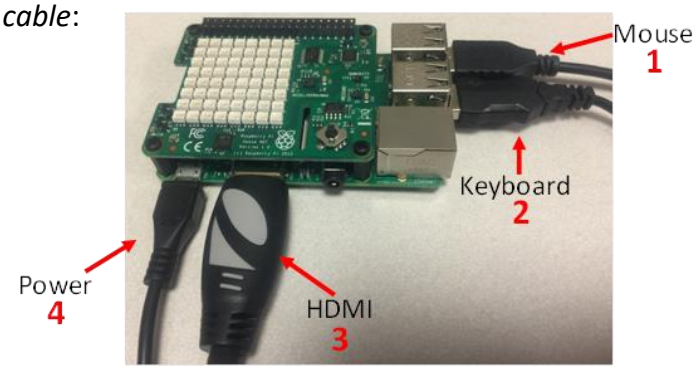
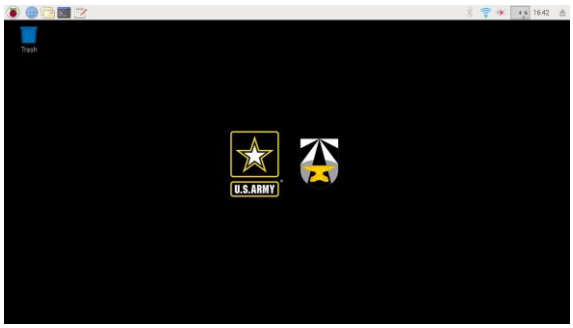
Man-In-The-Middle (MITM) Worksheet

Step 1 – Identify the ***Raspberry Pi*** labeled "***HACKER***". Connect the 1) *mouse*, 2) *keyboard*, 3) *HDMI cable* and **at the end** the 4) *power cable*:

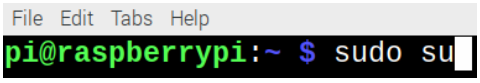


Step 2 – The ***Raspberry Pi*** will boot up. Please wait until you see the "***U.S. ARMY***" and "***AFC***" logos on your *Desktop*:

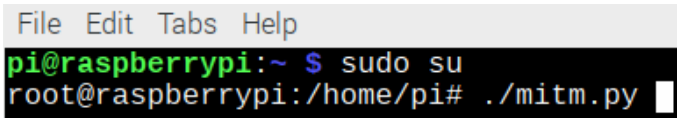


Step 3 – Open a ***Terminal Window***, by doing a single **left-click** on the icon shown below:

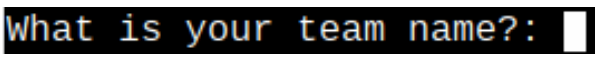
Step 4 – Inside the ***Terminal Window***, you will be typing several commands. **Do NOT forget** to press "**Enter**" or "**Intro**" in your keyboard after typing each command. The first command will give you ***Administrator Privileges***. Please type: **sudo su**



Step 5 – Type the following instruction: **./mitm.py**



Step 6 – Please choose a ***NAME*** for your ***TEAM*** and type it when asked:



Step 7 – Please provide your names and email addresses when asked, we will email you a ***Certificate of Completion*** (**Note:** You must type your email addresses twice to confirm. If at the end of the workshop, you do **NOT** receive your ***Certificate of Completion***, email us to **salvador.melendez3.civ@army.mil**):

```
At the end of this workshop, you will get an email with a certificate of participation!
Please enter the e-mail address of each of the team members (one by one):

How many members in your team? <-- Enter number of team members (for example: 2)
Name of team member #1: <-- Name of team member #1
Email address of team member #1:
Confirm Email address of team member #1: <-- Email address of team member #1 (two times)
Name of team member #2: <-- Name of team member #2
Email address of team member #2:
Confirm Email address of team member #2: <-- Email address of team member #2 (two times)
```

Step 8 – When prompted, type the following IP address: **192.168.11.1**

```
What is your IP address?
192.168.11.1
```

Step 9 – Type the following command to get your IP address: **ifconfig eth0**

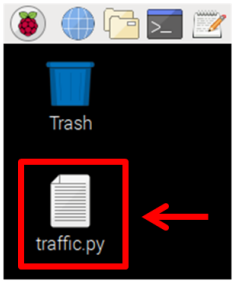
```
Enter the command to get your IP address: ifconfig eth0
```

Step 10 – This should be the output on your screen:

```
Enter the command to get your IP address: ifconfig eth0
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.11.1  netmask 255.255.255.0  broadcast 192.168.11.255
        ether b8:27:eb:49:4f:b6  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

Please press ENTER to continue...
```

Step 11 – Press "**Enter**" or "**Intro**" in your keyboard to continue, and start answering the questions to create a "**Man-In-The-Middle**" program that will scan the network for unsecured communications.

Note: If all questions were answered correctly, you should see a file on your *Desktop* called: "traffic.py"



Step 12 – The command used to reboot the Raspberry Pi is: **reboot**

Step 13 – After the **system reboots**, open a ***Terminal Window***, by doing a single **left-click** on the icon shown below:

Step 14 – Inside the ***Terminal Window***, type the following commands as shown in the image below. **Do NOT forget** to press "**Enter**" or "**Intro**" in your keyboard after typing each command:

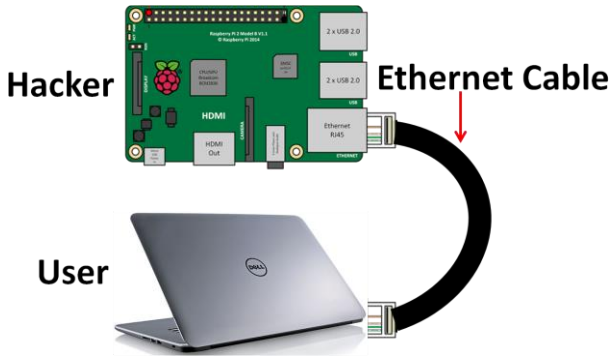
```
File  Edit  Tabs  Help
pi@raspberrypi:~ $ sudo su
root@raspberrypi:/home/pi# cd Desktop/
root@raspberrypi:/home/pi/Desktop# ./traffic.py
```

Step 15 – The **Network Scanner** will start and it will ask you to connect the ***Ethernet Cable***. At this point, please ***STOP*** working with the "***HACKER***" *Raspberry Pi* and continue with ***Step 16***.

```
**********NETWORK SCANNER**********
Loading configuration...

Connect the Ethernet cable and press ENTER...
```

Step 16 – Now, you will be using the "***USER***" (***Computer***). Please boot it up.

Step 17 – Connect the "***HACKER***" *Raspberry Pi* with the "***USER***" *Computer* using the ***Ethernet Cable***:



Step 18 – After connecting the ***Ethernet cable***, press "**Enter**" or "**Intro**" in your "***HACKER***" *Raspberry Pi*:

```
**********NETWORK SCANNER**********
Loading configuration...

Connect the Ethernet cable and press ENTER...
* |==================================================>| 100.00 %

Loading network scanner...

Waiting for credentials...
```

Step 19 – In your "***USER***" *Computer*, open a ***Terminal Window*** (Linux/iOS) or a ***Command Prompt*** (Windows).

Step 20 – Inside the ***Terminal Window*** (Linux/iOS) or ***Command Prompt*** (Windows), verify the ***ip address*** of the "***USER***" *Computer* by typing the following command:

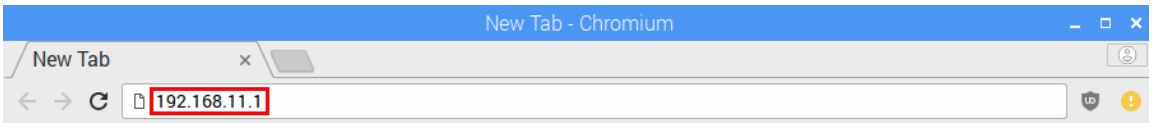
Linux/iOS → ***ifconfig eth0***

Windows → ***ipconfig***

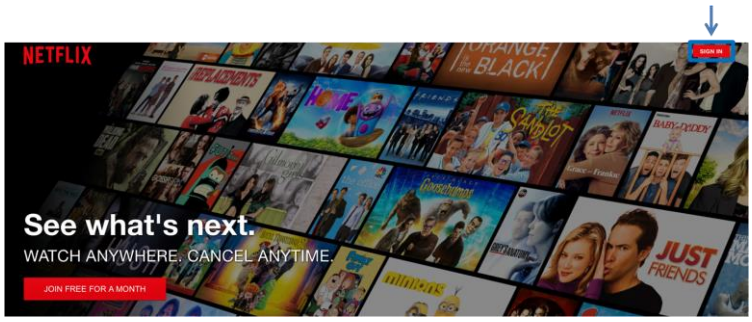
Note: The ***ip address*** should start with the following numbers: 192.168.11.**x** ← where "**x**" can be '2', '3', '4', '5' or '6'.

Step 21 – In your "***USER***" *Computer*, open a ***Web Browser***.

Step 22 – Inside the ***Web Browser***, type ***192.168.11.1*** in the address bar and press "**Enter**" or "**Intro**" in your keyboard:

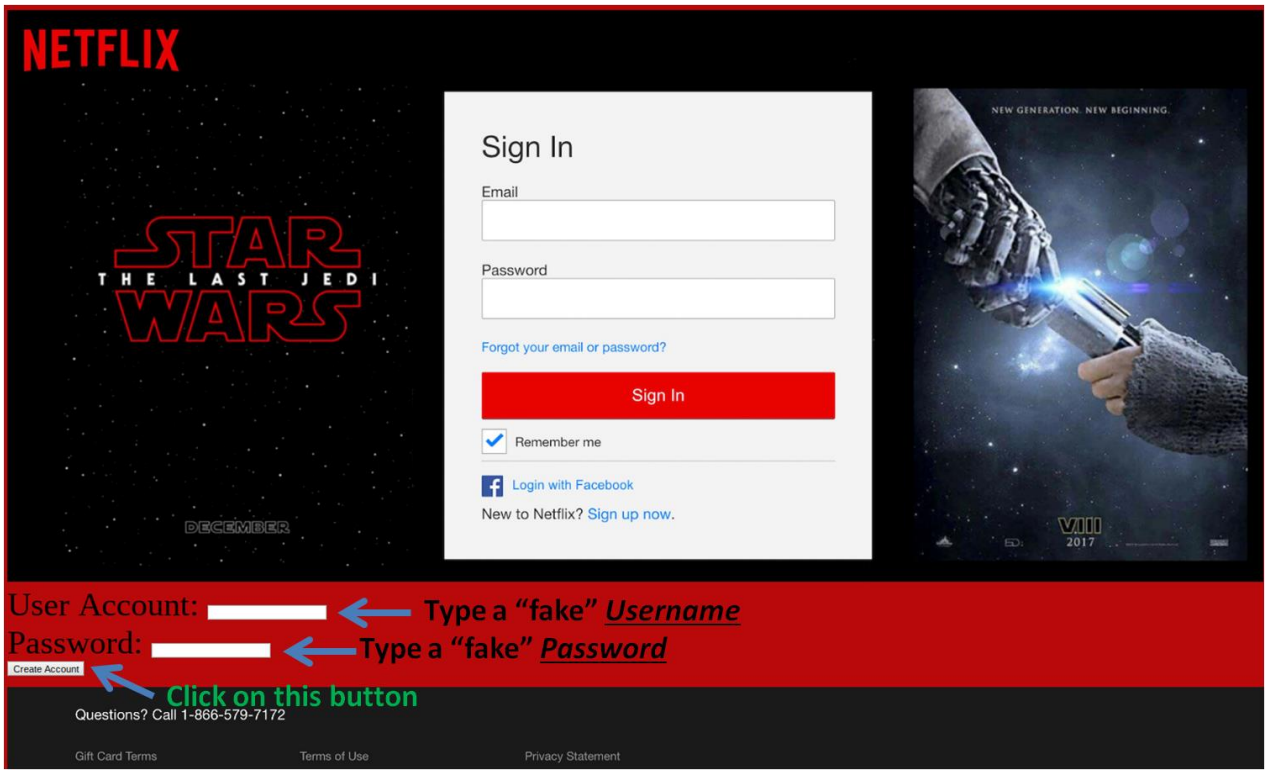


Step 23 – After the website is loaded, click on "***Sign In***" in the upper right corner:



Step 24 – Go to the bottom of the website and please type **any username and password you want** (***avoid*** typing **real usernames** and **passwords**) on the "***User Account***" and "***Password***" fields. Then click on the "***Create Account***" button.

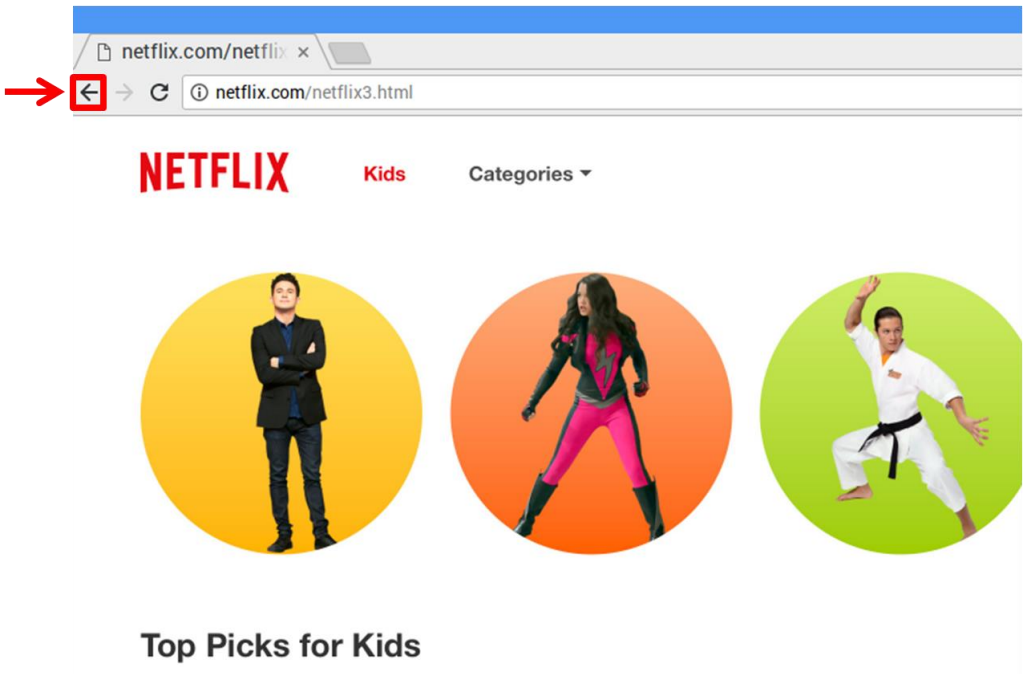
Note: After you click on the "***Create Account***" button, take a look at the ***SenseHat*** of the "***HACKER***" *Raspberry Pi*. You will see the ***User*** and ***Password*** you just typed in the "***USER***" *Computer*.



Step 25 – The ***Terminal Window*** of the "***HACKER***" *Raspberry Pi* will display the *users* and *passwords* you are capturing from the "***USER***" *Computer*:

```
**********NETWORK SCANNER**********
Loading configuration...

Connect the Ethernet cable and press ENTER...
* |================================================>| 100.00 %

Loading network scanner...

Waiting for credentials...

1 -->   User:
        Pass:
        Website: http://netflix.com/netflix2.html

2 -->   User: User1
        Pass: my_password1234
        Website: http://netflix.com/netflix2.html

3 -->   User: User2
        Pass: abcd1234
        Website: http://netflix.com/netflix2.html

4 -->   User: User3
        Pass: !@#$%^&*()_+
        Website: http://netflix.com/netflix2.html
```

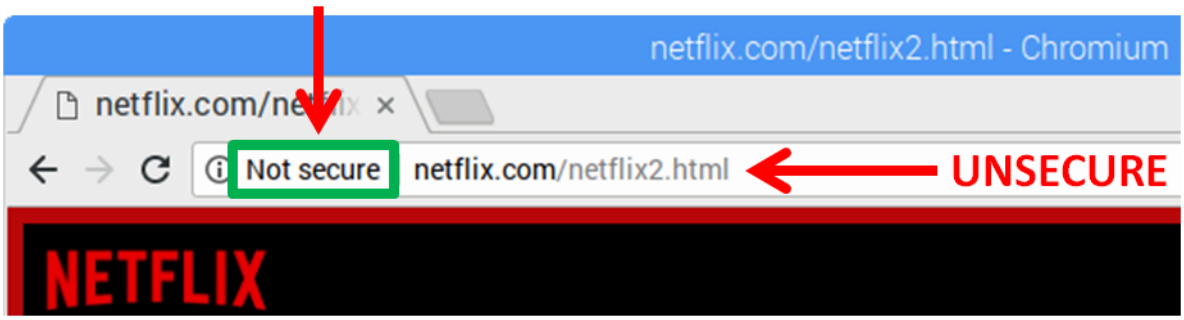
Step 26 – Click on the ***left arrow*** (as shown below) to go back to the previous page. You can try different *users* and *passwords* (**Step 24**):



Step 27 – **Congratulations!** You just created a "***Man-In-The-Middle***" device that can help you verify if your network connection is unsecure.

Note: When using the ***Internet*** and ***before*** you enter your ***personal information***, ***ALWAYS*** remember to check if the ***website address*** starts with "***https***", otherwise someone may be able to steal your information.

UNSECURE VERSION:



SECURE VERSION: