**CYBERSECURITY**

**CA2**

**TOPIC’s:**

1. **PHISHING**
2. **SEToolkit: By using pre available tools**

**b.Cloning a website**

1. **HONEYPOT**

**WEQAT FATIMA**

**18BIT046**

**PHISHING**

TOPICS CLEARED:

1. What is phishing?
2. How phishing works?
3. How to use phishing?
4. How to be safe from phishing?

What is phishing?

* Searching for products on the web browser, one web site is very popular, safe and a secured e commerce website while the other website Is not safe at all!
* Phishing is a technique of gathering sensitive information of a target such as username, password, etc., by disguising as a trustworthy entity.

How phishing works?

* Phishing is a web based application mainly used to steal credentials, every web app is connected to a web server. There are some data packets sent from the web app to the web server and vice versa, this is the communication.
* In phishing, attack the hacker disguises himself as the web server, and the user thinks that they are talking to the legitimate or a trustworthy web server, but they are not.

What must the hacker do?

1. Hacker creates a fake website.
2. Fake website is sent to the victim.
3. Victim thinks that the website is a trustworthy website and enters the credentials.
4. Hacker gets the credentials.

How to use phishing?

There are 2 ways:

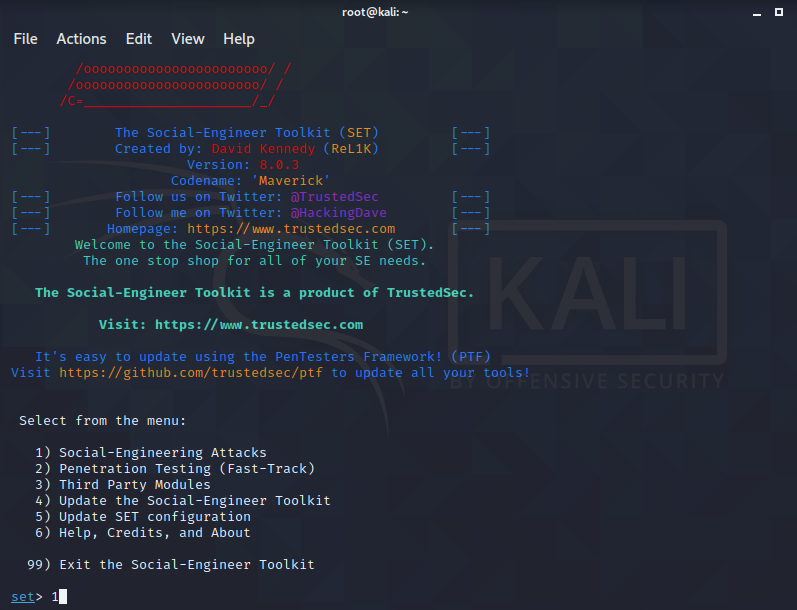
Using available site cloning tools: **SEtoolkit**, Weeman, SocialFish

* 1. Use pre available templates.
  2. Clone a website: We will create a phishing page of a web application that is not avail as a web template. For this select the 2nd option “clone a website”

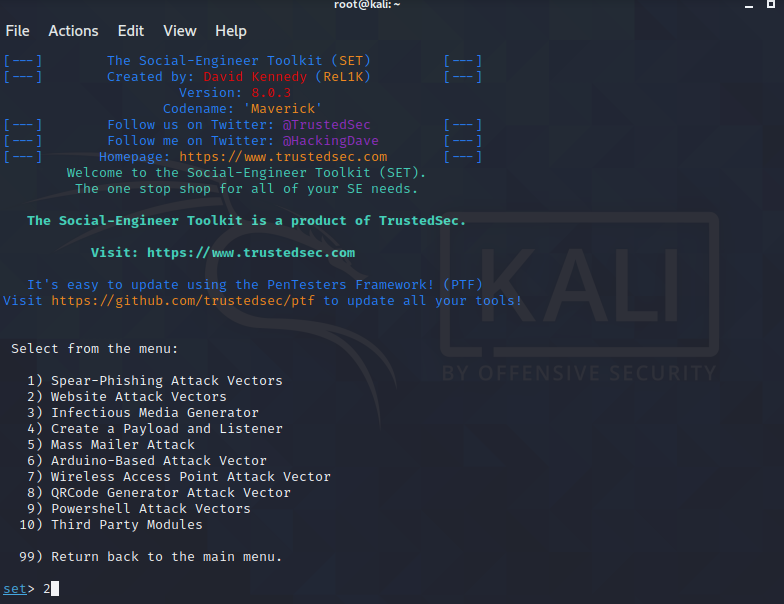
METHOD 1: A

Root:

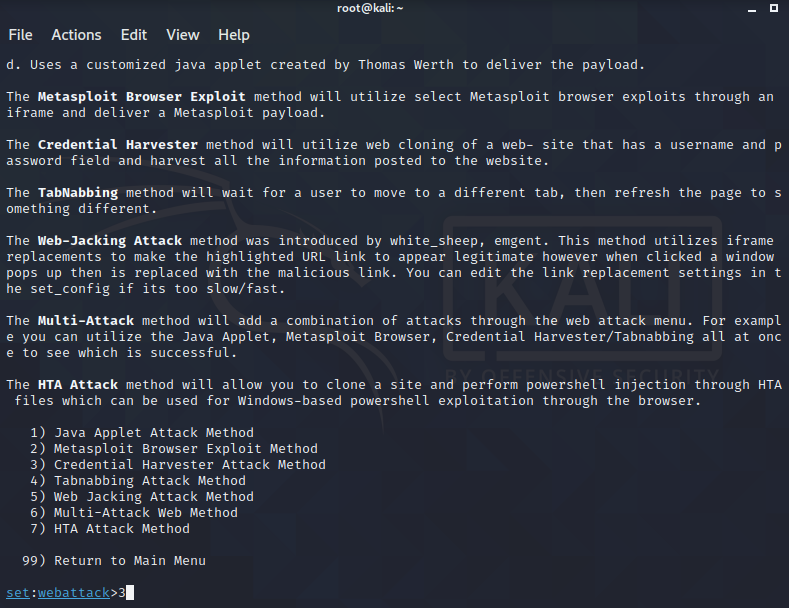
* Sudo –i
* Setoolkit



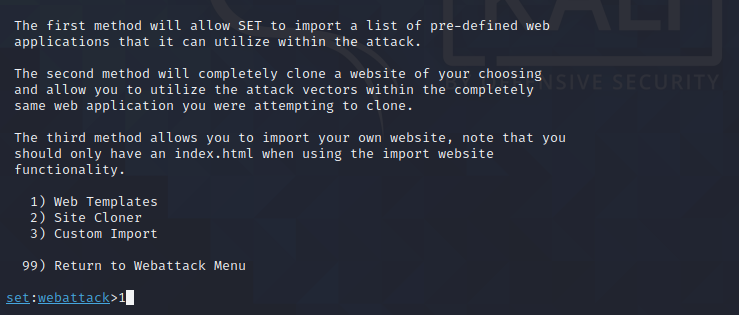
Select option 1: Social –Engineering Attacks



Select option 2: Website Attack Vectors



Select option 3: Credentials Harvester Attack Method because we are trying to steels the victims credentials.

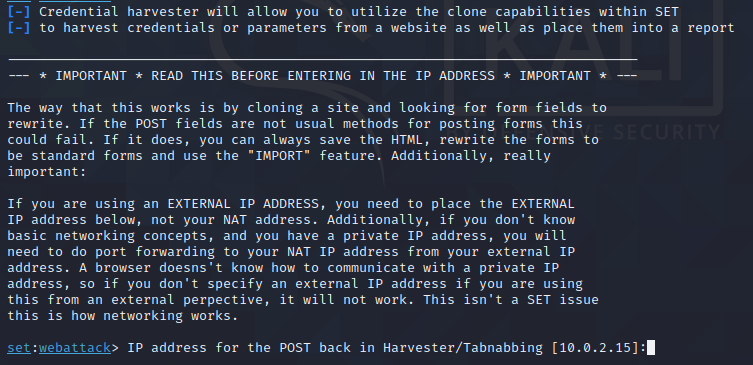


Select option 1: Web templates

Here we will create a fake phishing web page using pre available template.

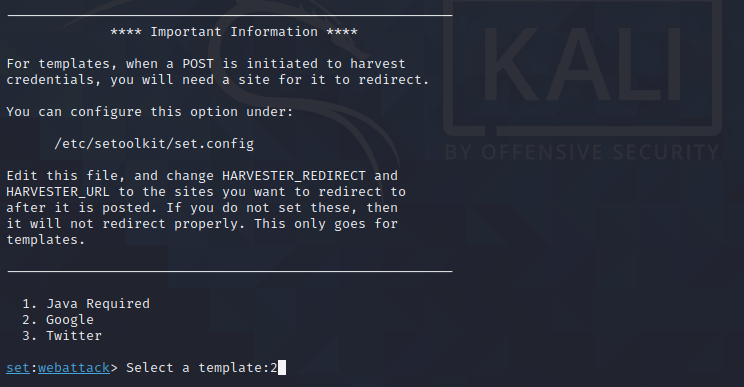
Now do the following:

1. Enter the IP address that the results of the phishing have to be returned to.



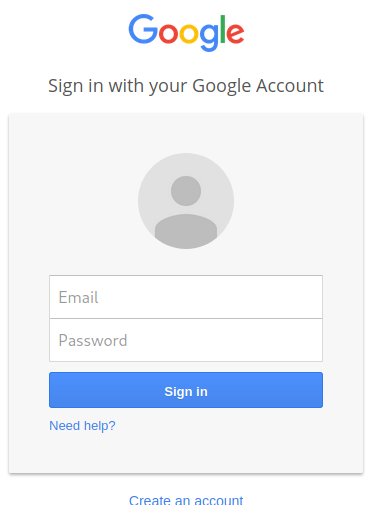
The ip address of my machine is 10.0.2.15 so I wont be making any changes and hit enter

Since we are creating a phishing page for Google so ill choose option 2: Google



Now the tool will run and create a web application or phishing web application, hit enter

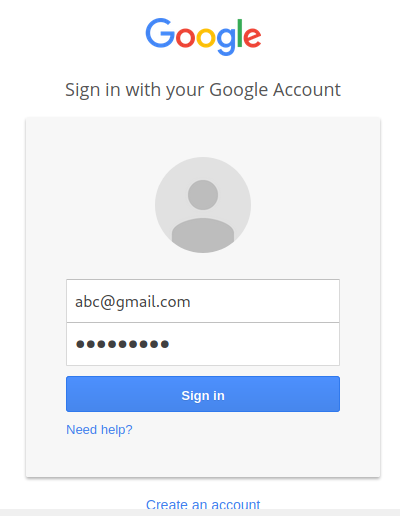
Now go to Mozilla Firefox and type “localhost” and hit enter

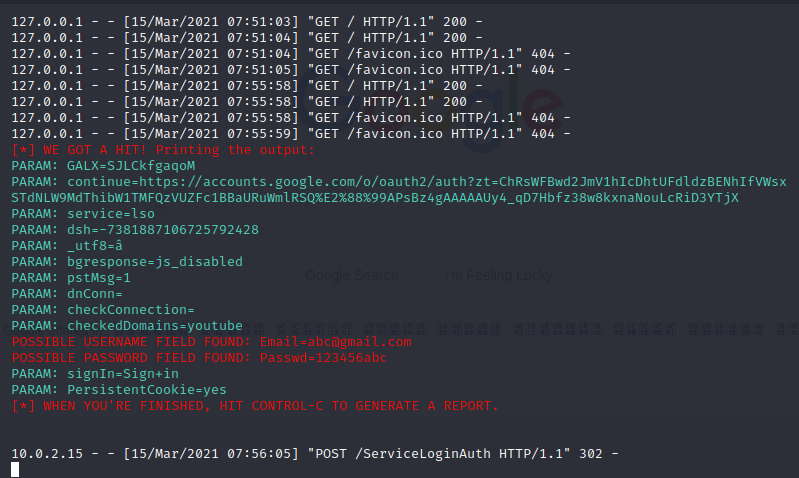


There is a Google login page, asking for an email id and a password, this is not the actual Google page because Google has a different URL.

Observe the terminal page, whatever the victim enters will be seen on the terminal.

After creating a fake phishing page, you have to send this page to the victim and when you send this page to your victim and the victim enters some details and some password and when he hits the enter button🡪 observe the terminal



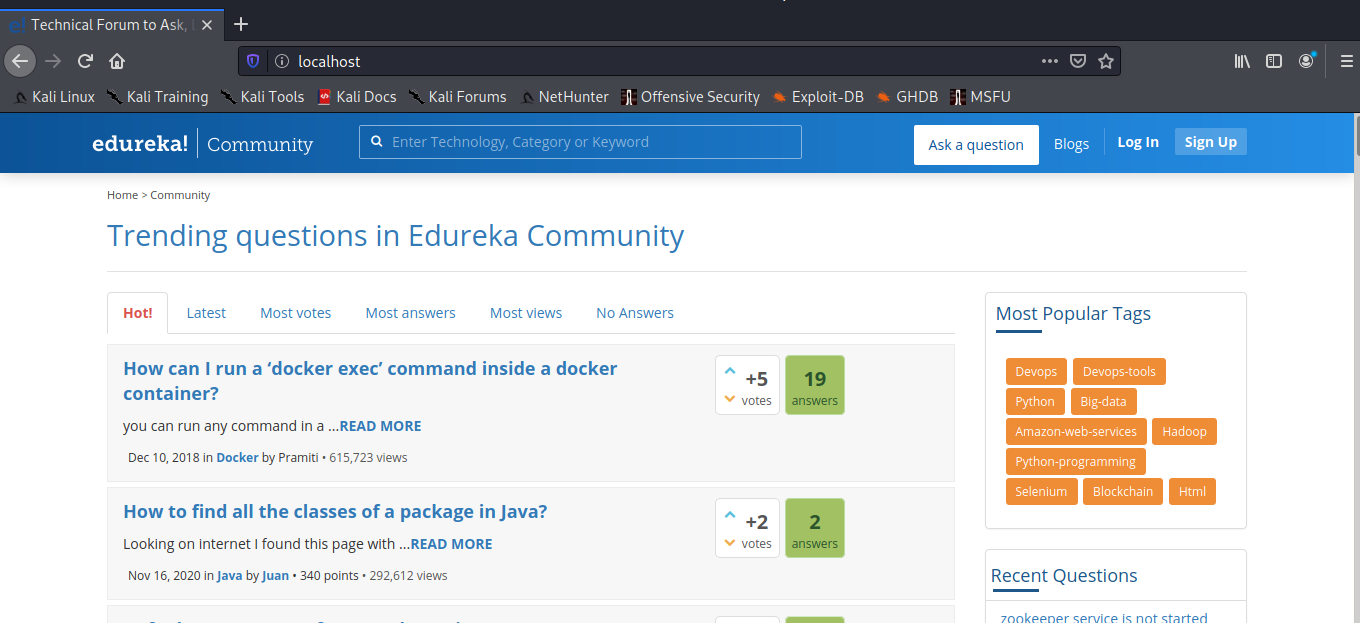


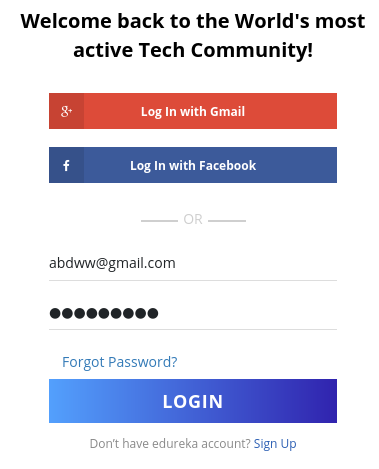
As we can see the username and password that has been entered by the victim,

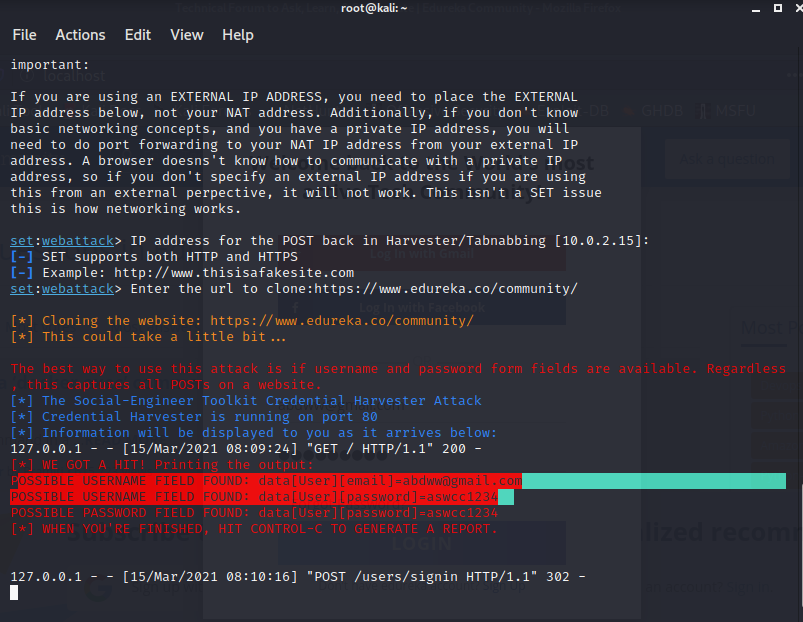
This is how to use pre available templates to create a phishing page.

METHOD 1: B

Using site cloner to create a phishing page







HONEYPOT

* Honeypot is a computer system that is setup to act as a decoy to lure cyber attackers, and to detect, deflect or study attempts to gain unauthorized access to information systems.
* Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked.
* Eg: police baiting a criminal, conducting undercover surveillance, and final punishing the criminal
* A honeypot is a security resource whose value lies in being probed, attacked or compromised.
* Honeypots are weapons against spammers, honeypot detection systems are spammer-employed counter-weapons. As detection systems would likely use unique characteristics of specific honeypots to identify them.
* Honeypots can be setup inside, outside or in the DMZ of a firewall design or even in all of the locations although they are most often deployed inside of a firewall for control purposes. in a sense, they are variants of standard intruder detection systems (IDS) but with more of a focus on information gathering and deception.
* Honeypots can be classified based on their deployment (user/action) and based on their level of involvement. Based on deployment, honeypots may be classified as:

1. Production Honeypots
2. Research Honeypots

* Production Honeypots are easy to use, capture only limited information, and are used primarily by corporations. Production honeypots are placed inside the production network with other production servers by organizations to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots.
* Research honeypots are run to gather information about the motives and tactics of the Black hat community targeting different networks. These honeypots do not add direct value to a specific organizations face and to learn how to better protect against those threats. Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations

Log in to your Kali Linux machine as an admin user. Open a terminal window and download pentbox with the command:

*wget http://downloads.sourceforge.net/project/pentbox/pentbox18realised/pentbox-1.8.tar.gz*

Once that file has finished downloading, extract the archive with the command:

*tarxvfz pentbox-1.8.tar.gz*

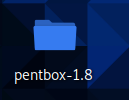
This will create a new directory named pentbox-1-8. Change into that new directory with

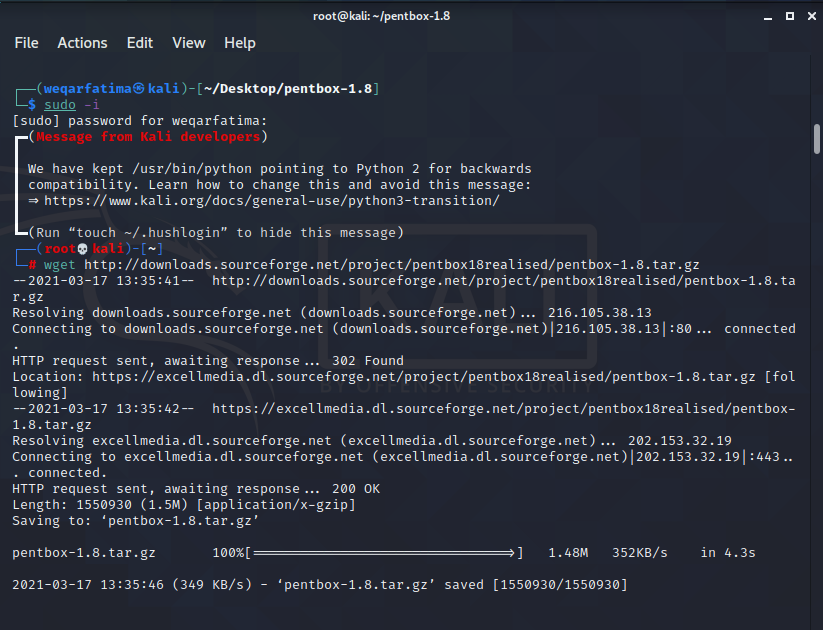
*cd pentbox-1.8*.

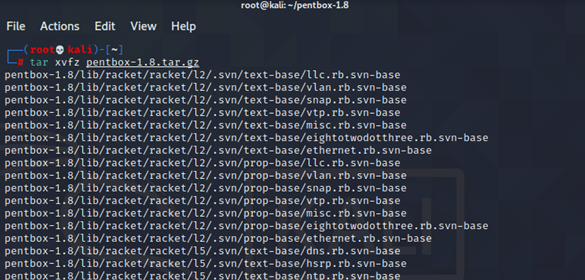
**How to run pentbox**

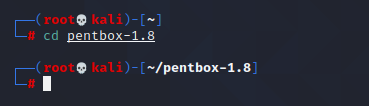
The next step is to run the pentbox Ruby script with the command:

*./pentbox.rb*



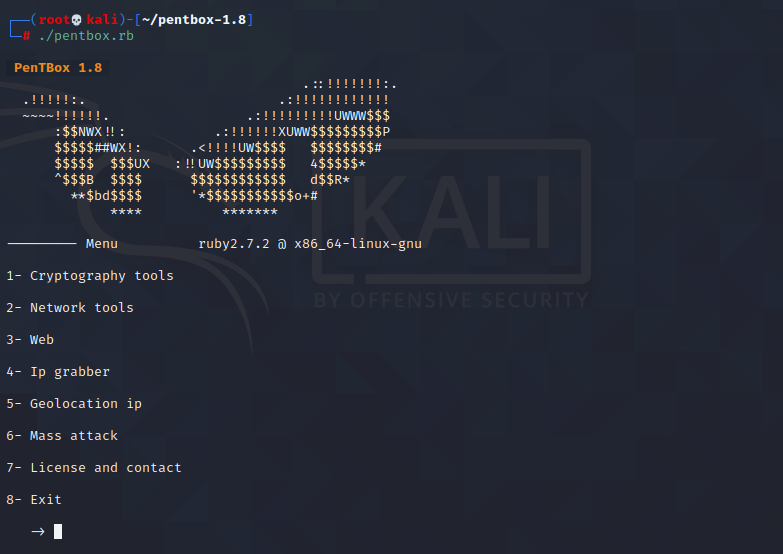


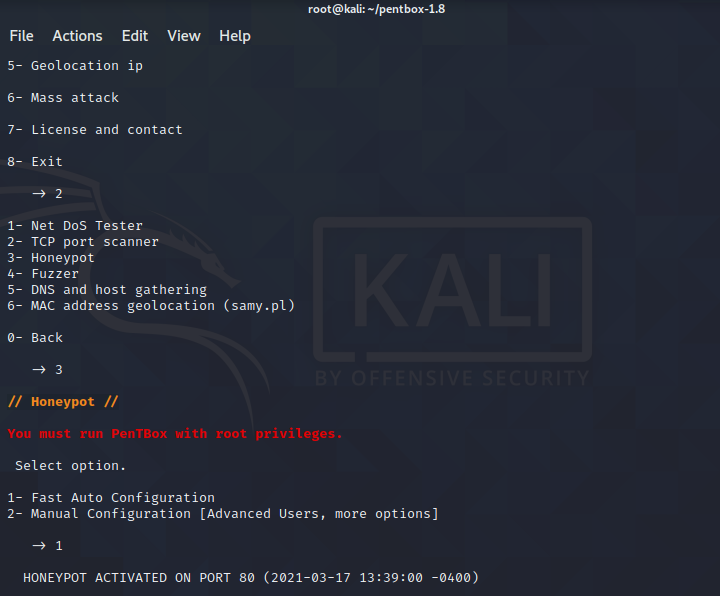




When you issue the command, you'll be greeted by a menu. From that menu select 2 (for Networking tools) and then 3 for Honeypot

Launching the Honeypot script



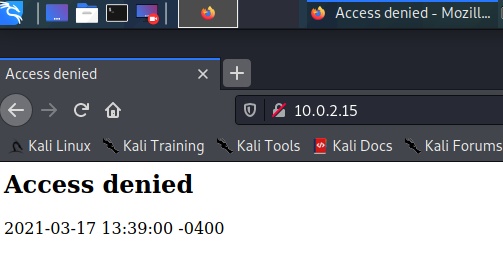


In the next menu select 1 (for Fast Auto Configuration). This will launch a honeypot listening on port 80.

METHOD 1: AUTOMATIC

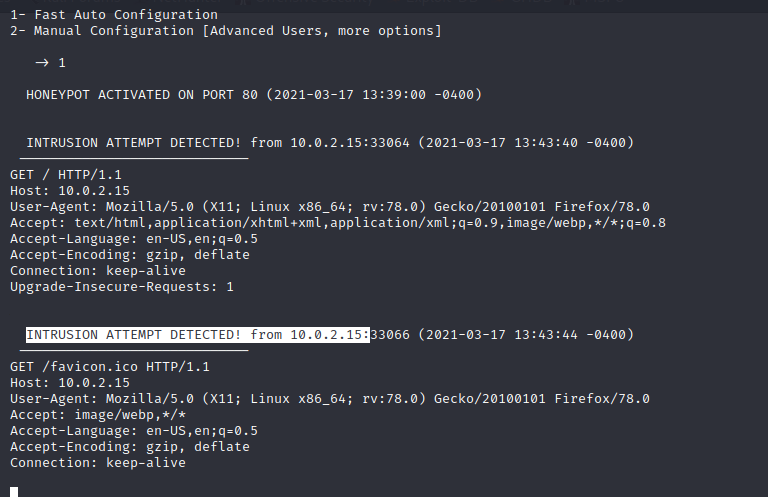
Launching a simple port 80 honeypot.

Next, open a web browser on another machine (connect to the same network as the honeypot) and point it to (where SERVER\_IP is the IP address of your Kali machine). You should see an Access Denied error in the browser.



Access denied.

Go back to the terminal window on the Kali Linux machine and you should see the honeypot picked up the attempted connection



Attack on port 80.

METHOD 2:

**How to launch a specific instance**

Now we want to launch a honeypot to listen on a specific port. To deploy pentbox such that it's listening in on port 4444, you'd run the script and select 2 and then 3, followed by 2. When prompted for a port to open, type 4444 on the firefox

4444 port

