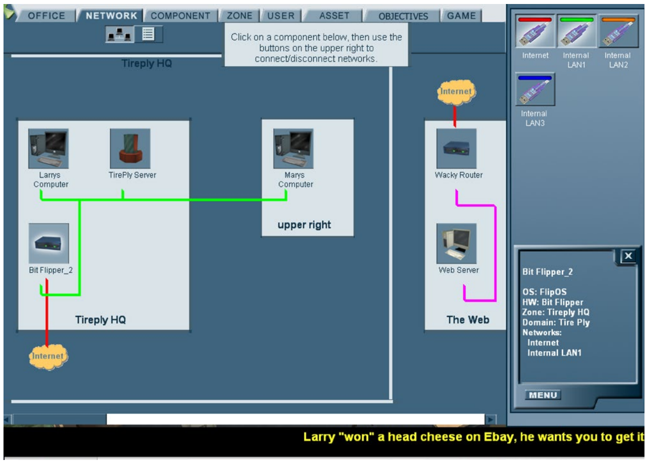
CyberCIEGE

Phase 1

In this part, we need to connect Larry to the internet. For that, I bought a router and connected it to the internet and to LAN1. This is the original "Network" tab, before any of that. We can see that Larry's computer is not connected to the internet.



Here is the same tab after the connection has been made.



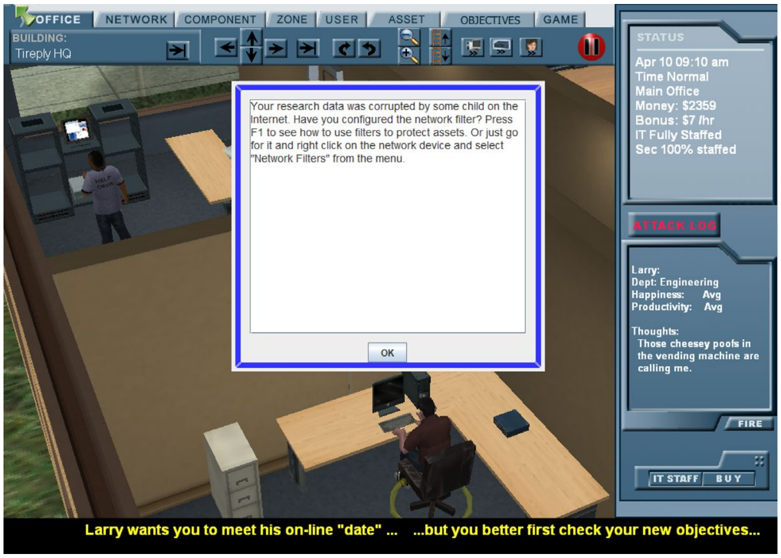
Click on a component below, then use the buttons on the upper right to connect/disconnect networks.

Bit Flipper_2

OS: FlipOS
HW: Bit Flipper
Zone: Tireply HQ
Domain: Tire Ply
Networks:
Internet
Internal LAN1

Larry "won" a head cheese on Ebay, he wants you to get it

After that we can see that Larry's happiness and productivity increased. What I expect to happen now is for Larry to be able to surf the internet and work. Also, I expect him to be exposed to attacks from the internet (maybe receiving spam emails, or corrupted links, etc…)



BUILDING: Tireply HQ

Your research data was corrupted by some child on the Internet. Have you configured the network filter? Press F1 to see how to use filters to protect assets. Or just go for it and right click on the network device and select "Network Filters" from the menu.

Apr 10 09:10 am
Time Normal
Main Office
Money: $2359
Bonus: $7 /hr
IT Fully Staffed
Sec 100% staffed

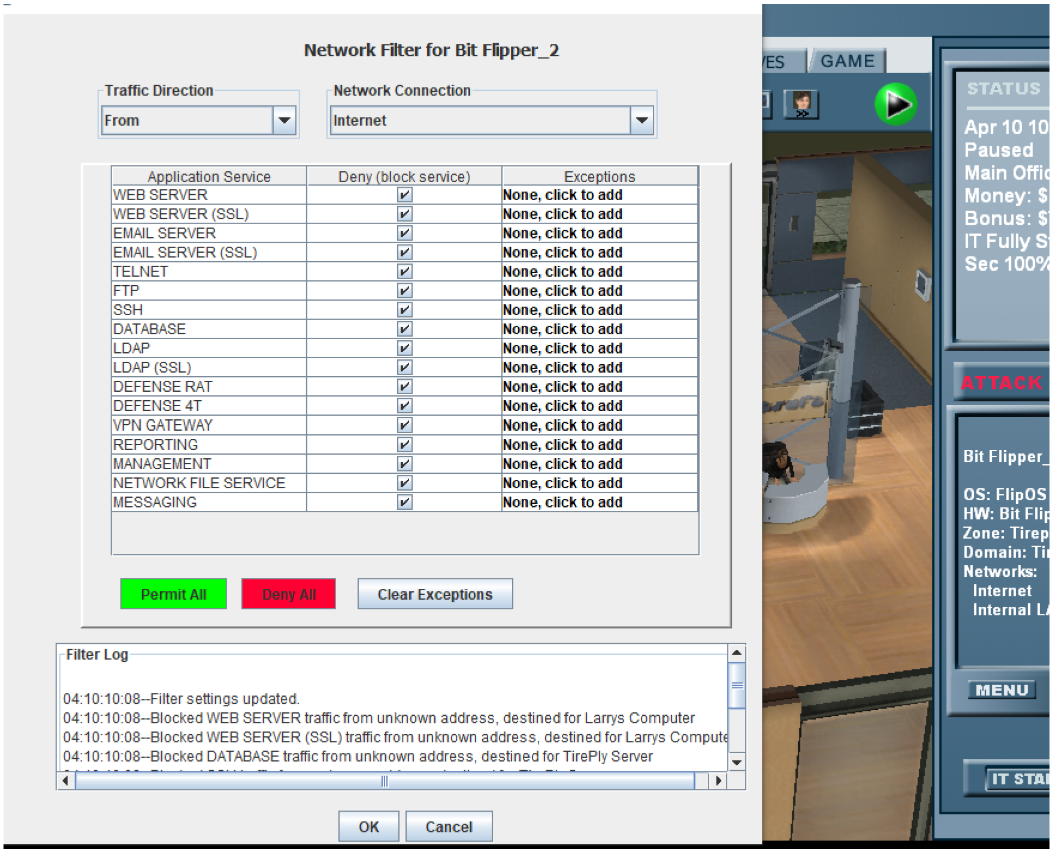
Larry:
Dept: Engineering
Happiness: Avg
Productivity: Avg

Thoughts:
Those cheesey poofs in the vending machine are calling me.

Larry wants you to meet his on-line "date" ... ...but you better first check your new objectives...

Phase 2

To restrict traffic coming from the internet, I configured the network filters, here is a screenshot:



Network Filter for Bit Flipper_2

Traffic Direction: From

Network Connection: Internet

Application Service	Deny (block service)	Exceptions
WEB SERVER	☑	None, click to add
WEB SERVER (SSL)	☑	None, click to add
EMAIL SERVER	☑	None, click to add
EMAIL SERVER (SSL)	☑	None, click to add
TELNET	☑	None, click to add
FTP	☑	None, click to add
SSH	☑	None, click to add
DATABASE	☑	None, click to add
LDAP	☑	None, click to add
LDAP (SSL)	☑	None, click to add
DEFENSE RAT	☑	None, click to add
DEFENSE 4T	☑	None, click to add
VPN GATEWAY	☑	None, click to add
REPORTING	☑	None, click to add
MANAGEMENT	☑	None, click to add
NETWORK FILE SERVICE	☑	None, click to add
MESSAGING	☑	None, click to add

Filter Log

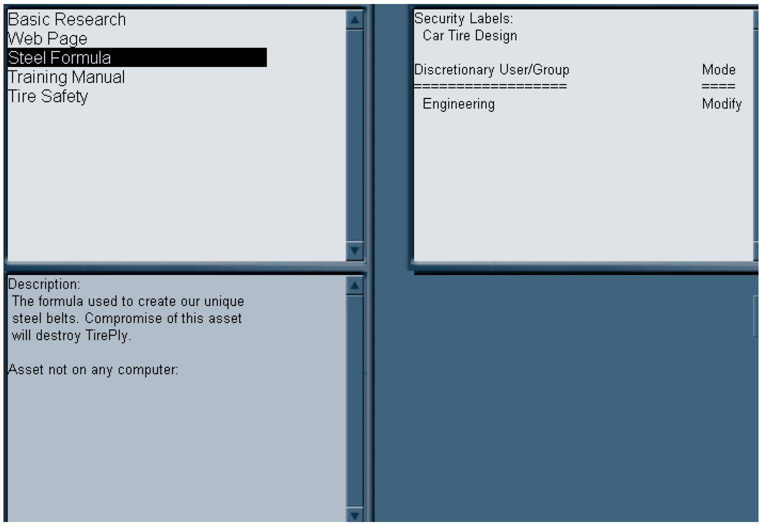
```
04:10:10:08--Filter settings updated.
04:10:10:08--Blocked WEB SERVER traffic from unknown address, destined for Larrys Computer
04:10:10:08--Blocked WEB SERVER (SSL) traffic from unknown address, destined for Larrys Compute
04:10:10:08--Blocked DATABASE traffic from unknown address, destined for TirePly Server
```

Apr 10 10
Paused
Main Offic
Money: $
Bonus: $
IT Fully S
Sec 100%

Bit Flipper_
OS: FlipOS
HW: Bit Flip
Zone: Tirep
Domain: Ti
Networks:
Internet
Internal L

Phase 3

Here is a screenshot that shows the value of the asset that is the steel formula



Basic Research
Web Page
Steel Formula
Training Manual
Tire Safety

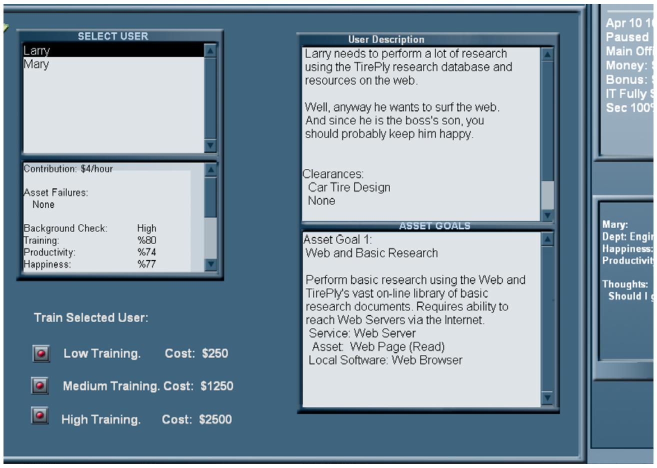
Security Labels:
Car Tire Design

```
Discretionary User/Group          Mode
==================                ====
 Engineering                      Modify
```

Description:
The formula used to create our unique steel belts. Compromise of this asset will destroy TirePly.

Asset not on any computer:

Here are screenshots showing users' descriptions:



Larry
Mary

Contribution: $4/hour

Asset Failures:
None

Background Check:	High
Training:	%80
Productivity:	%74
Happiness:	%77

Larry needs to perform a lot of research using the TirePly research database and resources on the web.

Well, anyway he wants to surf the web. And since he is the boss's son, you should probably keep him happy.

Clearances:
Car Tire Design
None

Asset Goal 1:
Web and Basic Research

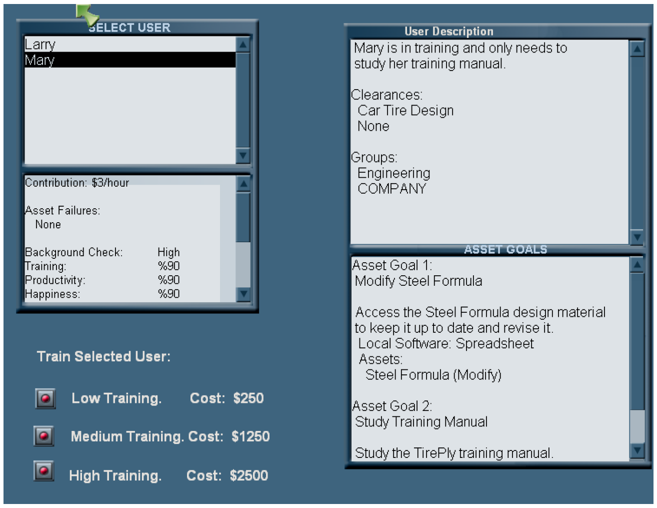
Perform basic research using the Web and TirePly's vast on-line library of basic research documents. Requires ability to reach Web Servers via the Internet.
Service: Web Server
Asset: Web Page (Read)
Local Software: Web Browser

Train Selected User:

○ Low Training. Cost: $250

○ Medium Training. Cost: $1250

○ High Training. Cost: $2500



Larry
Mary

Contribution: $3/hour

Asset Failures:
None

Background Check:	High
Training:	%90
Productivity:	%90
Happiness:	%90

Mary is in training and only needs to study her training manual.

Clearances:
Car Tire Design
None

Groups:
Engineering
COMPANY

Asset Goal 1:
Modify Steel Formula

Access the Steel Formula design material to keep it up to date and revise it.
Local Software: Spreadsheet
Assets:
Steel Formula (Modify)

Asset Goal 2:
Study Training Manual

Study the TirePly training manual.

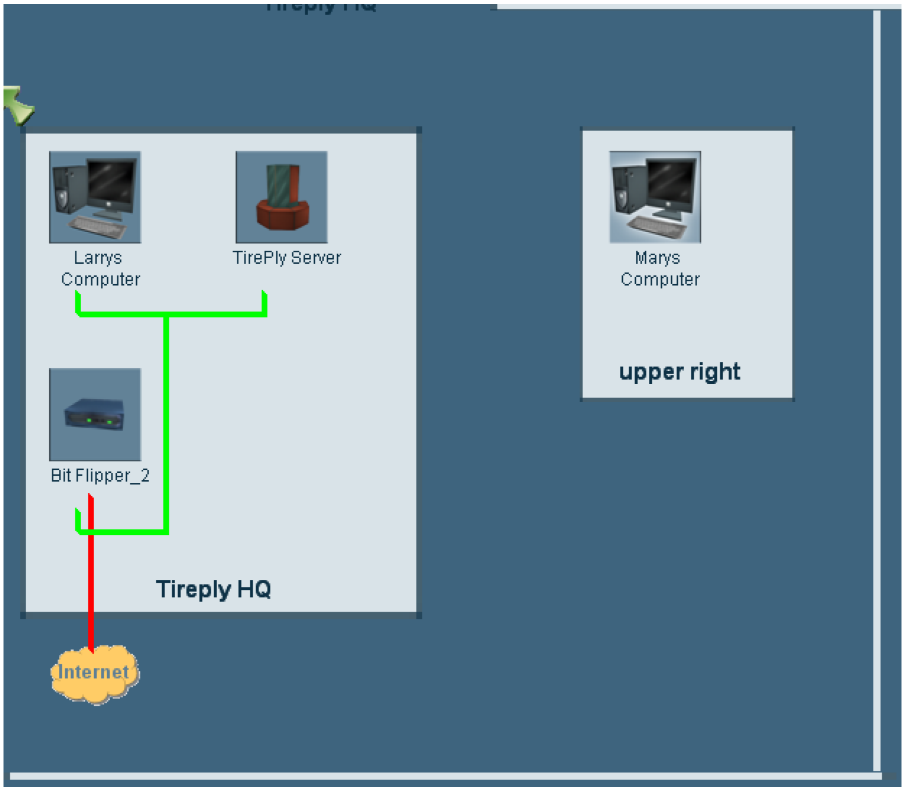
Train Selected User:

○ Low Training. Cost: $250

○ Medium Training. Cost: $1250

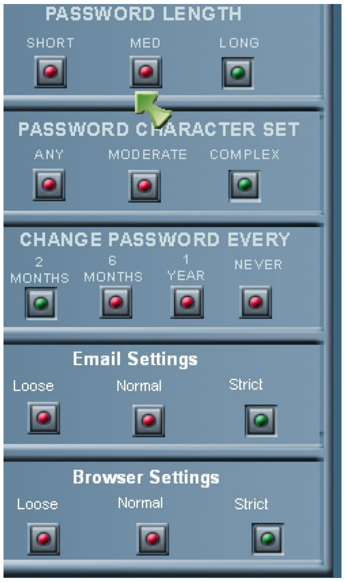
○ High Training. Cost: $2500

Mary needs access to the steel formula to work with it and modify it. Therefore, it makes sense to disconnect Marry from the network so that you avoid any threat on the formula.



Question 1:

I didn't think of that in the beginning, I tried to increase security by changing password length, character set properties, etc… just as shown below. Also, I tried to buy some stuff from the physical security tab. But I later realised that the solution is simply to disconnect Mary from the internet after many trials, to avoid any kind of threat or attack.



PASSWORD LENGTH

○ SHORT ○ MED ● LONG

PASSWORD CHARACTER SET

○ ANY ○ MODERATE ● COMPLEX

CHANGE PASSWORD EVERY

● 2 MONTHS ○ 6 MONTHS ○ 1 YEAR ○ NEVER

Email Settings

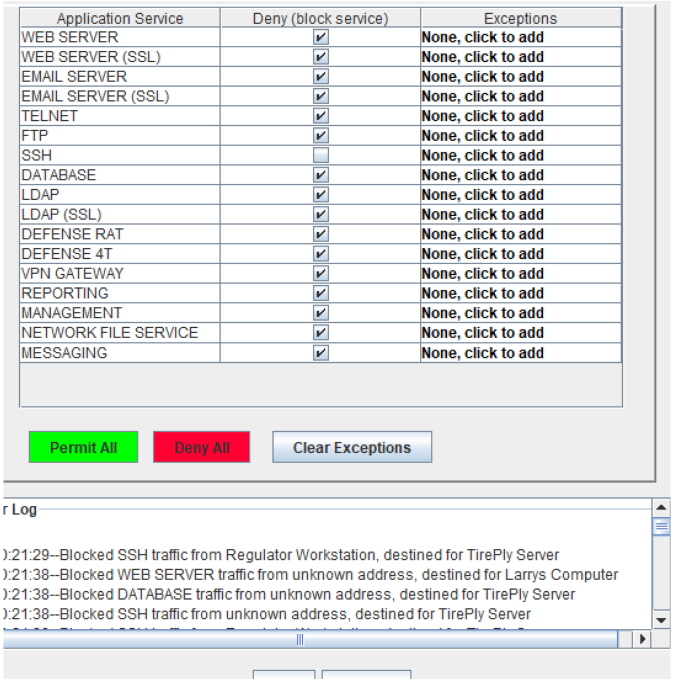
○ Loose ○ Normal ● Strict

Browser Settings

○ Loose ○ Normal ● Strict

Phase 4

To support offsite access to the service, we should allow SSH:



Application Service	Deny (block service)	Exceptions
WEB SERVER	☑	None, click to add
WEB SERVER (SSL)	☑	None, click to add
EMAIL SERVER	☑	None, click to add
EMAIL SERVER (SSL)	☑	None, click to add
TELNET	☑	None, click to add
FTP	☑	None, click to add
SSH	□	None, click to add
DATABASE	☑	None, click to add
LDAP	☑	None, click to add
LDAP (SSL)	☑	None, click to add
DEFENSE RAT	☑	None, click to add
DEFENSE 4T	☑	None, click to add
VPN GATEWAY	☑	None, click to add
REPORTING	☑	None, click to add
MANAGEMENT	☑	None, click to add
NETWORK FILE SERVICE	☑	None, click to add
MESSAGING	☑	None, click to add

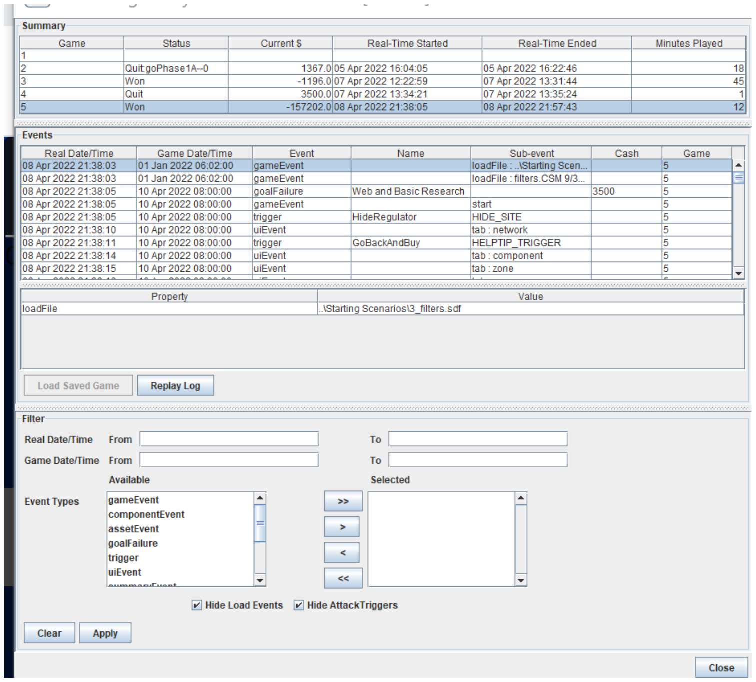
r Log

```
):21:29--Blocked SSH traffic from Regulator Workstation, destined for TirePly Server
):21:38--Blocked WEB SERVER traffic from unknown address, destined for Larrys Computer
):21:38--Blocked DATABASE traffic from unknown address, destined for TirePly Server
):21:38--Blocked SSH traffic from unknown address, destined for TirePly Server
```

Question 2:

SSH (Secure Shell) is a network protocol that allows two devices to communicate, so it makes sense to allow it for that particular situation.

Here is a screenshot of my event log analyser:



Summary

Game	Status	Current $	Real-Time Started	Real-Time Ended	Minutes Played
1					
2	Quit:goPhase1A--0	1367.0	05 Apr 2022 16:04:05	05 Apr 2022 16:22:46	18
3	Won	-1196.0	07 Apr 2022 12:22:59	07 Apr 2022 13:31:44	45
4	Quit	3500.0	07 Apr 2022 13:34:21	07 Apr 2022 13:35:24	1
5	Won	-157202.0	08 Apr 2022 21:38:05	08 Apr 2022 21:57:43	12

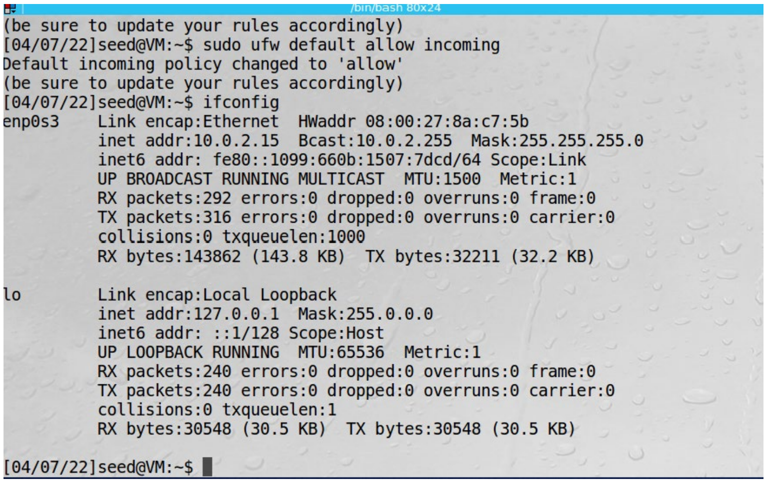
Events

Real Date/Time	Game Date/Time	Event	Name	Sub-event	Cash	Game
08 Apr 2022 21:38:03	01 Jan 2022 06:02:00	gameEvent		loadFile : ..\Starting Scen...		5
08 Apr 2022 21:38:03	01 Jan 2022 06:02:00	gameEvent		loadFile : filters.CSM 9/3...		5
08 Apr 2022 21:38:05	10 Apr 2022 08:00:00	goalFailure	Web and Basic Research		3500	5
08 Apr 2022 21:38:05	10 Apr 2022 08:00:00	gameEvent		start		5
08 Apr 2022 21:38:05	10 Apr 2022 08:00:00	trigger	HideRegulator	HIDE_SITE		5
08 Apr 2022 21:38:10	10 Apr 2022 08:00:00	uiEvent		tab : network		5
08 Apr 2022 21:38:11	10 Apr 2022 08:00:00	trigger	GoBackAndBuy	HELPTIP_TRIGGER		5
08 Apr 2022 21:38:14	10 Apr 2022 08:00:00	uiEvent		tab : component		5
08 Apr 2022 21:38:15	10 Apr 2022 08:00:00	uiEvent		tab : zone		5

Property	Value
loadFile	..\Starting Scenarios\3_filters.sdf

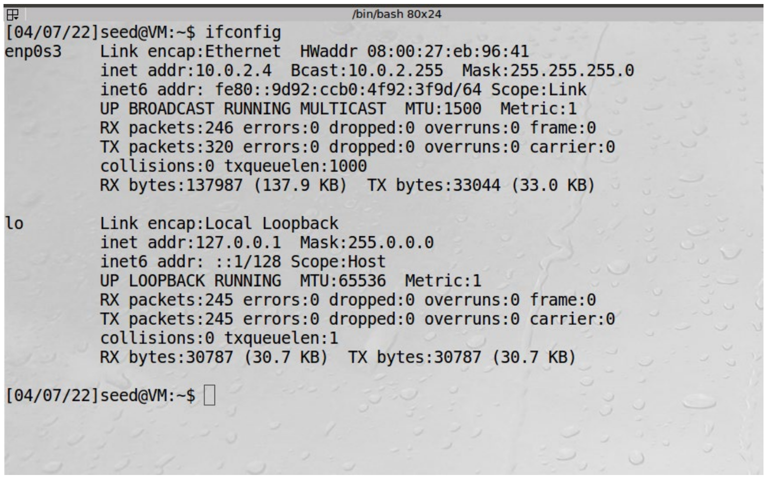
Firewall Seed Lab

1) Here is the command window on Machine A. I got the IP address which is 10.0.2.15



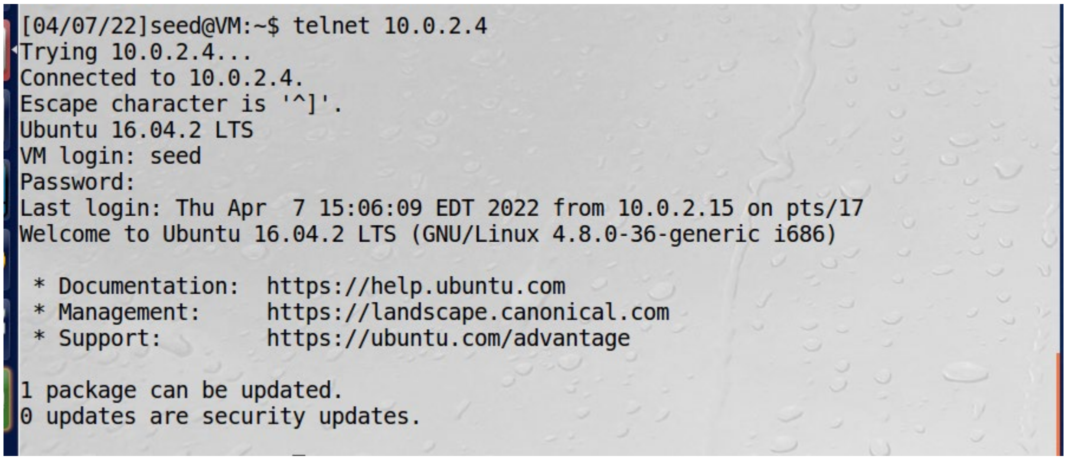
```
(be sure to update your rules accordingly)
[04/07/22]seed@VM:~$ sudo ufw default allow incoming
Default incoming policy changed to 'allow'
(be sure to update your rules accordingly)
[04/07/22]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:8a:c7:5b
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::1099:660b:1507:7dcd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:292 errors:0 dropped:0 overruns:0 frame:0
          TX packets:316 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:143862 (143.8 KB)  TX bytes:32211 (32.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:240 errors:0 dropped:0 overruns:0 frame:0
          TX packets:240 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:30548 (30.5 KB)  TX bytes:30548 (30.5 KB)

[04/07/22]seed@VM:~$ 
```

Here is the command window on Machine B. The IP address is 10.0.2.4



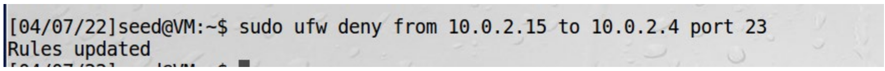
```
[04/07/22]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:eb:96:41
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::9d92:ccb0:4f92:3f9d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:246 errors:0 dropped:0 overruns:0 frame:0
          TX packets:320 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:137987 (137.9 KB)  TX bytes:33044 (33.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:245 errors:0 dropped:0 overruns:0 frame:0
          TX packets:245 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:30787 (30.7 KB)  TX bytes:30787 (30.7 KB)

[04/07/22]seed@VM:~$ 
```

2) Here is how I started a telnet connection from Machine A to Machine B. The screenshot shows terminator in Machine A



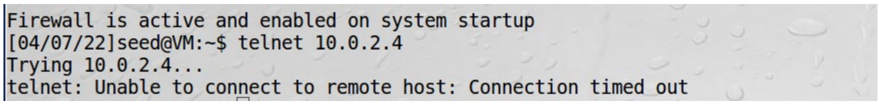
```
[04/07/22]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Apr  7 15:06:09 EDT 2022 from 10.0.2.15 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.
```

3) a) To prevent machine A to do telnet to machine B, I wrote the following command in terminator of Machine B:



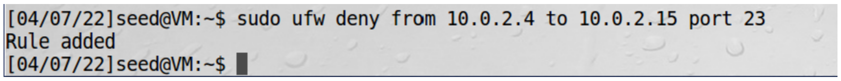
```
[04/07/22]seed@VM:~$ sudo ufw deny from 10.0.2.15 to 10.0.2.4 port 23
Rules updated
```

To check, I went to Machine A and tried to connect it (telnet) to Machine B, it wasn't able to do that, as shown below



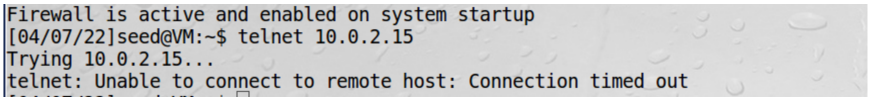
```
Firewall is active and enabled on system startup
[04/07/22]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
telnet: Unable to connect to remote host: Connection timed out
```

b) To prevent machine B to do telnet to machine A, I wrote the following command in the terminator of Machine A:



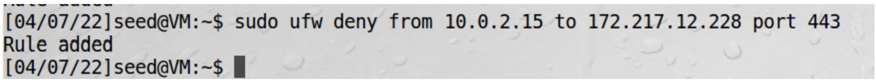
```
[04/07/22]seed@VM:~$ sudo ufw deny from 10.0.2.4 to 10.0.2.15 port 23
Rule added
[04/07/22]seed@VM:~$ █
```

To check, I went to Machine B and verified in the same way that it can't connect to A.



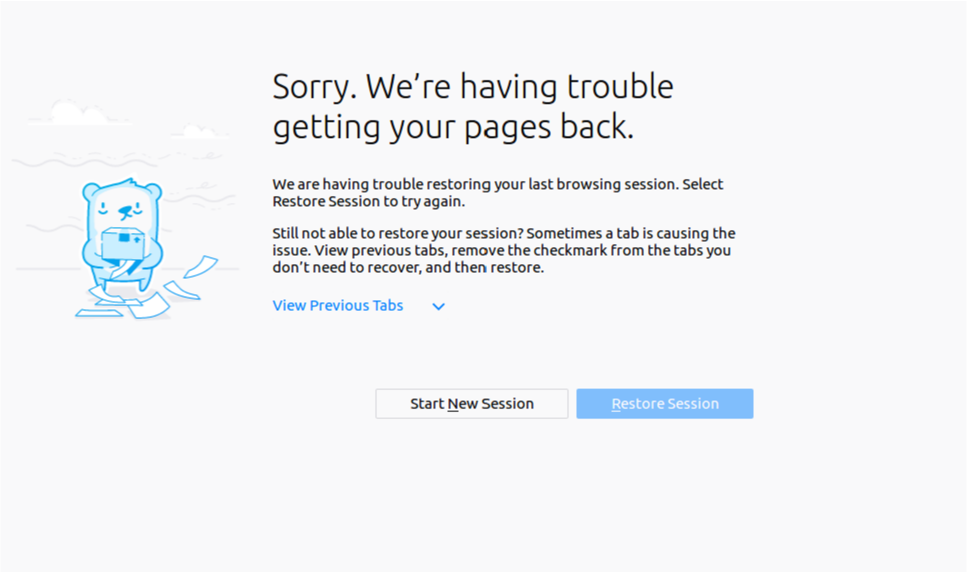
```
Firewall is active and enabled on system startup
[04/07/22]seed@VM:~$ telnet 10.0.2.15
Trying 10.0.2.15...
telnet: Unable to connect to remote host: Connection timed out
```

c) I decided to block google. The IP address is 172.217.12.228 and the port number is 443. Here is a screenshot of the command I used in Machine A:



```
[04/07/22]seed@VM:~$ sudo ufw deny from 10.0.2.15 to 172.217.12.228 port 443
Rule added
[04/07/22]seed@VM:~$ █
```

To check, I simply opened Firefox, and I wasn't able to connect to Google, as shown below



Sorry. We're having trouble getting your pages back.

We are having trouble restoring your last browsing session. Select Restore Session to try again.

Still not able to restore your session? Sometimes a tab is causing the issue. View previous tabs, remove the checkmark from the tabs you don't need to recover, and then restore.

In conclusion, we got to see how the moment we are connected to the Internet, threats can come in our way. Also, we modified network filters to satisfy our needs. For Mary, we had to absolutely secure the working on the Steel formula, and therefore learned that disconnecting her from the internet is the best solution, because even if we improve security (passwords, etc…), she is still exposed to a great deal of threats. On the other hand, we got to see how entities communicate with each other using their IP address and port numbers. We got to establish a connection, block it, and also block a connection to an actual website which was Google in my case.